Endpoint Security Vendor Evaluation Guide

kaspersky

Endpoint Security Vendor Evaluation Guide

Small and mid-sized businesses (SMBs) understand that without the right security solution, a breach could damage their business, potentially permanently. Cyber risk is increasing as criminals continue to innovate and create attack techniques, and remote working and the proliferation of information exchange methods increase the likelihood of a successful targeted attack.

But SMBs are faced with a myriad of software security vendors all clamouring for their business. With limited resources, SMBs should follow a disciplined approach when considering all the options available. But how to cut through the noise and decide what is really needed?

Simplify the choice with these three steps.

1. **Find out what the market is saying**
   Do your research to get a consensus on the best vendors in the market for your needs.
2. **Sort out a security criteria list**
   Ask the tough questions to get the right answers.
3. **Check out the overall profile of the vendor**
   Find out about the vendor's culture, stability, scalability, innovation, research & investment and range of products and services

Find out what the market is saying

There is a large amount of material on the internet from software security vendors promoting their products and services. These vendor resources claim, either directly or indirectly, that their products and services fulfil the criteria potential customers require. However, their claims are rarely backed up by test results. Mostly these resources lack one vital ingredient – an independent and objective assessment of how specific vendor products and services actually perform.

Our suggestion is to take a long, hard look at what the specialists, the experts, the analysts and above all the customers write about specific vendor products and solutions in the market. The relevant judgement is not: what are the capacities of a vendor's products and solutions, but how these capacities perform. A vendor may claim to offer exactly what an organization needs, but how can this claim be validated if the actual performance is an unknown?

It is time to evaluate the security software vendor marketplace objectively by asking the tough questions:

- How much is really known about a vendor's performance?
- What do the customers really think? How satisfied are they with performance and service?
- Where are the independent verification of performance claims?
- For what reasons do vendors limit or avoid their products being subjected to rigorous testing or analysis?

Who can be a better judge than the customer?

What does the customer think?

At the end of the day, who can be a better judge than the customer? When evaluating a potential security software vendor, check for customer reviews and evidence of customer satisfaction. A gold standard to use for starters is the Gartner Peer Insights customers' Choice for Endpoint Protection Platforms, which compiles real user reviews in a highly analytic form to reach a dedicated score about which vendors are best rated by their customers. These customer reviews, from businesses of all sizes and in all sectors, provide relevant information and often clarify issues and answer specific questions more effectively than technical marketing datasheets.

Also check out forums where typical product problems are described. One of the best indicators to look out for is how quickly these problems were addressed and resolved by the vendor.

In conclusion, a scan of customer feedback on the internet reveals a pattern of preferences which will be invaluable when creating a shortlist of security vendors.

Tests are the most accurate verification of marketed capabilities against the current threat landscape[1]

What do independent tests and reviews reveal?

A simple way to assess a security vendor is to check their aggregate scores in the security industry's most respected, independent tests and reviews. If a vendor either does not participate or does not perform well, there may be valid reasons, but it is advisable to find out why. Tests are the most accurate verification of marketed capabilities against the current threat landscape. Check how many first places and top-three positions vendors have achieved in tests, and look for evidence of sustained performance across multiple tests; obviously a more meaningful assessment than a one-off performance in a single test.

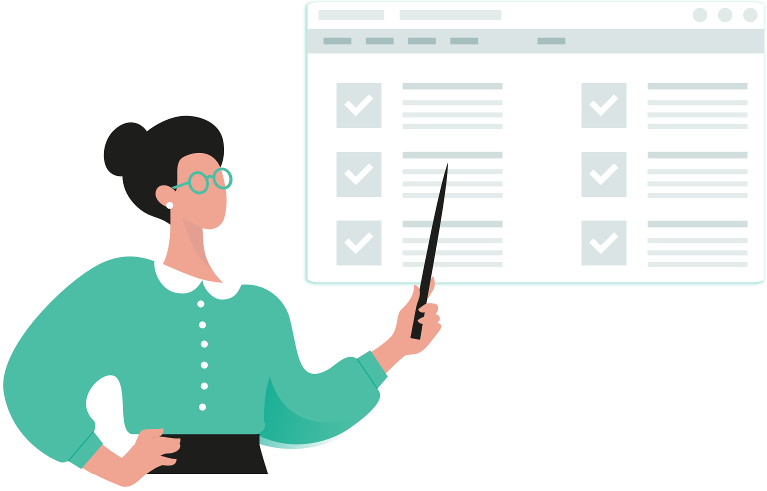
So which tests to look at? To get an overall picture, check out all SE Labs tests, all the AV-Test's awards, in particular the AV-Test Advanced Endpoint Protection Test, AV-Comparatives, MRG Effitas, ICSA Labs and NSS Labs' Advanced Endpoint Protection group test. These test laboratories evaluate full technology stack efficiency against known, unknown and advanced threats.

What are the analyst's conclusions?

One of the key starting points in evaluating security vendors, is to look at the conclusions of the leading analytical agencies. How do they rate vendors - as Leaders? Top Players? Visionaries? And for what reasons? These ratings are compiled by experts who combine specialist knowledge with a breadth of vision covering the whole sector. If one of your short-listed vendors appears low down or is simply not on the analysts' radar, it is necessary to investigate for what reasons. Check out in particular the Gartner Magic Quadrant for Endpoint Protection Platforms, the Forrester Wave for Endpoint Security Suites and Radicati Market Quadrant for Endpoint Security.

Sort out a security criteria list

Ask the tough questions to get the right answers



Research on how analysts and customers rate vendors and their products and services is a necessary step, but only a start. To make a meaningful choice, small and mid-sized businesses (SMBs) should start by defining the security they need. That means drawing

[1] https://www.kaspersky.com/top3

up a list of what is essential to protect for their business security and profitability. Consequently, in addition to being able to ask vendors the right questions, SMBs will cut through the marketing floss and can reappraise the tests, reviews and analysts' conclusions through a more critical lens.

The single most important factor when choosing a vendor is to make a correct judgment concerning the quality and capacity of the vendor's endpoint protection. For SMBs effective endpoint protection is the cornerstone of a cyber safe business. 70 percent of successful cybersecurity breaches, according to global market intelligence provider IDC, originate on endpoint devices.[2] IDC also concluded that the value of affiliated security products, such as Threat Intelligence and Endpoint Detection and Response are undermined by ineffective Endpoint Protection.

Endpoint Protection

However, selecting an endpoint protection solution is not a straightforward process. Effective endpoint protection must include sophisticated detection technologies to counter today's multi-vector attack techniques, as well as evolving threats. But it must also be easy to deploy and manage, and non-intrusive for end users. There are a large number of factors to decide on when choosing endpoint protection but here are a few pointers to assist making a well-informed decision.

Look for an endpoint protection solution that:

- offers multi-layered protection including pre-execution before malware detonates, behaviour monitoring and remediation, on-premise and in the cloud. Endpoint protection that addresses threats at all levels of the IT infrastructure provides continuous visibility into attacks and root-cause analysis to protect against unseen, unknown and zero-day threats, enabling rapid detection and remediation. For vendor endpoint protection comparison, check out test performances in the NSS Labs' Advanced Endpoint Protection group test and the AV-Test Advanced Endpoint Protection Test.

- includes threat behavior-based protection expertise protecting against 'undetectable' fileless malware that uses legitimate processes on the operating system. (PowerShell, WMI, .NET etc.) to perform malicious activities. Legacy security software cannot reliably detect fileless malware. Only behaviour-based protection armored by behavior heuristics and Artificial Intelligence (AI) can analyse activity in real time to reveal the malicious nature, terminate the process and roll back the changes.
  Compare vendor performances in the Fileless Threat Protection Test by AV-TEST.

- automates security and management tasks, such as vulnerability scanning, patch management, hardware and software inventory and application rollouts.

- controls all security tasks from a single, integrated console to provide full visibility and simplify security management.

- provides Sandbox capacity, an additional security layer that isolates and detonates threats designed to bypass endpoint protection, automating detection and response even to advanced exploits used in targeted attacks. Ask also about the vendor's Sandbox's capacity to automate the creation of new detection rules which will detect and block similar malware attacks from entering a network.

- integrates all tools for data encryption in endpoint protection, automating encryption of files and folders stored on local and removable drives to minimize the risk of information leaks.

- combines flexible deployment model, on-premise and in the cloud, with extendable, adaptive architecture of the management console, which will allow you to install plug-ins and manage any other security product from the vendor in the future without the need to learn new tools and reinvent the whole architecture.

- offers predefined categories in application control, a vital additional defense that allows or blocks an application from accessing an operating system or personal data according to pre-set rules or prompts to select an action.

- automates response activities including adaptive anomaly control and malware outbreak policy and automatic rollback of malicious activities.

Does the vendor offer...

- a unified management console (on-premises, cloud and hybrid)
- a single product for both endpoint protection and endpoint detection and response functionality
- sandbox capacity
- integrated fileless protection
- anti-exploit technology
- integrated encryption management
- shared folders protection from ransomware
- vulnerability and patch management functionality
- mobile devices protection
- app control, lockdown functionality
- high performance to prevent user and network slowdowns
- endpoint protection for MacOS and Linux
- effective tech support in your local language

[2] https://www.idc.com/getdoc.jsp?containerId=US45794219

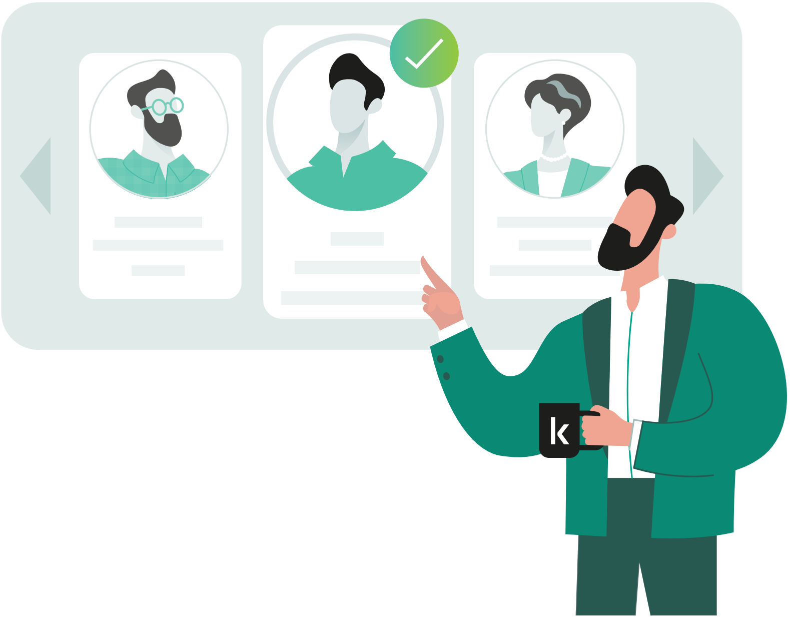
«A weak EPP solution will destroy the value of an EDR tool»

«People and time thus become the new ROI metric for EDR tool»[3]

Endpoint Detection and Response

Building comprehensive security in the contemporary threat landscape is impossible without effective Endpoint Detection and Response (EDR), offering security managers a real-time view of any threat, no matter how complex. EDR provides such essential capabilities as deep visibility and the ability to reveal the true scope and root cause of threats, as well as instant automatic response across all endpoints. A vendor on your short list must demonstrate these EDR capabilities as well as ways to increase security efficiency with automation, simple controls and deployment.

Check out the overall profile of the vendor



Cybersecurity is of such overall concern, SMBs can only benefit from a security vendor with the capacity to be longer-term business partner, offering varied security solutions and better return on investment and productivity.

When selecting a vendor watch the product videos to see how the products perform. But don't just focus solely on specific security solutions. Do research also on what is noteworthy about the vendor:

- What expertise is it recognised for?
- What is its image?
- How recognised is its brand?
- What is its reputation?
- What is the feedback from customers and analysts?
- How transparent is it?

Look at specific indicators:

- What is the depth and quality of the vendor's security portfolio? Can the vendor offer multiple solutions? Can the vendor scale up as your business expands? Does its portfolio cover all stages of Gartner's Adaptive Security Architecture?[4]
- What is the vendor's commitment to research and development? What is the vendor's testing policy?
- How are the vendor's security products rated by analysts? How does the vendor ensure its products and services maintain the highest standards?
- What is the vendor's policy on data privacy? How does the company's data policy earn and maintain the trust of its customers? Does the vendor commit to global transparency and accepted ethical principles concerning data use? How innovative is the vendor? Security solutions have to be constantly adapted and a vendor's innovation track record, and specifically how those innovations improve the value/expense ratio and drive down costs, is a key indicator. The Derwent Top 100 Global Innovator 2019-2020 as well as 2018-2019 by Clarivate Analytics records strong innovation levels in the software industry.What is the customer feedback? What is the level of customer support? What is the vendor's track record in earning and maintaining its customers' trust? What is the vendor's policy on education and training?

[3] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc # US45794219, 2020

[4] https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/

- How transparent is the vendor's pricing structure? How do implementation costs for each solution stack up against comparable vendor implementation costs? How effectively do the vendor's security solutions maximise return on investment and maximize productivity without increasing manpower costs?
- How highly rated is the vendor's technical support? Does the vendor deliver technical advice in a timely manner in your local language when it is most needed 24/7/365?

Conclusion

The best way to achieve evaluation clarity in a confusing market, is to combine a meticulous analysis of what security your organization requires, with thorough research into expert advice, opinion and the results of objective testing and customer feedback. But in addition it is important to think longer term and decide the kind of partner you really want to work with.

Cyberspace is uniquely vulnerable and cybersecurity is an evolving engagement. Attackers will always explore new techniques and tools and security vendors must constantly review and update defences. Constant innovation is absolutely necessary and important but longevity is a sign of success. Today's fast-growing cybersecurity company could be history in ten years. It is not easy to work out which vendors are succeeding. But a good track record says a lot, so when in doubt stick with tried and tested solutions.

Fundamentally your choice of security vendor is of great importance because the role of cybersecurity is only going to grow as the digital revolution gathers pace, transforming whole sectors of the economy. So do your research well and good luck!

Kaspersky Endpoint Security Cloud Plus, premium cloud security capability and cloud data protection from the **world's most tested, most awarded** security vendor, protects Windows desktops and file servers, Mac OS workstations, iOS and Android smartphones and tablets; manages endpoints from anywhere via the cloud-based console; saves time and resources with no need for hardware/software procurement, provisioning and maintenance. **Learn more** from a peace of mind provider.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.com