HOBSON & COMPANY

Understanding the Total Cost of Ownership for Endpoint Security Solutions

A TCO White Paper

Author: Kara Casten
Hobson & Company
March 2009

Executive Summary

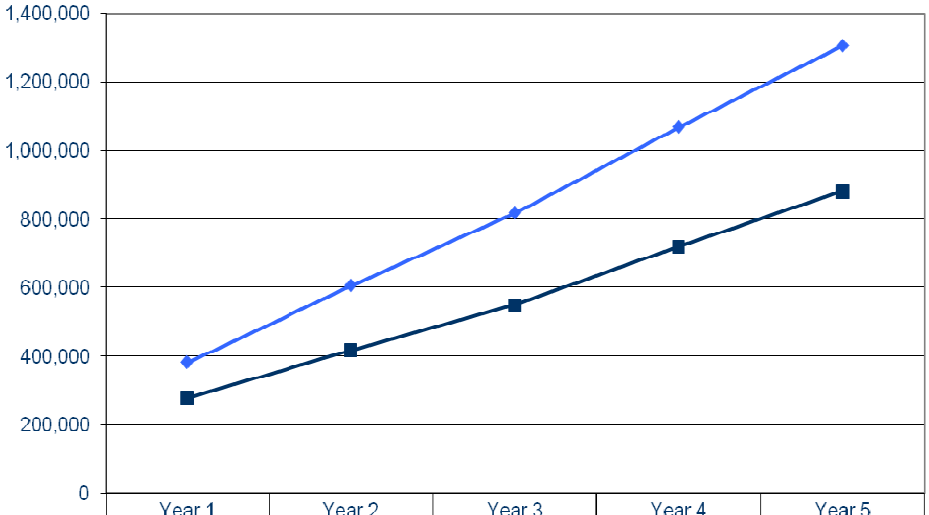
Organizations considering moving to an endpoint security solution often assume that the costs of switching from their current anti-virus vendor will be greater than upgrading with that vendor. To shed some light on this issue, Sophos, a leading endpoint security vendor, commissioned an independent research study to uncover and quantify all of the cost areas involved in migrating (upgrading or replacing) to an endpoint security product and managing the solution to gain a total cost of ownership (TCO) comparison between the leaders in the field.

The nine companies interviewed for this study had previously been running Symantec's or McAfee's anti-virus product before switching to Sophos Endpoint Security and Control. Real data from customers' experiences was collected to compare the true and complete costs of switching to and managing with Sophos versus upgrading and managing with the current vendor.

Companies interviewed in depth, and whose costs were analyzed, included:

- Amica Mutual Life Insurance
- AW Chesterton
- Central Ohio Primary Care Physicians
- CGH Medical Center
- Escambia County School District
- Lincoln Public Schools
- British Services Company
- US Healthcare Provider
- German Company

The results show that the value of switching to and managing endpoint security with Sophos is immediate and significant. The overall TCO costs of switching to Sophos are actually less than upgrading with the existing vendor. Moreover, there are no net new cost areas in switching to Sophos that would not be still be incurred in upgrading with the existing vendor. A sample company with 3,400 users can save $110,000 in Year 1 and a total of $504,000 over five years by switching to Sophos. The chart below shows the present value of the total costs for Symantec and McAfee (collectively referred to as the Installed Endpoint Protection Vendors in this study) and Sophos over five years.



	Year 1	Year 2	Year 3	Year 4	Year 5
Installed Endpoint Protection Vendors	381,083	605,718	817,638	1,069,028	1,306,188
Sophos	277,625	417,339	549,144	719,946	881,079

Key Sources of Cost

The cost savings of switching to the Sophos Endpoint Security and Control solution rather than upgrading with an Installed Endpoint Protection Vendor (specifically Symantec Endpoint Protection and McAfee Total Protection for Enterprise) are clear and compelling. Based on interviews with technical decision-makers and influencers at a number of corporate and public sector organizations in the US and Europe, the cost savings fall into two main categories:

- Upgrade or Replace (Year 1 Costs)
- Manage/ Ongoing Operations (Annual Costs)

These two cost areas can be further broken down into a set of specific costs. These costs will be fully explained and supported in the next section.

COST AREA	SPECIFIC COSTS
Upgrade or Replace	• Licensing • Additional Hardware and Software • Upgrade or Replacement Effort
Manage / Ongoing Operations	• Infrastructure Management • Help Desk Team • Escalation Team • End User Productivity

The following TCO example illustrates the potential cost savings of switching to Sophos Endpoint Security and Control for a sample corporation with 3,400 users and the expected operational statistics post upgrade for one of the Installed Endpoint Protection Vendors:

Cost Element	Sample Company
Time to manage endpoint security	20 hours per week
Help Desk calls related to endpoint security (Tier 1 issues)	75 calls per month
# of endpoint security detections (spyware, adware, viruses, etc.) prior to execution	20 detections per week
Time to remediate Tier 2 issues	3 hours per week
Time to remediate Tier 3 issues	10 hours per week
# of annual service interruptions due to endpoint security issues	1 interruption per year
# of users affected per interruption	10 users
Hours of downtime per interruption	6 hours
Lost productivity due to downtime and bandwidth reduction	15 minutes per user per week

Tier 1 issues have arisen before and the solutions have been documented for the Help Desk Team to follow.
Tier 2 issues are common threats that can be handled by internal technical staff.
Tier 3 issues are new threats that require vendor support to remediate.

In addition, the sample company required an extra physical server for both scenarios (upgrading with the current vendor and switching to Sophos). No other extra hardware (physical or virtual servers) or software (server licenses) was needed for migration.

Cost Source 1: Upgrade or Replace

1. Licensing (software and technical support). Interviewees consistently cited licensing costs as the key reason why they switched to Sophos Endpoint Security and Control rather than upgrading to Symantec Endpoint Protection or McAfee Total Protection for Enterprise. However, licensing typically only represents 20% of the TCO (the labor costs were 3X to 4X more significant). The Sophos license price was lower even for customers who were comparing it against the upgrade price for their current vendor (no new licenses). Customers also mentioned that the pricing was more straightforward with Sophos because it included all six endpoint security components (anti-malware, HIPS, application control, device control, client firewall and basic network access control) in one price whereas the Installed Endpoint Protection Vendors charged separately for several of these security components.

   For the sample corporation with 3,400 users, a three-year deal with Sophos cost $117,300, 10% less than the cost of upgrading with the current vendor.

   Impact for sample company:
   $12,648 Year 1 cost savings

   > *"McAfee proved to be more expensive from the point of view that it charged for every module. When we reviewed Sophos it was all part of one purchase and the price was less than for McAfee."*
   > – Technical Services Manager, British Services Company

   Standard technical support is included in the license price and there is an additional charge for a higher level of support for both Sophos and the Installed Endpoint Protection Vendors. The companies included in this study did not evaluate the higher levels of support so this cost was not a factor in the TCO.

2. Additional Hardware and Software. For the companies interviewed the cost of additional hardware and software to migrate to an endpoint security product was not significant. These costs include: console, messaging and updating servers as well as server licenses. The cost of additional hardware and software can be significant for organizations that need to manage platforms other than Windows (educational institutions) or multiple platforms as well as large numbers of remote users.

   With Sophos a single, automated management console centrally deploys and manages endpoint security for Windows, Mac and Linux whereas the Installed Endpoint Protection vendors either require multiple consoles or do not support these platforms. The companies interviewed for this study did not meet these criteria so the additional hardware and software costs were not significant whether upgrading with the current vendor or switching to Sophos. To calculate these costs in the model the following industry averages were used: $8,000 for a physical server, $2,000 for a virtual server and $1,000 for a server license.

> *"Sophos was the only solution that didn't care if clients are Macs or PCs – it was the only cross platform solution at the time."*
>
> - Director of Technology, Lincoln Public Schools

The additional hardware and software cost was the same for the two options (upgrading or replacing) for the sample company. In both cases one additional virtual server was required at a cost of $8,000.

Impact for sample company:
Year 1 cost is the same for the two options

3. Upgrade or Replacement Effort (internal and external professional services). Migrating to an endpoint security solution involves planning, building the infrastructure, deploying the new product and post-deployment cleanup of any remaining detections. Some companies rely solely on their Infrastructure Manager to do this work while others purchase professional services contracts with the vendor to alleviate the workload on the Infrastructure Manager. Interviewees described upgrading to an endpoint security product with Symantec as a daunting task. This was primarily due to the difficulty in removing all of the old versions of the product, which is required before installing an endpoint security solution.

   Customers found replacement easier than upgrading because of the effectiveness of Sophos' client removal tool and the ability to deploy the solution automatically from a single console. Companies interviewed estimated that it would take 1 hour to upgrade 10 endpoints with Symantec and McAfee. For medium to large enterprises with 2,000 to 20,000 users that adds 200 to 2,000 hours to the Infrastructure Manager's workload. On the Sophos side, the replacement process takes 35 hours regardless of the number of users.

   The Infrastructure Manager at the sample company spent 35 hours to migrate the company's 3,400 users to Sophos. This same effort would have required 340 hours with Symantec or McAfee. With an annual salary of $80,000 this totaled $1,400 for Sophos, 90% less than the cost would have been to upgrade with the existing vendor.

   > *"Sophos has saved me a lot of time with their administration tools. The deployment is easier and I've been impressed with the client removal tool, it removes Symantec well."*
   >
   > – IT Manager, CGH Medical Center

   This cost savings enabled the sample company to purchase onsite professional services from Sophos to assist the Infrastructure Manager in this effort and still resulted in a lower cost than if the company upgraded with its current vendor (with no professional services included).

   Impact on sample company:
   $1,600 Year 1 cost savings

Cost Source 2: Manage/ Ongoing Operations

1. Infrastructure Management. The key tasks that fall under managing endpoint security are: adding new users, managing policies, managing updates, managing upgrades, troubleshooting, reporting, managing multiple platforms and managing remote users. Companies interviewed for this study universally agreed that

it is easier to do these tasks from the Sophos management console than from Symantec or McAfee's console. The single Sophos console centralizes and automates the key tasks involved in managing endpoint security and the dashboard provides instant visibility of the protection status for all Windows, Mac and Linux users so that it's easy to identify machines that require attention. If the Infrastructure Manager needs vendor support, Sophos offers unlimited access to in-house support experts 24x7x365.

"The Sophos console provides a snapshot of what's going on at a glance. Symantec is definitely not easy to use. We need to see at a glance if there's something wrong."
– Technical & Operations Security Administrator, US Healthcare Provider

The Infrastructure Manager at the sample company spent 5 hours per week managing endpoint security with Sophos. In comparison this would require 20 hours per week with either Symantec or McAfee. With an annual salary of $80,000 this totaled $10,000 per year for Sophos, resulting in a 75% cost savings.

Impact for sample company:
$30,000 annual cost savings

2. Help Desk Team. The Help Desk Team is responsible for fielding user calls, collecting user data and remediating issues. They deal with Tier 1 issues that have arisen before and the solutions have been documented for the Help Desk Team to follow. Interviewees have experienced a much smaller volume of Help Desk calls related to endpoint security issues with Sophos compared to Symantec and McAfee. With Sophos the Infrastructure Manager has greater central control and visibility into the protection status of all users therefore potential security flaws, like out-of-date antivirus protection or a disabled firewall, are addressed before they impact the user.

The sample company's Help Desk Team was used to getting 75 endpoint security calls per month with one of the Installed Endpoint Protection Vendors. With Sophos that number has decreased to 25 calls per month. The average Tier 1 call takes 45 minutes to resolve and at $25 per hour the Sophos cost was $6,683, which was 66% less than the cost for the former vendor.

"The high volume of calls to our IT Department with McAfee was one of the key reasons why we switched to Sophos."
- Head of Global System & Security Solutions, German Company

Impact for sample company:
$13,567 annual cost savings

3. Escalation Team. The companies included in this study admitted they had a false sense of security with the Installed Endpoint Protection Vendors. The first evidence of this was when Sophos detected issues during the replacement process that the former vendor missed. A key reason for switching to Sophos was better protection and companies have experienced a 50% increase in the number of detections prior to execution with Sophos. Sophos detects viruses, spyware and adware, suspicious behavior and files, removable storage devices and unauthorized applications. Sophos definition file updates are small and are released as frequently as every five minutes for fast protection with low impact on network resources. Additionally, Sophos' HIPS prevention provides detection that automatically guards against new and

emerging threats. In a 2007 study conducted by Cascadia Labs, Sophos detected 86% of newer threats compared to 43% for McAfee and 51% for Symantec. The Escalation Team deals with Tier 2 and Tier 3 issues. Tier 2 issues are ones that internal technical experts can remediate on their own while Tier 3 issues require vendor support to resolve. The breakdown of Tier 2 and Tier 3 issues is typically 75% and 25% respectively, according the to interviewees.

Not only does Sophos detect more issues before they execute but it also requires less effort to handle them. The visibility provided by the Sophos management console enables the Escalation Team to easily find machines that need attention and in many cases issues can be resolved remotely from the console. For Tier 3 issues, such as new threats that require a new definition file, Sophos' in-house technical experts are available 24x7x365 and the interviewees have seen a 50% improvement in response time with new definition files with Sophos compared to Symantec and McAfee.

"With Sophos we're being proactive rather than reactive. We're trying to avoid infections so we don't have to spend time cleaning them up."
- Network Administrator Manager, AW Chesterton

"The time I spent resolving spyware and adware issues with Symantec will be cut in half or more with Sophos."
– IT Manager, CGH Medical Center

The number of endpoint security detections pre execution increased 50% to 30 per week when the sample company switched to Sophos. Conversely, the time to resolve these detections decreased by 50% to 1.5 hours (Tier 2) and 5 hours (Tier 3) with Sophos. With an annual salary of $60,000 the total Escalation Team cost was $129,675 with Sophos, 24% less than the cost for the Installed Endpoint Protection Vendor.

Impact for sample company:
$39,725 annual cost savings

For companies that are not large enough to have an Escalation Team this work is handled by the Infrastructure Manager.

4. End User Productivity. While end user productivity has not historically been measured, the companies interviewed have seen an improvement with Sophos in two areas: i) downtime due to infections and version upgrades, and ii) the bandwidth reduction due to definition file updates and the memory required to run the endpoint security solution. With the Installed Endpoint Protection Vendors companies typically experience one service interruption per year, which affects 10 users for about 6 hours on average. Companies did not have a single downtime event with Sophos due to its ability to catch more threats, especially new and emerging threats with its HIPS technology.

   Sophos definition file updates are small (2K-70K) and frequent (every 5 minutes) so they provide more protection with less impact on the end user. McAfee and Symantec updates are sent out once a day so they are larger and expose the network to more potential threats. In addition to the impact of the updates, the memory footprint when the program is running is smaller with Sophos than McAfee or Symantec. As companies begin to track this metric the magnitude of the cost savings will likely grow.

"Right out of the gate Sophos was finding more vulnerabilities. There is the potential for less downtime at the individual desk. Sophos is finding more things up front so there is less potential for issues at the endpoint."
– Network Operations Section Manager, Amica Mutual Life Insurance

"Sophos' memory footprint and program footprint are much smaller than Symantec's."
- Network Administrator, Central Ohio Primary Care Physicians

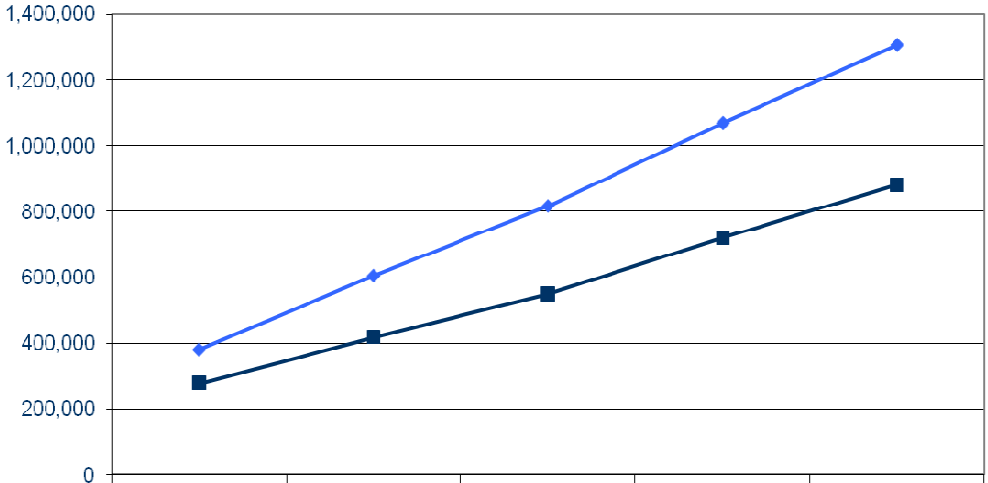
With 3,400 users and an average salary of $50,000 the sample company saved $1,500 a year since it did not experience any service interruptions with Sophos (compared to one annual interruption that affected 10 users for 6 hours with the former vendor).

The company's 3,400 users also regained 5 minutes per week in lost productivity with Sophos. The cost was $10,625 with Sophos and 50% less than the cost with the Installed Endpoint Protection Vendor.

Impact for sample company:
$12,125 annual cost saving

Overall Costs

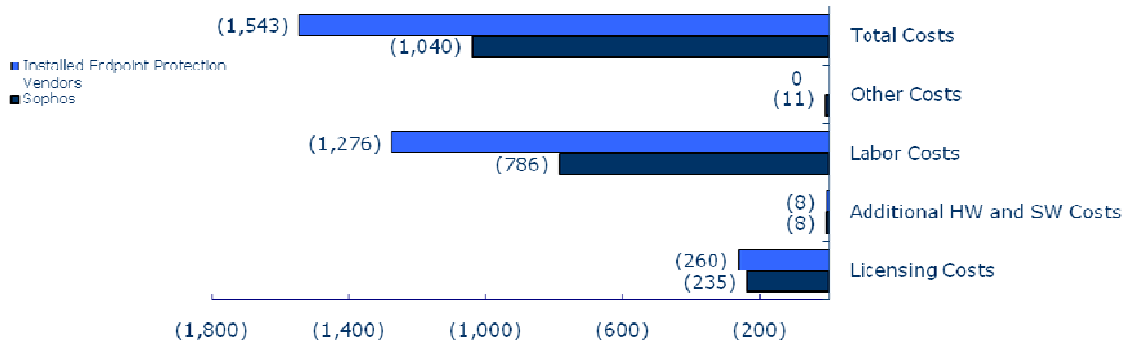
For the sample company, the present value of the total costs of upgrading to the endpoint security product for the Installed Endpoint Protection Vendors and managing the solution over five years was $1.3 million. In comparison, the total cost of switching to and managing Sophos Endpoint Security and Control over five years was $880,000. The costs were calculated based on licensing, infrastructure and operational data provided by the companies interviewed. In total there is a $504,000 cost savings in switching to and managing Sophos Endpoint Security and Control.



	Year 1	Year 2	Year 3	Year 4	Year 5
Installed Endpoint Protection Vendors	381,083	605,718	817,638	1,069,028	1,306,188
Sophos	277,625	417,339	549,144	719,946	881,079

The chart below shows the extent to which each of the cost categories contributes to the total costs for Sophos and the Installed Endpoint Protection Vendors over five years. The labor and licensing costs were the major costs and the Sophos costs are 2/3 of the costs for Symantec and McAfee. The labor costs represent the lion's share of the TCO at 3x to 5x the licensing fee for Sophos and the Installed Endpoint Protection Vendors respectively.

Installed Endpoint Protection Vendors and Sophos Cost Comparison Years 1-5
(Figures in Thousands)



About Sophos

Sophos is a world leader in IT security and control. The Company offers complete protection and control to business, education and government organizations – defending against known and unknown malware, spyware, intrusions, unwanted applications, spam, and policy abuse, and providing comprehensive network access control (NAC). Sophos' reliably engineered, easy-to-operate products protect over 100 million users in over 150 countries. The Company's vision, commitment to research and development, and rigorous attention to quality have enabled it to maintain strong year-on-year growth and the highest levels of customer satisfaction in the industry.

For more information, please visit www.sophos.com

About Hobson & Company

Hobson & Company helps technology vendors and purchasers uncover, quantify and validate the key sources of value driving the adoption of new and emerging technologies. Our focus on robust validation has helped many technology purchasers more objectively evaluate the underlying business case of a new technology, while better understanding which vendors best deliver against the key value drivers. Our well researched, yet easy-to-use ROI and TCO tools have also helped many technology companies better position and justify their unique value proposition.

For more information, please visit www.hobsonco.com