

Scan Speed Optimization and Caching Technologies: A Comparison of Endpoint Security for the Enterprise

A test commissioned by McAfee, Inc. and performed by AV-Test GmbH
Date of the report: February 11th, 2011 (last update: March 18th, 2011)

Executive Summary

In February 2011, AV-Test performed a comparative review of five security solutions for the enterprise. The goal was to determine whether speed optimization and modern caching technologies are used by today's malware detection engines. For this, an on-demand scan performance test (with a default scan of the system partition) was considered. McAfee commissioned AV-Test to run an independent test of McAfee, Kaspersky, Sophos, Symantec and Trend Micro offerings.

Overview

The IT infrastructure of the enterprise is usually protected by a multi-layered security model which starts with a network firewall on the most outer layer and goes to each client protected by endpoint security software on the most inner layer. The endpoint security software usually does impact the system's performance in a more or less noticeable manner as it has to check all accessed resources for malware and attacks, which are endangering the enterprise. To achieve that goal the security software has to handle millions of digital malware signatures and complex algorithms to detect a dramatically raising number of threats. With more complexity the resources required for protection increase and the vendors of security software have to find new ways to preserve those resources, e.g. by using in-the-cloud or intelligent caching technologies.

As many files - like files belonging to the operating system - on a typical endpoint system do not change over time, these files do not have to be scanned by the endpoint security solution every time a scheduled full system scan runs. To increase scan speed, one approach could be to scan all files of the system on an initial full system scan and to scan only the files which have been changed on any further scan. If such a further scan takes much less time, it can be scheduled more often without disrupting the employees. Otherwise if a full system scan does make use of many system resources, it has to be scheduled in the breaks, in the evening or even at night and the computer consumes power when nobody is working.

This comparison of five endpoint security products for the enterprise will disclose which vendors already have integrated new resource-saving technologies in their products.

Products Tested

The following five products were tested, using the latest signature updates available at the beginning of the test:

Product	Software Version
Kaspersky Anti-Virus for Windows Workstations	6.0.4.1424 d
McAfee VirusScan Enterprise ¹	8.8.0.765
Sophos Endpoint Security and Control	9.5.5
Symantec Endpoint Protection	12.0.1001.95
Trend Micro OfficeScan ²	10.5.1083

Figure 1: List of tested products

¹ including Host Intrusion Prevention Client 7.0.0.1159 and SiteAdvisor Enterprise Plus 3.0.0.561

² Including Intrusion Defense Firewall Plug-In

Methodology and Scoring

Platform

All tests have been performed with identical PCs equipped an Intel Xeon Quad-Core X3360 CPU, 4 GB Ram, 500 GB HDD (Western Digital) and an Intel Pro/1000 PL (Gigabit Ethernet) NIC. The operating system was Windows 7 (RTM, 32 Bit) on a NTFS formatted system partition³.

Testing methodology

The testing was performed with each solution configured with its default settings. If possible, a required administration interface was installed to the same machine⁴ as the endpoint protection client. Otherwise a separate PC⁵ was used for the specific administration interface. The test has been performed according to the following methodology:

1. **Internet Access.** The PCs had access to the Internet at all times in order to use any in-the-cloud queries that each of the solution may offer.
2. **Product Configuration.** For on-demand scanning, a new default scan task was created with the scan target set to the NTFS formatted system partition. The last signature update was executed before the beginning of the testing.
3. **On-demand Scan Speed.** The initial scan was executed right after installation and update of the product has been finished and the system was rebooted. The scan task was repeated then nine times. After every second scan, the system was rebooted to clear the hard disk cache.

Test Results

On-demand Scan Speed

McAfee performed best in scanning the system partition (figure 2). Kaspersky and McAfee definitely make use of caching technologies to speedup regular scheduled scans. Both products had an identical speedup of 87%. Sophos and Trend Micro might use some minor optimizations, but the speedup of 9% could also depend on hard disk caching. Symantec's scan times vary quite a bit but a true speedup is not visible.

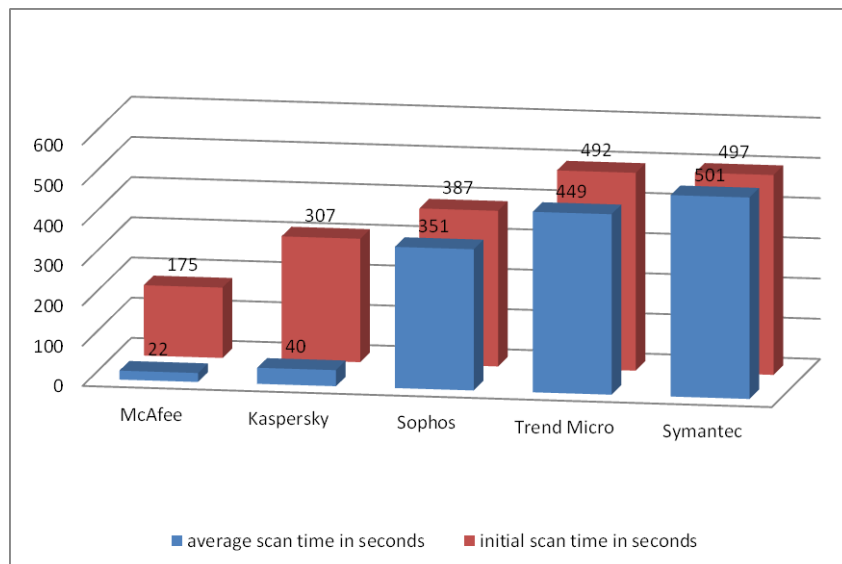


Figure 2: Time to perform a scan of the system partition (lower values indicate better results)

³While Windows 7 can only be installed on a NTFS partition, the partition type is an important fact as some product's caching technologies may not work with a FAT32 formatted partition, which could be still in use on some older enterprise computers running Windows XP.

⁴For Trend Micro OfficeScan the administration interface ran on the same machine

⁵Separate administration interfaces were used for the McAfee and Symantec products

Data Throughput

As shown in figure 3, Trend Micro achieves a little bit more data throughput than Sophos. The longer scan time of Trend Micro (figure 2) follows from the more used disk space due to the installed administration interface.

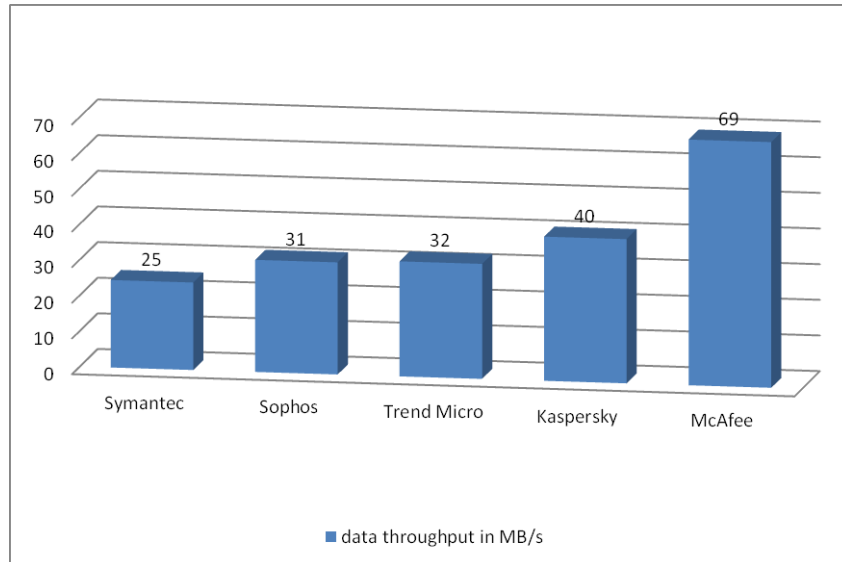


Figure 3: data throughput on initial scan of the system partition (higher values indicate better results)

The data throughput was measured on the initial scan. The higher data throughput means that more data is scanned in a specific time which results into better performance for file I/O operations, like reading or copying files.

Conclusion

McAfee is a good choice when a large amount of data is scanned on a regular basis as it has the best data throughput and properly working speed optimization algorithms. The on-demand scanning demonstrates that not all vendors have implemented caching in their enterprise products yet. The bottom line is that performance shouldn't be the only decisive point. Good performance is just one feature of a good security solution, but other facts like detection rates and false positives should also be considered.