

Sophos Endpoint Protection & Sophos Cloud Endpoint Protection

Endpoint Security Management Usability & Functionality vs Kaspersky, McAfee, Microsoft, Symantec & Trend Micro

EXECUTIVE SUMMARY

Few would argue about the importance of endpoint security in any business IT environment. But, for a security solution to be effective it must be easy to deploy and maintain. Some solutions can be so complex to implement that features are either easily misconfigured or not used at all. The less effort involved, the more likely it is that the security features will be used and used correctly.

Sophos commissioned Tolly to evaluate its on-premise and cloud-based endpoint security solutions, Sophos Endpoint Protection & Sophos Cloud Endpoint Protection. Sophos has designed these solutions to provide broad security functionality “out of the box” and make it easy for users to respond to common security threat scenarios. These solutions were compared to other prominent offerings from Kaspersky, McAfee (Intel Security), Symantec and Trend Micro. Of the solutions tested, only the Sophos offerings provided a range of functionality, including pre-configured best practices and templates, that were ready to use upon installation and simple to manage. See Figure 1 for a summary of the results.
...<continued on next page>

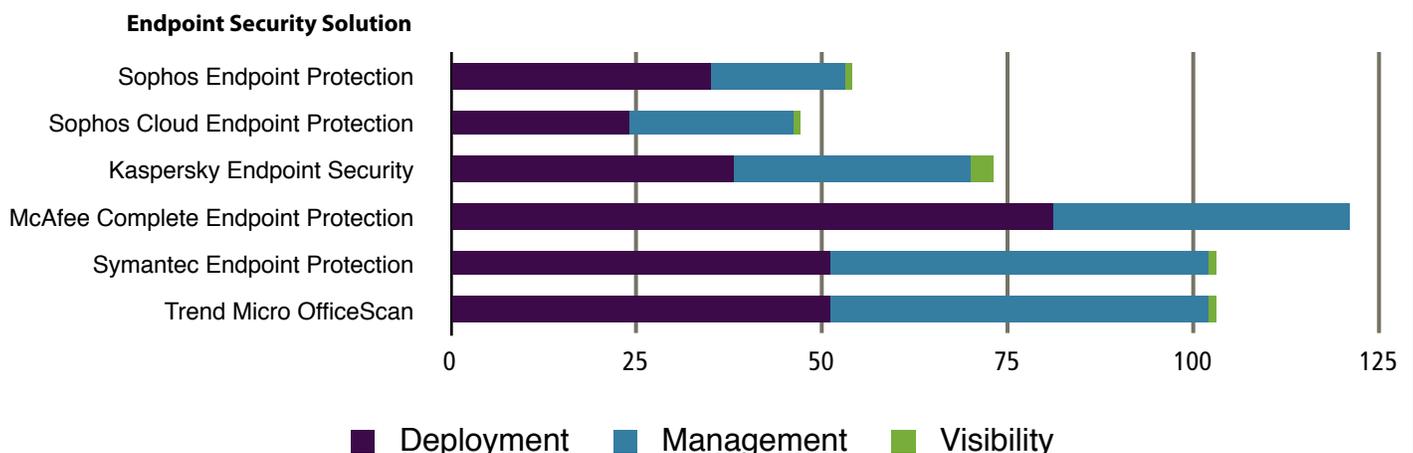
THE BOTTOM LINE

Sophos endpoint security solutions are:

- 1 Easy to configure and deploy “out of the box”
- 2 Designed for rapid access to common management & visibility tasks
- 3 Better able to deliver pre-configured, ready to use security functionality than other tested solutions

Endpoint Security: Summary of Steps Required for Various Tasks

Lower numbers are better



Notes: 1. The figure summarizes the number of steps required to perform various tasks that are detailed in the feature tables of this report. Tasks measured in time, such as installation, are not included. McAfee does not offer the single visibility task.

Source: Tolly, March 2015

Figure 1



Tolly engineers profiled common scenarios in the areas of deployment, management and visibility using each of the solutions under test. Usability was evaluated by counting the number of steps required to complete the task - except for the initial installation where setup time was logged. Typing a word, clicking or double-clicking would each be counted as a step. Summary tables were prepared where entries were color coded to indicate fewest steps with green indicating best and orange and

yellow indicating 2nd and 3rd place and white indicating results after 3rd place. In some cases where results were very close, more than one vendor could be listed in 2nd or 3rd place.

Deployment Scenarios

Installation

Because Sophos Cloud is a hosted service, there is no deployment required. With

Sophos, Ltd.

Endpoint Protection & Cloud Endpoint Protection



Endpoint Protection Usability

Tested March 2015

Deployment: Installation, Endpoint Deployment and Basic Configuration

Number of Steps to Accomplish Task

Solution/Task	Sophos Endpoint Protection	Sophos Cloud Endpoint Protection	Kaspersky Endpoint Security	McAfee Complete Endpoint Protection	Symantec Endpoint Protection	Trend Micro OfficeScan
Install Server & Prerequisites (minutes)	22 min.	Cloud. No installation	17 min.	25+ min. (additional updates took place during install)	5 min.	17 min.
Deploy Endpoint	14	7	22	30	17	10
Block Access to Unwanted Website	7	17 (For first website, subsequent require fewer steps)	15	10	18	10
Enable HIPS "Best Practices"	0	0	0	4	0	0
Configure to Send Email on Malware Detection	10	0 (default)	1 (configured during the installation)	31	0 (configured during the installation)	13
Apply Updating Policy to Roaming User Group ¹	4 Automatically update from closest source to conserve bandwidth	0 (uses public Sophos Cloud server)	0 (automatically uses public Kaspersky server when roaming)	6+ Automatically choose the update source using ping or hops. But need to configure the update source (repository) list and credentials first	16	18+
Data Loss Prevention Support	Yes with the default installation	No	No	Yes with additional component installation and license	No	Yes with additional plug-in
Total Steps (Lower number is better)	35	24	38	81	51	51

Notes: 1. Sophos Endpoint Protection supports the unique Location Roaming feature. The roaming laptops attempt to locate and update from the nearest update server location by querying other (fixed) endpoints on the local network they are connected to, minimizing update delays, bandwidth costs and administrative overhead. See <http://www.sophos.com/en-us/support/knowledgebase/112830.aspx> for detail. 2. In some cases, functionality is not available in default and/or trial versions of the software and would require additional installation. A click, double-click or typing a word is counted as one step. Legend: Green= best, yellow=2nd, orange=3rd, white=4th or beyond.

Source: Tolly, March 2015

Table 1



traditional, on-premise solutions, administration is provided via a Windows Server system. Tolly engineers were able to deploy Sophos Enterprise Console in about 20 minutes with all pre-requisite software automatically downloaded and installed as part of the Sophos installation task. Table 1 summarizes all deployment tasks.

For some other solutions, manual installations of components such as the Microsoft .NET Framework required additional steps and increased complexity of the installation. Furthermore, for certain solutions, the full range of functionality covered in this test was not installed with the base system.

McAfee and Trend Micro require the installation of a separate plugin for the data loss prevention (DLP) functionality while for Symantec, the DLP functionality requires a separate product. Kaspersky does not offer a DLP solution.

Where the Kaspersky and Symantec solutions install device control as part of the standard installation, that is not the case for either McAfee or Trend Micro.

Endpoint Deployment & Basic Configuration

For Sophos Cloud, endpoint deployment is as simple as generating an email to the prospective user. Similarly, Sophos Endpoint Protection provides for straightforward deployment of the client endpoint software. This contrasts with other solutions such as those from Kaspersky and McAfee that require 20 to 30 steps for completion.

For both Sophos solutions, host intrusion prevention services (HIPS) best practices are enabled by default.

Policy & DLP Setup

The Sophos solutions provide quick access to policy information allowing the administrator to find which groups are using a particular policy as well as to copy a policy from one group to another.

Furthermore, Sophos Endpoint Protection provides a unique feature called "location roaming". This allows roaming devices like laptops to automatically reconfigure update settings so they update from the nearest update server rather than from a fixed server that might, at times, be situated across a slower, remote connection.

Finally, only Sophos Endpoint Protection provides DLP as part of the standard installation. Some other vendors either don't offer it at all or require the installation of a separate plug-in and possible additional licensing costs.

Importantly, Sophos Endpoint Protection provides DLP templates for commonly protected items such as credit card numbers. This allows the DLP feature to be implemented without complication and provide immediate benefits to the organization.

Management

Allow Blocked Device

In daily use, a series of tasks are typically required to respond to common security situations. Thus, it is useful for the management system to provide an easy flow among related tasks.

The Sophos solutions provide such linkage so that a group of related tasks can be performed with just a few clicks.

When a user's device is blocked and that user contacts the security administrator, the Sophos on-premise needs only around a dozen clicks to find the user's machine, group and associated policy, find the blocked device and then, assuming it is the appropriate action, allow the blocked device. For Sophos Cloud, this takes just a few clicks.

Other solutions require up to 40 or more steps to complete the same set of tasks or even require a separate tool to be run on the client. Table 2 summarizes all management tasks.

Authorize Potentially Unwanted App

Finally, in response to an application that is classified as potentially unwanted but is determined to be allowable, Sophos provides that authorization. In the case of Sophos Cloud, it is just a few clicks from the dashboard to authorize an application.

Microsoft System Center

Originally, the Endpoint Protection feature of Microsoft System Center was to be included in this test. Tolly engineers found the effort required to bring that solution online was disproportionate with the endpoint security feature set that it offered.

Given this, Tolly thinks it unlikely that this solution would be installed and considered as a standalone security solution and excluded it from the test.



Management: Policy, Responses to Blocked Device & Allow Potentially Unwanted App Number of Steps to Accomplish Task

Solution/Task		Sophos Endpoint Protection	Sophos Cloud Endpoint Protection	Kaspersky Endpoint Security	McAfee Complete Endpoint Protection	Symantec Endpoint Protection	Trend Micro OfficeScan
Copy Policy Between Group		6	9	9	8	6	15
Allow one blocked device for a user	Find Users Machine	1+	3 with search	2 with user complaint from the agent	5+ search in Events	9 with search	4 with search
	Find Associated Group & Policy	+4	+1	+1	+0	+5	0
	Find Blocked Device	+4	+3	+0	+1	+5	Many steps to run a tool on the client (10 steps for purpose of calculation)
	Allow Blocked Device	+4 choose	+3 choose	+9 choose	+20 manual enter	+18	+11 manual enter
	Sub-Total	7 to 13+*	10	12	26	37	25
Authorize Potentially Unwanted App		5 auto display and choose	3 auto display and choose from dashboard	11 manual enter	6 manual enter	8 auto display and choose	11 manual search and choose
Total Steps (Lower number is better)		18 to 24	22	32	40	51	51

Notes: In some cases, functionality is not available in default installation of the software and would require additional plug-ins. A click, double-click or typing an entry is counted as one step. A "+" before a number represents additional steps beyond prior task. *7 steps to exempt the device for all policies. 13+ steps to exempt the device for a specific policy. Legend: Green= best, yellow=2nd, orange=3rd, white=4th or beyond. Blue = Individual items that are part of total.

Source: Tolly, March 2015

Table 2



Visibility

Finally, it is important to have quick access to information about the state and status of endpoints. Table 3 summarizes the visibility results.

Sophos solutions allow the user to take action from the display screen. Some solutions, such as Symantec Endpoint Protection, do not allow the administrator to take action from the screen listing the endpoints.

Both Sophos solutions provide 1-click access to listing all active protected endpoints which checks in with the management server. Furthermore, both

Visibility Number of Steps to Accomplish Task						
Solution/Task	Sophos Endpoint Protection	Sophos Cloud Endpoint Protection	Kaspersky Endpoint Security	McAfee Complete Endpoint Protection	Symantec Endpoint Protection	Trend Micro OfficeScan
List Active Protected Endpoints	1	1	3	Does not list by status	1 (Cannot take action from view screen)	1

Legend: Green= best, yellow=2nd, orange=3rd, white=4th or beyond. Because most solutions could accomplish tasks in 3 clicks or fewer, those are all listed as "best".

Source: Tolly, March 2015 Table 3

Endpoint Security Solutions Under Test	
Solution	Version
Sophos Endpoint Protection	Management Server: Sophos Enterprise Console 5.2.2, Agent: Sophos Endpoint Security and Control 10.3
Sophos Cloud Endpoint Protection	Agent: Sophos Endpoint Security and Control, version 11.0.1 Cloud
Kaspersky Endpoint Security	Suite: Kaspersky Endpoint Security for Business - Advanced Management Server: Kaspersky Security Center 10.2.434, Agent: Kaspersky Endpoint Security 10 SP1
McAfee Complete Endpoint Protection (Intel Security)	Management Server: McAfee ePolicy Orchestrator 5.1.0 (Build: 509), Agent: McAfee Agent 4.8, McAfee Data Loss Prevention and Device Control 9.3, McAfee Host Intrusion Prevention 8.0, McAfee SiteAdvisor Enterprise Plus 3.5, McAfee VirusScan Enterprise 8.8
Symantec Endpoint Protection	Management Server: Symantec Endpoint Protection Manager 12.1.5337.5000, Agent: Symantec Endpoint Protection 12.1.5337.5000,
Trend Micro OfficeScan	Management Server: Trend Micro OfficeScan Server 11.0 Patch 1 Build 1454, Agent: Trend Micro OfficeScan Agent 11.0.1454

Source: Tolly, March 2015 Table 4



Test Setup & Methodology

Setup

Each solution was set up according to vendor requirements. Traditional solutions were deployed in a VMware virtual environment. Server environments were Windows Server 2008 R2. Additional components, such as SQL Server, installed as required by the solution under test.

Details of the solutions under test can be found in Table 4.

Task Execution

Tolly engineers quantified the process and number of steps required to complete each task outlined in this report. Each “click”, “double-click” or typing of a word was counted as a step. Relevant details of each task can be found in the task tables elsewhere in this report.

Engineers attempted to follow the most direct path to completing a task but may not always have found the best path. Thus, users concerned about a specific task or process should evaluate that process for themselves.



About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 25 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 by E-mail at sales@tolly.com, or by telephone at +1 561.391.5610.

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

Interaction with Competitors

In accordance with our Fair Testing Charter, Tolly contacted the competing vendors inviting them to review the test methodology and their results prior to publication. Kaspersky, McAfee, Symantec and Trend Micro responded to our invitation, reviewed the test methodology and provided comments on their test results, which were integrated into the Test Report as appropriate.

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.