

Business Trends

**A Strategic Overview
Featuring Gartner Content**



Featuring:

A Buyer's Guide to Endpoint Protection Platforms

In This Issue:

Examine the formula that fuels success in the competitive security and data protection market. 2

Explore life without comprehensive data protection. 3

Understand the total cost of ownership for endpoint security solutions: A TCO white paper 4

From the Gartner Files
A Buyer's Guide to Endpoint Protection Platforms . . . 10

The evolution of endpoint security

Welcome to this complimentary copy of Gartner's *Buyers Guide to Endpoint Protection Platforms*. This newsletter explores how the traditional methods for endpoint security should evolve. You'll learn how Sophos's recent integration of Utimaco affects the highly competitive security and data protection market. You'll find out how the lack of data protection can affect your bottom line, and lastly, gain insight into the true costs involved in migrating and managing an endpoint security product.

SOPHOS

Traditional markets for dedicated endpoint security products — particularly anti-virus tools and personal firewalls — have been, according to the report, eclipsed by endpoint protection platforms. Sophos now offers a unique solution, Sophos Endpoint Security and Data Protection, which provides simplified cross-platform security, centralized management, full-disk encryption and control of devices, applications and network access.

We invite you to learn more about simply securing your business at every level, and how to reduce the risks associated with non-compliant, unmanaged and unauthorized computers.

Visit www.sophos.com for more information.

Featuring research from
Gartner

Examine the formula that fuels success in the competitive security and data protection market

Sophos CEO in the spotlight with SearchSecurity.com

Sophos CEO Steve Munford recently sat down with SearchSecurity.com's Senior Technology Editor, Neil Roiter to discuss the formula behind Sophos's success in the competitive security and data protection market, and what the future holds for the company.

In this interview, Munford explained how Sophos is aggressively taking market share away from Symantec and McAfee, and examined how — even in the economic downturn — Sophos continues to experience year-over-year growth and its channel partners are achieving double-digit growth.

With the increase external and internal threats, limited IT staff, tighter budgets, and mounting industry and government compliance and regulatory mandates, it's clear that businesses today are facing more security challenges than ever before.

However with the latest encryption offerings post Utimaco acquisition, Sophos customers can further achieve regulatory and compliance mandates while getting more value for their budget.

Listen to the Newsmaker
podcast with Sophos
CEO Steve Munford.

Sophos offers proven proactive Genotype protection backed by SophosLabs™ expertise and our HIPs technology. Here's a snapshot of what they have discovered in the past six months:

- 23,500 new infected webpages are discovered every day. That's one every 3.6 seconds, four times worse than the same period in 2007.
- 40,000 new suspicious files are every day.
- 15 new bogus anti-virus vendor websites are discovered every day. This number has tripled, up from an average of five detected per day, during 2008.
- 89.7% of all business email is spam.
- Approximately 6,500 new spam-related websites are discovered every day — accounting for one new website every 13 seconds, 24 hours a day. This figure is almost double the same period in 2008.

Source: Sophos mid-year threat report

Explore life without comprehensive data protection

Sophos Endpoint Security and Data Protection defends against data loss through full disk encryption and information security encryption for removable storage devices and portable media. Learn why this is important, how data loss can affect your bottom line — and more importantly — what businesses can do to stop it:

Data leakage remains a top concern in 2009, with scandals continuing to dominate the headlines. Many corporations and government institutions have failed to protect their confidential information — including the identities of their workforce, customers and general public.

It is not only the threat of negative publicity that is driving interest in data protection, but also concern that the organization is failing to comply with regulatory security standards.

A variety of techniques are being used by corporations around the world to prevent data loss in a mobile connected world. These include anti-virus software, encryption and firewalls, access control, written policies and improved employee training.

Nevertheless, users are routinely using and sharing data without giving enough thought to confidentiality and regulatory requirements. This has led to numerous incidents of data loss in the first six months of 2009 — some accidental, some malicious:

- **May** Hackers broke into a Virginia government website, stealing the details of almost 8.3 million patients, and threatening to auction them to the highest bidder.
- **May** The theft of a single laptop in the UK put the personal identities of

109,000 pension holders at risk. The laptop contained names, addresses, dates of birth, National Insurance numbers, employer names, salary details and bank account information.

- **June** 530,000 Virginia patients were individually notified that their Social Security Numbers had potentially been exposed after a hacker gained access to the Virginia Prescription Monitoring Program 14.
- **June** Authorities arrested a former Goldman Sachs employee who uploaded the company's secret source code to an FTP server based in Germany.

Encryption

The most important step in stopping data leakage is to encrypt sensitive information, laptops and removable storage devices. If data is encrypted with a password, it cannot be deciphered or used unless the password is known. This means that even if all other security measures fail to prevent a hacker from accessing your most sensitive data, he or she will not be able to read it and so compromise the confidentiality of your information.

The second step is controlling how users treat information. You want to stop any risky behavior, such as transferring unencrypted information onto USB sticks and via email. Organizations should extend their anti-malware infrastructure in order to:

- Protect data in motion and data in use
- Guarantee efficient operations
- Ensure that they meet regulatory requirements

Source: Sophos mid-year threat report

Hear from those that have gotten more with Sophos

"Selecting Sophos Endpoint Security & Control just made sense as we were able to meet all of our needs and top security solution. Prior to Sophos, we were using a separate anti-adware solution along with a security solution to stop viruses and spyware. This approach worked, but by consolidating into one solution, we improved the efficiency of the workstation and manageability for the administrators, therefore lowering our TCO."

– Pramesh Naik, enterprise support manager at Kilpatrick Stockton

"From the Sophos console, you manage every aspect of security as well as endpoint control. Any malware detected shows an alert so you know which computer needs attention and what to do. In many cases, you can do it from within the console, and if not, you know immediately which machine to go to. During normal operation, the Anti-virus and Anti-spyware is updated hourly — that's right, hourly. In the event of an outbreak somewhere in the world, it will update even more often."

– Dave Coe, Independent Security Specialist, Longmont Toyota

"The Sophos endpoint solution simplified management for Ferrellgas, enabling threats to be monitored at the desktop level. Technicians can automatically deploy and manage the assessment, control and protection from one console. This has enabled us to be proactive in confronting issues, which in turn has increased end-user confidence in our abilities."

– Greenwood Leflore Hospital

"Sophos has an intimate understanding of the complexity of the university environment and the need to manage multiple threats through an integrated solution, while allowing a high degree of user control."

– University of British Columbia

Understand the total cost of ownership for endpoint security solutions

A TCO white paper

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

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 one 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.

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.

TCO Example

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.

Cost Example

COST AREA	SPECIFIC COSTS
Upgrade or replace	<ul style="list-style-type: none"> • Licensing • Additional Hardware and Software • Upgrade or replacement effort
Manage / Ongoing operations	<ul style="list-style-type: none"> • Infrastructure management • Help desk team • Escalation team • End user productivity

These costs will be fully explained and supported in the next section.

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:

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

“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

(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

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

“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*

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.

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 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*

Sophos, 90% less than the cost would have been to upgrade with the existing vendor.

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 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

“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*

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 anti-virus 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.

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's 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

“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*

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 to the 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 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

“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

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.

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

“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’s memory footprint and program footprint are much smaller than Symantec’s.”

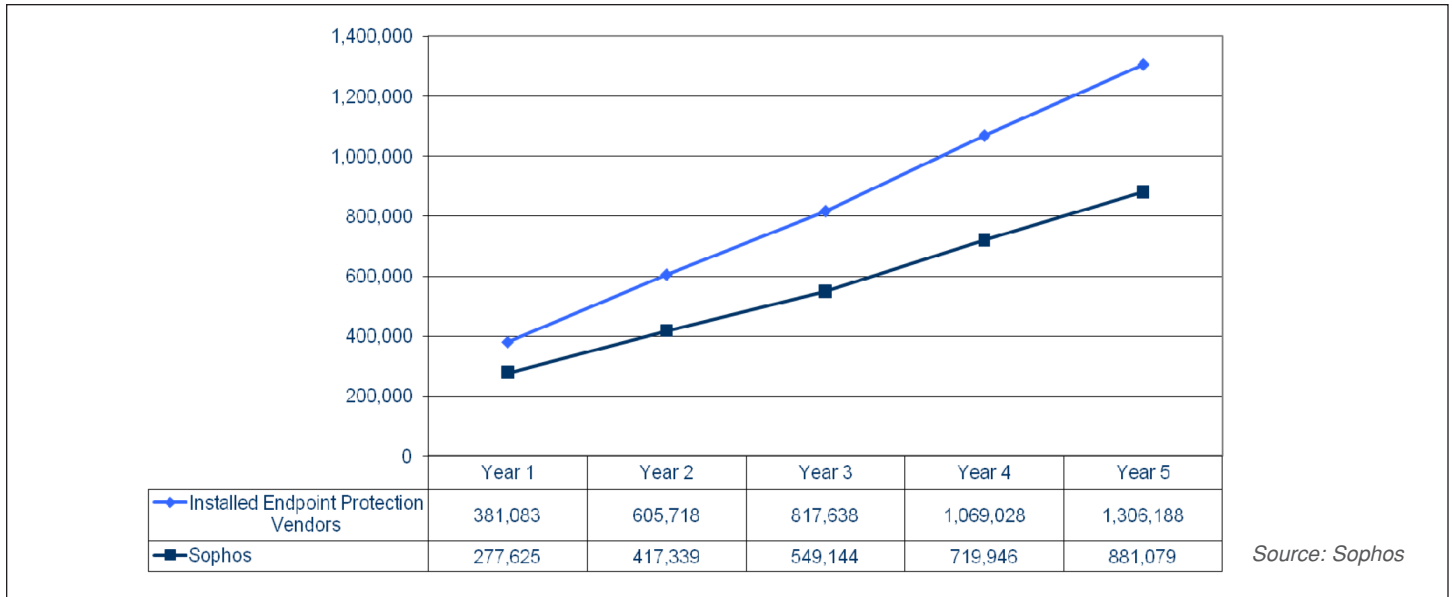
– Network Administrator,
Central Ohio Primary Care
Physicians

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

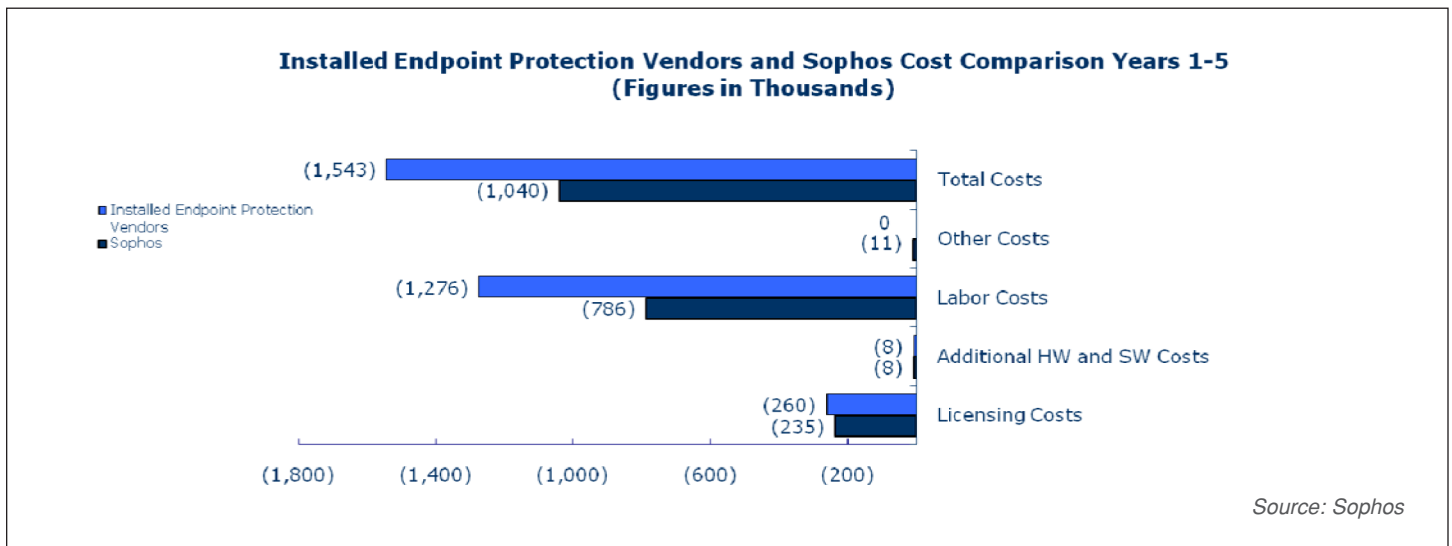
provided by the companies interviewed. In total there is a \$504,000 cost savings in switching to and managing Sophos Endpoint Security and Control.



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.



From the Gartner Files

A Buyer's Guide to Endpoint Protection Platforms

The traditional “point” markets for antivirus (AV) tools and personal firewalls have been eclipsed by broader suites of related security technologies, which Gartner has identified as endpoint protection platforms (EPPs). The choice of an EPP will depend heavily on enterprise-specific requirements, so chief information security officers (CISOs) and other security professionals evaluating EPP offerings should use Gartner’s guidance to identify their most-likely current and future needs, and select the EPP that will most-effectively address them.

Key Findings

- The market for EPP suites is marked by a broad range of solutions, with significant differentiation among vendors and their offerings.
- No single vendor leads in all functional areas, so buyers need to prioritize their requirements to address the needs of their specific business, technical and regulatory environments.

Recommendations

- Make plans to phase out point products for AV and anti-spyware tools, host-based intrusion prevention systems (HIPSs) and personal firewalls, and replace them with an EPP suite as support contracts expire.
- Demand that your current AV technology vendor identify the HIPS techniques included in its base AV client and detail its road map. Deploy full-blown HIPS capabilities for systems with high security requirements, but prepare for some increases in administration requirements.

- If you haven’t already instituted a full-disk encryption program for mobile clients, then do so immediately for notebook computers carrying sensitive data. Consider encryption from your incumbent end-node protection vendor, because common management, established client-side presence and suite pricing may make this option attractive.
- Consider the need for data loss prevention (DLP) capabilities in endpoint protection. The ability to simplify client-side agents with a common management framework is an advantage, but this consideration will often be outweighed by broader enterprise DLP requirements.
- Resist vendor “packaging” that includes gateway protection with endpoint protection. Focus on the client and server as one domain, and gateways as a separate domain. Resource-constrained small and midsize businesses (SMBs) may want to consider the advantages of centralized management of both domains, but they must also place higher priority on the unique requirements of each domain.

ANALYSIS

The traditional markets for dedicated endpoint security products — particularly AV tools and personal firewalls — have been eclipsed by broader suites of related security technologies, which Gartner has designated as “endpoint protection platforms.” An EPP suite typically includes AV and anti-spyware tools, a personal firewall, and may also offer network access control (NAC) capabilities and data

protection technologies, such as DLP and full-disk encryption. The demand for holistic NAC solutions and the management requirements of large enterprises are also forcing EPP suite vendors to replicate some PC operations infrastructure, such as security configuration management, patching and software management. By combining multiple technologies into a single management framework, EPPs offer the promise of increased security while simultaneously lowering complexity, cost and administrative overhead.

1.0 Basic EPP Component Features and Functionality

The basic components of an EPP are an anti-malware signature database (containing information on malicious code, such as viruses, trojans and spyware), an HIPS and a personal firewall, linked by a common management and reporting console. An EPP may also include full-disk encryption and DLP tools. Increasingly, EPP management capabilities will emulate and integrate with operational tools to provide security configuration management, vulnerability assessment, application control and remediation tools for resilient infections. As data security and reimaging remediation become more pervasive, EPP suites will begin offering managed backup services and tools.

2.0 Advanced EPP Component Features and Functionality

CISOs and other enterprise security decision makers should consider advanced component features, which are becoming available, when designing RFPs or

scorecards to differentiate products under evaluation. No EPP will have all these features, and buyers must focus on the specific features they consider most important for their enterprises. The following list isn't intended to be comprehensive, but rather representative of advanced functions that may compose part of a more-appropriate EPP solution.

2.1 Manageability and Scalability Capabilities

Reduced administration is one of the most-critical concerns of EPP administrators, and improved manageability and greater scalability will help reduce it and the associated overhead. A well-designed, task-oriented graphical user interface (GUI) and a comprehensive management interface will deliver lower total cost of ownership (TCO). Gartner recommends that when security professionals evaluate EPPs, they should develop a list of the top 10 to 20 most-common or most-critical endpoint security tasks (see Note 1), and use this list as a guideline for comparison testing and demonstration of solutions. The necessary management capabilities will depend heavily on enterprise-specific needs and available technical skills. The following representative list details advanced EPP management capabilities as well as the factors influencing them.

2.1.1 Management GUI

- A task-oriented (not feature-based) management GUI can simplify management by hiding unnecessary complexity from less-sophisticated users, but enable more-technically skilled users to drill down to granular details (see Note 2).
- Management pages should ideally have a consistent look and feel, as well as the ability to switch over from dash-

boards to configurations of different elements. This is especially important because suite vendors often grow by acquisition, and, as a result, the degree of management and reporting integration into a common, centralized management console may vary.

- Granular role-based administration should ideally include predefined roles as well as the ability to customize and add/remove options.
- The EPP should offer the capability to create different management GUI work space views (for example, administra-

tor or help desk view), preferably with users' ability to adjust their default views.

- A customizable "toolbox" element that allows the consolidation of common tasks into a single user-defined menu is useful.
- "Globalization" capabilities — including global support, centralized management and reporting, and necessary language support for the management interface and the end-user interface — are important for enterprises with operations across multiple regions.

Note 1

Examples of Common Tasks

- Review the home page dashboard and pay particular attention to the placement of indicators that illustrate negative changes in the security posture of endpoints. Look for direct links to more information, recommendations and action steps to resolve events.
 - Tour the report center, create a custom report, and schedule it for delivery to an e-mailbox or Web server/portal.
 - Show alert configuration capability and integrate an alert with an external subscriber identity module.
 - Show real-time data that lists clients on a network that doesn't have an EPP agent installed.
 - Create or edit the policy elements that can be delegated (or restricted) to end users.
 - Create or edit the policy for client update distribution.
 - Create or edit the policy to automatically push the EPP client to an endpoint that doesn't have it installed.
 - Configure scheduled scans for endpoints. Focus on the ability to limit CPU use, and delegate the ability for end users to delay scan execution.
 - Create or edit the port (that is, USB, CD or infrared) control configuration, and pay particular attention to the granularity of the restrictions, the linkage to file types, and encryption, if any.
 - Create or edit a VPN policy (that is, deny split tunneling) for a specific Active Directory group.
 - Create or edit a location-based policy, and pay attention to the level of automation in selecting when a policy should be invoked.
 - Create or edit a Wi-Fi-specific policy.
 - Create or edit a whitelisting and/or lockdown configuration for a certain group of PCs. Add a new executable program to the whitelist. Autogenerate a whitelist from the installed applications on a PC. Authorize a software distribution method and directory as a whitelisted source of applications.
 - Show a single-page summary of client configuration information and print it for review.
 - Review the HIPS policy configuration and step through the false-positive handling process, including deactivating a specific HIPS rule for a specific application.
 - Edit role-based administration and hierarchical administration to add a new role.
-

Note 2

Task-Based System

A task-based system can be evaluated by creating a list of common tasks and comparing the number of steps required to complete each task.

- EPP vendors are gradually adding PC life cycle tools (such as asset discovery, configuration management, vulnerability assessment and software management) as a way to inoculate PCs against unknown threats that target known vulnerabilities. Buyers should evaluate their needs with regard to the integration of these tools and consider the strategic direction of prospective EPP vendors.

2.1.2 Scalability

- Centralized management with automatic configuration and policy synchronization among management servers may be particularly useful in large deployments.
- Native management-server redundancy — for example, using load balancing active/active clustering within and across LANs, or automatic active/standby failover without a single point of failure, such as a designated master/slave — can be a useful differentiator.
- EPPs should include multiple directory integration options — including Active Directory and Lightweight Directory Access Protocol (LDAP) — as well as the ability to integrate with multiple directories and traverse directories to find user groups and authentication information.
- A software-as-a-service- (SaaS-) based managed console that eliminates the need for a dedicated server to manage

endpoints may be useful, particularly for SMBs.

- The ratio of management servers to clients is an important consideration for large enterprises, and one that will impact the TCO. For smaller businesses, the management server should work on a shared server.

2.1.3 Reporting and Dashboards

- Buyers should look for a real-time home page dashboard that enables rapid troubleshooting of security events or server issues — ideally with actionable dashboard elements that make it possible to click on an event or graph and initiate steps that enable better understanding of the issues involved and the steps required for alert resolution.
- Threshold alerting capabilities may use delivery mechanisms such as e-mail, Short Message Service (SMS) and Simple Network Management Protocol (SNMP), with threshold alerts for dashboard statistics and policy thresholds.
- The appropriate range of client information that can be collected and reported to the management server is growing in importance as a differentiator. Most EPP suites collect information only about the status of the EPP suite. However, as endpoint hygiene becomes more critical, information about the status of patch levels, configurations, software inventories and vulnerabilities is becoming more important.
- The management server should be capable of collecting client status information in real time, rather than in scheduled delta updates. The ability to collect information from mobile endpoints that aren't connected to the network hosting the management server can be a significant competitive differentiator.

- The management system should be able to automatically detect new or rogue endpoints that don't have an EPP client installed. This is a function that may be integrated into the enterprise's NAC system, but shouldn't be dependent on NAC, and should be able to detect clients that have already joined the domain.

2.1.4 Policy Management

- A “wizard type” installation mechanism with optimal default settings for different-size environments can reduce deployment complexity.
- A single-page policy with intelligent drop-down “pick lists” and fields that change based on previous optional selections (without multiple pop-up windows or the need to visit several tabs to create a single policy) make policy development easier and more intuitive.
- There should be an option to view or print a human-readable policy summary that greatly simplifies auditing and troubleshooting.
- A complete audit log of policy changes is essential, especially for organizations that take advantage of extensive role-based administration and delegated end-user administration to ensure audit compliance.
- The ability to stage signatures or policies and to quickly roll back changes is increasingly important because fewer enterprises are testing signatures before deploying them.
- The EPP suite policy must allow off-LAN clients to automatically update from the EPP vendor's primary database for signature and HIPS updates, when the enterprise server is unreachable or otherwise unavailable.

- A configuration backup utility and configuration preservation between version upgrades can save administration time and resources.

2.1.5 Client Agents

- The number of required clients and the client disk and memory footprint are good indicators of the level of integration among EPP components and the efficiency of the client. Ideal solutions will provide a single consolidated agent with component parts that can be remotely enabled and disabled.
- The ability to natively distribute the full client agent and remove competing products is a useful differentiator. Some solutions simply provide a multisourcing service integrator (MSI) file (Windows Installer package) for use by other software distribution tools, while other solutions won't remove other AV products, which can create conflicts.
- The client interface should be adaptable to allow for a full range of delegated end-user control. Advanced solutions enable administrators to delegate or restrict any client option.
- Scheduled scans are one of the most-problematic aspects of signature-based anti-malware tools. Options that limit the client impact of scheduled scans are a significant EPP differentiator. Advanced features include the ability to delay scans based on battery life, running process or CPU usage. More rare is the ability to "wake and scan" PCs during off-hours. Scheduled memory scans should be independent of disk scans.
- Specific features and licensing for virtualized environments, such as VMware, Citrix and Hyper-V, remain rare, but are increasing in importance. EPP buyers

should seek clarity on what's actually supported and what back-end processes have been changed. It's important to ensure that the vendor's support personnel are properly trained, that its labs are appropriately configured and that its software products are certified for virtualization. Most host-based software provides no protection for the hypervisor layer.

2.2 Malware Detection Capabilities

The quality of the malware scan engine — the "anchor" solution of an EPP suite — should be a major consideration in any RFP. The following are some of the advanced malware-oriented features of EPPs that buyers should be looking for:

- Most enterprises' IT security organizations' capability to accurately test malware engines in real-world situations is limited, at best. Test results from organizations such as AV-Comparatives.org and AV-Test.org are useful guides of scanning accuracy (including false positives) and scanning speeds. In the absence of other information, good test scores are better than poor test scores, but buyers should be aware that these tests don't accurately reflect how users encounter malware in the real world. Moreover, they don't test all proactive techniques for blocking malware, such as HIPS, vulnerability detection and configuration management. Buyers should be very wary of vendor-sponsored tests and not put too much weight on specific test results.
- Signatures should be as broad as possible so they can detect new variants of old threats without new signatures, and, thus, avoid causing false positives.

Retrospective testing (that is, testing old signature databases against new variants of old malware) is the best way to evaluate this capability.

- Ideally, EPP solutions should provide much-faster identification and rapid distribution of signatures for new threats. However, this is a difficult benchmark to test. Some solutions will have slower signature distribution for a new threat, because their generic signatures or HIPS rules are already effective in blocking that threat.
- Signature databases should include all types of malware (including spyware, adware, viruses, trojans, keystroke loggers, droppers, back doors and hacking tools) in a single database, with a single update mechanism and a single scan engine agent.
- The capability to detect rootkits and other forms of low-level malware, once they're resident in enterprise systems, is a significant consideration. Some solutions' functionality is limited to catching rootkits as they install, while others have the ability to inspect raw PC resources and compare them to Windows file tables, seeking discrepancies that will indicate the presence of rootkits.
- Malware engines should continuously monitor system resources (for example, host file, registry, Internet Explorer settings and dynamic-link-library changes) for changes that might indicate the presence of suspicious code:
 - Malware removal features and outbreak filters to stop propagation are important differentiators among vendors and their offerings. These capabilities should be understood and tested, because modern mal-

ware is significantly more complex than that of previous generations, and often involves multiple components with sophisticated “keep alive” routines.

- EPP solutions should include client-based URL filtering to block clients from visiting Web sites that are known security risks, because malware is increasingly shifting to Web distribution methods.

2.3 Advanced HIPS Capabilities

AV/anti-spyware databases are 90% to 99% effective at detecting well-known, widely circulated threats, but only 20% to 50% are effective at detecting new or low-volume threats. Security effectiveness is significantly enhanced by HIPS, but there’s no generally accepted method of testing the HIPS effectiveness of different solutions.

EPP buyers should take the time to understand how many and which of the nine HIPS protection styles are included in the base malware signature engine that’s used to detect and block unknown threats (zero-day or targeted threats), and which are additional HIPS capabilities that can often increase the administration burden due to management of false positives. For these reasons, Gartner recommends focusing on ease-of-management functions, which make HIPS adaptable enough for the enterprise network:

- The HIPS solution must, as a core principle, enable the administrator to choose and tune the styles of protection that are needed, based on the requirements and resources of the endpoint,

and to configure protection to reflect the enterprise’s overall tolerance for risk and administrative overhead.

- Despite the need for fine-tuning capabilities, the best solutions will provide preconfigured “out of the box” templates for common application and system configurations, as well as a learning mode for enterprise environments and the ability to test policy in a log-only mode.
- HIPS techniques have no standard terminology; therefore, it’s essential that buyers ask vendors to list and describe the HIPS techniques in detail, so that buyers can create a standardized list of techniques and compare their breadth and depth across vendors. Buyers should also understand which techniques are included in the base client, which are optional, and what other charges, if any, are required for additional protection styles.
- Some vendors offer only binary control over HIPS, which allows administrators to turn them on or off. Enterprise IT organizations are unlikely to concern themselves with every setting in detail, but it’s important to have granular control that makes it possible to turn off certain rules for specific applications to accommodate false positives.
- One very effective HIPS technique is “vulnerability shielding” — the ability to inspect and drop attacks based on knowledge of the specific vulnerabilities they exploit. This technique allows protection against attacks and against known vulnerabilities before the vendor releases a patch, and makes it possible

to “buy time” to propagate patches to all endpoints.

- The simulation of unknown code before the code is executed to determine malicious intent, without requiring end-user interaction with the unknown code (for example, using static analysis, simulation or reverse compilation techniques) is another deterministic technique, but it can be highly resource-intensive and should be used selectively.
- Buffer overflow memory protection is common, and should address heap-and-stack memory.
- Application control capabilities (for example, application whitelisting, also known as lockdown) are gaining significant interest as the volume of malware begins to surpass the volume of “good” corporate applications. There is significant R&D in this area, and this capability will be an important differentiator in the future. Application control features that EPP buyers should investigate include:
 - How applications are identified and prevented from executing (for example, do they block the installation of applications or only the execution?) is an important differentiator.
 - The mechanisms available for creating a whitelist will be critical to lower the administration overhead. Administrators should, for example, be able to automatically authorize applications that are properly signed, or come from trusted locations, processes or installers.
 - Solutions should ideally provide signatures of known-good applica-

tions as a service, similar to current malware databases.

- Application control should extend to the execution of browser helper objects/controls within the context of Internet Explorer and other browsers.

2.4 Personal Firewall Capabilities

Basic personal firewall functionality (inbound port defenses) are available in the Windows XP Professional, Windows 2003 and Windows Vista operating systems. The Vista firewall has bidirectional capabilities, although outbound is turned off by default and activation requires significant setup. The Windows firewall is adequate for most desktop PCs that also have the benefits of network firewalls and network-based intrusion prevention. However, notebook computers and PCs with higher security requirements require more-comprehensive, two-way protection that adapts to multiple network contexts. Personal firewalls are differentiated by the flexibility of their policies (for example, an autosensing location-based policy), the breadth of their application profile policies (for example, the ability to prevent applications from exhibiting unusual network behaviors), the virtual private network (VPN) integration and the range of ports (for example, Universal Serial Bus [USB], FireWire, infrared, Wi-Fi and Bluetooth) they can protect:

- The ability to manage the Windows firewall and a more-advanced personal firewall in the same management console is a distinct advantage, because some enterprises will adopt the Windows firewall for on-LAN PCs.
- EPP solutions should offer the ability to create different firewall policies

based on connection type — different network interface cards (NICs) or different networks — as well as the ability to dynamically apply policies based on network location — for example, Wi-Fi policy, on-corporate-LAN policy and public Internet policy.

- The integration of a client (IPsec) VPN is useful for enforcing remote access policies. Ideally, EPP solutions should allow unfettered Internet authentication, and then enforce VPN startup to direct remote access traffic back to the LAN.
- The ability to enforce a “one active NIC at a time” policy to block network bridging is a useful feature, and options that allow the disabling of inactive NICs are ideal.
- Application profiles that define normal application behavior, and can restrict network access for applications that aren’t approved or are potentially compromised, are useful application control features.
- A firewall must have the ability to block malicious attacks and end users attempting to disable the firewall.
- Log data — especially related to security incidents — should be extensive, searchable and accessible via the report engine to enable forensic investigation.

2.5 Port Control

Enterprises are increasingly concerned about USB ports as a channel for accidental or malicious data loss, or as an access point for malware, such as the recent Conflicker worm. For this reason, granular port control is becoming a common feature of the personal firewall or

an encryption component of an EPP suite:

- EPP solutions should provide the ability to create policies to control the broadest range of devices and device formats — for example, CD, DVD, USB, Bluetooth, 3G and general packet radio services — with policies defined, at minimum, by device class.
- The level of granularity that makes it possible to distinguish among device classes (for example, a mouse from a data storage device), and potentially to distinguish specific devices by serial number or manufacturer, is a worthwhile differentiator.
- Policies will ideally be file-type-aware so that they can allow or restrict access based on file type and action (for example, allowing “read only” access or allowing only document file types), and so that they can restrict application execution (for example, blocking auto-execute or all execution from a data drive).
- EPP offerings, when combined with encryption solutions, often allow policies to force encryption — for example, with “allow write but encrypt” and “password-protect files written to USB or CD storage” provisions.
- To minimize help-desk interaction, it’s useful to enable remote workers to “self authorize” device usage, and to allow privileged end users to use devices, but warning them that it’s against policy and that they should log their usage. At a minimum, EPP solutions should allow remote help desk activation of ports for users with administrator passwords.
- Advanced solutions will also include

options for protecting data by blocking the “cut/copy/paste,” “print screen” and “print” commands.

2.6 Reporting Capabilities

Reporting capabilities are a significant differentiator for EPP offerings, and can make a significant difference in the administration overhead that’s associated with them. Buyers should consider “point in time” reporting, as well as “real time” dashboard capabilities:

- The dashboard should provide a real-time graphical and table-based view of system events, including system information, version information and actionable alerts.
- EPP solutions will ideally provide holistic security information about the current security status of endpoints, not simply the status of the EPP components. This may, for example, include information about vulnerabilities, compliance violations and unpatched machines, for managed and unmanaged machines on the network.
- Dashboards that offer Really Simple Syndication (RSS) feeds with relevant external news — for example, concerning global malware activities and vulnerabilities — are desirable. External trending information allows administrators to better understand internal activity levels and compare them to global events.
- The dashboard should be administrator-configurable so that the most-relevant information can be moved to the top of the page. Display options (for example, pie charts, bar charts and tables) should also be configurable so that information can be displayed in the format that specific administrators need.
- Reports and dashboards should include trending information against customizable parameters. For example, it should be possible to create a dashboard view or a report that shows percentage compliance against a specific configuration policy over time.
- Dashboards should be configurable for different roles so that each administrator can create a role-specific view.
- Information should be aggregated, and should also allow single-management server, cluster, LAN, geographical or global views in the same window, depending on administrator options and role limitations.
- Dashboard information should always allow administrators to drill down to the necessary level of detail with one click, instead of forcing them to switch to the reporting application, manually select the appropriate report and re-create the parameters that include the condition they want to investigate.
- Dashboards should also offer quick links to remediation actions (for example, clean quarantine, patching and software distribution), as well as quick links to malware encyclopedia information to resolve alerts.
- EPP offerings should include the ability to import or export data and alerts with security information and event management systems, or other reporting systems.
- The reporting engine should have the capability to run on-box for smaller solutions, or move to a centralized reporting server for consolidation and storage of multiple management servers’ log information, without changing the look and feel of the reports.
- The reporting engine should also have the capability to create custom reports (in the HTML, XML comma-separated value and PDF output types), save them and schedule them for distribution via e-mail or FTP, or by moving them to the network directory.
- The database must enable rapid report queries and the ability to preserve historical data for long-term storage in a standard format.
- Reporting functionality should include active filtering to narrow the results in longer reports so that specific events can be identified.
- Reporting engines should facilitate the creation of completely ad hoc reports, similar to SQL queries, rather than just modify the parameters of predeveloped reports.
- Multiple chart types (such as pie charts and bar charts) should be supported, as well as summary data.
- Summary reports should include active links that allow drill-down into detailed reports, as well as back-navigation that makes it easy to return to the top-level view.

2.7 DLP

Enterprises are becoming increasingly concerned about data loss, and many EPP vendors are adding endpoint DLP capabilities in response. Some EPP DLP solutions are components of broader enterprise DLP solutions, while others are stand-alone, endpoint-only solutions. Endpoint DLP that's integrated into an EPP suite offers the promise of more content-aware port/firewall and encryption policies, simplified agent management and distribution, and reduced costs. Stand-alone EPP DLP will likely satisfy many enterprises' early needs, but may not be suitable for more-ambitious data protection plans in the future. Buyers should evaluate prospective EPP DLP capabilities as well as vendors' longer-term road maps to determine how well they align with their business needs:

- Basic solutions will offer described-content detection (for example, for specific number formats, such as U.S. Social Security Numbers [SSNs] and keywords).
- More-advanced solutions will enable the detection of specific corporate data or

“registered data,” such as specific database elements or specific files identified by name, hashmarks or watermarks. These solutions will also have the ability to detect partial data matches to identify content that has been altered slightly, but remains largely intact.

- EPP DLP functionality will be differentiated by the number of predefined dictionaries and lexicons offered (for example, financial terms, patent health-care terms and legal terms).
- Dictionaries should be able to assign weightings to specific words, “wild card” operators and case-sensitivity/insensitivity indicators.
- “Smart” number identifiers (for example, the ability to recognize that “999 999 999” isn't a valid SSN) are a more-advanced capability.
- Solutions should have the ability to perform deep inspection for content matches within a large number of file types.
- Stand-alone endpoint DLP capability (sometimes known as “channel DLP”) is useful and shows advanced technical ability. Most enterprises will want the

ability to integrate with broader enterprise DLP solutions or share policies with other enforcement points, such as e-mail and secure Web gateways.

2.8 Service and Support

Service and support are essential concerns for EPP suites because they're for any business-critical technology offerings.

Capabilities to consider include:

- Dedicated product engineers' resources or direct access to Level 2 support
- Global support footprint with local language support engineers in necessary geographies
- Evidence of extended tenures of the support staff
- Vendor willingness to agree to high service-level agreements for callback responses
- Support resources, including user forums, best-practice guidance and white papers
- Installation assistance and training

*Gartner RAS Core Research Note G00167208,
Peter Firstbrook, 7 May 2009*

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