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 protection solution should include: anti-malware, host-based intrusion prevention (HIPS), web protection, patch assessment, application and device control, network access control, data loss prevention, firewall and other capabilities. In addition, 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, McAfee, Symantec and Trend Micro. Each vendor's solutions are evaluated on:

- Product Features and Capabilities
- Effectiveness
- Performance
- Usability and Management
- Technical Support

In addition, we provide tools and checklists to help you select the best endpoint solution for your organization.

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

Product Features and Capabilities

Basic endpoint security solutions include antivirus, anti-spyware, host-based intrusion prevention and firewall technologies. According to industry analysts, more advanced endpoint solutions also include cloud-based protection, device and application control, patch assessment, web productivity filtering, network access control, data loss prevention and full-disk encryption. 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.

When it comes to independent reviews of endpoint solution features and availability, only Sophos received top category placement in each review. See our chart for at-a-glance information, and read the report summaries for more information on test results by vendor.

	Sophos	Kaspersky Lab	McAfee	Symantec	Trend Micro
Enex TestLab Usability of Endpoint Security	Complete	Partial	Complete	Partial	Partial
Forrester Wave	Leader	Leader	Leader	Leader	Strong Performer
Gartner EPP Magic Quadrant	Leader	Leader	Leader	Leader	Leader
Info-Tech Research Group's Enterprise Anti-Malware	Champion	Champion	Champion	Champion	Market Pillar
Ovum Decision Matrix: Endpoint Security	Leader	Challenger	Leader	Leader	Challenger
Spiceworks community rating	★★★★½	★★★★	★★	★★★	★★★

Enex TestLab Usability of Endpoint Security

Enex TestLab tested the various feature sets, compatibility and usability of endpoint security products. Of the six products Enex TestLab evaluated, it singled out Sophos and McAfee as enterprise-grade solutions largely due to their data loss prevention, device protection and full-disk encryption capabilities. Only these two vendors have "complete" products, meaning they offer a complete endpoint solution, whereas the others are missing some features.

In terms of usability, McAfee had the most involved and lengthy installation processes, and Trend Micro was close behind. Sophos, Kaspersky and Symantec offer more simplified installation procedures. Of the five vendors, Sophos came out on top due to the integration of security capabilities in a single package, ease of installation and deployment and data protection capabilities.

Forrester Wave: Endpoint Security

According to Forrester, Wave Sophos is a leader, standing out for our "extensive security capabilities and approach for integrated management." Sophos delivers strong security capabilities, and our anti-malware product has one of the best malware detection rates on the market today. We also received recognition for our support for mobile device management and anti-malware for Mac, a necessity for enterprise environments, according to the report.

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 17 vendors. Sophos, Kaspersky Lab, McAfee, Symantec and Trend Micro were placed in the Leaders Quadrant. For the sixth consecutive year, Sophos is a Leader. We believe we're a Leader again because we innovate how we deliver endpoint protection: from integrating UTM and endpoint into a single console, to including mobile device management (MDM) and endpoint as a single, per-user license. Plus we offer Sophos Cloud, a solution that's painless to deploy and easy to manage. Our endpoint protection covers end users, wherever they are and whatever devices they use, in a way that's fast, effective, and easy.

Info-Tech Research Group's Vendor Landscape: Endpoint Anti-Malware

In this report, Info-Tech Research Group assesses vendors on the strength of their offering and their enterprise strategy. Champions receive high scores for most of the criteria—features, usability, affordability and architecture—and offer excellent value. A Champion, Sophos ranks highest among all vendors profiled in the report.

Vendor Landscapes: Features Evaluated

✔ = Feature fully present ✓ = Feature partially present / pending ✗ = Feature absent

	Reputation Scanning	Host IPS	Device Control	Application Control	URL Filtering	DLP	NAC	Endpoint Encryption
Sophos	✓	✔	✔	✔	✔	✔	✔	✔
ESET	✓	✔	✔	✗	✓	✗	✓	✗
Kaspersky	✓	✔	✔	✓	✓	✗	✓	✓
McAfee	✔	✔	✔	✗	✔	✗	✔	✔
Symantec	✔	✔	✔	✓	✗	✔	✓	✓
Total Defense	✓	✔	✔	✔	✓	✗	✓	✗
Trend Micro	✔	✔	✔	✓	✔	✔	✓	✓

Ovum Decision Matrix: Endpoint Security

The Ovum Decision Matrix categorizes vendors based on customer satisfaction, how well their solutions have evolved to meet changing business needs, and how each is positioned to address mobile devices. Vendors are designated as Leaders, Challengers or Followers. Leaders Sophos, McAfee and Symantec provide the core elements of endpoint security, as well as comprehensive platform coverage for traditional endpoints and extensive coverage for mobile operating platforms.

Effectiveness

The basic goal of an endpoint security solution is to prevent malware infection. "As the anchor solution in EPP suites, the quality of the malware scan engine should be a major consideration in any RFP," according to Gartner. However, no antivirus engine can provide 100% protection. Furthermore, overly aggressive detection can lead to false positives or frequent prompts for users to decide how to proceed. Both of these decrease user productivity and increase the risk that a valid warning will be ignored.

Independent tests, like the ones listed below, compare detection and false positive rates in a controlled lab environment. Laboratory conditions, though, do not always mirror protection in the real world. You should therefore also consider each solution's available detection capabilities, from HIPS to web protection and advanced behavioral detection.

	Sophos	Kaspersky Lab	McAfee	Symantec	Trend Micro
AV-Comparatives					
Real-World Protection Test	Advanced+	Advanced+	Advanced	Not tested	Advanced
AV-Test					
Overall score	★★★★★½	★★★★½	★★★★	★★★★★★	★★★★
Zero day malware blocked	96%	100%	95.5%	100%	100%
Widespread malware blocked	99%	100%	100%	99.5%	100%
False warnings/blocks	0	1	2	0	0

AV-Comparatives

AV-Comparatives' Whole Product "Real World" Protection Test reviewed the antivirus programs of 20 vendors including all protection features. It "achieves the most realistic way of determining how well the security product protects the PC." Factors rated included behavioral protection, URL blocking and wrongly blocked domains and files. Sophos received an "Advanced+" rating in this test.

AV-Test

The AV-Test Institute evaluated the ability of top endpoint security solutions to protect against malware infections with scores focused on average slowdown of the computer by the security software in daily use; false malware positives; and false warnings and false blocking of certain actions during download, installation and use of legitimate software. Out of a total possible score of 6, Sophos received an overall score of 5.5; Kaspersky Lab received 4.5; McAfee and Trend Micro came in last, each with a score of 4; and Symantec received a 6.

Performance

Evaluating performance means determining how a security solution impacts system resources and user experience. Ideally, users won't experience slowdown when a security solution is scanning their system: during scheduled scans, at boot up or when opening and copying files. Strong performance from your security software can improve end-user productivity, while decreasing the frequency of help desk calls and user attempts to disable their security software.

	Sophos*	Kaspersky Lab	McAfee	Symantec	Trend Micro
AV-Comparatives Performance Test	Advanced+ *Of the companies compared Sophos received the highest AV-Comparatives and PCMark® cumulative score (189.0).	Advanced+	Standard	Advanced+	Standard

Usability and Management

Usability–which includes deployment, configuration, policies and ongoing management–impacts the time you spend on day-to-day security tasks. IT teams need a straightforward solution with single-console management, easy implementation, a simple user interface and the ability to make changes easily. Policies should be flexible, and not so complex that they confuse or overwhelm.

Management and deployment options

When it comes to ease of use, it's important to look at software management and deployment options that fit your organization's needs. Endpoint security can be managed by an on-premise management console, or via a cloud deployment option which does not require a server to house the management console.

Deployment option	Sophos	Kaspersky Lab	McAfee
Cloud-managed	Sophos Cloud	N/A	SaaS Endpoint
UTM-managed	Sophos UTM	N/A	N/A
On-premise server-based	Sophos Enterprise Console	Kaspersky Security Center	McAfee ePO

Ease of use and accessibility of features/functions

As traditional endpoint antivirus evolves to become a complete endpoint protection platform, vendors are including more and more features and functions. In addition to traditional signature-based antivirus, modern endpoint protection products also include features to enhance protection, reduce the attack surface and protect data. While most vendors tout these additional features, it is also important to consider ease of deployment and manageability of these functions. A good measure of usability is whether a product's features have been adopted by your peers. For example, most endpoint protection suites now include HIPS, patch assessment, application control, device control, data loss prevention (DLP) and encryption. Once you have narrowed your choice to a short list of vendors, ask your peers if anyone uses these features to enhance their security.

Integration and policy management

When evaluating endpoint protection platforms you need to understand each vendor's integration strategy. Does the vendor use a single integrated agent to manage and receive policies from the console, eliminating policy conflict? For example, many endpoint protection platforms now include web filtering capabilities. Does the vendor take into account whether an endpoint is behind a firewall or outside of the corporate network? Can the endpoint protection agent take advantage of your network security and make sure the policies are consistently and automatically enforced? Some vendors may appear to have an integrated console but use multiple endpoint agents for different functions. This not only creates a heavier footprint, impacting your deployment, but also may potentially cause policy conflict.

To help you evaluate usability, we offer three reports from AV-Comparatives, Enex TestLab and Ovum. Read the report summaries and see the at-a-glance tables for more information.

	Sophos	Kaspersky Lab	McAfee	Symantec	Trend Micro
AV-Comparatives IT Security Products for Business Users	Approved Business Product	Not tested	Not tested	Approved Business Product	Not tested
Enex TestLab Usability of Endpoint Security	★★★★★	★★★★	★★★	★★★	★★★
Ovum Decision Matrix: Endpoint Security	Leader	Challenger	Leader	Leader	Challenger

AV-Comparatives

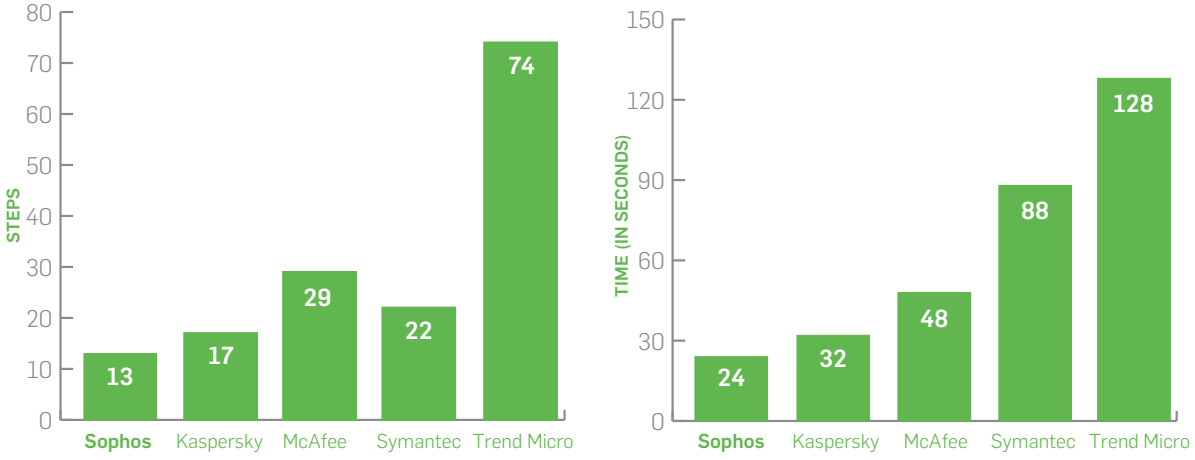
In its IT Security Products for Business Users product review, AV-Comparatives notes that our endpoint product "could be used to protect larger networks but is equally well-suited to small business. Installation and deployment should not present a professional administrator with any problems, and the straightforward design of the console makes important tasks and information easy to find. The software worked very efficiently and reliably in our test." The testers further concluded that our console is “straightforward to navigate” and not only would IT professionals feel comfortable using our software but also that “with minimal training it could be used by non-expert administrators too.”

Enex TestLab Usability of Endpoint Security

Enex TestLab evaluated Sophos, Kaspersky, McAfee, Symantec and Trend Micro for ease of use, evaluating the number of steps required to complete various scenarios. McAfee and Trend Micro had the most involved and lengthy installations. McAfee required the most steps to complete a given task. For example, specific device management tasks required a total of 69 steps from McAfee while Symantec (which came in second for this group of tasks) required 64 and Trend Micro (on the low end in this case) required 13. The table and graph below compare the number of steps and time associated with two key installation tasks.

	Sophos		Kaspersky Lab		McAfee		Symantec		Trend Micro	
	Steps	Time (mm:ss)	Steps	Time (mm:ss)	Steps	Time (mm:ss)	Steps	Time (mm:ss)	Steps	Time (mm:ss)
Find unmanaged endpoints on network and deploy agents to new endpoints	12	0:13	25	0:30	17	0:41	17	3:53	13	2:40
Import active directory structure	13	0:24	17	0:32	29	0:48	22	1:28	74	2:08

Task: Import AD Structure



Ovum Decision Matrix: Endpoint Security

The Ovum Decision Matrix for endpoint security solutions categorizes vendors based on customer satisfaction, how well the vendors' solutions have evolved to meet changing business needs, and how each is positioned to address mobile devices. Vendors are designated as a Leader, Challenger or Follower. Leaders Sophos, McAfee and Symantec provide the core elements of endpoint security, plus comprehensive platform coverage for traditional endpoints and extensive coverage for mobile operating platforms.

Overall, Sophos was considered the easiest to use and was recognized for its streamlined dashboard.

Data Protection

Data protection technology is becoming more important in today's distributed work environment. Educating users about encryption and content awareness makes them cognizant of how they handle sensitive information and the importance of data protection. Having encryption and data loss prevention (DLP) incorporated in an endpoint security solution offers a number of benefits, including simplified management and cost savings.

Sophos, McAfee, Symantec and Trend Micro all offer content rules (for example, Social Security numbers), predefined dictionaries and weightings to specific words. However, Sophos is the only vendor to provide these DLP capabilities integrated into a single endpoint agent. Trend Micro offers an optional hosted DLP agent as part of its endpoint security platform. McAfee and Symantec use separate agents and licenses to provide host DLP capabilities. Kaspersky Lab does not have a DLP offering. Sophos and McAfee provide encryption capabilities in their endpoint protection, while the others do not.

In addition to encryption capability in endpoint protection products, Sophos offers SafeGuard Enterprise, which helps make us a Leader in the Gartner Magic Quadrant for Mobile Data Protection. We believe we're a Leader because we address the increasing needs of a global market that demands more than just encryption.

Review	Sophos Endpoint Security and Data Protection 9.7	Kaspersky Business Space Security 10	McAfee Total Protection for Endpoint (ePO 4.6)	Symantec Endpoint Protection 12.1	Trend Micro OfficeScan 10.5
Enex TestLab Usability of Endpoint Security	Data protection and encryption capabilities	Data protection Full-disk encryption, not DLP (only available in certain packages; encryption for smartphones only)	Data protection and encryption capabilities	Data protection and encryption capabilities not available in this license	Data protection and encryption capabilities not available in this license

Enex TestLab Usability of Endpoint Security

Enex TestLab examined the features in six endpoint security products and determined that Sophos offers the most comprehensive endpoint security suites, designating us and McAfee as the only enterprise-grade solutions. As the only two solutions to offer full-disk encryption, Sophos and McAfee provide the most complete data protection. Sophos offers the added benefit of providing DLP capabilities without adding complexity to our solution.

Mobile Security

Mobile is the new endpoint in IT. However, many organizations still struggle with mobile device management (MDM) and mobile security. To ensure organizational productivity, secure collaboration, and data security on mobile devices, an MDM solution is critical. Sophos Mobile Control provides an easy and effective way to manage all smartphones and tablets, from initial setup and enrollment all the way through device decommissioning. It helps organizations secure, monitor and control mobile devices with over-the-air control. Malicious or "leaky" apps and mobile malware are among the top security concerns for IT professionals. In order to have full control over your mobile protection, choose a solution that gives you the option to integrate mobile security apps into your MDM console and fully manage security from one console. The Enterprise Mobility Management Buyers Guide provides a detailed view of what to look for in your mobile security solution to protect this new endpoint.

Technical Support

You can hope you'll never need tech support for your endpoint security solution, but it should be a key part of any vendor's product. Tech support requirements are fairly straightforward: a vendor that offers 24/7 local language support, with knowledgeable engineers answering the phone and short wait times (if you have to wait at all). In the chart below we provide certification and customer satisfaction measurements, which provide proof that vendors deliver a level of customer support that buyers expect.

Review	Sophos	Kaspersky Lab	McAfee	Symantec
Ovum Decision Matrix: Endpoint Security	Outstanding	Mediocre	Mediocre	Mediocre

Ovum Decision Matrix: Endpoint Security

When determining how to categorize product vendors for its Endpoint Security Decision Matrix, Ovum takes into account a number of dimensions. Sophos, McAfee and Symantec dominated most of the technology dimensions, but only Sophos appeared regularly across most of the dimensions in the customer satisfaction survey. According to the report, Sophos' customer satisfaction ratings for support and service were "outstanding." Kaspersky, McAfee, Symantec and Trend Micro received "mediocre" ratings across most dimensions of the survey.

Extending Your Security: Consider Complete Protection

An endpoint protection solution needs to provide comprehensive security at the endpoint. But it is just one part of an overall security strategy. You also have to protect your data, email, web, server and mobile environments. Today's companies are wise to consider how a vendor's endpoint solution integrates with these other solutions. Ideally, a single vendor provides an integrated suite of solutions to address all of these needs. This simplifies security administration and lowers costs.

When you look at the top endpoint vendors presented here, Kaspersky offers a partial approach to security, while Symantec, McAfee and Trend Micro offer a security portfolio. Only Sophos offers complete integrated security. Our single security system includes endpoint, data, email, web, server and mobile protection—all-in-one license.

✔ = Yes ✓ = Limited ✗ = No

	Sophos Complete Security Suite	Kaspersky Total Security for Business	McAfee Complete Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition	Trend Micro Enterprise Security Suite
AV/HIPS/Firewall	✔	✔	✔	✔	✔
Application Control	✔	✔	✗	✔	✗
Device Control	✔	✔	✔	✔	✔
Endpoint Web Filtering	✔	✔	✔	✗	✗
DLP	✔	✗	✓	✗	✗
Patch	✔	✔	✗	✗	✗
Web & Email Gateway	✔	✔	✔	✔	✔
Encryption	✔	✔	✔	✗	✗
Mobile	✔	✔	✔	✗	✔
Microsoft Exchange	✔	✔	✔	✔	✔
SharePoint	✔	✔	✗	✗	✗
Backup & Recovery	✗	✗	✗	✔	✗
Platforms (Win / Mac / Linux)	✔	✔	✔	✔	✔
Standard Support level	24/7 Phone	Business hours only	24/7 Phone	Business hours only	Business hours only
License	User based				

Summary

Endpoint security at its best is complete and simple. It protects your organization from threats and data loss across all platforms from a single management console. Finding the right solution may seem daunting, but asking the right questions can help you find the vendor that will serve your company best. This chart sums up how the major vendors fared in third party tests in each of the areas evaluated.

✔ = Best ✓ = Good ✗ = Fair

	Sophos	Kaspersky	McAfee	Symantec	Trend Micro
Overall	✔	✗	✓	✓	✗
Features and Capabilities	✔	✓	✓	✗	✗
Effectiveness	✓	✓	✗	✓	✗
Performance	✔	✓	✗	✔	✗
Usability	✔	✓	✗	✔	✓
Data Protection	✔	✗	✔	✗	✗
Technical Support	✔	✗	✗	✗	✗

Evaluating Endpoint Protection: Questions to Ask

Endpoint security solutions claim many different features. To learn if a product satisfies your minimum required capabilities, start by asking vendors the following questions:

1. Is it easy to implement?
2. Is it easy to manage with a single console?
3. Does it support all of my platforms?
4. What impact will it have on end users?
5. Does it include data protection?
6. Can it ensure compliance?
7. Does it include expert support in the local language?
8. Does it include free upgrades?
9. Does it protect against malware?
10. Does it improve IT efficiency?
11. Does it improve end-user flexibility and productivity?
12. Does it provide web protection wherever my users are?
13. Does it include patch assessment?
14. Is it part of an integrated suite of security solutions?

Recommended Features Checklist

Below are the primary capabilities and features found in advanced EPP solutions. Not every solution will have every item on the list. As you begin researching solutions, use this checklist to create your requests for proposal or as a scorecard to evaluate different products.

Product features and capabilities

- ☐ Web protection that includes URL filtering, malware scanning, and content filtering
- ☐ Application control capabilities
- ☐ Patch assessment capabilities
- ☐ Manages list of known good/unwanted applications
- ☐ Extensive firewall log data
- ☐ Creates firewall policies based on connection type
- ☐ Creates device policies based on device class (i.e., CD, DVD, USB, etc.)
- ☐ Distinguishes between classes of devices based on serial number or manufacturer
- ☐ RSS feeds into dashboard with relevant news
- ☐ Imports or exports data and alerts with other security systems
- ☐ Creates custom reports in HTML, XML, CVS and PDF
- ☐ Installs protection on Windows, Mac, UNIX, Linux, storage and virtual platforms
- ☐ Assesses computers accessing your network to ensure they meet your security policies, and blocks or quarantines them if they do not

Effectiveness

- ☐ Dashboard of real-time events
- ☐ Broad malware signatures that detect new variants of old threats without causing false positives

Performance

- ☐ Native management server redundancy capabilities
- ☐ Single signature database and scanning engine for all forms of malware

Usability

- ☐ Easy installation that includes optimal default settings for your environment
- ☐ Role-based administration
- ☐ Object-oriented policy creation
- ☐ Administrator-configurable dashboard with real time graphical and table-based view of events
- ☐ Removes competitive endpoint products on installation

Data protection

- ☐ DLP content inspection for removable storage, email clients, web browsers and IM clients
- ☐ Creates content detection for organization specific intellectual property
- ☐ Encrypts computer hard disks and files

Technical support

- ☐ Installation assistance and training
- ☐ Support resources such as user forums and whitepapers
- ☐ Independently certified, follow-the-sun support operations

Extending your security: Consider complete protection

- ☐ Integration of security solutions
- ☐ Endpoint, data, email, web, server and mobile protection all in one license

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

3.14.GH.bgna.simple

SOPHOS