THE TOLLY GROUP

No. 208316 July 2008

McAfee, Inc.

McAfee Total Protection for Endpoint

Anti-Malware Detection Accuracy Test on Windows XP

TOLLY Up to Spec CERTIFIED Test Summary

Premise: *Malware continues to grow in volume and sophistication. Accordingly, anti-malware software grows in scope, accuracy and complexity to keep up with the new threats. Most tests of anti-malware products use a default setting to measure accuracy. This methodology can be misleading since enterprises often fine-tune the configuration of anti-malware solutions before deployment in their networks. In this review, the anti-malware products have been configured to maximize protection against malware as they would be deployed in a live environment.*

McAfee commissioned The Tolly Group to evaluate the effectiveness of its McAfee Total Protection for Endpoint security software offering that provides comprehensive security to protect against viruses, spyware, hackers and other threats.

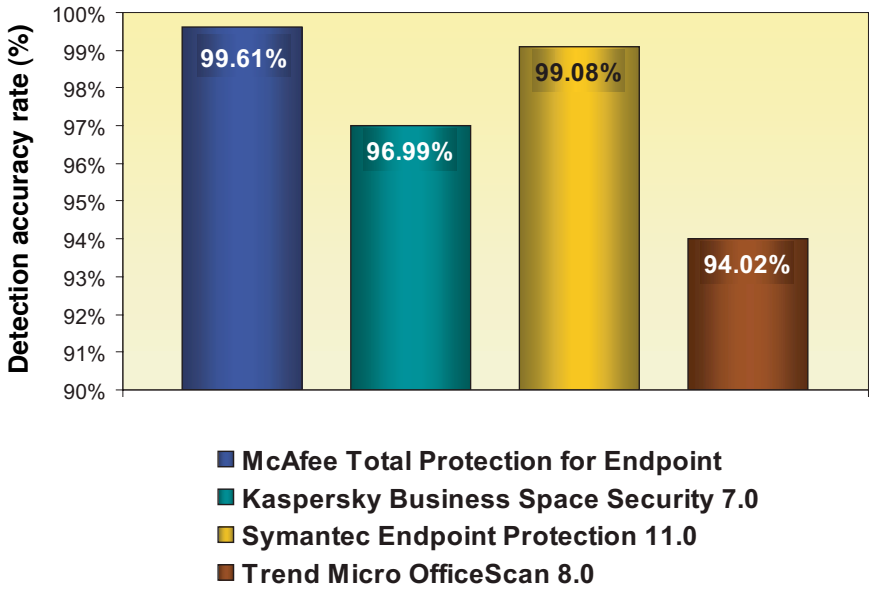
The Tolly Group conducted a hands-on evaluation of the "on-access" detection accuracy and compared McAfee Total Protection with other anti-malware solutions for Windows XP: Trend Micro OfficeScan Client/Server Edition 8.0, Symantec Endpoint Protection 11.0 and Kaspersky Business Space Security 7.0.

Tests focused on measuring the detection accuracy rate and speed of "on-access" file scanning. Tests were conducted in June 2008.

Test Highlights

- McAfee Total Protection for EndPoint provides the highest detection accuracy rate among the anti-malware products tested with a 99.61% detection rate
- McAfee Total Protection for EndPoint exhibits the fastest scanning speed among the products tested by scanning 86 malware files per minute during "on-access" scan

Anti-Malware "On-access" Scanning Detection Accuracy Test Results for Windows XP



Source: The Tolly Group, June 2008

Figure 1

Executive Summary

McAfee's Total Protection for Endpoint solution illustrated excellent security performance by scoring the highest in malware detection and removal, and was fastest in file scanning speed.

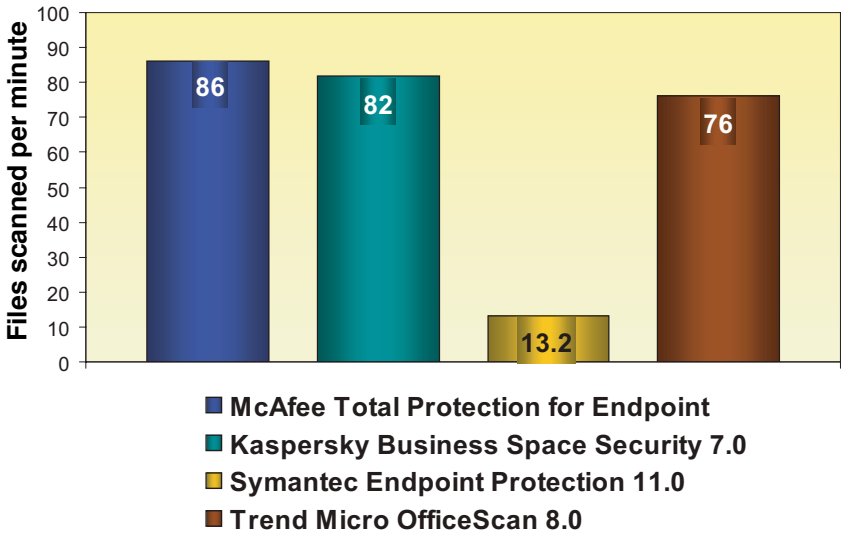
Test results show that McAfee Total Protection for Endpoint outperformed other anti-malware solutions in both detection accuracy and scanning speed when operating in "on-access" mode.

The accuracy test reveals that McAfee Total Protection for Endpoint has a detection rate of 99.61%. Symantec Endpoint Protection 11.0, which came in second, has a score of 99.08%; followed by Kaspersky Business Space Security 7.0 and Trend Micro Office-Scan Client/ Server Edition 8.0 that reported 96.99% and 94.02%, respectively.

Tolly Group engineers also measured the scanning speed from the same test in which each product processed about 115,000 malware files continuously. The results showed that McAfee Total Protection for Endpoint scored the highest with 86 files scanned per minute (fspm), followed by Kaspersky with 82 fspm, Trend Micro in third place with 76 fspm and Symantec last with 13.2 fspm.

Engineers attempted to test Sophos Endpoint Security and Control 7. This version of the Sophos solution apparently had memory issues when processing the malware set. Because results were inconsistent, Sophos was dropped from test.

Anti-Malware "On-access" File Scanning Speed Test Results for Windows XP



Source: The Tolly Group, June 2008

Figure 2

In this test, Tolly Group engineers installed the anti-malware products and configured them for "on-access" scanning.

McAfee confirmed that the malware samples used in this test were actual malware samples submitted to McAfee researchers. These samples were collected through multiple methods including, but not limited to, honey pots, customer forwards, crawlers, spam feeds and samples from industry researchers. McAfee further confirmed that the company did not build a special malware sample set by modifying the samples to its advantage.

Results

Detection Accuracy Rate

In the test, McAfee's Total Protection for Endpoint performed better than the competitors by achieving a 99.61% detection rate. In other words, McAfee missed only 0.39% of malware. This compares to Symantec's 0.92%, Kaspersky's 3.01% and Trend Micro's 5.98%.

While these numbers may not seem significant, they show that Symantec Endpoint Protection 11.0, for instance, missed almost 2.4X more malware than McAfee. Kaspersky Business Space Security 7.0 and Trend Micro OfficeScan Client/ Server Edition 8.0 missed 7.8X and 15.4X more malware than McAfee, respectively. (See Figure 3.)

Scanning Speed

The test results show that, during "on-access" scanning, McAfee's Total Protection for Endpoint anti-malware solution processed 86 malware files per minute under extreme conditions where malicious files were constantly copied into the system.

Kaspersky and Trend Micro performed similarly with McAfee by scanning 82 and 76 malware files per minute, respectively. Whereas, Symantec's solution was only able

to process 13.2 malware files per minute.

Test Setup & Methodology

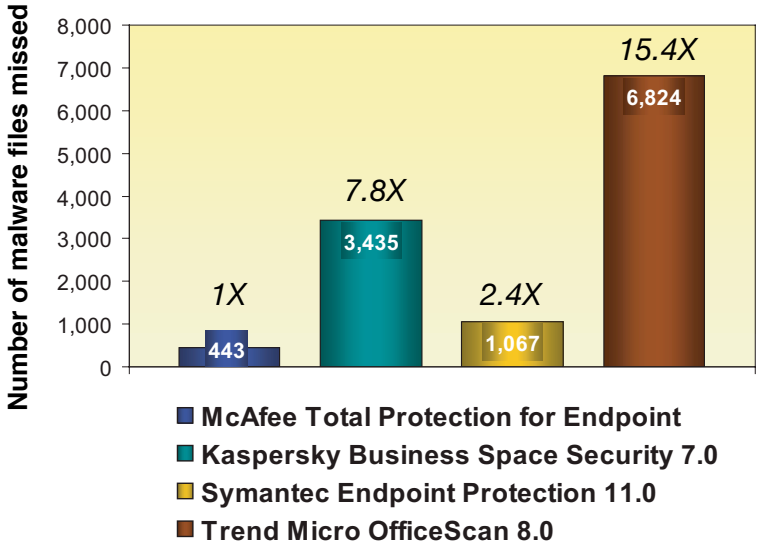
Engineers tested McAfee Total Protection for Endpoint (Engine Ver. 5200, DAT Ver. 5327), Symantec Endpoint Protection 11 (Defs Ver. 100626al), Trend Micro OfficeScan Server/ Client Edition 8.0 (Rel 5.371.00, Pattern 5.371.00), Kaspersky Business Solution 7.0 (Def Ver. 7.0.0.223) and Sophos Endpoint Security and Control 7 (Def Ver. 4.30).

All software solutions were run on identical PCs, supporting Windows XP SP2 running on a 3.0-GHz Intel Pentium 4 CPU, with 1 Gbyte of memory and a 70-Gbyte hard drive. All of the anti-malware software was updated to the newest signature releases, and the systems were inspected to make sure that no solution had an advantage over the others. The systems were configured to inspect the contents of malware files to ensure maximum accuracy.

After that, engineers deactivated the anti-malware software and moved the malware samples (114,036 files whose size was 14.7 GB) to one of the logical drives in the system that was not protected by anti-malware software. Engineers then activated the scanning engine and started moving the malware files to protected empty folder using the "xcopy" command.

Engineers verified the results by counting the number of malware files in the destination folder and comparing them with the report from the software itself. Each test was run twice and the results were averaged as per standard Tolly Group policy. The two readings were consistent for all the products under test.

Number of Malware Files Missed by Anti-Malware Products During Testing



Source: The Tolly Group, June 2008

Figure 3

McAfee, Inc.

Total Protection for EndPoint

Anti-Malware Detection Accuracy Test

TOLLY Up to Spec CERTIFIED

Product Specifications

Vendor-supplied information not necessarily verified by The Tolly Group

McAfee
Total Protection for Endpoint

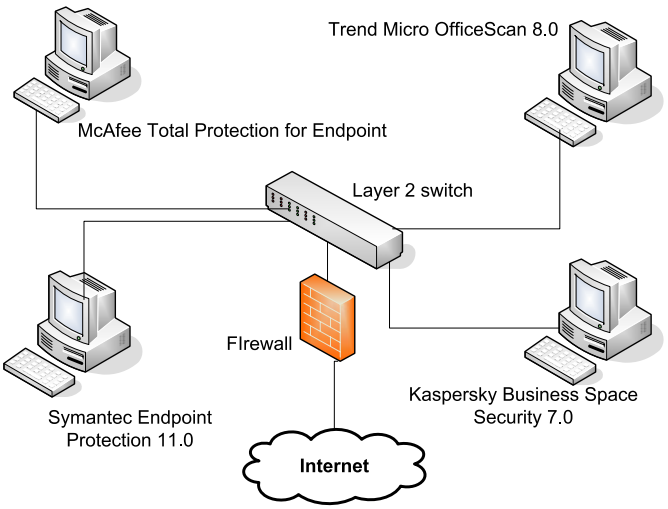
- **Single management console**—easy-to-use, Web-based, McAfee SecurityCenter—for remote monitoring and reporting
- **Integrated desktop and file server anti-virus and anti-spyware** – automatically secures systems from known threats and unwanted programs, and provides basic E-mail protection for Outlook applications
- **Centralized desktop firewall** is an immediate barrier between your critical data and malicious intrusions
- **Advanced E-mail anti-spam and anti-virus service** provides up-to-date E-mail protection that assures business continuity
- **Advanced E-mail server protection** stands guard over your mail servers with virus protection and content filtering
- **Real-time browser protection** offers users safer Web surfing

For more info contact:

McAfee, Inc.

3965 Freedom Circle
Santa Clara, Calif. 95054
Phone: 866.338.8754
URL:www.mcafee.com

Test Bed Diagram



Source: The Tolly Group, June 2008

Figure 4

The Tolly Group is a leading global provider of third-party validation services for vendors of IT products, components and services.

The company is based in Boca Raton, FL and can be reached by phone at (561) 391-5610, or via the Internet at:

Web: http://www.tolly.com,
E-mail: sales@tolly.com

Fair Testing Charter™
Interaction with Competitors

As the products are designed to be "user installable" without support, The Tolly Group did not deem it necessary to contact the competing vendors. The Symantec Endpoint Protection 11, Trend Micro OfficeScan Server/Client Edition 8.0 and Kaspersky Business Solution 7.0 were acquired by The Tolly Group through normal distribution channels.

Terms of Usage

USE THIS DOCUMENT ONLY IF YOU AGREE TO THE TERMS LISTED HEREIN.

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase must be based on your own assessment of suitability.

This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions and certain tests may have been tailored to reflect performance under ideal conditions; performance may vary under real-world conditions. Users should run tests based on their own real-world scenarios to validate performance for their own networks. Commercially reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. In no event shall The Tolly Group be liable for damages of any kind including direct, indirect, special, incidental and consequential damages which may result from the use of information contained in this document.

The test/audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers.

When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from The Tolly Group's Web site.

All trademarks are the property of their respective owners.

208316-Npabsu2-ks-03Jul08