westcoast labs

Commercial in Confidence

April 2008

Symantec Custom Test

Performance Comparison

Symantec Custom Test Performance Comparison

Vendor Details

Vendor Name:
Symantec Corporation

Vendor Address:
Stevens Creek Boulevard, Cupertino, California, USA.

Vendor Telephone Number: +1(408) 768 0067

Product:
Symantec Endpoint Protection and Competitors products

Test Laboratory Details

Test Laboratory Name:
West Coast Labs

Test Laboratory Address:
Unit 9 Oak Tree Court, Mulberry Drive, Cardiff Gate Business Park,
Cardiff CF23 8RS

Test Laboratory Telephone Number: +44 (0) 2920 548 400

Date: 25th April 2008 **Issue***:* 1.0

Author: Richard Thomas, Michael Parsons, Matt Garrad

Contact Points for Technical Queries on the Test Report

Contact Name: Richard Thomas, Michael Parsons, Matt Garrad

Contact Telephone Number*:* +44 (0) 2920 548 400

Symantec Custom Test Performance Comparison

Contents

Symantec Custom Test Performance Comparison

Executive Summary

Symantec commissioned West Coast Labs (WCL) to perform a series of comparative tests of Symantec Endpoint Protection 11.0 against other equivalent security products. The tests were designed to focus on both performance impact and effectiveness when compared with the industry average against hard to counter threats – in this case, rootkits and rogue antispyware programs.

Testing was conducted by West Coast Labs between October 2007 and January 2008. The competitive products included in the test program to provide the Industry Average are:

McAfee Total Protection inc. ePolicy Orchestrator 4.0
Microsoft Forefront Client Security
Trend Micro OfficeScan 8.0
Kaspersky Anti Virus 6.0
SOPHOS Endpoint Security
CA ITM r8.1

All products were installed on hardware of the same base specification. This report displays particular areas of the resulting data, which Symantec wished to highlight where they proved that Symantec Endpoint Protection 11.0 was the most effective.

Symantec Custom Test Performance Comparison

About Symantec Endpoint Protection 11.0

“Symantec Endpoint Protection 11.0 is an integrated security application that provides a centralized solution for organization-wide endpoint management. It integrates antivirus, antispyware, desktop firewall, intrusion prevention, device and application control, and optional network access control capabilities. It lets IT security managers monitor and protect all critical endpoints—including desktops, laptops, and servers—from a single, easy-to-use management console.”

http://www.symantec.com/business/products/overview.jsp?pcid=2241&pvid=endpt_prot_1

Symantec Custom Test Performance Comparison

Detection Rates

The focus of testing included the detection and removal of rootkits, plus rogue antispyware programs - programs which purport to be genuine removal toolsets, but either do nothing, or infect the machine on which they are installed.

In order to measure the effectiveness of each product, West Coast Labs performed a series of comparisons among known clean machines, infected machines, and post-install, scan and clean machines to determine whether the removal of the offending software was adequate.

In both categories, the Symantec Endpoint Protection 11.0 detection rate compared well against that of the industry average. Table 1.1 shows that Symantec detected more rootkits than the industry average, whilst Table 1.2 shows that the detection of rogue antispyware programs far outstrips the industry average.

Symantec Custom Test Performance Comparison

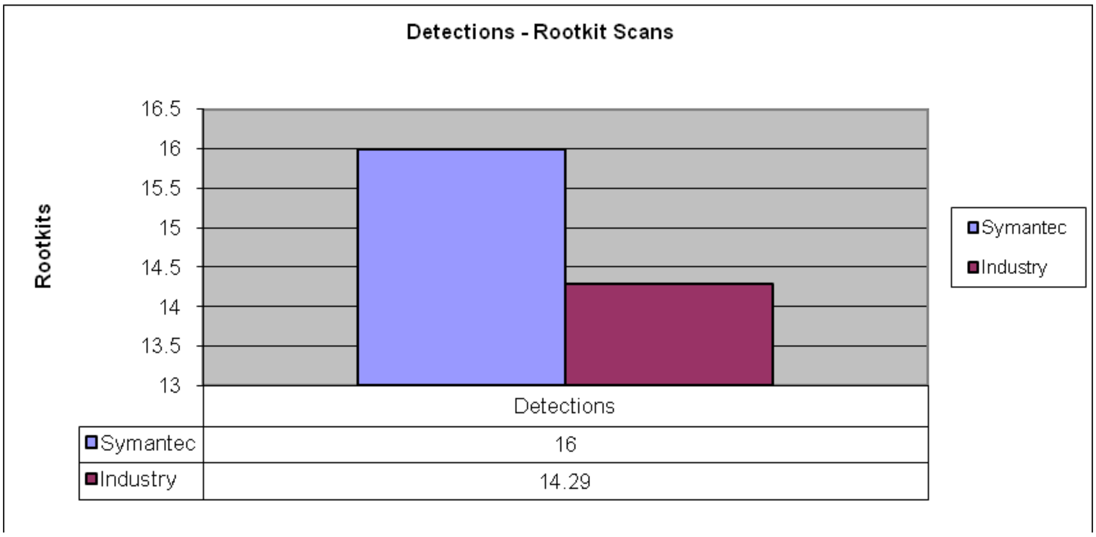


Table 1.1: Rootkit detections from a scan

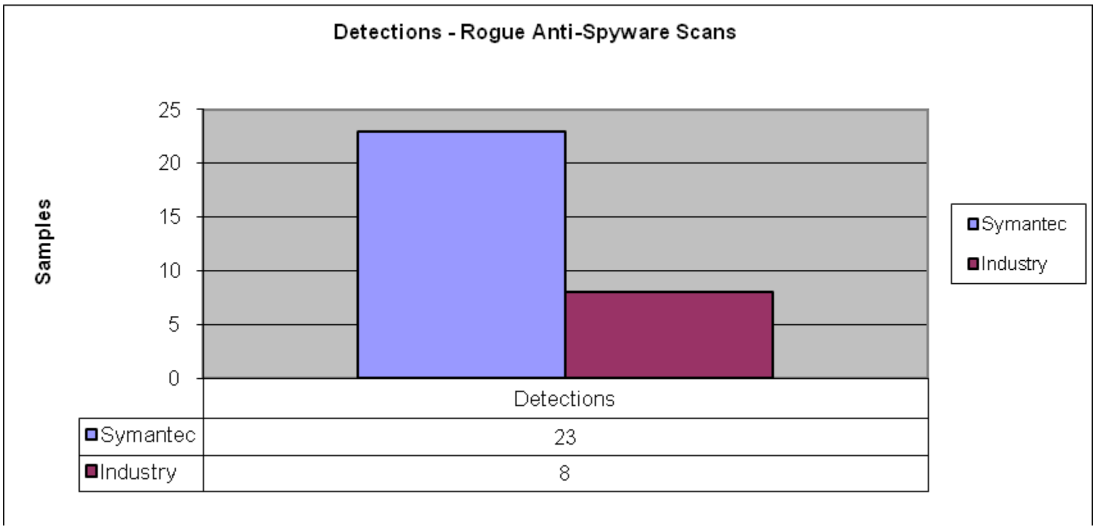


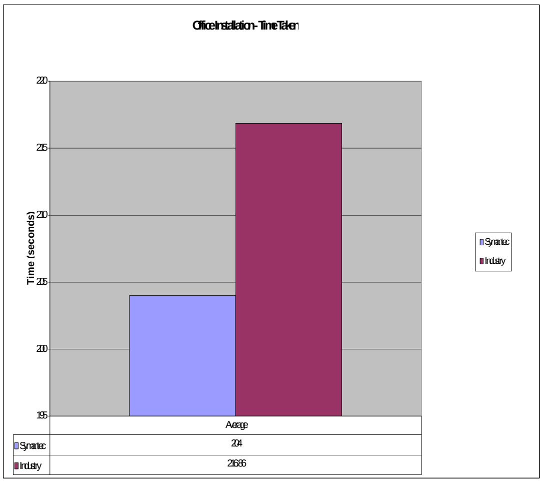
Table 1.2: Rogue Antispyware detections from a scan

Symantec Custom Test Performance Comparison

Performance Analysis

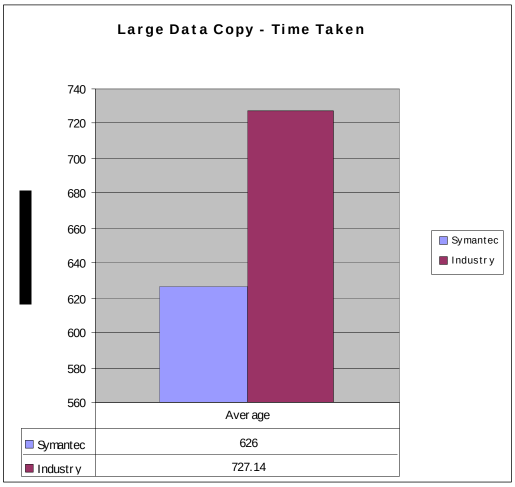
Symantec states that one of the design goals for Symantec Endpoint Protection 11.0 was to decrease memory usage and increase the overall system performance.

In terms of system resource efficiency, one of the areas in which Symantec Endpoint Security performed extremely well was that of the average time taken to perform common user tasks. Tables 1.3 and 1.4 (below) show the time taken to perform a default installation of Microsoft Office 2000, and the time taken to copy 10,000 files, totalling 1Gb of data, from DVD to a local disk.



	Average
🟦 Symantec	204
🟥 Industry	216.86

Table 1.3 – Time taken to install Office



	Average
🟦 Symantec	626
🟥 Industry	727.14

Table1.4 – Time taken to copy data

Symantec Custom Test Performance Comparison

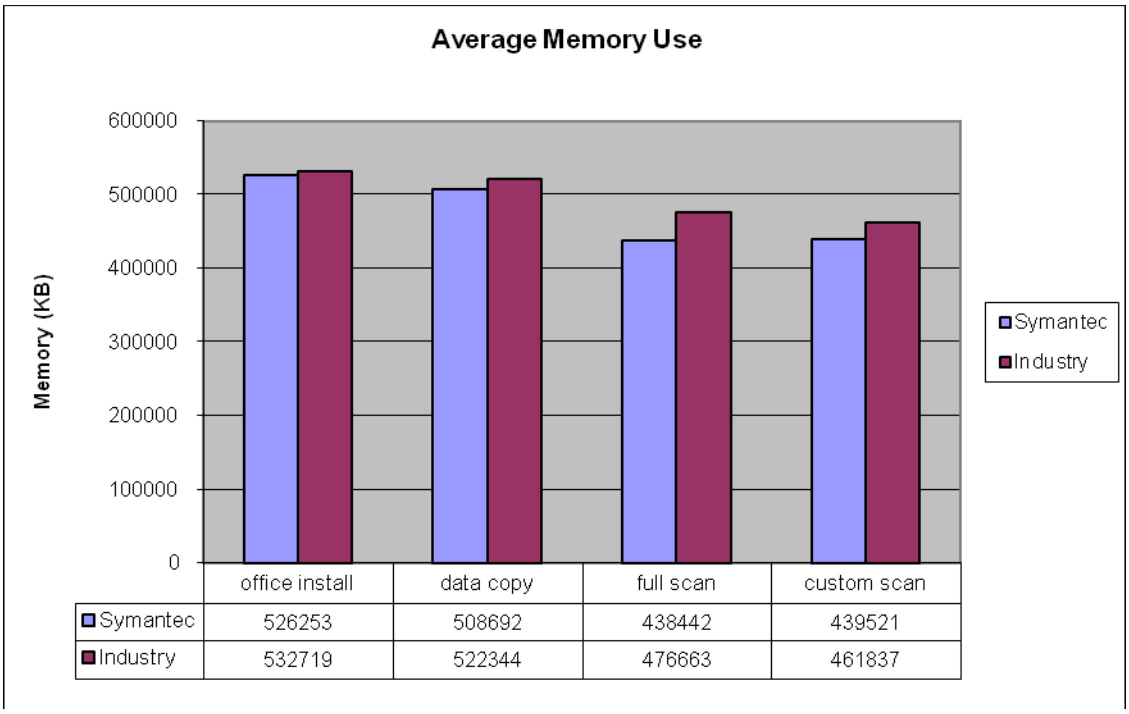
Memory Usage

The real challenge for any security product is to minimize resource usage when the system needs to be performing tasks such as scanning. WCL measured the overall memory usage of a Windows XP SP2 system based around a reasonable hardware specification, while performing typical tasks such as scanning full drives and copying data.

Measuring the overall system memory usage is a critical way to accurately determine the memory consumption when conducting a like for like study of this kind, as some products may only use their own processes, whilst others may increase process resource consumption on already existing Windows processes. It should be noted that the memory use being shown includes the memory reserved for common Windows operations, not just that of security solutions.

The average memory use for an installation of Microsoft Office, a copy of 10,000 files totaling 1Gb of data, a full scan of the hard drives, and a custom scan that included specific target directories, boot sector scans and comparable disinfection methods can be seen in Table 2.1. Symantec used less memory than the industry average in each scenario.

Symantec Custom Test Performance Comparison



	office install	data copy	full scan	custom scan
🟦 Symantec	526253	508692	438442	439521
🟥 Industry	532719	522344	476663	461837

Table 2.1 Overall memory usage during a number of common tasks

Symantec Custom Test Performance Comparison

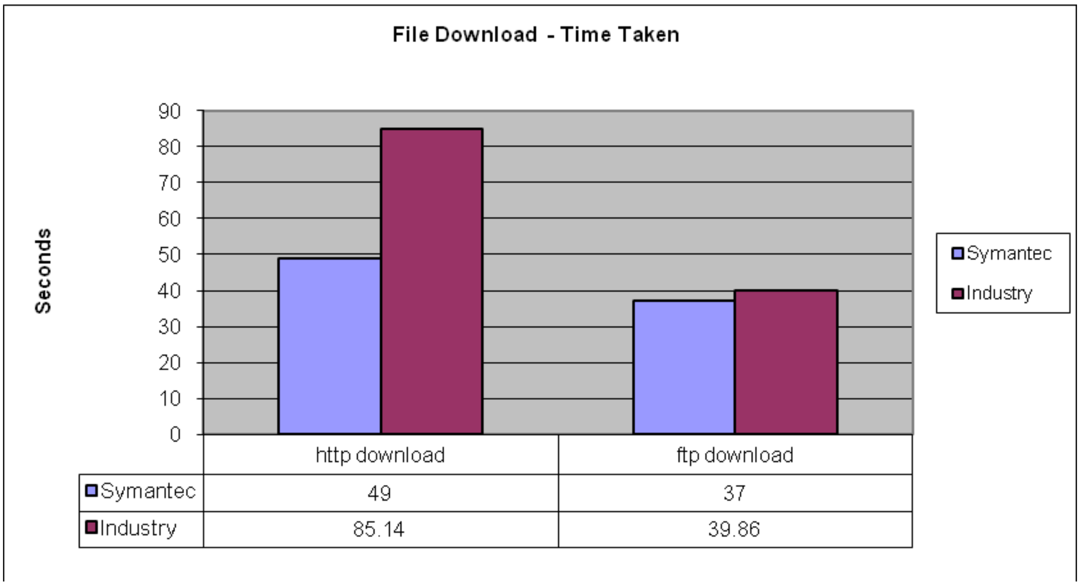
Network Impact

Many vendors have built in additional security functionality such as firewall and network inspection capabilities to their endpoint security solutions. Symantec is one such vendor, implementing network based IPS technologies. These network-based technologies can potentially have a negative impact on network performance.

To measure the exact impact, WCL measured the time it takes to download files over some common protocols. In order to accurately assess the network lag, each product was tested on an isolated network using a 1Gb switch with the same large amount of data being downloaded and uploaded over both ftp and http.

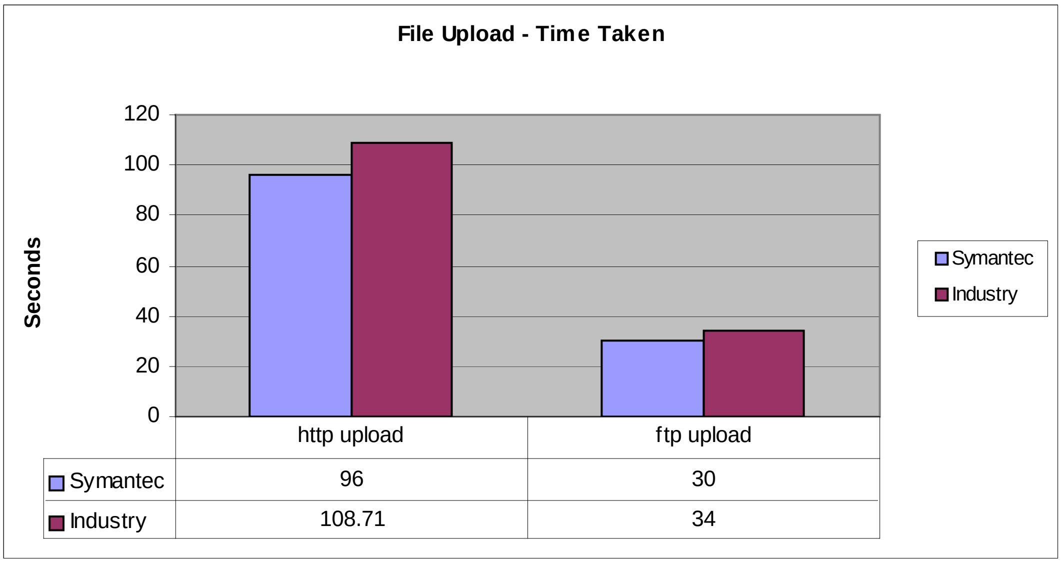
The results can be seen on page 11 in Table 3.1 and Table 3.2. With Symantec Endpoint Protection 11.0 downloads and uploads over ftp and http were faster than the industry average.

Symantec Custom Test Performance Comparison



	http download	ftp download
□ Symantec	49	37
■ Industry	85.14	39.86

Table 3.1 Comparison of download speeds



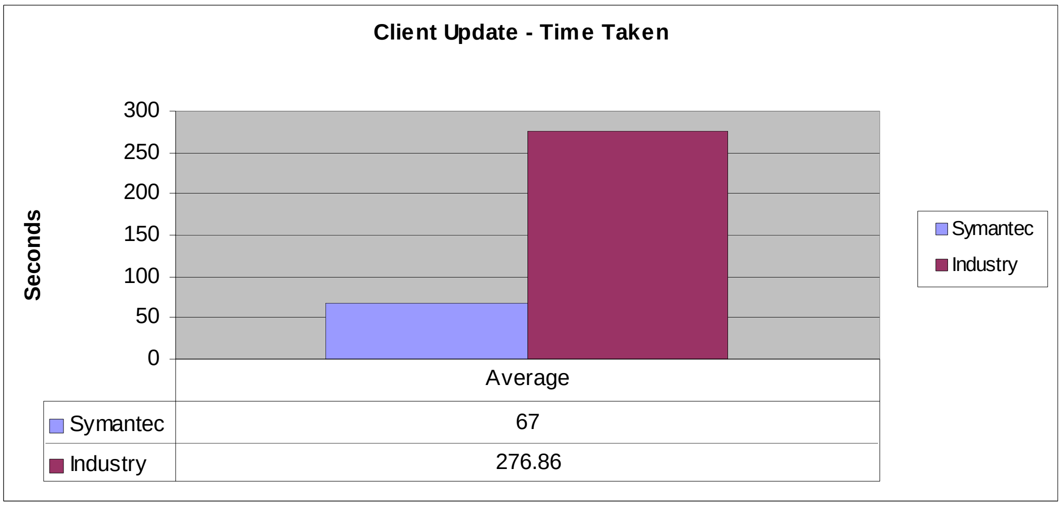
	http upload	ftp upload
□ Symantec	96	30
■ Industry	108.71	34

Table 3.2 Comparison of upload speeds

Symantec Custom Test Performance Comparison

Network Impact

Each of the solutions in this comparison provide a wide variety of technologies each of which require various updates, ranging from antivirus and antispyware to IPS signatures. The amount of time taken to get updates from the internet to any appropriate server and deployed to the endpoint clients was measured to give the figures in table 3.3. It is important to note that these figures may vary dependent upon transient network conditions, and that all testing conducted was from a base install to fully patched to the latest available updates on the day of testing. Results can be seen below in Table 3.3



	Average
Symantec	67
Industry	276.86

Table 3.3 Comparison of patching times

Symantec Custom Test Performance Comparison

Summary

From the results in this Executive summary, Symantec Endpoint Protection 11.0 is extremely competitive when compared to the industry average in a variety of performance scenarios. In particular Endpoint Protection avoids the performance problems that some customers have reported with its predecessor Symantec AntiVirus Corporate Edition.

Symantec Custom Test Performance Comparison

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and / or functionality of any particular product tested and / or guarantee that any particular product tested is fit for any given purpose .

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

Revision History

Issue	Description of Changes	Date Issued
1.0	Symantec Performance Comparison	25/04/08

westcoast labs

US SALES
T +1 717 423 5575

EUROPE SALES
T +44 2920 548400

GLOBAL HEADQUARTERS
West Coast Labs
Unit 9, Oak Tree Court
Mulberry Drive
Cardiff Gate Business Park
Cardiff CF23 8RS, UK

T +44 2920 548400
F +44 2920 548401
E info@westcoast.com
W www.westcoastlabs.com