SOPHOS

Security made simple.

Endpoint Buyers Guide

Evaluating the many components that make up an endpoint security solution can be overwhelming. This buyers guide provides independent research and test results to help you determine your endpoint security solution requirements and identify the vendor that best meets your needs.

It takes more than antivirus to stop today's advanced threats. An endpoint protection solution is an important part of your IT security strategy to protect corporate assets. Your endpoint solution should be able to prevent, detect and remediate malware and advanced threats. In addition, it should include features like web filtering and device control that let you enforce consistent security policy across your organization. Finally, you need a solution that's easy to install and manage, and that can grow with your needs—saving you time and ensuring comprehensive protection for years to come.

We examine the top vendors according to market share and industry analysis: Sophos, Kaspersky Lab, Intel Security (McAfee), Symantec and Trend Micro. Each vendor's solutions are compared based upon:

- Product Features and Capabilities
- Industry Analyst Ratings
- Third Party Test Results
- Community Feedback

In addition, we provide additional information to help you select the best endpoint solution for your organization:

- Extending Your Security: Consider Complete Protection
- Evaluating Endpoint Protection: Questions to Ask

Product Features and Capabilities

Basic endpoint security solutions include antivirus, anti-malware and anti-spyware capabilities. According to industry analysts, businesses need more than this basic level of security to protect against today's advanced threats and to prevent data loss. Features like malicious traffic detection, device control, application control, web productivity filtering and data loss prevention can help. Even if you don't need these advanced capabilities today, your organization will likely need them in the future, given the increasing complexity of threats.

In addition, organizations have to consider the management features available to make the product simple to deploy, configure and maintain.

The following chart lists the features available within each vendor's centrally-managed business endpoint protection products:

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
On-premise management	✔	✔	✔	✔	✔
Cloud-based management (SaaS)	✔	✔	✗	✔	✔
Device-based policies	✔	✔	✔	✔	✔
User-based policies	✔	✔	Limited	✔	✗
Device Control	✔	✔	✔	✔	✔
Data Loss Prevention (DLP)	✔	✔	✗	✔	✔
Application Control	✔	✔	✔	✔	✗
Category-based web filtering	✔	✔	✔	✔	✔
Malicious traffic detection	✔	✔	✗	✗	✔
Active Directory sync	✔	✔	Import Only	✔	✔
Synchronized security (Endpoint + Network)	✔	Add-on	✗	✗	✗

Industry Analyst Ratings

Industry analysts, such as Gartner and Info-Tech Research Group, are independent companies that rate and evaluate technology vendors on behalf of their corporate clients. Their annual reports, such as the ones cited below, provide unbiased information to help organizations make informed purchasing decisions.

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Gartner Magic Quadrant for Endpoint Protection Platforms	Leader	Leader	Leader	Leader	Leader
Info-Tech Endpoint Protection Vendor Landscape	Champion & Best Overall Value	Market Pillar	Innovator	Market Pillar	Champion

Gartner Magic Quadrant for Endpoint Protection Platforms

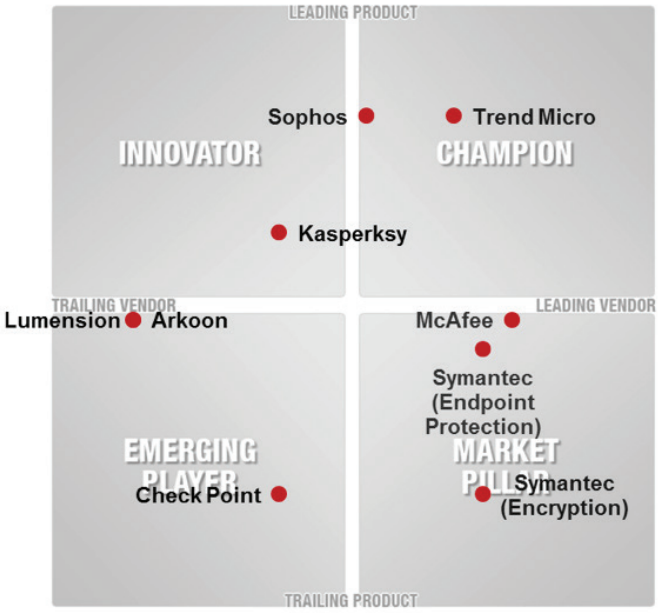
Gartner's Magic Quadrant for Endpoint Protection Platforms, a research tool that rates vendors on completeness of vision and ability to execute, reviewed eighteen vendors in 2014. Sophos, Kaspersky Lab, Intel Security (McAfee), Symantec and Trend Micro were placed in the Leaders Quadrant. Sophos is a Leader for the eighth consecutive year.

Magic Quadrant for Endpoint Protection Platforms by Peter Firstbrook, John Girard, Neil MacDonald, December 22, 2014

DISCLAIMER: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Info-Tech Endpoint Protection Vendor Landscape

In this report, Info-Tech Research Group assesses vendors on the strength of their offering and their enterprise strategy. According to the report, "Champions receive high scores for most evaluation criteria and offer excellent value. They have a strong market presence and are usually the trend setters for the industry." Sophos is one of only two Champions in the 2014 report. Info-Tech also named Sophos the Best Overall Value.



Third Party Test Results

Independent tests, like the ones listed below, compare detection rates, false positive rates and performance (effect on a computer's speed) in a controlled lab environment. Laboratory conditions, though, do not always mirror protection and performance in the real world. You should therefore also consider each solution's available prevention, detection and remediation capabilities.

		Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
AV-Test Business Windows Client May-Jul 2015	Protection Score	6.0/6.0	6.0/6.0	6.0/6.0	6.0/6.0	6.0/6.0
Dennis Technology Labs Small Business Anti-Virus Protection Jan-Mar 2015	Award	AAA	A	AAA	AAA	B
	Total Accuracy	94%	84%	100%	100%	73%
AV-Comparatives Performance Test May 2015	Award	Advanced+ ★★★	Advanced+ ★★★	Advanced+ ★★★	Not tested	Advanced ★★

Community Feedback

Sometimes, the best way to evaluate a vendor is to ask existing customers what they think. That's exactly what Spiceworks does by soliciting online reviews from its community of six million IT professionals. Here are the results for the leading endpoint security vendors:

	Sophos	Intel Security (McAfee)	Kaspersky Lab	Symantec	Trend Micro
Average rating (out of 5 stars)	★★★★½	★★	★★★★·	★★½	★★★½

In addition, Information Security™ magazine and SearchSecurity.com asked over 1,700 information security executives and managers to rate their favorite products across 22 categories. Sophos was one of two winners of the publications' 2014 Readers' Choice Awards in the category of Endpoint Security.

Extending Your Security: Consider Complete Protection

An endpoint security solution protects your computers from malware and helps enforce your security policy on those computers. But it is just one part of an overall security strategy. Today's organizations are wise to look beyond the endpoint to the protection of the entire enduser environment. Ideally, a single vendor provides a bundle of solutions that work together to give you consistent protection and policy enforcement throughout your organization. Working with a single vendor can provide better security, reduce administration and lower costs.

Some specific technologies to consider along with endpoint protection include:

- Full disk encryption
- Mobile device management (MDM)
- Mobile security (antivirus)
- Secure email gateway (anti-spam, anti-malware, encryption)
- Secure web gateway (content filtering, anti-malware, reporting)
- Specialized server or virtual machine protection
- Synchronized security - endpoint and network working together to make faster decisions

Evaluating Endpoint Protection: Questions to Ask

Endpoint security solutions claim many different features. To evaluate a particular product, start by asking the vendor the following questions:

1. What is involved in deploying the solution and configuring it for optimal or "best practice" protection?
2. What steps are required to add exceptions to policies (e.g., allowing a specific USB drive to be accessed or a specific website to be visited)?
3. What impact (performance and usability) will the product have on end users?
4. What level and hours of support are included standard with the product?
5. How has the product evolved recently to protect against new, advanced threats?
6. Does the product provide web protection and filtering, even when users are off the corporate network?
7. What bundles or suites are available that can extend the endpoint product to more completely protect users and data?
8. How does the vendor enable you to extend the capability of your endpoint protection by integrating it with network security?

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

2015-10 BG-NA (NP)