



#209110
April 2009

Commissioned by Symantec
Corporation

Tolly.

Symantec Endpoint Protection Small Business Edition 12.0 Competitive Windows XP Performance Evaluation Versus AVG Technologies, BitDefender, Kaspersky Lab, McAfee Inc., Sophos Plc, and Trend Micro Incorporated

EXECUTIVE SUMMARY

In small businesses with limited budgets for hardware upgrades, it is important that security software does not significantly impact computer performance.

This comprehensive test which includes 7 vendors, 44 test scenarios, and over 2000 individual test runs, concentrates on real world use cases and common pain points with traditional endpoint security solutions.

Overall, Symantec delivered the best performance, including fastest boot times and file decompression times. Symantec's overall performance clearly sets it apart from all other vendors, who often slow down computers considerably.

THE BOTTOM LINE

- 1 Consistently provides security coverage with less impact overall to user experience than the other solutions tested
- 2 Opens local Microsoft Word, PowerPoint, Excel and Adobe Acrobat files faster than the other solutions tested
- 3 Boots considerably faster than any other solution tested
- 4 Symantec opened documents faster while performing a full scan than did McAfee and Trend Micro when no scan was taking place

Overview

With a more responsive computer, users can be more productive. Symantec Endpoint Protection Small Business Edition 12.0 provides a better user experience than competing solutions right from the beginning.

The Symantec system booted faster than any of the other solutions. The Sophos system took more than twice as long to boot, McAfee and Trend Micro impacted the boot time three times as much as Symantec. This, and all of the tests referenced in this report, illustrate results as compared to a "baseline" system. That baseline system was the test PC without any endpoint security system loaded. This likely represents the best case for performance but, obviously, it is neither practical nor desirable to run a system without any security protection.



The solutions tested are designed for small business where the most common use scenarios include working with documents and spreadsheets stored on the local drive.

To make the test as realistic as possible, different file sizes were used ranging from 100KB to 10MB.

In over 30% of the tests Symantec had no negative impact at all and never impacted the client system by more than 6%. All other vendors impacted the performance by over 30% in at least one scenario.

McAfee showed the biggest negative impact when handling small files adding between 50% to 100% to the task time.

AVG demonstrated the most extreme degradation when it required over 2 minutes to open a 10MB PowerPoint presentation that opened in 8.5 seconds on the unprotected, baseline system.

Another scenario tested was how fast users could access files over the network. This is a very typical scenario as organizations store important files on a server like Windows Small Business Server.

Test results demonstrated that Symantec is either the fastest or within a tenth of a second of the fastest solution.

Many security experts recommend that users perform a full scan of their computer's drive on a regular basis. In most small business environments this occurs during normal business hours.

Users often complain that, during a full scan, the performance of the computer degrades to such an extent

that the system is rendered almost useless.

Symantec has the lowest impact of any solution when performing a full scan of the hard drive and allows users to continue working normally.

In fact, the Symantec offering opened documents faster while performing a full scan than did McAfee and Trend Micro when no scan was taking place.


Test Background

In this round of tests, conducted in March 2009, the Symantec Endpoint Protection Small Business Edition 12.0 was compared with six endpoint security solutions targeting the small business segment. (See Figure 8.) Tests focused on measuring the time to complete common user tasks on Windows XP. Tests were first run on a system that had no endpoint security system installed and then repeated with each solution.

Symantec Corporation

Symantec Endpoint Protection Small Business Edition 12.0

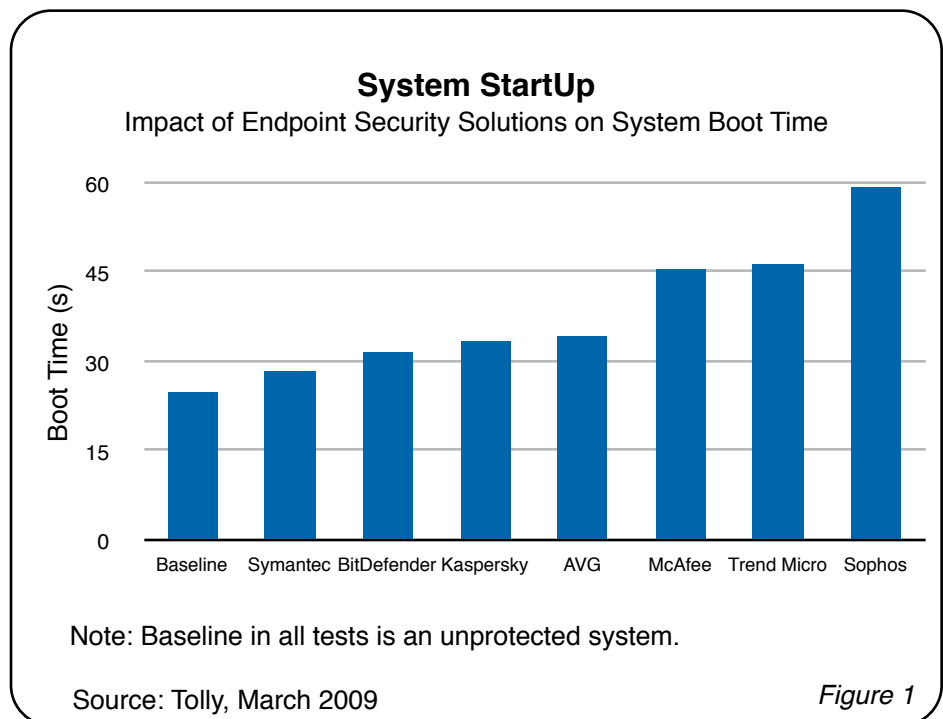
Windows XP Performance



March 2009

In addition to Microsoft Office usage, the tests measured the time to boot the system and the impact on compressing and decompressing files.

As part of its focus on improving performance, the Symantec system balances its use of system resources when performing full scans. Normal file operations are not slowed down when a full security scan is in progress.





Results

Because of the volume of test results, the raw results are reported in a separate document - Tolly document 209110Appendix. This document can be found on both the Tolly and Symantec websites. Graphs represent the additional time required to complete a task as a percentage increase over the baseline.¹

System Boot Time

Computer users have been subject to lengthy boot times since the dawn of the PC. Adding more services on startup, such as virus protection, generally prolong the boot time.

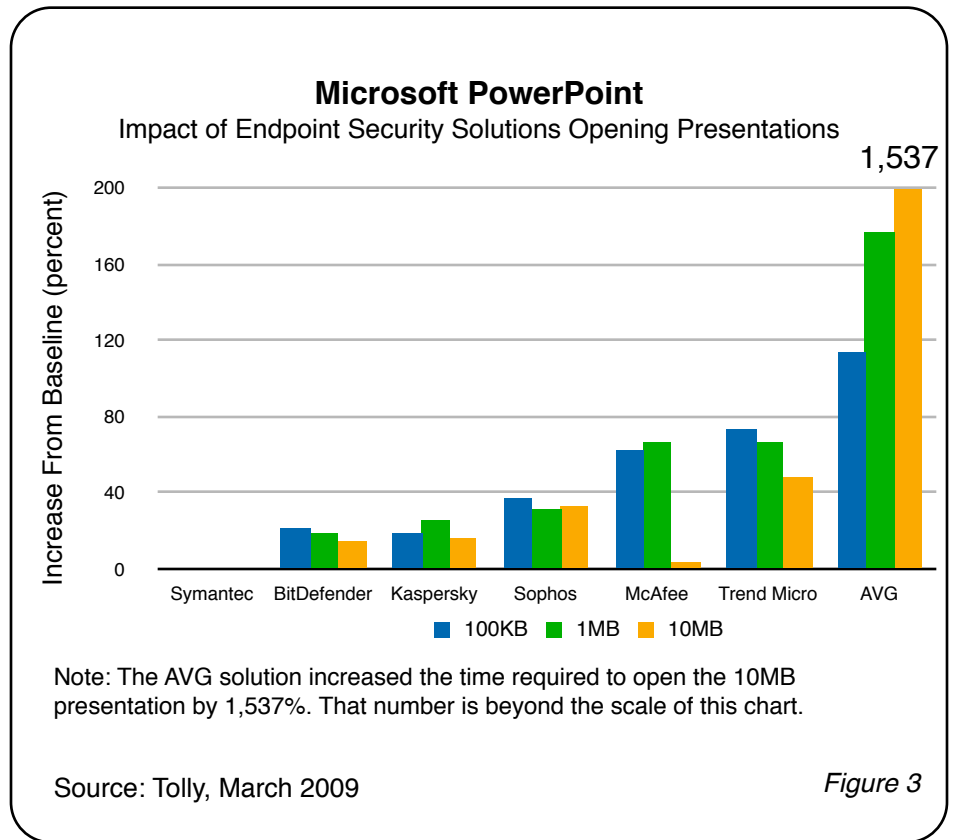
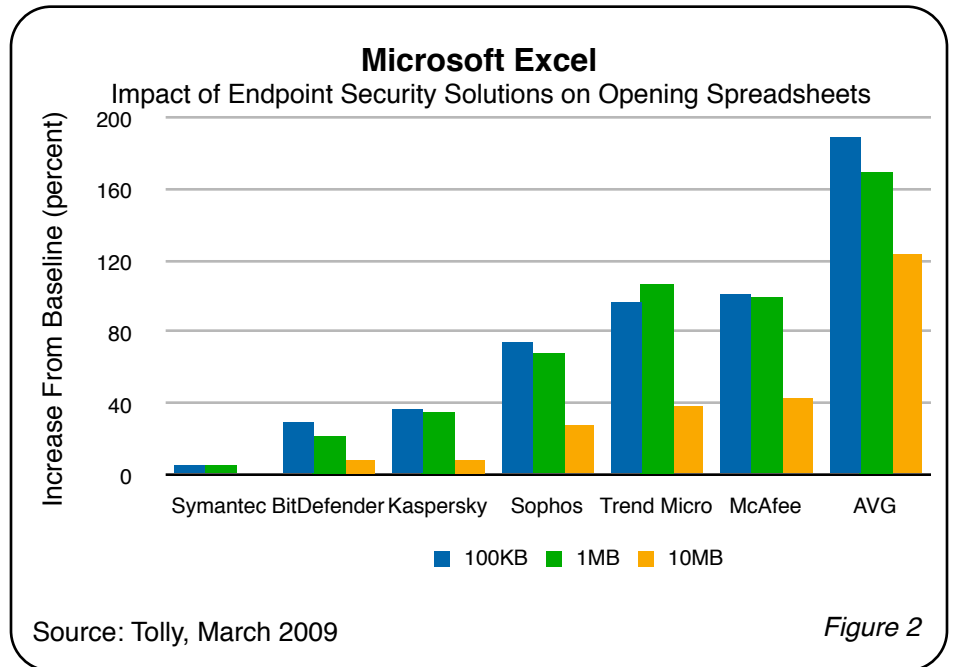
The baseline of an unprotected Windows XP SP3 machine, was 25.0 seconds. The PC running Symantec Endpoint Protection impacted the baseline by a mere 3.8 seconds while McAfee Total Protection Service, added more than 5 times that, at 20.47 seconds. (See Figure 1.)

Microsoft Excel

Symantec once again led the field regardless of the document size, taking just .24 seconds longer to open a 1MB spreadsheet, whereas McAfee and Trend Micro both double the time from less than 5 seconds to almost 10 seconds. (See Figure 2.)

Microsoft PowerPoint

For the baseline test, engineers measured a time of 6.13 seconds when opening a 1MB presentation, Symantec once again had no negative impact, while both McAfee and Trend Micro



¹ In cases where the protected system ran faster than the baseline, those results are represented graphically as having zero impact.



elongated the process by more than four seconds, a significant difference when compared to the near six second baseline. (See Figure 3.)

Microsoft Word

Symantec had no negative impact opening a 100KB word document. McAfee, on the other hand, needed 2.03 seconds to open the file, an 82.6% increase over the baseline. (See Appendix.)

For the second set of Microsoft Word tests, engineers recorded the time taken to copy text and paste it into a new file, then save the document.

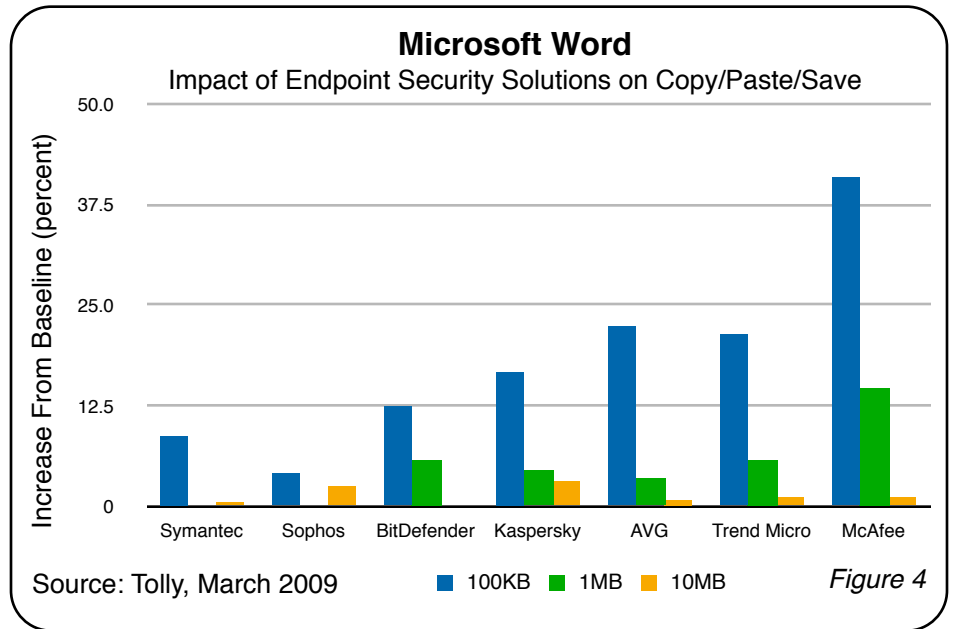
When performing this test on the 100KB document Symantec ran the test in 4.91 seconds, a mere 9% increase from the baseline. McAfee came in last at 6.35 seconds: 41% slower than the baseline. (See Figure 4.)

Sophos performed the operation in 4.7 seconds, 4.4% slower than the baseline.

Archive Decompression

“On-Access” scanning scans files when opened by the user. In the case of archived files, antivirus software must check inside the archive for any malware or viruses that could compromise the system.

With large files this test proved challenging for all vendors. Symantec, once again the top performer, impacted the baseline by 24.1 seconds. Kaspersky and McAfee impeded 4x and 6x more compared to Symantec. (See Figure 5.)

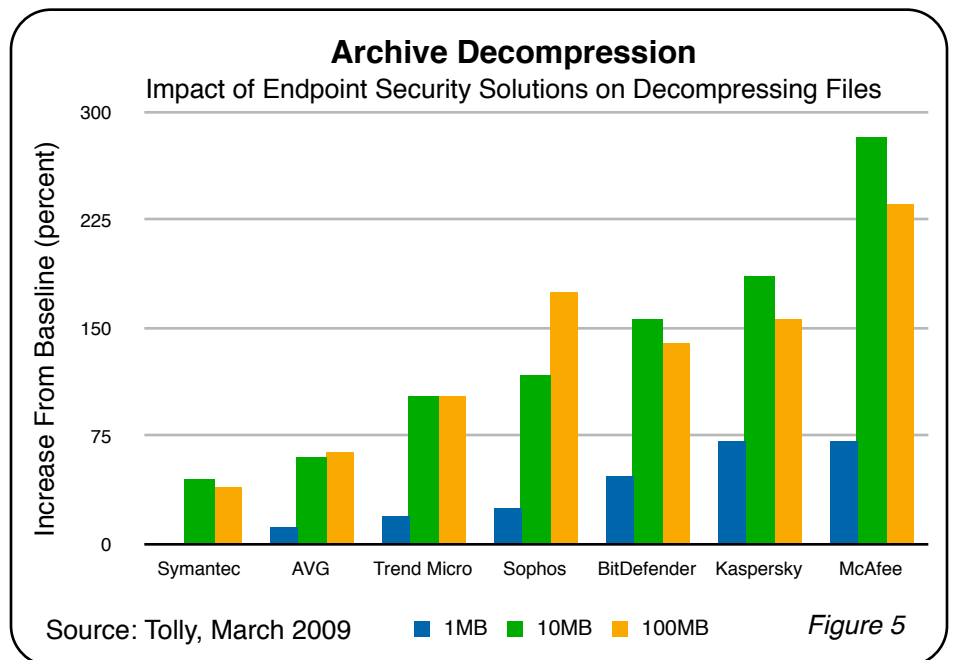


Adobe Reader

When sharing documents in the workplace or over the internet, the accepted format is the PDF. It can be viewed on nearly every platform while preserving formatting and other attributes.

Symantec’s solution outperformed all others exhibiting no system slow down.

Trend Micro’s Small Business solution impacted the baseline system by 97%, effectively doubling the time it takes to open a PDF document.





Mapped Network Drive

Tolly personnel recorded the amount of time needed to perform the same set of core office tests (PDF, PowerPoint, Excel, and Word) while opening the files from a mapped network drive. By averaging the impacts from the baseline for all tests in question, engineers were able to estimate the overall performance impact of the endpoint security solutions when working with server-hosted files.

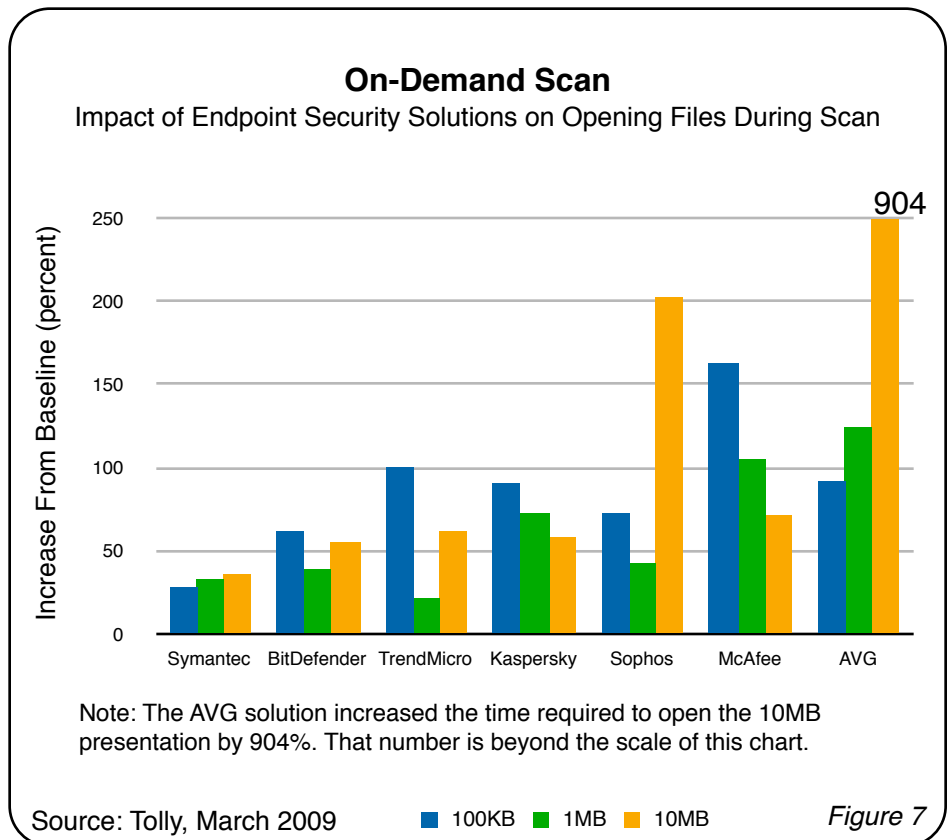
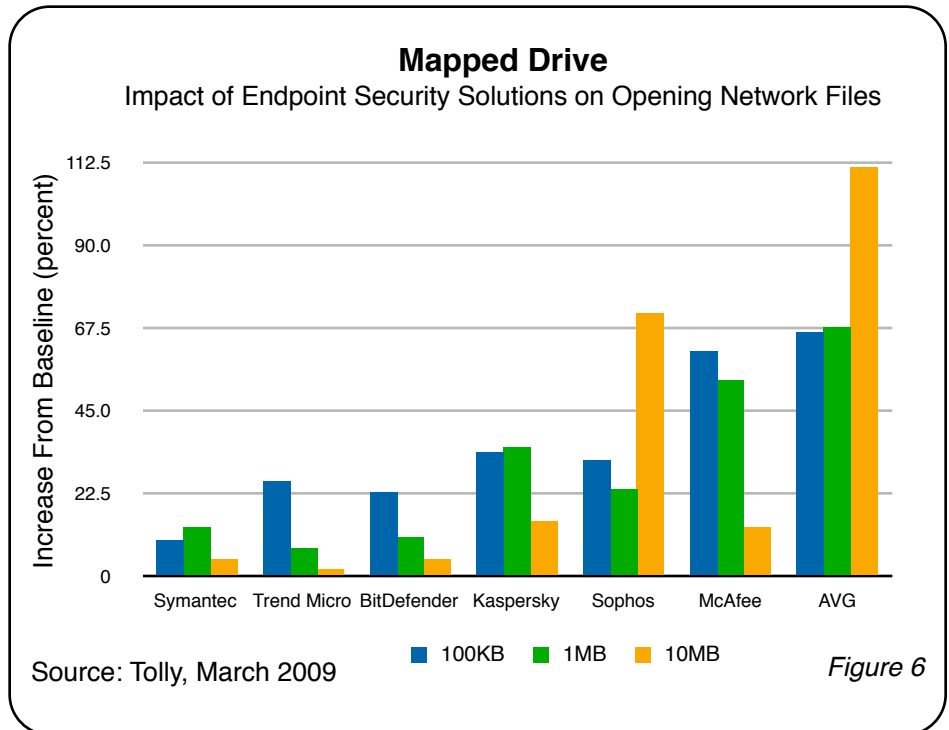
Symantec led the pack in this set of tests, having an average baseline impact of 9.8%. Though McAfee did best Symantec in one scenario, its service lagged behind in all others, ending up with a 43.1% on the baseline, more than 4 times that of Symantec.

“On-Demand” Scanning

The same suite of tests were performed on the systems while running an “On-Demand” scan on a standardized set of data in order to measure what impact the scan had on opening files.

Taking the average deviation from the baseline in the same manner of the previous test, led Tolly engineers to determine how the scanning would affect the systems while opening the batches of 100KB, 1MB, and 10MB files.

All in all, Symantec was the best pick once again, averaging 33.2% over the baseline. Kaspersky’s service impacted the baseline system by more than twice that, at 74.8%, while McAfee tipped the scales at 113.7% impact, nearly 3.5 times that of Symantec.





Test Systems

In order to guarantee both accuracy and precision of the test data, measures were taken to eliminate variables across systems. Each Client PC was equipped with a Pentium 4 running at 3.4GHz, 2GB RAM on a 200MHz system bus, a 160GB SATA HDD at 7200 RPM, and a Gigabit Ethernet NIC. The initial system was loaded with Microsoft Windows XP Pro SP3, Adobe Reader 9.1, and Microsoft Office 2007 Enterprise. Windows Update was run, and all available updates were installed.

This baseline system became the starting point for all endpoint security solutions. Engineers then cloned this system onto the other client PCs, where each vendor’s solution was installed. The server systems were created in the same way, with the exception of running Windows Server 2003 Small Business Edition SP2.

Methodology


For all testing, AutoIT scripts were configured to measure the elapsed time between certain system events,

triggered by the application in question. For example, the tests involving PowerPoint, Excel, and Adobe Reader, were timed from the double-click to when the final page of the document was readable. This approach, which eliminated human error, yielded very low standard deviations, averaging well under .5 seconds for all scenarios. All tests were performed five times.

The Microsoft Word tests and zip-archive tests were performed in the same manner. The system boot test was timed from the initial Windows logo until the CPU utilization remained under 5% for 5 seconds, indicating that the system was idle.

For the mapped drive testing, the test files were placed on the server , and the PowerPoint, Word, Excel, and PDF files were opened sequentially, with gaps of 20 seconds between each file. This method produced different baseline results than when performed on a local drive, but are still valid.

When gathering the data for performing these operations during an “On-Demand” scan, the same method was



The test methodology used for this report relies upon test procedures, metrics and documentation practices as defined by Tolly Common RFP, #1086 Endpoint Security Performance.

To learn more about Tolly Common RFPs, go to:
<http://www.CommonRFP.com>

used, opening each batch of files serially, while the endpoint security solution was scanning the computer for threats. After each iteration of testing, the client system was rebooted and left for 5 minutes before continuing.

To view the complete set of results, please see Tolly document 209110Appendix, which can be found on both the Tolly and Symantec websites.

Windows XP Endpoint Security Solutions Tested

Vendor	Product	Version
AVG Technologies	Internet Security Network Edition	8.0.0.225
BitDefender	Client Security	3.0.45.0
Kaspersky Lab	Open Space Security	6.0.3.851
McAfee, Inc.	Total Protection Service	14.0.0.370.x86
Sophos Plc.	Computer Security	7.6.4
Symantec Corporation	Endpoint Protection Small Business Edition	12.0.106.155
Trend Micro Incorporated	Worry-Free Business Security Standard	15.1

Source: Tolly, March 2009

Figure 8



About Tolly...

The Tolly Group companies have been delivering world-class IT services for 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company via E-mail at sales@tolly.com, or via telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
<http://www.tolly.com>

Interaction with Competitors

As the products are designed to be "user installable" without support, it was not deemed necessary to contact the competing vendors. Default configurations were used and only modified if required to ensure equivalent configurations across products



For more information on the Tolly Fair Testing Charter, visit:
<http://www.tolly.com/FTC.aspx>

Terms of Usage

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 a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. 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.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. 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. Accordingly, this document is provided "as is", and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com.

No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

209110-tb5-jft-21Apr09-verL final