NSS Labs

Security. Certified.

Host Anti-Malware Performance

COMPARATIVE TEST REPORT

HOST MALWARE PROTECTION
METHODOLOGY VERSION: 2
JANUARY 16, 2009

Published by NSS Labs.

CONTACT:

5115 Avenida Encinas
Suite H
Carlsbad, CA 92008

Tel: +1.760.412.4627
E-mail: info@nsslabs.com
Internet: http://www.nsslabs.com

EXECUTIVE SUMMARY

HOST ANTI-MALWARE PERFORMANCE

While malware threats continue to multiply, the resources available to corporate IT security organizations do not. The amount of RAM and CPU consumed by applications can make a significant difference in the usability of a workstation, as well as the lifetime of these corporate assets.

During November & December 2008, NSS Labs performed extensive performance testing of several enterprise class host anti-malware products, including those from McAfee, Sophos, Symantec, and Trend Micro. NSS Labs measured the performance impact of these products while performing a range of common tasks; including booting, scanning directories, downloading files and launching applications.

Our test of boot time showed McAfee, Symantec and Trend added just about 9 seconds to the boot sequence. However, Sophos made users wait an additional minute and 12 seconds. Once up and running, all of the products consumed roughly equivalent CPU cycles. However, Sophos devoured 1 GB RAM, while McAfee required merely 60 MB, and Symantec and Trend Micro took 123 MB and 139 MB respectively.

When downloading clean Word, Excel and PDF files from the web via HTTP, Trend Micro and McAfee proved fastest. Symantec and Sophos trailed, but on the border of user perceptibility. All the products performed well when copying files remotely to a local folder, with the noted exception of Sophos which took considerably longer.

Warm application start tests are more important than cold starts, and show how long a user must wait to load an application after it has previously been in memory. In this category, Trend Micro consistently displayed the fastest warm start times, followed closely by Symantec. McAfee and Sophos both added 1 sec on average.

For on-demand scans, Trend Micro was by far the fastest, registering between 3 and 11 times faster than the other products. However, in that short time, it consumed approximately 15 to 20% more CPU. This can be a welcome advantage and reduce down-time when a complete scan is required.

Performance is one important aspect of anti-malware and endpoint protection products. Organizations should also consider security effectiveness, manageability and total cost of ownership (TCO).

For the full report, and other endpoint protection evaluations see: http://www.nsslabs.com/anti-malware

CONTENTS

1 INTRODUCTION

The amount of new viruses, Trojans, spyware, worms, bots and other malicious code is exploding. This malware is simultaneously becoming more specific and targeted. Security researchers and vendors are reporting anywhere between 15,000 and 50,000 new samples daily, posing real challenges to the security industry to keep up with the evolving threats. Vendors are adding new signatures, heuristics and other mechanisms in this digital arms race to detect and thwart attacks. But with what effect and at what cost?

This report examines the performance impact of host-based security products. While threats change, IT organizations are charged with trying to deliver more business applications and security within the confines of existing workstations and laptops with limited RAM and CPU constraints.

The amount of RAM and CPU consumed by applications can make a significant difference in the usability of a workstation. After all, nobody bought a computer to run antivirus software. To the extent that security degrades performance, it increases the likelihood that the security will be disabled by impatient users. NSS Labs measures performance in the context of executing daily work tasks.

ABOUT THIS TEST

The NSS Labs test reports are designed to address the challenges faced by IT professionals in selecting security products. While NSS Labs methodologies include comprehensive analysis of security effectiveness, performance and management/usability, this particular test analyses and compares the performance of 4 leading anti-malware products across a range of real-world use cases. These include starting the workstation, opening popular business file types, and downloading and copying files from the web, network folders and USB drives.

These tests were performed during Q4 of 2008 by NSS Labs in our Austin, TX offices according to the detailed methodology described below.

These performance-related findings represent only one important aspect to consider when purchasing and deploying host malware protection products. Furthermore, these performance numbers can change with every DAT update. Thus, the reader is advised to consult additional NSS Labs technical reports for information regarding security effectiveness and manageability and check back frequently for updates.

2 The Systems Under Test

NSS Labs evaluated four popular corporate host anti-malware products.

Software	Engine & Signature File
McAfee Virus-Scan Enterprise	version 8.5
Sophos Antivirus	version 7.6.0
Symantec Endpoint Protection 11	version-11.0.2021.50
Trend Micro Office Scan 8	v8, SP1

The host anti-malware products tested were all generally available software (GA), and obtained from the vendors' web sites via normal procedures. They were installed and configured using default settings.

3 Host Malware Protection Test Environment

The aim of this procedure is to provide a thorough test of the main components of a host anti-malware product in a controlled and repeatable manner and in the most "real world" environment that can be simulated in a test lab. All tests were executed in a controlled manner. No internet access was permitted during this test. Results were meticulously recorded and archived.

3.1 Client Host Description

All tested software was installed on separate physical machines with the following specifications.

Software:

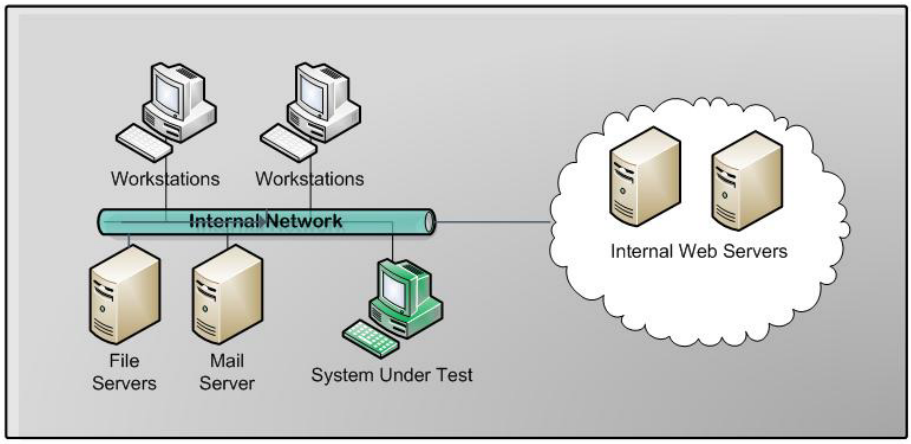
- Microsoft Windows XP, SP3
- One of the anti-malware products specified above
- Microsoft Office
- Internet Explorer 7
- Firefox 3

Hardware:

DELL SC440
Two 3.0 GHz processors
2 GB RAM

3.2 Network Description

NSS Labs tests the ability of host anti-malware products to protect the host in "connected" use cases. Thus, our tests consider and analyze the functionality and performance of anti-malware products over the network using various relevant applications such as e-mail, file server access, webmail etc.



The host system has one network interface card (NIC) and is connected to the network via a 1Ge switch port. The NSS Labs test network is a multi-Gigabit infrastructure based around Cisco Catalyst 6500-series switches (with both fiber and copper Gigabit interfaces).

The network also contained Windows file servers and linux-apache web servers for the remote access portions of the test.

3.3 Malware Collections

NSS Labs maintains a continuously growing archive of Malware and Viruses that contains tens of thousands of confirmed samples. Measuring the accuracy of malware detection was not part of this research, however, NSS Labs' malware collection was used in measuring file transfer tasks.

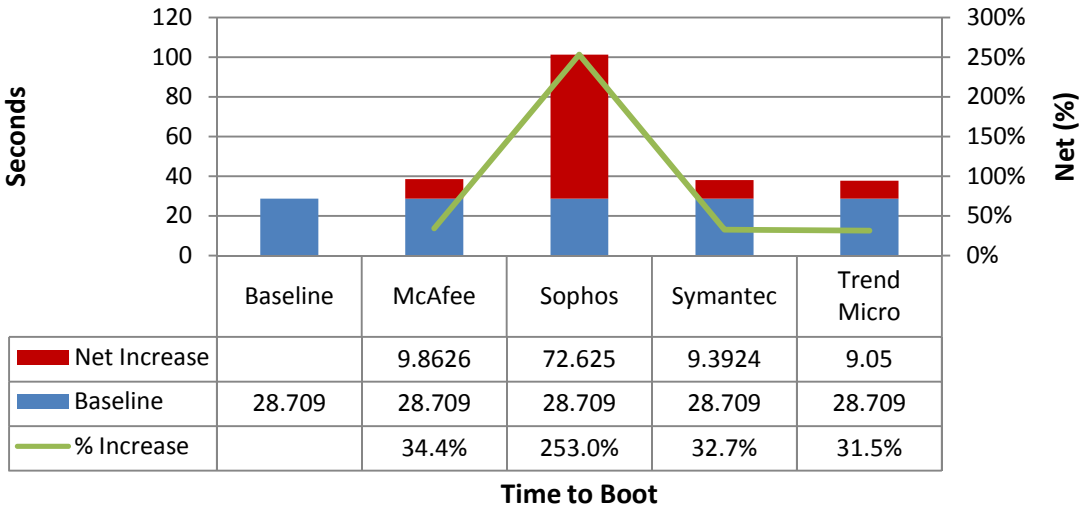
4 Performance Use Cases

Host-based software can have a considerable impact on the usability of a workstation. NSS Labs host-anti-malware testing measures the impact of specific use cases on performance and memory utilization. They are designed to represent the most common tasks performed by corporate employees.

All times are measured in seconds, unless noted otherwise. Each test was performed 30 times in order to provide the maximum confidence level and ensure that no single "poor" data point would skew the test. Results were then averaged and outliers beyond one standard deviation were discarded. Where appropriate, NSS Labs provides results in a range with the mean highlighted.

4.1 Boot Time

This test measures the net increase in time required to boot the system. Mcafee, Symantec and Trend Micro all added less than 10 seconds, allowing the system to boot within 40 seconds. Meanwhile, the machine with Sophos took over 100 seconds to complete booting, over 7 times as long as the other products.

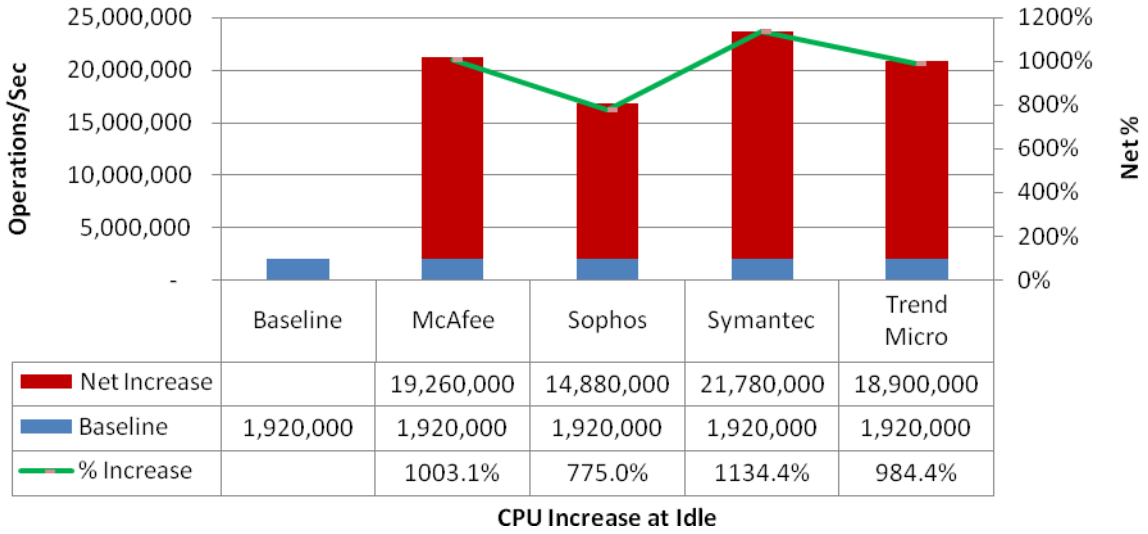


4.2 CPU Usage

CPU Utilization is measured in terms of the number of interrupts per second, which will vary with the processor speed and number of processors. Thus, a 3 GHz CPU will perform 3,000,000,000 interrupts per second. In these tests, dual processors were used so 6,000,000,000 interrupts per second are possible.

4.2.1 CPU Usage at Idle

While the increased CPU utilization was dramatic in absolute terms, the CPU load was still less than 0.1% Neither of the tested products should be humanly perceptible when the machine is idle.



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		19,260,000	14,880,000	21,780,000	18,900,000
Baseline	1,920,000	1,920,000	1,920,000	1,920,000	1,920,000
% Increase		1003.1%	775.0%	1134.4%	984.4%

CPU Increase at Idle

4.2.2 CPU Usage During Scanning

These measurements reflect peak CPU usage during on-demand scanning of a 1 GB directory of files with 10% malicious content.

	Baseline	McAfee	Sophos	Symantec	Trend Micro
Average CPU	0.032%	30%	25%	35%	49%
Net Increase		1,809,876,00	1,519,620,00	2,103,852,00	2,926,080,00

Net CPU Utilization During Scanning

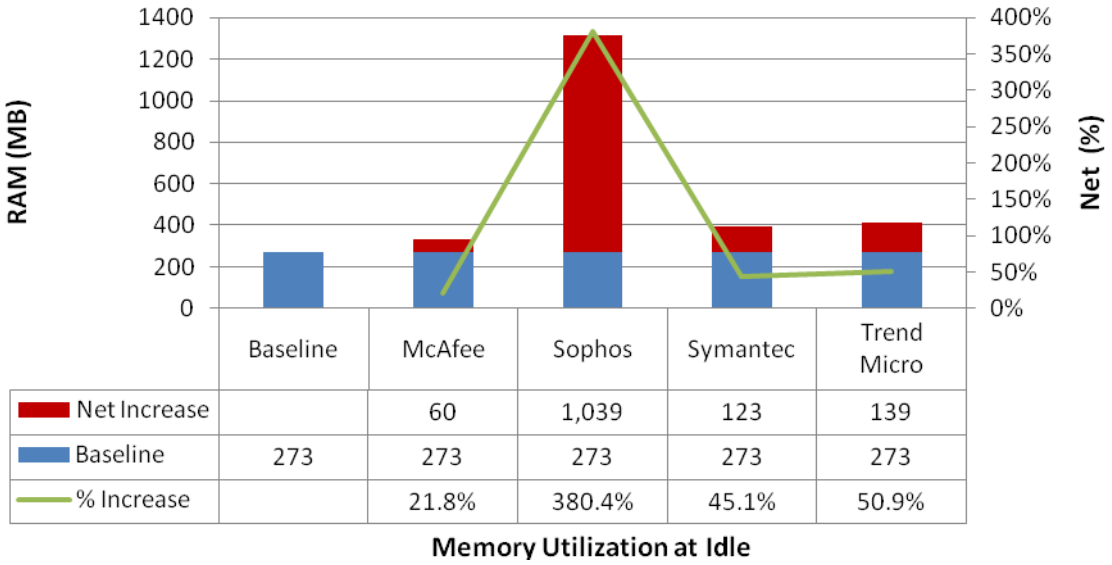
Trend Micro took more CPU, but scanned the 1GB directory in under 9 seconds. McAfee, Symantec and Sophos all used less CPU, but maxed out the memory. With today's multi-core/multi-processor systems, it was interesting to see Trend Micro use only one processor, leaving the other for work functions. This approach allowed Trend Micro to reduce memory usage and overall impact. McAfee, Symantec and Sophos took a more traditional approach – trying to balance CPU & memory across processors.. This approach of

binding additional processors could be responsible for the higher memory utilization of these applications during on-demand scans (see Memory Utilization During Peak Scan).

4.3 Memory Utilization

The net increase in memory utilization is calculated by measuring the reduction in available memory with the anti-malware product under test installed compared to the baseline without it. NSS Labs has noted that other methods which attempt to identify individual processes and DLLs can be quite inaccurate. Some applications attempt to hide or piggyback memory utilization on other processes. All figures reported in MB unless otherwise noted.

4.3.1 Memory Utilization at Idle

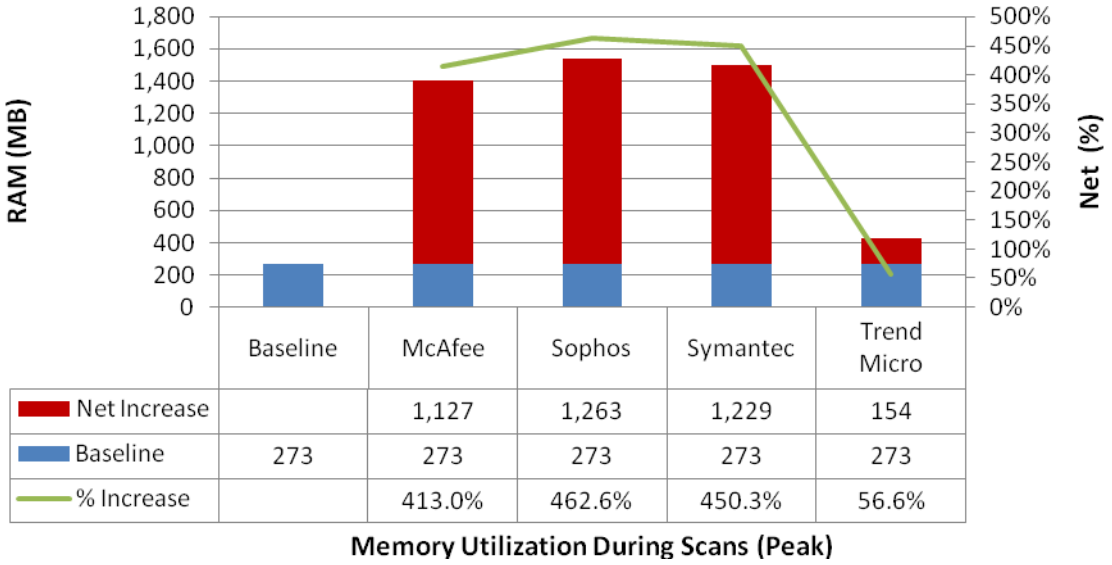


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		60	1,039	123	139
Baseline	273	273	273	273	273
% Increase		21.8%	380.4%	45.1%	50.9%

Memory Utilization at Idle

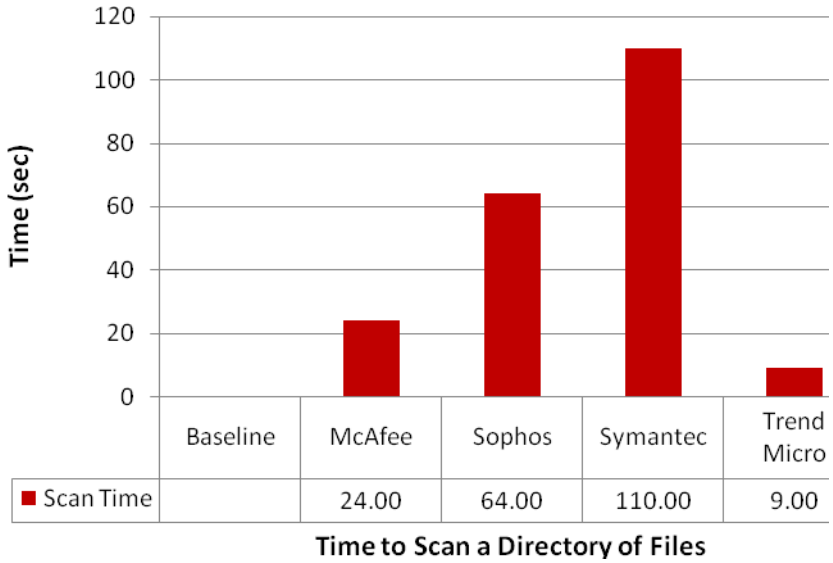
4.3.2 Memory Utilization During Peak Scan

Memory utilization also impacts performance, especially of other applications that a user may be running during a scan. If a system does not have enough RAM it could spend waste cycles swapping applications and data in and out of memory from slower disk-based page files. Trend Micro clearly made the most efficient use of memory, consuming on average 1GB less than competing products.



4.4 Time to Scan a Directory of Files

This test measures the time to perform a scan of a directory with approximately 1Gb of files, 10% of which contain malicious content. Detection settings are configured to automatically quarantine or delete so as not to require human interaction during the test.



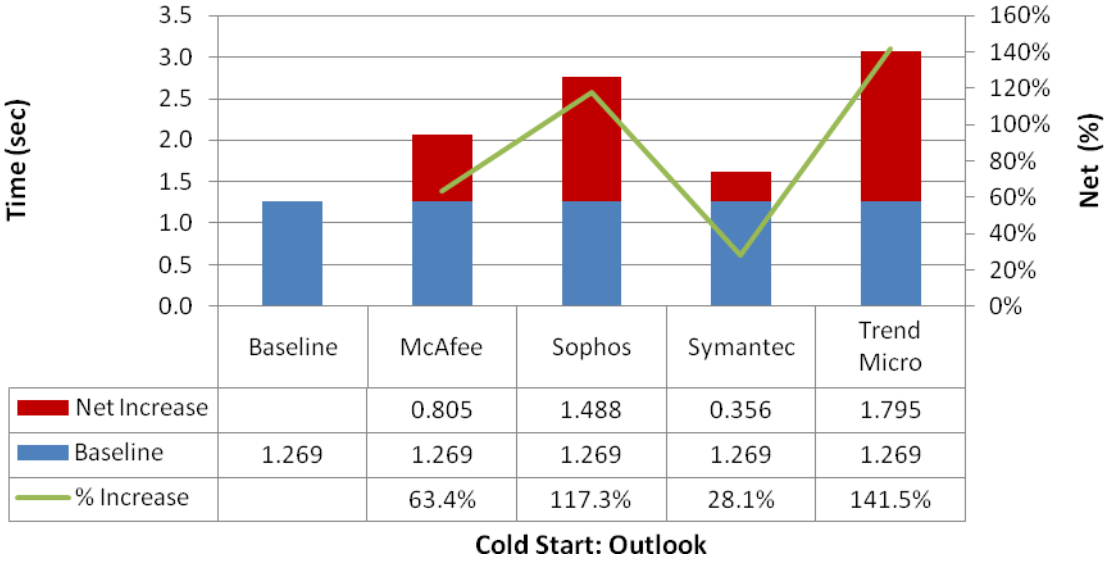
Trend Micro was significatnly faster than any of its competitors, finishing in less than 1/10th the time of Symantec, and 1/5th that of Sophos.

4.5 Time to Start an Application

Cold starts are application launches from a fresh system with no traces of the application in memory from a previous start. Warm starts refer to subsequent launches of an application where some traces of software

may still reside in memory (e.g. libraries, DLLs, reserved memory, etc.). This applies to both productivity and security software. Typically, a user will launch an application (cold), and then minimize or close it, only later to re-open the application when needed. Thus, warm starts represent the more frequent use case and more important statistic.

4.5.1 Application Cold Start: Outlook 2007

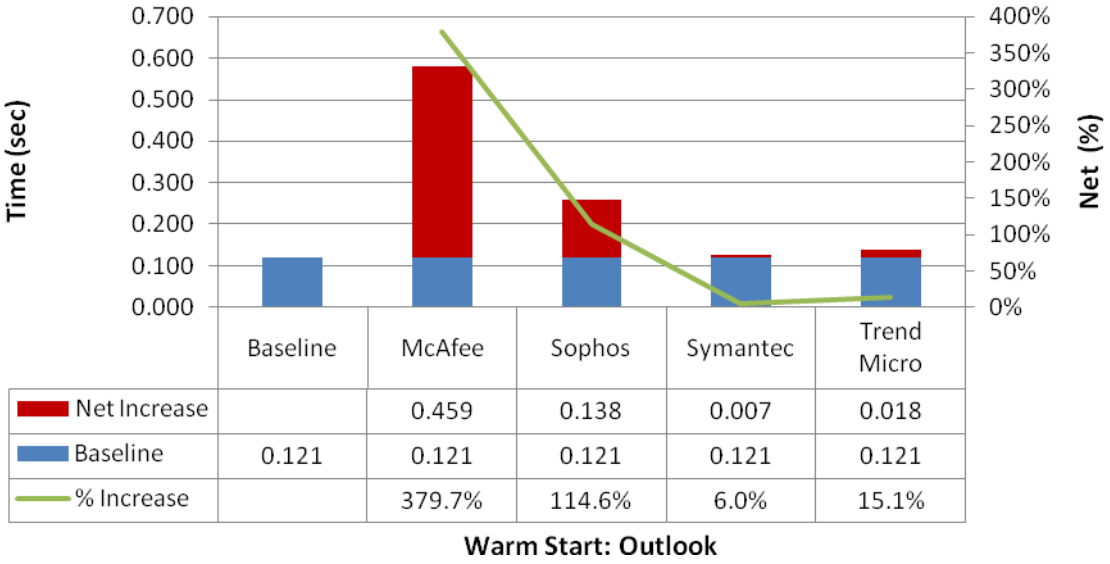


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.805	1.488	0.356	1.795
Baseline	1.269	1.269	1.269	1.269	1.269
% Increase		63.4%	117.3%	28.1%	141.5%

Cold Start: Outlook

Our baseline system took 1.268 seconds to load Microsoft Outlook. Symantec was fastest at 1.62 seconds, adding about 1/3 second. McAfee was next, adding 4/5th of a second. Sophos added 1.5 seconds.

4.5.2 Application Warm Start: Outlook 2007

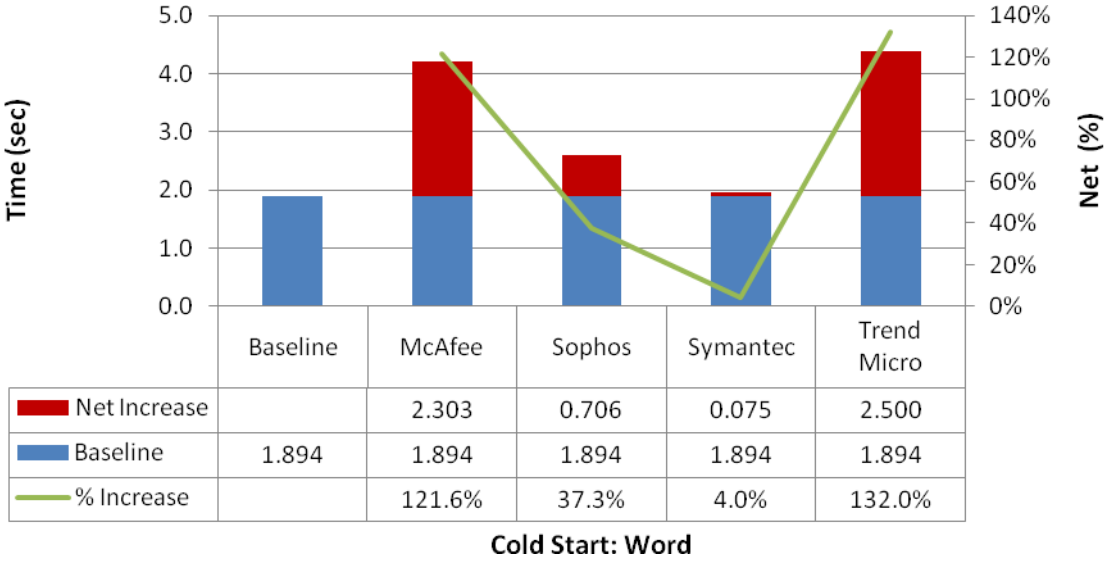


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.459	0.138	0.007	0.018
Baseline	0.121	0.121	0.121	0.121	0.121
% Increase		379.7%	114.6%	6.0%	15.1%

Warm Start: Outlook

Cold starts generally took between 1 and 2 seconds additional time with the security software. Warm starts were all generally within acceptable limits. The differences between cold and warm starts are generally attributable to caching. McAfee added the most time, but the overall start time was still under 0.6 seconds. The threshold for people noticing delay is 0.5 seconds, so this was barely noticeable.

4.5.3 Application Cold Start: Word 2007

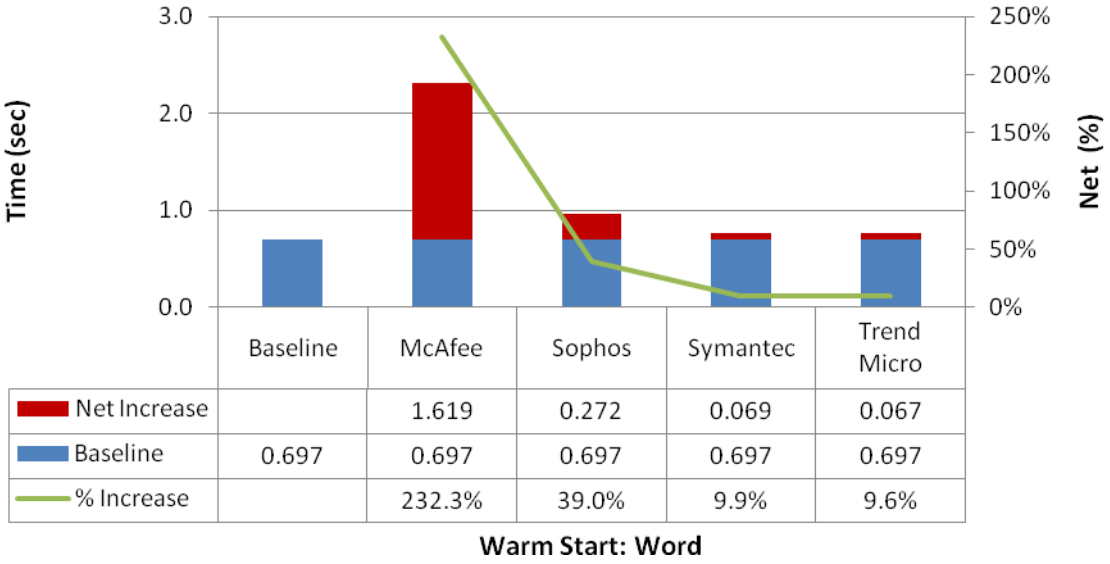


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		2.303	0.706	0.075	2.500
Baseline	1.894	1.894	1.894	1.894	1.894
% Increase		121.6%	37.3%	4.0%	132.0%

Cold Start: Word

Symantec was fastest on cold boot. McAfee and Trend Micro added over 2 seconds, doubling the start time for the application.

4.5.4 Application Warm Start: Word 2007

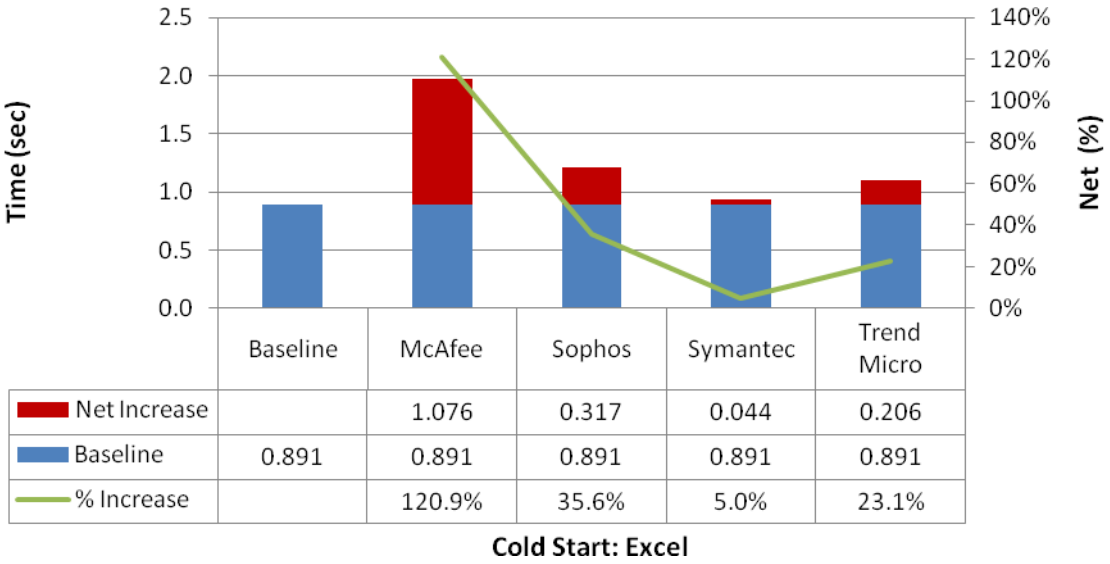


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		1.619	0.272	0.069	0.067
Baseline	0.697	0.697	0.697	0.697	0.697
% Increase		232.3%	39.0%	9.9%	9.6%

Warm Start: Word

When it came to opening Word on warm start, most products were considerably faster. Of these, Trend Micro was the fastest, with Symantec close behind.

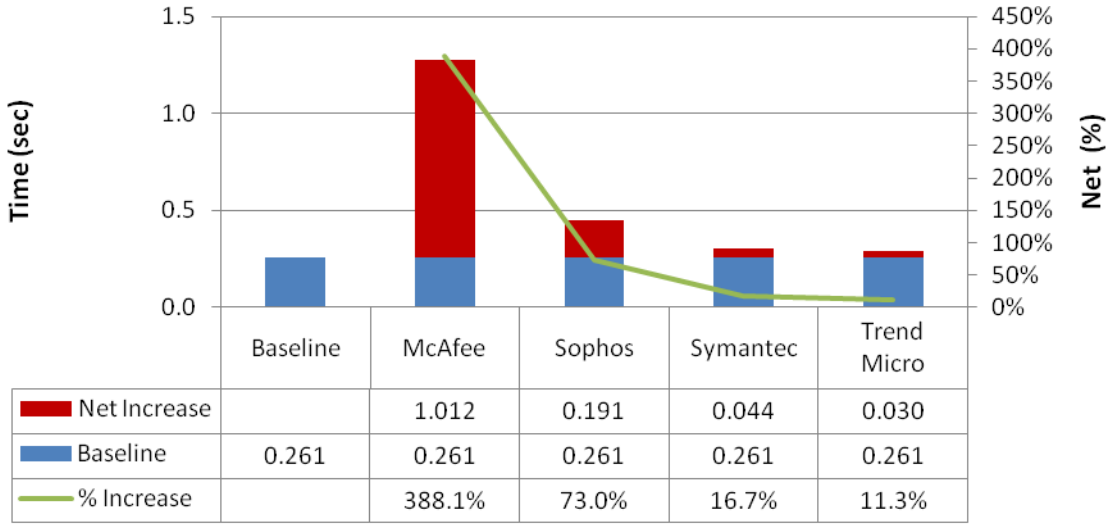
4.5.5 Application Cold Start: Excel 2007



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		1.076	0.317	0.044	0.206
Baseline	0.891	0.891	0.891	0.891	0.891
% Increase		120.9%	35.6%	5.0%	23.1%

Cold Start: Excel

4.5.6 Application Warm Start: Excel 2007



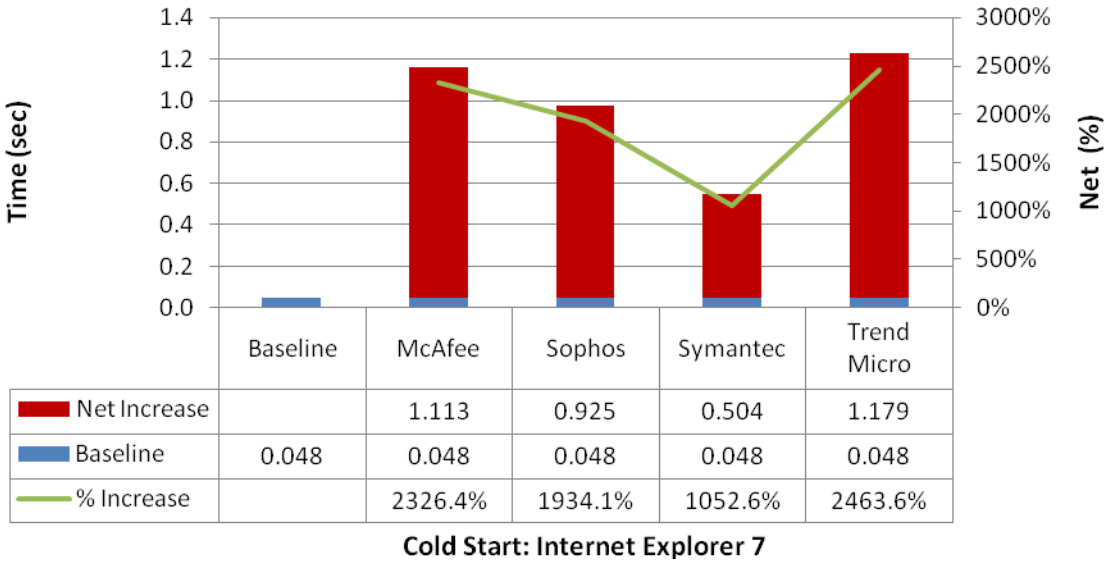
	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		1.012	0.191	0.044	0.030
Baseline	0.261	0.261	0.261	0.261	0.261
% Increase		388.1%	73.0%	16.7%	11.3%

Warm Start: Excel

All products except McAfee seemed to take advantage of caching. This improved performance, but introduces risk should an exploit change a DLL because the antivirus assumes the DLL is good. McAfee made the judgement that an extra second per application load was a reasonable price to pay for added security.

4.5.7 Application Cold Start: Internet Explorer 7

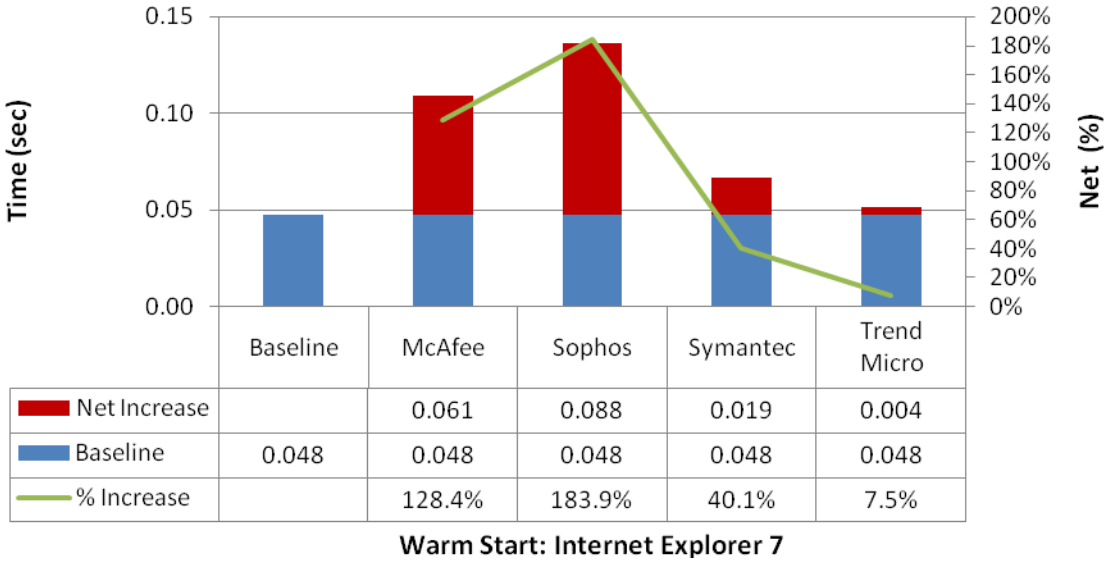
When launching IE7, security applications added approximately 1 second to the cold start time, except for Symantec at .5 sec.



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		1.113	0.925	0.504	1.179
Baseline	0.048	0.048	0.048	0.048	0.048
% Increase		2326.4%	1934.1%	1052.6%	2463.6%

Cold Start: Internet Explorer 7

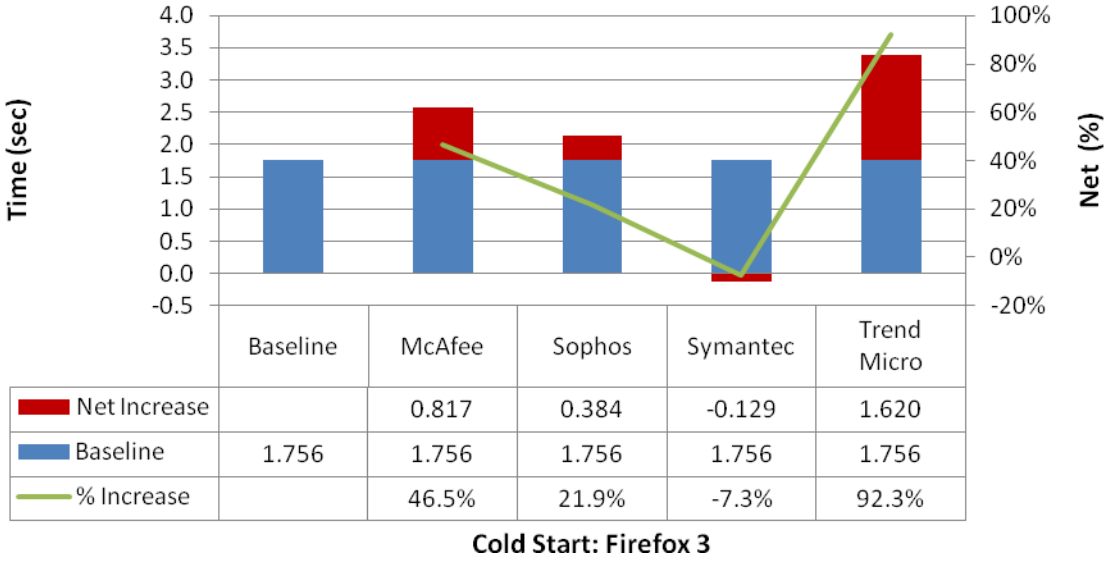
4.5.8 Application Warm Start: Internet Explorer 7



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.061	0.088	0.019	0.004
Baseline	0.048	0.048	0.048	0.048	0.048
% Increase		128.4%	183.9%	40.1%	7.5%

Warm Start: Internet Explorer 7

4.5.9 Application Cold Start: Firefox 3

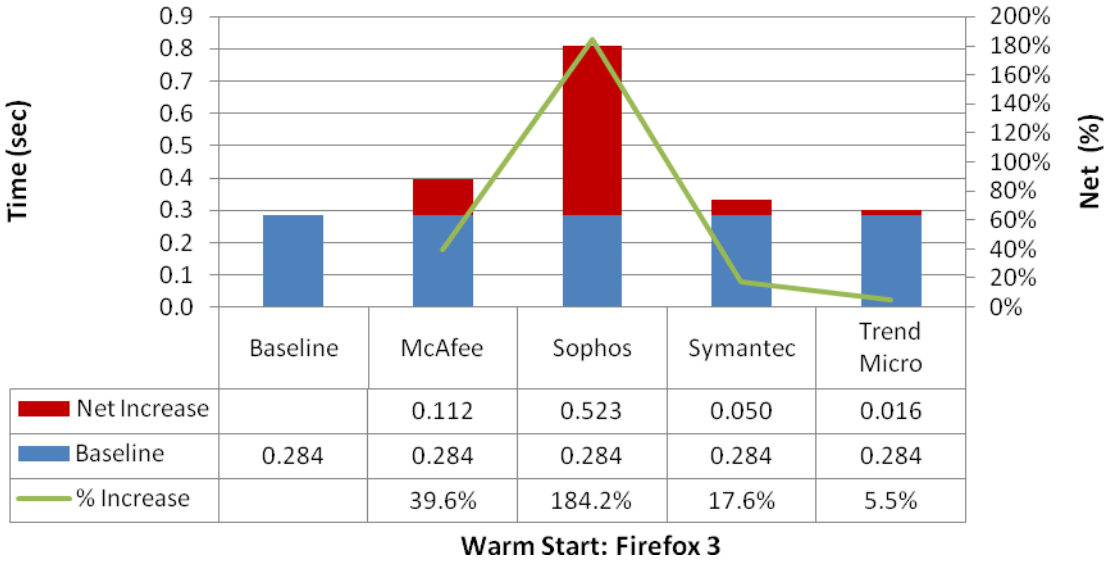


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.817	0.384	-0.129	1.620
Baseline	1.756	1.756	1.756	1.756	1.756
% Increase		46.5%	21.9%	-7.3%	92.3%

Cold Start: Firefox 3

We have certainly come a long way when security software speeds up the existing applications. It would, at first glance, appear that this is the case with Symantec. However, there is a zero sum balance between memory and CPU utilization, and there are a couple unconfirmed hypotheses as to how Firefox got faster with Symantec – especially on a cold start.

4.5.10 Application Warm Start: Firefox 3

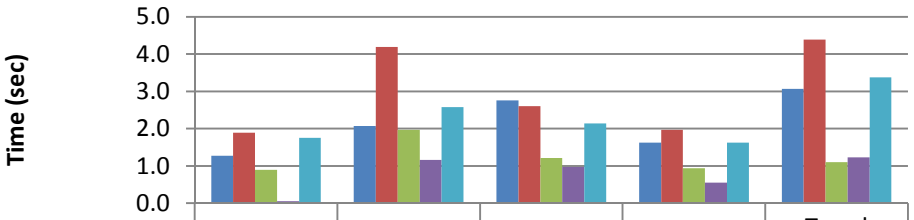


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.112	0.523	0.050	0.016
Baseline	0.284	0.284	0.284	0.284	0.284
% Increase		39.6%	184.2%	17.6%	5.5%

Warm Start: Firefox 3

4.5.11 Application Start Time Summary: Average Net Increase - Cold

This shows average application start times by individual application (outlook, word, excel, IE, and Firefox) as collected in over 30 iterations per application.

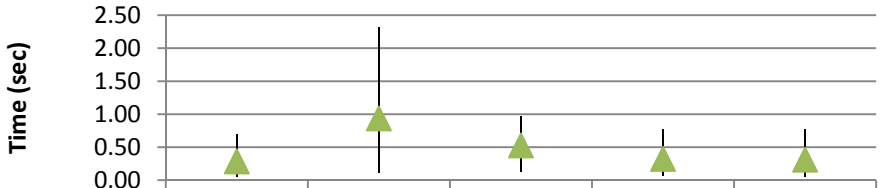


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Outlook 2007	1.269	2.073	2.756	1.625	3.064
Word 2007	1.894	4.197	2.600	1.969	4.393
Excel 2007	0.891	1.967	1.208	0.935	1.097
IE 7	0.048	1.161	0.973	0.551	1.226
Firefox 3	1.756	2.573	2.141	1.627	3.376

Average Application Start Times

4.5.12 Application Start Time Summary: Average Net Increase - Warm

This chart shows the averages for all recorded application start times (outlook, word, excel, IE, and Firefox). At least 30 measurements were taken per application. Included are low, high and average start times for the combined applications due to the anti-malware products under test.



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Hi	0.70	2.32	0.97	0.77	0.76
Low	0.05	0.11	0.14	0.07	0.05
Average	0.28	0.93	0.52	0.32	0.31
% Increase		231.4%	86.0%	13.4%	9.5%

Warm Start Applications

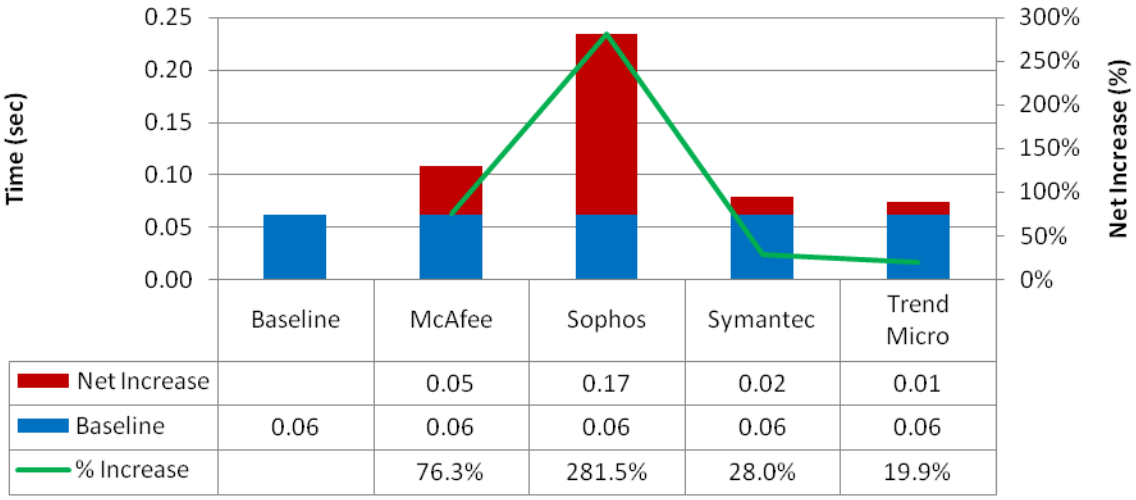
Average start times with security products remained below 1 sec, a relatively imperceptible figure considering the average baseline start time of the office applications of 0.28 seconds. Trend Micro and Symantec

showed the least impact overall. McAfee exhibited the greatest variability and overall highest impact, although generally under 2.3 sec.

4.6 Time to Download Files via HTTP

Scanning downloaded files from the web is becoming an increasingly important use case as the hosted malware threat vector gains popularity.

4.6.1 HTTP Download: Clean Word Files 500KB

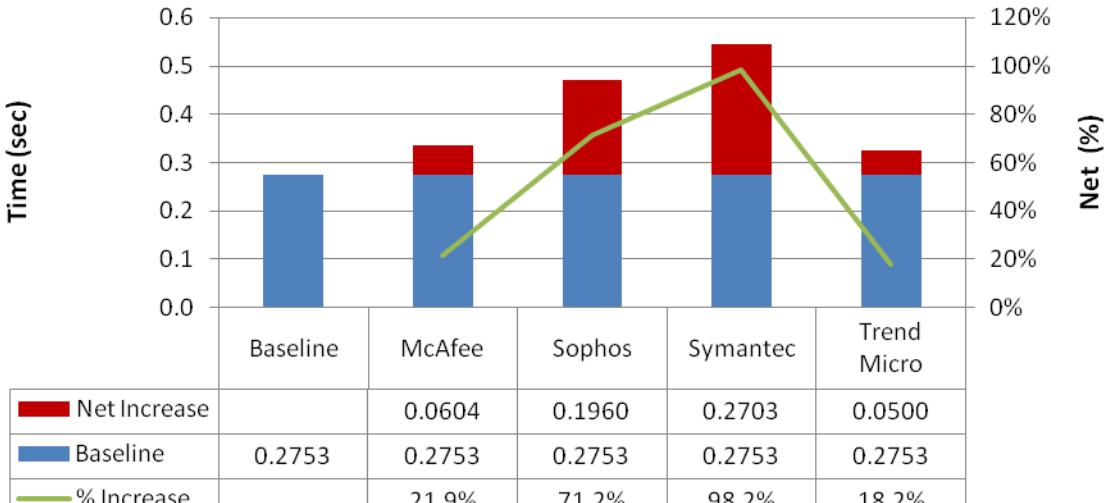


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.05	0.17	0.02	0.01
Baseline	0.06	0.06	0.06	0.06	0.06
% Increase		76.3%	281.5%	28.0%	19.9%

HTTP Download Clean Word Files - 500KB

4.6.2 HTTP Download of Clean Word Files – Mixed Sizes

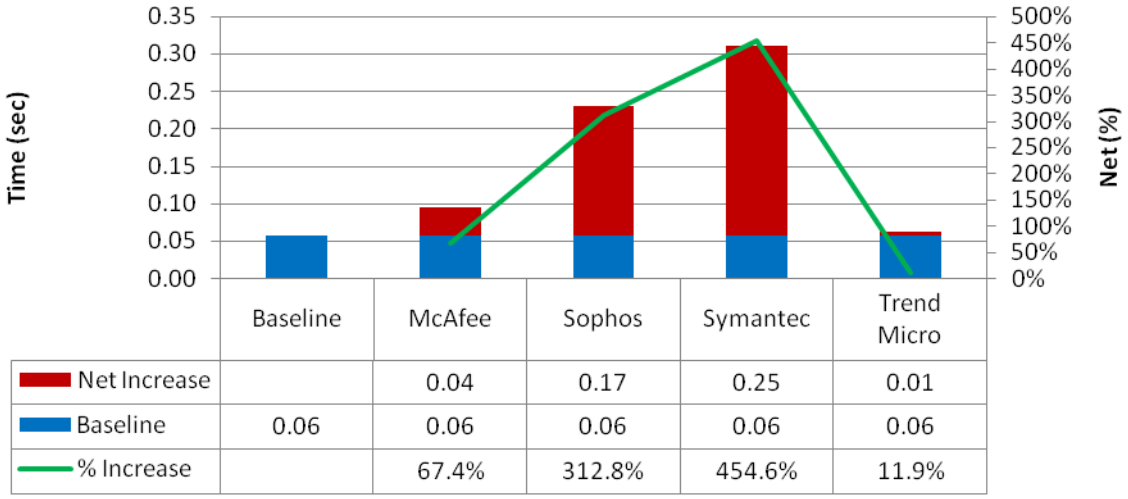
Across all file sizes, Trend Micro and McAfee exhibited the best overall times. File sizes included 500KB, 1MB, 3MB, 10MB and 30MB.



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.0604	0.1960	0.2703	0.0500
Baseline	0.2753	0.2753	0.2753	0.2753	0.2753
% Increase		21.9%	71.2%	98.2%	18.2%

HTTP Download of Clean Word Files

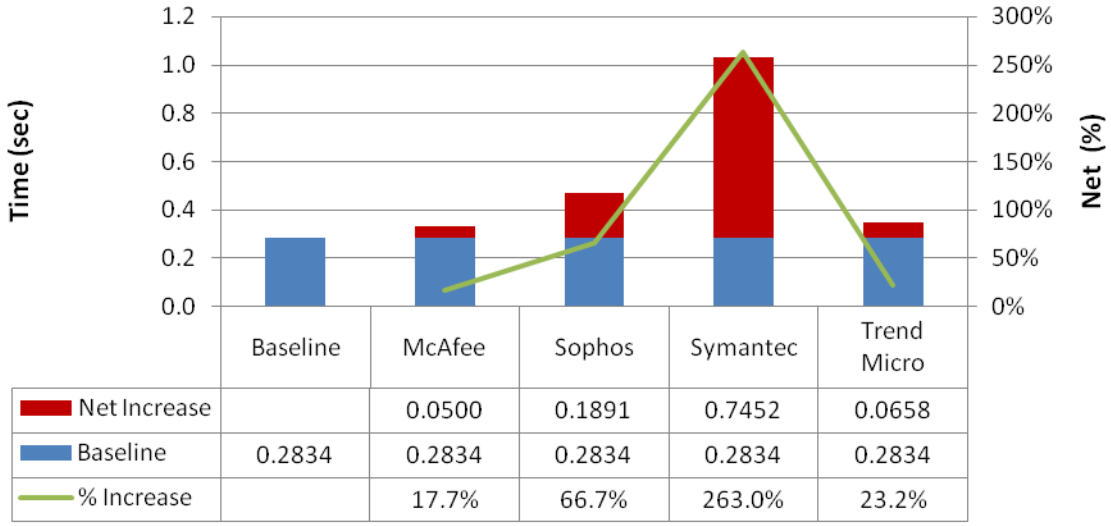
4.6.3 HTTP Download: Clean PDF Files 500KB



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.04	0.17	0.25	0.01
Baseline	0.06	0.06	0.06	0.06	0.06
% Increase		67.4%	312.8%	454.6%	11.9%

HTTP Download of Clean PDF Files - 500KB

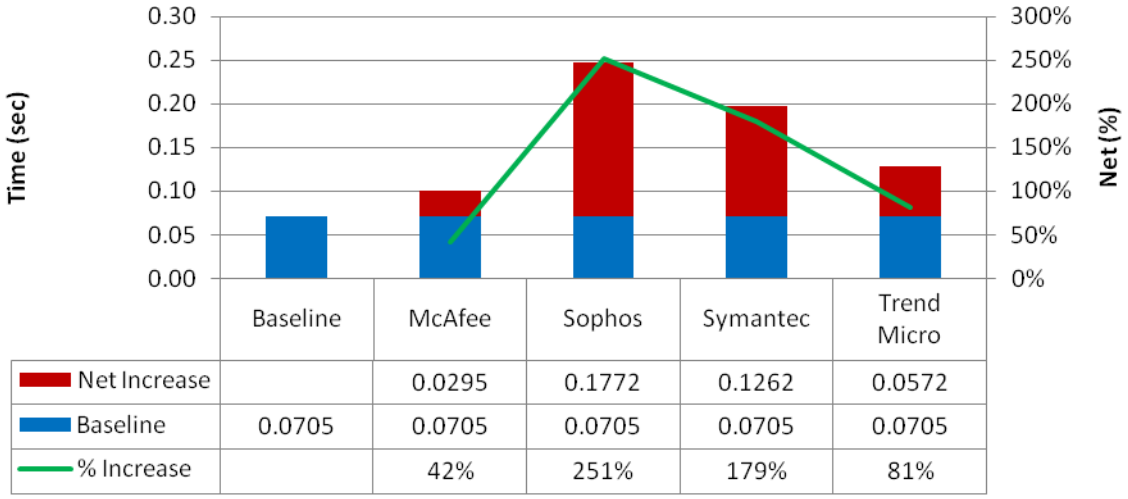
4.6.4 HTTP Download of Clean PDF – Mix of File Sizes



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.0500	0.1891	0.7452	0.0658
Baseline	0.2834	0.2834	0.2834	0.2834	0.2834
% Increase		17.7%	66.7%	263.0%	23.2%

HTTP Download of Clean PDF Files

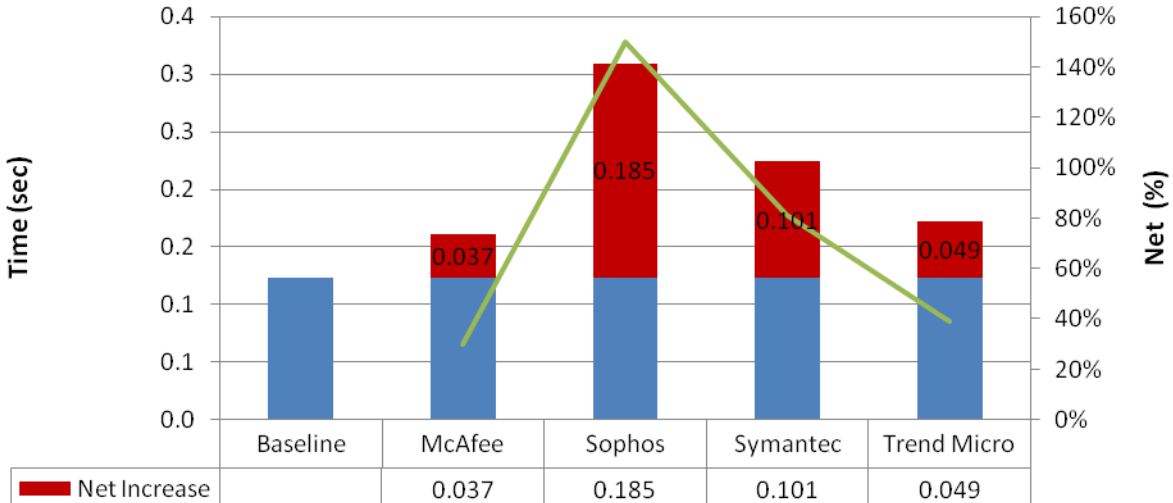
4.6.5 HTTP Download: Clean Excel Files 500KB



	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.0295	0.1772	0.1262	0.0572
Baseline	0.0705	0.0705	0.0705	0.0705	0.0705
% Increase		42%	251%	179%	81%

HTTP Download of Clean Excel Files - 500KB

4.6.6 HTTP Download of Clean Excel Files – Mix of File Sizes

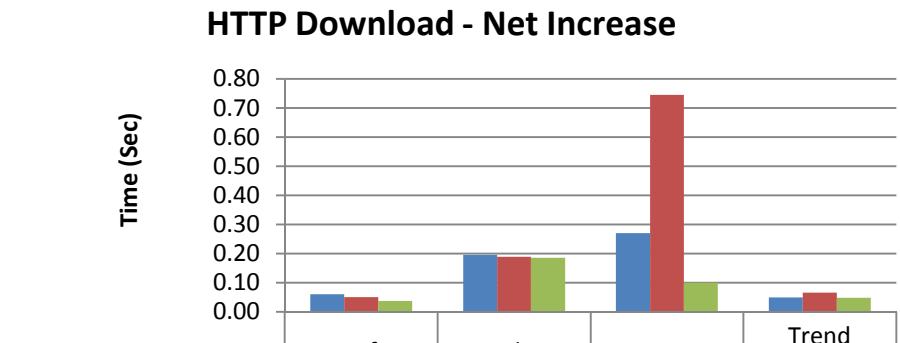


	Baseline	McAfee	Sophos	Symantec	Trend Micro
Net Increase		0.037	0.185	0.101	0.049
Baseline	0.124	0.124	0.124	0.124	0.124
% Increase		30.1%	149.8%	81.2%	39.2%

HTTP Download of Clean Excel Files

4.6.7 HTTP Download Summary – all file types

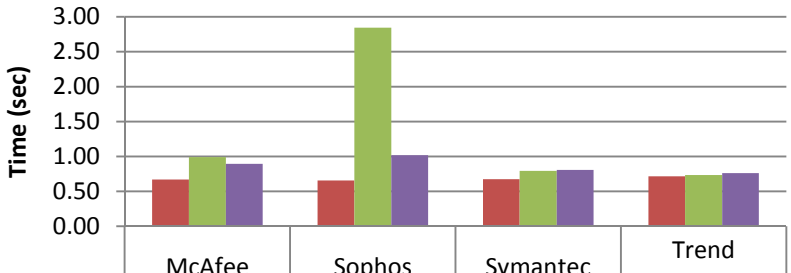
The following graphic shows the average net impact of all tested file types on the download speed. The products from McAfee and Trend Micro exhibited the least overall impact across all tested file types.



	McAfee	Sophos	Symantec	Trend Micro
Average Net Increase - Word	0.0604	0.1960	0.2703	0.0500
Average Net Increase - PDF	0.0500	0.1891	0.7452	0.0658
Average Net Increase - Excel	0.037	0.185	0.101	0.049

4.7 File copy times/speeds from external USB to local folder

Copying 1, 10 and 30 MB files from a USB drive to a local computer folder did not show much variation, except for Sophos' handling of PDF files. The chart below shows the average transfer times across file sizes.

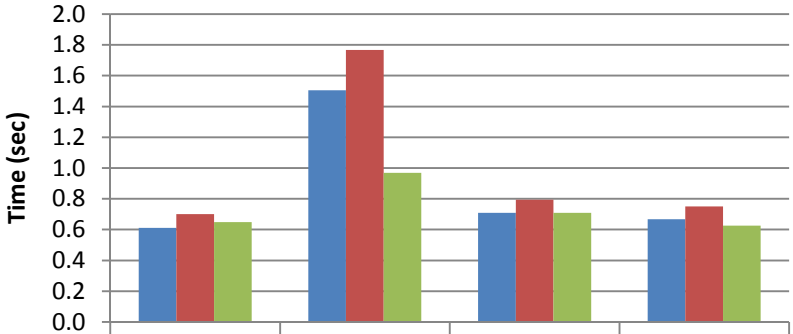


	McAfee	Sophos	Symantec	Trend Micro
Word	0.668	0.657	0.673	0.715
PDF	0.992	2.844	0.795	0.736
Excel	0.892	1.017	0.806	0.762

File Copy: USB to Local

4.8 File Copy Times/Speeds from a Network Folder to a Local Folder

More frequently, users will copy files from a network file server to a local drive. In this case, when copying files of varying sizes (1 MB to 30 MB), very little variation was observed between products, with the exception of Sophos' handling of PDF and Word files which took approximately twice as long as the other products.



	McAfee	Sophos	Symantec	Trend Micro
Word	0.610	1.506	0.709	0.668
PDF	0.701	1.767	0.794	0.750
Excel	0.649	0.970	0.709	0.626

File Copy: Network to Local

5 Appendix A: Test Infrastructure

Special thanks go to our test infrastructure partners who provide much of the equipment, software, and support that make this testing possible: