

# Symantec Corporation

## Symantec Endpoint Protection 11.0.3

### Competitive Performance Evaluation versus Kaspersky, McAfee and Trend Micro on Windows XP



## Test Summary

*Premise: Minimizing the performance impact of security solutions on host PC response times increases user acceptance of security programs and reduces the desire of disabling such programs. By installing a low-impact solution, organizations may be able to postpone investments in new client hardware and achieve a better user experience in parallel.*

Symantec Corporation commissioned The Tolly Group to evaluate the impact of enterprise-class endpoint security offerings on PC client responsiveness.

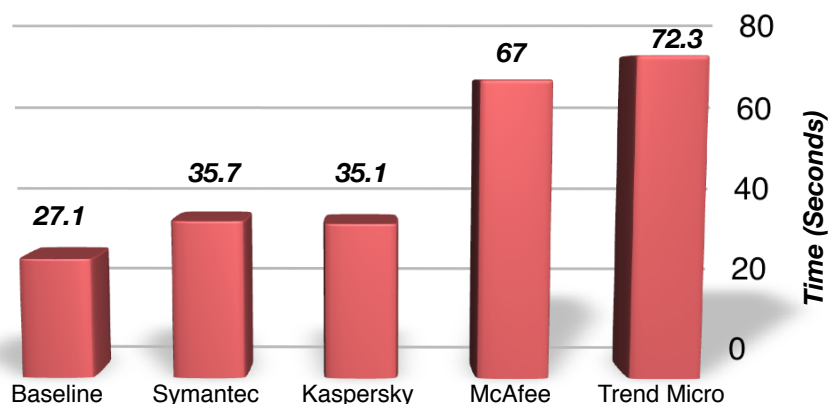
The Tolly Group compared the Windows XP client version of Symantec Endpoint Protection 11.0.3, which provides anti-virus, anti-spyware, firewall, host intrusion prevention and device and application control functionality in a single agent versus security offerings from Kaspersky Lab, McAfee, Inc. and Trend Micro, Inc. (See Figure 8 for a detailed list of products tested.)

The Tolly Group examined system start-up time, the impact on Microsoft Office 2007, on Internet Explorer, on file operations and on the time required to decompress a file archive. Tests were run in October 2008.

### Test Highlights

- ▶ A PC with Symantec Endpoint Protection booted up twice as fast as a PC with Trend Micro OfficeScan and 51% faster than a system with McAfee Total Protection for Endpoint
- ▶ Symantec was the only vendor that did not slow opening of Microsoft Word files and PowerPoint presentations, while McAfee doubled time required to open 1.2-MB Word document
- ▶ Symantec's impact on launching Internet Explorer was less than 10% while Kaspersky, McAfee, Trend Micro slowed systems by more than 50%

### Start-up Time from Initial Windows XP Logo Screen to Idle State



Lower bars are better

Note: Start-up time was measured from the Windows XP logo screen until the host CPU reached idle state.

Source: The Tolly Group, October 2008

Figure 1

## Executive Summary

**Symantec Endpoint Protection 11.0.3 consistently delivered faster response time than competing products tested. At its best, Symantec Endpoint Protection 11.0.3 achieved response times that are twice as fast as some competing products tested.**

Endpoint security solutions are designed to inspect and scan every file that is opened or written to the hard drive. The anti-virus engine scans the file and compares it to its repository of known viruses to ensure that no malicious content is embedded and that no harmful scripts are present in the file. This operation can have a non-trivial impact on the performance of applications such as Microsoft Word and PowerPoint, or on other normal PC processes.

On systems with Symantec Endpoint Protection 11.0.3 Word documents and PowerPoint presentations opened faster than on systems with Kaspersky Work Space

**Windows XP Start-up Time from Windows Logo to Idle State**

Vendor	Product	Average start-up time (seconds)	Time delta to baseline (percentage)
Baseline	Operating system only	27.1	0
Kaspersky Lab	Work Space Security	35.1	22%
McAfee	Total Protection for Endpoint	67	247%
Symantec	Symantec Endpoint Protection 11.0.3	35.7	24%
Trend Micro	OfficeScan 8.0	72.3	267%

Source: The Tolly Group, October 2008

Figure 2

**Response Times Associated with Opening a 1.2-MB Word File on a Windows XP PC**

Vendor	Product	Average file open time (seconds)	Time delta to baseline (percentage)
Baseline	Operating system only	3.7	0
Kaspersky Lab	Work Space Security	4.8	23%
McAfee	Total Protection for Endpoint	7.3	129%
Symantec	Symantec Endpoint Protection 11.0.3	3.6	-2%
Trend Micro	OfficeScan 8.0	5	26%

Source: The Tolly Group, October 2008

Figure 3

Security, McAfee Total Protection for Endpoint, or Trend Micro Office-Scan.

Tolly Group engineers tested the products in six response-time scenarios:

- Start-up time from a Windows logo screen to “idle” state
- Opening a 1.2-MB Word document
- Time to open a PowerPoint presentation
- Time required to launch Internet Explorer and open a Web page
- Time to copy and paste a 1-GB text file
- Time to decompress a 1-GB file archive

Tests show that Symantec Endpoint Protection 11.0.3 delivers faster response times over other products tested on a regular basis, often paralleling the response times delivered by a baseline test of running the operation with no security software present.

**RESULTS**

**START-UP TIME**

In times of instant-on smart phones, users be-

come increasingly dissatisfied with long start-up times, which is why manufacturers like Dell and Intel invest heavily in technologies to speed up the boot process. Many security applications, on the other hand, prolong boot time. Tests show that Symantec Endpoint Protection added only 8.6 seconds to the boot process.

This test measured the time taken to boot a machine from the initial Windows logo until the System Idle process stabilizes at 99% for 10 seconds. This indicates that all services have been loaded and the PC is responsive to user input.

The baseline, with just the Windows XP SP3 operating system running and no security software, took 27.1 seconds to boot. See Figure 2.

The PC with Symantec Endpoint Protection, booted in 35.7 seconds, twice as fast as the system with Trend Micro OfficeScan (72.3 seconds) and 51% faster than the system with McAfee Total Protection for Endpoint (67 seconds).

Symantec Endpoint Protection 11.0.3 was on par with Kaspersky Work Space Security (35.1 seconds).

**MICROSOFT WORD**

Microsoft Word is the most popular office application and a security software should not significantly interfere with its

Symantec Corporation



Endpoint Protection 11.0.3

Response Time Impact of Endpoint Security Systems on Windows XP client PCs

**Product Specifications**

*Vendor-supplied information not necessarily verified by The Tolly Group*

**Symantec Endpoint Protection 11.0.3**

**Benefits:**

- Symantec Endpoint Protection combines Symantec AntiVirus with advanced threat prevention to deliver unmatched defense against malware for laptops, desktops and servers. It seamlessly integrates essential security technologies in a single agent and management console, increasing protection and helping lower total cost of ownership
- Improved end-user Quality-of-Experience through efficient use of system resources

**Features:**

- Seamlessly integrates essential technologies such as antivirus, anti-spyware, firewall, intrusion prevention, device and application control
- Requires only a single agent that is managed by a single management console
- Provides unmatched endpoint protection from the market leader in endpoint security
- Enables instant NAC upgrade without additional software deployment for each endpoint
- Optimizes client footprint and resource utilization to fit all business environments

**Symantec Corporation**

20330 Stevens Creek Blvd.  
Cupertino, CA 95014  
URL: [www.symantec.com](http://www.symantec.com)

performance when opening a document. Engineers measured the time required to open a 1.2-MB Word document until it was ready to be edited.

Tests show that Symantec Endpoint Protection did not slow down this operation. Microsoft Word was able to open the document in 3.6 seconds on a system with Symantec Endpoint Protection 11.0.3 installed, or twice as fast as with McAfee Total Protection for Endpoint (7.3 seconds). See Figure 3.

Kaspersky Work Space Security needed 4.8 seconds, McAfee Total Protection used 7.3 seconds, and Trend Micro needed 5.0 seconds to complete the same operation.

**MICROSOFT POWERPOINT**

PowerPoint presentations usually are larger than Word documents. Tolly Group engineers chose a 10-MB slide presentation and performed a test similar to the Word document test.

The McAfee solution again had the highest adverse impact, adding two seconds to the operation, followed by

**Response Times Associated with Opening a 10-MB PowerPoint File on a Windows XP PC**

Vendor	Product	Average file open time (seconds)	Time delta to baseline (percentage)
Baseline	Operating system only	4.2	0
Kaspersky Lab	Work Space Security	5.4	22%
McAfee	Total Protection for Endpoint	6.3	33%
Symantec	Endpoint Protection 11.0.3	4	-4%
Trend Micro	OfficeScan 8.0	4.7	11%

Source: The Tolly Group, October 2008

Figure 4

**Response Times Related to Launching Internet Explorer on a Windows XP PC**

Vendor	Product	Average file open time (seconds)	Time delta to baseline (percentage)
Baseline	Operating system only	3.4	0
Kaspersky Lab	Work Space Security	5.3	36%
McAfee	Total Protection for Endpoint	6.5	48%
Symantec	Endpoint Protection 11.0.3	3.7	8%
Trend Micro	OfficeScan 8.0	5.6	39%

Source: The Tolly Group, October 2008

Figure 5

Kaspersky with 1.2 seconds. Trend Micro added only a second to the process while Symantec added an unnoticeable 0.1 second. (See Figure 4.)

Kaspersky Workspace needed 5.4 seconds, McAfee Total Protection used 6.3 seconds, and Trend Micro needed 4.7 seconds to complete the same operation.

**INTERNET EXPLORER**

This test measured the responsiveness of Internet Explorer during launch and the time required to load a Web site, such as Yahoo and Reuters. As network speeds are dependent upon external throughput, an internal server was set up to mimic the sample site so a clean throughput was established.

Tests show that the baseline, with no security software present, loaded Internet Explorer in just 3.4 seconds.

Symantec Endpoint Protection 11.0.3 was right behind that with 3.7 seconds, or within 8% of the baseline time, representing the fastest of the products tested. The other products tested exhibited Internet Explorer

**Response Times of a Copy/Paste Operation with a 1-GB File on a Windows XP PC**

Vendor	Product	Average file open time (seconds)	Time delta to baseline (percentage)
Baseline	Operating system only	43.9	0
Kaspersky Lab	Work Space Security	46	5%
McAfee	Total Protection for Endpoint	45.8	4%
Symantec	Endpoint Protection 11.0.3	44.5	1%
Trend Micro	OfficeScan 8.0	44.9	2%

Source: The Tolly Group, October 2008

Figure 6

**Time to Decompress an Archive Containing a 1-GB Text File on a Windows XP PC**

Vendor	Product	Average file open time (seconds)	Time delta to baseline (percentage)
Baseline	Operating system only	339.4	0
Kaspersky Lab	Work Space Security	614.9	181%
McAfee	Total Protection for Endpoint	879.3	259%
Symantec	Endpoint Protection 11.0.3	422	20%
Trend Micro	OfficeScan 8.0	601.4	177%

Source: The Tolly Group, October 2008

Figure 7

load times that ranged from 36% to 48% slower than the baseline result. (See Figure 5.)

### FILE COPY

Security applications with automatic protection features like the ones tested invariably slow down file operations. Minimizing the impact should be the goal of any security vendor.

Tolly Group engineers measured the amount of time required to copy and paste a 1-GB text file. Once again, the system with the Symantec Endpoint Protection exhibited the least impact prolonging the process by 0.64 seconds (44.54 seconds versus the baseline of 43.9 seconds).

The impact of Kaspersky Work Space and McAfee Total Protection was 300% higher than the impact made by Symantec. The impact of the second-fastest product, Trend Micro OfficeScan, was still 150% higher than Symantec Endpoint Protection.

### ARCHIVE DECOMPRESSION

Security applications scan archives as they are being decompressed.

This measurement recorded the time required to decompress a collection of files zipped from one archive.

The baseline to decompress the 1-GB text file was 339.4 seconds. Symantec Endpoint Protection 11.0.3 completed the task within 20% of that time, at 422.3 seconds. Again, the Symantec security solution posted the best performance of all products tested.

Trend Micro OfficeScan needed 601.4 seconds to complete the task, Kaspersky Work Space Security needed 614.9 seconds and McAfee Total Protection used 879.3 seconds. (See Figure 7.)

### TEST SETUP & METHODOLOGY

Tolly Group engineers conducted a competitive evaluation of Symantec Endpoint Protection 11.0.3 along with security offerings from Kaspersky, McAfee and Trend-Micro. (See Figure 8 for a detailed list of products tested.)

Each security application was installed with default settings, but configured to measure accurately against all other security applications during test for an apples-to-apples comparison (i.e. all applications had automatic threat protection features enabled)


After the install and update, time was allotted to process

any required profiling, caching, or system configurations in the background as required by the application. Reboots were conducted after each test.

The test bed consisted of identical computer systems, all configured with the same Microsoft Windows XP SP 3 ghost image and Microsoft Office 2007 Professional. Another computer, connected to the isolated network, was used to deploy the XP images and software under test (SUT) to each computer. A key was added to the registry which enabled automatic logon as the local administrator.

Six test scenarios were conducted to benchmark the performance of the Symantec Endpoint Protection 11.0.3 against other leading vendors' comparable endpoint protection software. These tests included the following:

- Start-up time from a Windows logo screen to "idle" state
- Opening a 1.2-MB Word document
- Time to open a PowerPoint presentation
- Time required to launch Internet Explorer and open a Web page
- Time to copy and paste a 1-GB text file

 Time to decompress a 1-GB file archive

#### **START-UP TIME METHODOLOGY**

An AutoIt script recorded the time at the beginning of the boot process when the machine displayed the initial Windows logo screen and the time when the System Idle process was stable at 99% for 10 seconds.

After saving the times in a log file, the computer restarted and executed the script for three iterations.

#### **INTERNET EXPLORER METHODOLOGY**

An AutoIt script was written and executed for each computer. When the Internet Explorer icon was double-clicked, the script started recording the time required for the computer to launch the browser and navigate to a Web page on an HTTP server.

Engineers constructed an Apache Web server on the local network. Engineers copied some static Web pages from commercial Web sites onto the server. The script instructed users to reach the Web pages on the local server. After completely loading the Web

page, the script recorded the time in a log file, the computer restarted and executed the script for three iterations.

#### **MICROSOFT WORD METHODOLOGY**

An AutoIt script was written and executed for each computer. When a Word document icon was double-clicked, the script started recording the time it took the computer to open the Microsoft Word document and finished recording when it was fully loaded. The script recorded the time in a log file, the computer restarted and executed the script for three iterations. A script was added to the registry which enabled automatic logon as the local administrator.

#### **MICROSOFT POWERPOINT METHODOLOGY**

An AutoIt script was written and executed for each computer. When a PowerPoint document icon was double-clicked, the script started recording the time it took the computer to open the PowerPoint presentation and finished recording when it was fully loaded.

After completely loading the document, the script recorded the time in a log file, the computer restarted and executed the script for three iterations.

#### **FILE COPY METHODOLOGY**

An AutoIt script was written and executed for each com-

puter. When an icon to a 1-GB text document was right-clicked and copied, the script started recording the time it took the computer to copy the document and then paste it in a different subdirectory. The script finished recording when the file was copied to its destination and the file copy dialog box disappeared. The script recorded the time in a log file, the computer restarted and executed the script for three iterations.

#### **ARCHIVE DECOMPRESSION METHODOLOGY**

An AutoIt script was written and executed for each computer. Engineers right-clicked on the icon to an archived 1-GB text file, and selected the “Extract” option. This, in turn, kicked off a script that recorded the time it took the computer to decompress the zipped document’s contents and finished recording when it was fully decompressed into a folder on the desktop.

#### **TOOLS USED**

Performance Monitor: Standard software was installed on all Windows images where counters were used to monitor the resource processes by the second per test.

PerfMon Counters: Counter files were created for the security application. Counter files focused on the permanent processes opened during idle time measurements.

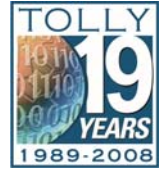
**Products Tested and Software Versions**

Vendor	Product	Version
Kaspersky Lab	Work Space Security	6.0.3.837
McAfee	Total Protection for Endpoint	8.7.0
Symantec	Endpoint Protection	11.0.3
Trend Micro	OfficeScan	8.0 Build 1004

Source: The Tolly Group, October 2008

Figure 8

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](mailto: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 vendor.



**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.*