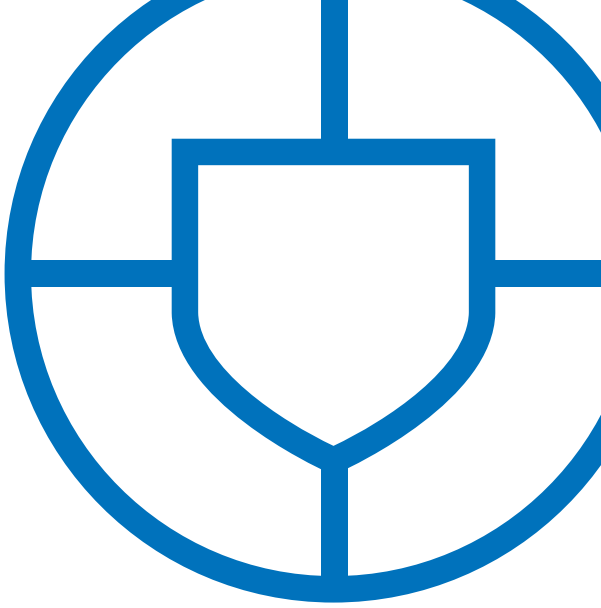
SOPHOS
Cybersecurity made simple.



Endpoint Security Buyers Guide

As cyber threats become ever more complex, the pressure on IT and security managers to have the right endpoint solution in place has also grown. However, the endpoint security marketplace has become congested with many different solutions, and is so full of indefensible marketing claims that making an educated decision for your organization is increasingly difficult.

The rapid pace of change, both in the threats we face as well as in preventative technology, has resulted in widespread confusion. This guide will provide clarity by walking you through the key preventative technologies to ensure you have the right defenses in place at the endpoint to protect your organization. It will also enable you to see how different vendors stack up in independent tests, helping your make an informed choice.

You Are Not Alone

Struggling to know what to look for in an endpoint security solution? Concerned you are not properly protected? You're not alone. Here is what other IT and Security Pros are saying[1]:

- 87% agree threats have become more complex over the last year
- 60% say their current cyber defenses are not enough to stop today's cyber threats
- 60% plan to implement machine learning in the next 12 months
- 56% don't understand of the differences between machine learning and deep learning
- 46% say they have anti-exploit technology in place – but 2/3 don't understand what anti-exploit technology actually is

In this light it's not surprising that many people are confused about endpoint security. This guide is designed to help you make an informed choice and put in place the best protection for your organization.

Product Features and Capabilities

Endpoint security solutions, sometimes referred to simply as antivirus solutions, may include a variety of foundational (traditional) and modern (next-gen) approaches to preventing endpoint threats. When evaluating solutions, it is important to look for solutions that have a comprehensive set of techniques to stop a wide range of threats. It also is important to understand the threats you are trying to prevent.

Endpoint Threats

While the threat landscape is constantly evolving, below are some key endpoint threats to consider when evaluating different solutions:

- **Portable executables (malware):** When endpoint protection is considered, malicious software programs (malware) is often the primary concern. Malware includes both known as well as never-seen-before malware. Often, solutions struggle to detect the unknown malware. This is important, as SophosLabs sees approximately four hundred thousand pieces of unknown malware every day. Solutions should be adept at spotting packed and polymorphic files that have been modified to make them harder to identify.
- **Potentially unwanted applications (PUA):** PUAs are applications that are not technically malware, but are likely not something you want running on your machine, such as adware. PUA detection has become increasingly important with the rise of cryptomining programs used in cryptojacking attacks.
- **Ransomware:** More than half of organizations have been hit by ransomware in the past year, costing on average $133,000 (USD)[2]. The two primary types of ransomware are file encryptors and disk encryptors (wipers). File encryptors are the most common, which encrypt the victim's files and holds them for ransom. Disk encryptors lock up the victim's entire hard drive, not just the files, or wipes it completely.
- **Exploit-based and file-less attacks:** Not all attacks rely on malware. Exploit-based attacks leverage techniques to take advantage of software bugs and vulnerabilities in order gain access and control of your computer. Weaponized documents (typically a Microsoft Office program that has been crafted or modified to cause damage) and malicious scripts (malicious code often hidden in legitimate programs and websites) are common types of techniques used in these attacks. Other examples include man-in-the-browser attacks (the use of malware to infect a browser, allowing attackers to view and manipulate traffic) and malicious traffic (using web traffic for nefarious purposes, such as contacting a command-and-control server).
- **Active adversary techniques:** Many endpoint attacks involve multiple stages and multiple techniques. Examples of active adversary techniques include privilege escalation (methods used by attackers to gain additional access in a system), credential theft (stealing user names and passwords), and code caves (hiding malicious code inside legitimate applications).

Modern (next-gen) techniques vs. foundational (traditional) techniques

While it may have different names, antivirus solutions have been around for a while and are proven to be very effective against known threats. There are a variety of foundational techniques that traditional endpoint protection solutions have relied on. However, as the threat landscape has shifted, unknown threats, such as malware that has never been seen before, have become more and more common. Because of this, new technologies have come to the marketplace. Buyers should look for a combination of both modern approaches, often referred to as "next-gen" security, as well as proven foundational approaches. Some key capabilities include:

Foundational capabilities:

- **Anti-malware/antivirus:** Signature-based detection of known malware. Malware engines should have the ability to inspect not just executables but also other code such as malicious JavaScript found on websites.
- **Application lockdown:** Preventing malicious behaviors of applications, like a weaponized Office document that installs another application and runs it.
- **Behavioral monitoring/Host Intrusion Prevention Systems (HIPS):** This foundational technology protects computers from unidentified viruses and suspicious behavior. It should include both pre-execution and runtime behavior analysis.
- **Web protection:** URL lookup and blocking of known malicious websites. Blocked sites should include those that may run JavaScript to perform cryptomining, and sites that harvest user authentication credentials and other sensitive data.
- **Web control:** Endpoint web filtering allows administrators to define which file types a user can download from the internet.
- **Data loss prevention (DLP):** If an adversary is able to go unnoticed, DLP capabilities would be able to detect and prevent the last stage of some attacks, when the attacker is attempting to exfiltrate data. This is achieved by monitoring a variety of sensitive data types.

Modern capabilities:

- **Machine learning:** There are multiple types of machine learning methods, including deep learning neural networks, ransom forest, bayesian, and clustering. Regardless of the methodology, machine learning malware detection engines should be built to detect both known and unknown malware without relying on signatures. The advantage of machine learning is that it can detect malware that has never been seen before, ideally increasing the overall malware detection rate. Organizations should evaluate the detection rate, the false positive rate, and the performance impact of machine learning-based solutions.
- **Anti-exploit:** Anti-exploit technology is designed to deny attackers by preventing the tools and techniques they rely on in the attack chain. For example, exploits like EternalBlue and DoublePulsar were used to execute the NotPetya and WannaCry ransomware. Anti-exploit technology stops the relatively small collection of techniques used to spread malware and conduct attacks, warding off many zero-day attacks without having seen them previously.
- **Ransomware-specific:** Some solutions contain techniques specifically designed to prevent the malicious encryption of data by ransomware. Often ransomware specific techniques will also remediate any impacted files. Ransomware solutions should not only stop file ransomware, but also disk ransomware used in destructive wiper attacks that tamper with the master boot record.
- **Credential theft protection:** Technology designed to prevent the theft of authentication passwords and hash information from memory, registry, and off the hard disk.

- **Process protection (privilege escalation):** Protection built to determine when a process has a privileged authentication token inserted into it to elevate privileges as part of an active adversary attack. This should be effective regardless of what vulnerability, known or unknown, was used to steal the authentication token in the first place.
- **Process protection (code cave):** Prevents use of techniques such as code cave and AtomBombing often used by adversaries looking to take advantage of the presence of legitimate applications. Adversaries can abuse these calls to get another process to execute their code.
- **Endpoint detection and response (EDR)/root cause analysis:** EDR and other analytical tools are not focused on preventing attacks, but rather analyzing and responding to previously detected incidents. Some also offer hunting capabilities to discover attacks that previous went unnoticed. It is important to match the size and skillset of your IT team with the complexity and ease of use of the tool being considered.
- **Incident response/Synchronized Security:** Endpoint tools should at a minimum provide insight into what has occurred to help avoid future incidents. Ideally, they would automatically respond to incidents, without a need for analyst intervention, to stop threats from spreading or causing more damage. It is important that incident response tools communicate with other endpoint security tools as well as network security tools.

The "power of the plus": combining multiple techniques for comprehensive endpoint security

When evaluating endpoint solutions, organizations should not just look for one primary feature. Instead, look for a collection of impressive features that encompass both modern techniques, like machine learning, as well as foundational approaches that have been proven to still be effective. Relying on one dominant feature, even if it is best-in-class, means that you are vulnerable to single point of failure. Conversely, a defense-in-depth approach, where there is a collection of multiple strong security layers, will stop a wider range of threats. This is what we often refer to as "the power of the plus" – a combination of foundational techniques, plus machine learning, plus anti-exploit, plus anti-ransomware, plus much more.

As part of an endpoint security evaluation, ask different vendors what techniques are included in their solution. How strong are each of their components? What threats are they built to stop? Do they rely only on one primary technique? What if it fails?

Sophos vs. the Competition

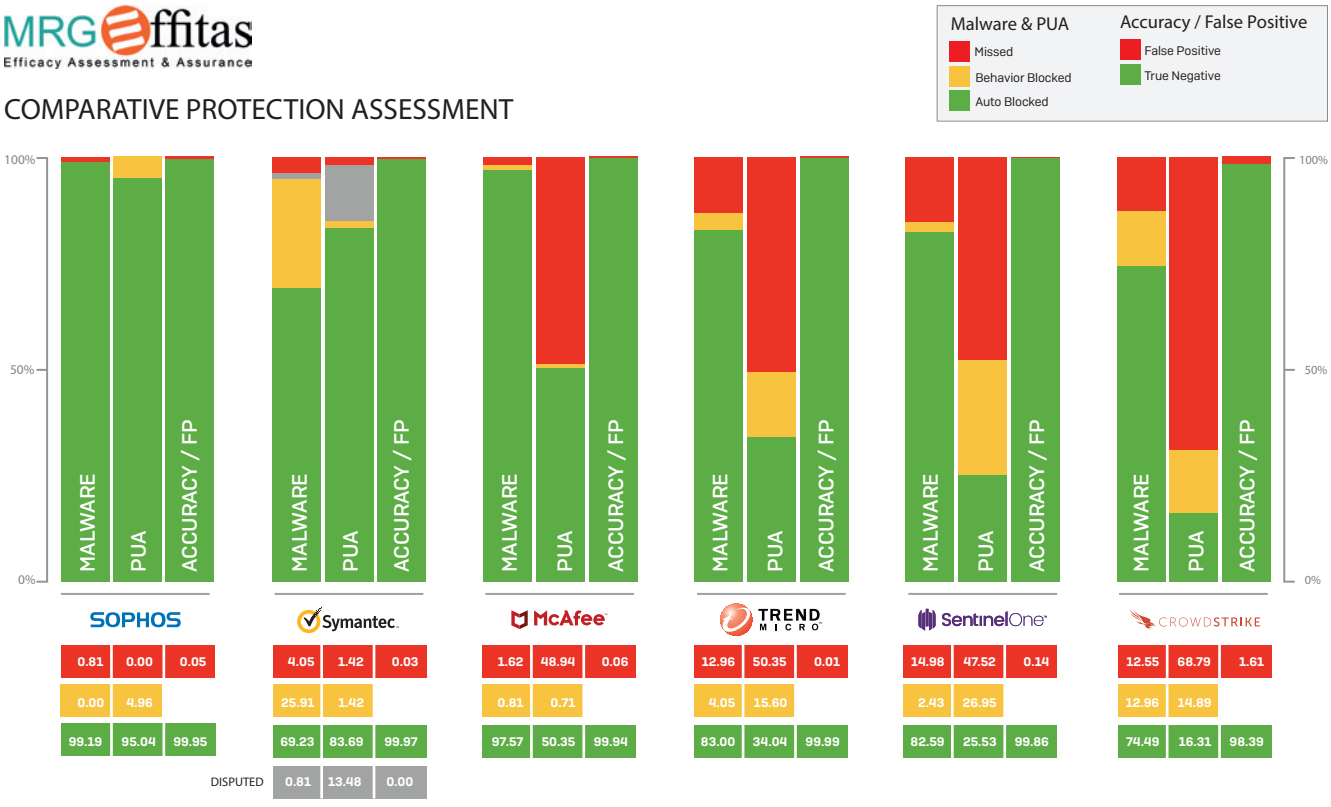
Comparing products with different features is hard enough, but comparing their performance in simulated attacks, where an attacker's actions are potentially infinite and unknown, is nearly impossible. For those who choose to test on their own, an introductory testing guide can be found here. However, many organizations choose to rely on third party assessments to aid their buying decisions.

MRG Effitas Malware Protection Test

MRG Effitas conducted a commissioned test comparing the ability of different endpoint protection products to detect malware and potentially unwanted applications (PUA). Six different vendors, including Sophos, were reviewed in the test. Sophos ranked #1 at detecting malware, as well as #1 at detecting potentially unwanted applications. Sophos also had an impressive false positive rate.

MRG Effitas
Efficacy Assessment & Assurance

COMPARATIVE PROTECTION ASSESSMENT



Read the complete results here.

MRG Effitas Exploit and Post-Exploit Protection Test

As a follow up to their malware protection test, MRG Effitas also release a report comparing different endpoint solutions stop specific exploitation techniques. Sophos Intercept X far outperforming the other solutions tested. In fact, Sophos was able to block more than twice the amount of exploit techniques relative to most of the other tools tested.

MRG Effitas
Efficacy Assessment & Assurance

EXPLOIT PROTECTION TEST RESULTS

The full report is available here.

Gartner Magic Quadrant for Endpoint Protection Platforms

Gartner's Magic Quadrant for Endpoint Protection Platforms is a research tool that rates vendors on completeness of vision and ability to execute. Sophos has been named a "Leader" in the Gartner Magic Quadrant for Endpoint Protection Platforms for the tenth consecutive report. Sophos is one of only three vendors named as a Leader.

Figure 1. Magic Quadrant for Endpoint Protection Platforms

Source: Gartner (January 2018)

The Forrester Wave™: Endpoint Security Suites

Forrester Research, Inc. conducts extensive product evaluations to create their report, interviewing both endpoint vendors and their customers. They evaluate vendors based on the strength of both their product and their strategy. Sophos has, once again, been named as a Leader in the Forrester Wave for Endpoint Protection Suites.

The full report is available here.

ESG Labs Intercept X Review

The Enterprise Strategy Group Lab tested Sophos Intercept X and determined:

"Intercept X stopped 100% of the exploit techniques that were missed by the traditional antivirus application."[3]

The full report is available here.

Extending Your Security: Consider Complete Protection

An endpoint security solution is just one part of an overall security strategy. Today's organizations are wise to look beyond the endpoint toward protecting the entire environment.

Ideally, a single vendor provides 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, mobile security, secure email gateway, specialized server or virtual machine protection, and Synchronized Security between endpoint and network devices.

Evaluating Endpoint Security: Top 10 Questions to Ask

To evaluate an endpoint protection solution, start by asking the vendor the following questions:

1. Does the product rely on foundational techniques, modern techniques, or a combination of both? Which specific features are core to the technology?
2. How does the product detect unknown threats? Does it utilize machine learning?
3. For products claiming to leverage machine learning, what type of machine learning is used? Where does the training data come from? How long has the model been in production?
4. What technology exists to prevent exploit-based and file-less attacks? What anti-exploit techniques are leveraged, and what types of attacks can they detect?
5. Does the product have technology specifically designed to stop ransomware?
6. Does the vendor have third party results validating their approach?
7. Does the product have an acceptable level of false positives? If a false positive is detected, how easy is it to reduce its impact?
8. What visibility into an attack does the vendor provide, such as root cause analysis?
9. Does the product automatically respond to a threat? Can it automatically clean up a threat and respond to an incident?
10. What level of effort is involved in the deployment and use of the solution?

Conclusion

As cyber threats continue to grow in both complexity and number it's more important than ever to have effective protection in place at the endpoint. Understanding the threats you need to block and the different security technologies available will enable you to make an informed choice of endpoint security, and give your organization the best protection against today's attacks.

Source:

1 Sophos State of Endpoint Security Report, January 2018

2 Sophos State of Endpoint Security Report, January 2018

3 MRG Effitas Comparative Malware Protection Assessment, February 2018

Gartner Magic Quadrant for Endpoint Protection Platforms, Ian McShane, Eric Ouellet, Avivah Litan, Prateek Bhajanka, 24 January 2018 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.

The Forrester Wave™: Endpoint Security Suites, Q4 2016 by Chris Sherman, October 19, 2016

Try Sophos Intercept X now for free.

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

2018-05-31 WP-UK (3017-DD)

SOPHOS