SE LABS

Endpoint Security
Enterprise

ONLINE REPORT

SE LABS ® tested a variety of anti-malware
(aka 'anti-virus'; aka 'endpoint security') products from
a range of well-known vendors in an effort to judge
which were the most effective.

Each product was exposed to the same threats, which
were a mixture of targeted attacks using well-established
techniques and public email and web-based threats that
were found to be live on the internet at the time of the test.

The results indicate how effectively the products were
at detecting and/or protecting against those threats
in real time.

Contents

Document version 1.0 Written 16th October 2024

Cyber Security Protection has Evolved

But do all endpoint security products now include next-generation anti-virus?

CEO
Simon Edwards

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our **website** and follow us on **LinkedIn**.

Top-tier anti-virus solutions are undeniably 'next-generation'. This term was introduced nearly a decade ago by newcomers to the industry: a marketing device designed to compete with almost unassailable anti-malware brands.

"Stop using that tired old anti-virus and try the new, improved approach! No more mistakes. No updates. Full protection!" Problem solved. Except in 2024 I don't think anyone would claim that malware is a thing of the past.

The industry has shifted to a point where the leading vendors have embraced advanced technologies to stay ahead of increasingly sophisticated threats. Traditional anti-virus relies solely (or mostly) on signature-based detection. That's not enough to defend against modern-day attacks like ransomware, file-less malware and zero-day exploits.

Next-generation is Now
Next-generation anti-virus is now the benchmark for the best security solutions. These systems go far beyond the old-fashioned model of looking for known malware signatures. Instead, they use a combination of machine learning, artificial intelligence and behavioural analysis to monitor how programs and processes behave in real-time.

This allows them to detect threats that have never been seen before, stopping malware based on its behaviour, not just its appearance.

These solutions can identify and block malicious activity at multiple stages of an attack, whether it's during initial infiltration, lateral movement within the network or data exfiltration.

Today's anti-malware technology is definitely better than it was, but it's not quite what was promised. All products still download chunky updates from the internet. Nothing can claim 100 percent protection with any credibility. And, if the problem of malware has been solved, why do large companies keep changing the products they use?

Tomorrow's World
All of the best endpoint protection products include the features that were once considered as 'next-generation'. It's why they all do well in the test you're reading, because we use real, new threats.

The products tested here don't rely solely on detecting known threats. They can determine an unknown threat from its behaviour and other similarities to known threats. When you dig into the details, check out the targeted attack results. These are new, never-before-seen files, delivered in a realistic way to the target.

'Next-generation' sounds current, rather than tired and old. In fact, it sounds futuristic! But when does it become outdated? If next-gen anti-virus has been around for nearly 10 years, does that mean it's next-gen anymore? What happens tomorrow? What do we call that?

Executive Summary

Product Names

It is good practice to stay up to date with the latest version of your chosen endpoint security product. We made best efforts to ensure that each product tested was the very latest version running with the most recent updates to give the best possible outcome.

For specific build numbers, see **Appendix E: Product Versions** on page 16.

Executive Summary

Products Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Broadcom Symantec Endpoint Security	100%	100%	100%
Kaspersky Endpoint Security	100%	100%	100%
Sophos Intercept X	99%	100%	100%
Microsoft Defender Antivirus (enterprise)	99%	100%	100%
Trellix Endpoint Security	99%	100%	99%
ESET Endpoint Security	99%	100%	99%
VIPRE Endpoint Security	98%	100%	99%
Fortinet FortiEDR	90%	100%	96%

● Products highlighted in green were the most accurate, scoring 85 per cent or more for Total Accuracy. Those in yellow scored less than 85 but 75 or more. Products shown in red scored less than 75 per cent.

For exact percentages, see **1.3 Total Accuracy Ratings** on page 9.

● **The endpoints were generally effective at handling general threats from cyber criminals ...**
All products were very capable of handling public email- and web-based threats such as those used by criminals to attack Windows PCs, tricking users into running malicious files or running scripts that download and run malicious files.

● **... but targeted attacks caused problems for some of the products.**
Seven of the eight products provided complete protection against the targeted attacks used in this test. While two products were only compromised by one or two attacks each, this is still a concerning result since it only takes one targeted attack to breach an organisation.

● **False positives were not an issue for the products.**
All of the products were perfectly good at correctly classifying legitimate applications and websites. None of them blocked or restricted access to these legitimate objects.

● **Which products were the most effective?**
Products from **Kaspersky**, **Broadcom**, **Sophos** and **Microsoft** produced extremely good results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites. All products performed well enough to achieve AAA awards.

Enterprise Endpoint Security Awards

The following products win SE Labs awards:

Broadcom Symantec Endpoint Security

Kaspersky Endpoint Security

Sophos Intercept X

Microsoft Defender Antivirus (enterprise)

Trellix Endpoint Security

ESET Endpoint Security

VIPRE Endpoint Security

Fortinet FortiEDR

SE LABS
AAA
JUL-SEPT 2024
ENTERPRISE ENDPOINT SECURITY

SE LABS PRESENTS

THE-C2

TUESDAY 25TH AND
WEDNESDAY 26TH MARCH 2025

Connecting business with cyber security

The-C2 is an exclusive, invite-only threat intelligence event that connects multinational business executives with the cutting edge of the cyber security industry. The event enables frank and open discussion of the developing digital threat landscape between global security leaders.

The-C2 is hosted by SE Labs, the world's leading security testing lab. Its unique position in the industry provides a route to understanding both the developing threat landscape and the evolving security measures for defending against attackers.

THE-C2.COM

Threat Responses

Full Attack Chain: Testing Every Layer of Detection and Protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means that, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection abilities. If the test concludes before any 'useful'

damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack Stages
The illustration (below) shows typical stages of an attack. In a test, each of these should be attempted to determine the security solution's effectiveness. This test's results record detection and protection for each of these stages.

We measure how a product responds to the first stages of the attack with a detection and/ or protection rating. Sometimes products allow threats to run yet still detect them. Other times they might allow the threat to run briefly before neutralising it.

Ideally, they detect and block the threat before it has a chance to run. Products may delete threats or automatically contain them in a 'quarantine' or other safe holding mechanism for later analysis.

Should the initial attack phase succeed, we then measure post-exploitation stages, which are represented by steps two through to seven below. We broadly categorise these stages as: Access (step 2); Action (step 3); Escalation (step 4); and Post-Escalation (steps 5-6).

In figure 1. you can see a typical attack running from start to end, through various 'hacking' activities. This can be classified as a fully successful breach.

In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 onwards.

It is possible for an attack to run in a different order with, for example, the attacker attempting to connect to other systems without needing to escalate privileges. However, it is common for password theft (see step 5) to occur before using stolen credentials to move further through the network.

How Hackers Progress

Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

1. Protection and Legitimate Handling Accuracy

1.1 Protection Details

These results break down how each product handled threats into some detail. You can see how many detected a threat and the levels of protection provided.
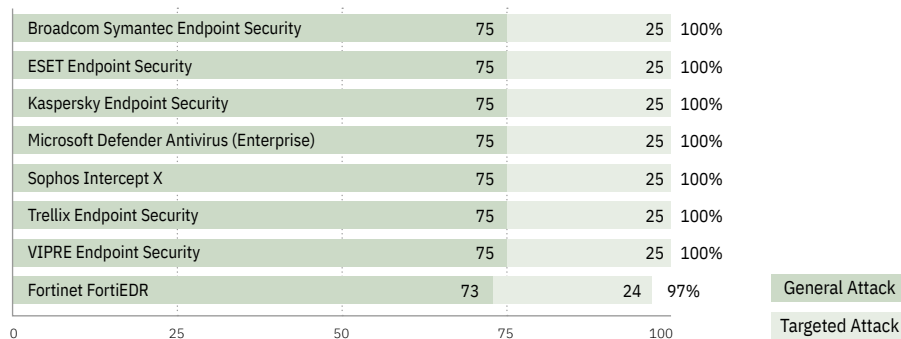
Products sometimes detect more threats than they protect against. This can happen when they recognise an element of the threat but aren't equipped to stop it. Products can also provide protection even if they don't detect certain threats. Some threats abort on detecting specific endpoint protection software.

Product	Detected	Blocked	Neutralised	Compromised	Protected
Broadcom Symantec Endpoint Security	100	100	0	0	100
Kaspersky Endpoint Security	100	100	0	0	100
Microsoft Defender Antivirus (enterprise)	99	99	1	0	100
Sophos Intercept X	100	98	2	0	100
Trellix Endpoint Security	100	98	2	0	100
VIPRE Endpoint Security	100	98	2	0	100
ESET Endpoint Security	100	97	3	0	100
Fortinet FortiEDR	98	87	10	3	97

● This data shows in detail how each product handled the threats used.

1.2 Attack Types

The graph shows how each product protected against the different types of attacks used in the test.

Broadcom Symantec Endpoint Security	75	25	100%
ESET Endpoint Security	75	25	100%
Kaspersky Endpoint Security	75	25	100%
Microsoft Defender Antivirus (Enterprise)	75	25	100%
Sophos Intercept X	75	25	100%
Trellix Endpoint Security	75	25	100%
VIPRE Endpoint Security	75	25	100%
Fortinet FortiEDR	73	24	97%

0   25   50   75   100
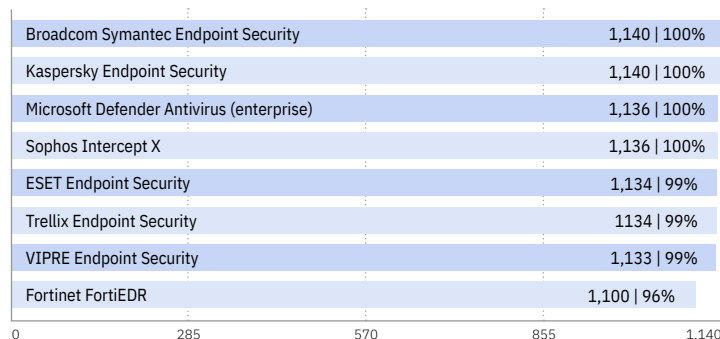
General Attack
Targeted Attack

1.3. Total Accuracy Ratings

Judging the effectiveness of an endpoint security product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier we've combined all the different results from this report into one easy-to-understand graph.

The graph takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

Not all protections, or detections for that matter, are equal. A product might completely block a URL, which stops the threat before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any further code to the target.

Broadcom Symantec Endpoint Security	1,140 | 100%
Kaspersky Endpoint Security	1,140 | 100%
Microsoft Defender Antivirus (enterprise)	1,136 | 100%
Sophos Intercept X	1,136 | 100%
ESET Endpoint Security	1,134 | 99%
Trellix Endpoint Security	1134 | 99%
VIPRE Endpoint Security	1,133 | 99%
Fortinet FortiEDR	1,100 | 96%

0   285   570   855   1,140

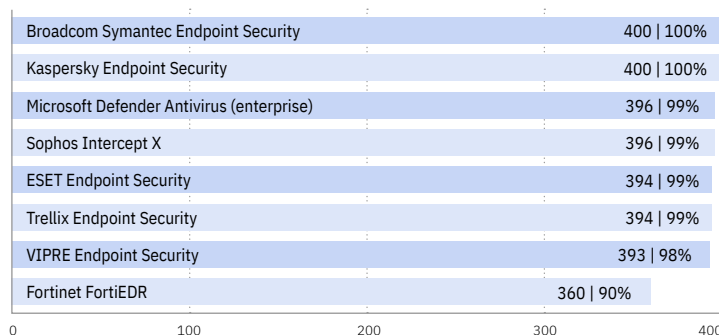● Total Accuracy Ratings combine protection and false positives

● Categorising how a product handles legitimate objects is complex, and you can find out how we do it in **Legitimate Accuracy Ratings** on page 10.

In another case malware might run on the target for a short while before its behaviour is detected and its code is deleted or moved to a safe 'quarantine' area for future analysis. We take these outcomes into account when attributing points that form final ratings.

For example, a product that completely blocks a threat is rated more highly than one that allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

1.4 Protection Accuracy

To understand how we calculate these ratings, see **Appendix A: Protection Ratings** on page 12.

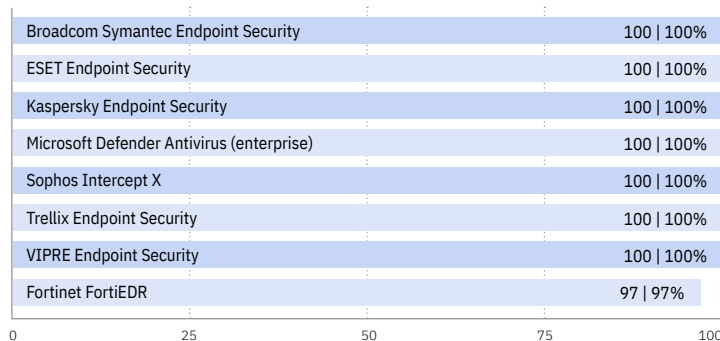|	
Broadcom Symantec Endpoint Security	400 | 100%
Kaspersky Endpoint Security	400 | 100%
Microsoft Defender Antivirus (enterprise)	396 | 99%
Sophos Intercept X	396 | 99%
ESET Endpoint Security	394 | 99%
Trellix Endpoint Security	394 | 99%
VIPRE Endpoint Security	393 | 98%
Fortinet FortiEDR	360 | 90%

0   100   200   300   400

● Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

Average 97%

1.5 Protection Scores

This graph shows the overall level of protection, making no distinction between neutralised and blocked incidents.

For each product we add Blocked and Neutralised cases together to make one simple tally.
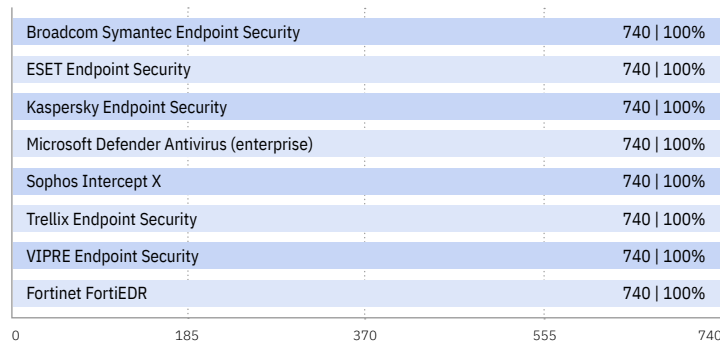
Broadcom Symantec Endpoint Security	100 | 100%
ESET Endpoint Security	100 | 100%
Kaspersky Endpoint Security	100 | 100%
Microsoft Defender Antivirus (enterprise)	100 | 100%
Sophos Intercept X	100 | 100%
Trellix Endpoint Security	100 | 100%
VIPRE Endpoint Security	100 | 100%
Fortinet FortiEDR	97 | 97%

0   25   50   75   100

● Protection Scores are a simple count of how many times a product protected the system.

1.6 Legitimate Accuracy Ratings

These ratings indicate how accurately the products classify legitimate applications and URLs, while also taking into account the interactions that each product has with the user. Ideally a product will either not classify a legitimate object or will classify it as safe. In neither case should it bother the user.

We also take into account the prevalence (popularity) of the applications and websites used in this part of the test, applying stricter penalties for when products misclassify very popular software and sites.

To understand how we calculate these ratings, see **Accuracy Ratings** on page 14.

Broadcom Symantec Endpoint Security	740 | 100%
ESET Endpoint Security	740 | 100%
Kaspersky Endpoint Security	740 | 100%
Microsoft Defender Antivirus (enterprise)	740 | 100%
Sophos Intercept X	740 | 100%
Trellix Endpoint Security	740 | 100%
VIPRE Endpoint Security	740 | 100%
Fortinet FortiEDR	740 | 100%

0   185   370   555   740

● Legitimate Accuracy Ratings can indicate how well a vendor has tuned its detection engine.

2. Conclusion

Attacks in this test included threats that affect the wider public and more closely targeted individuals and organisations. You could say that we tested the products with 'public' malware and full-on hacking attacks.

We introduced the threats in a realistic way such that threats seen in the wild on websites were downloaded from those same websites, while threats caught sending email were delivered to our target systems as emails.

All the products tested are well-known and should do well in this test. While we do 'create' threats by using publicly available free hacking tools, we do not write unique malware so there is no technical reason why any vendor being tested should do poorly.

The results were generally strong, particularly in the way that the products handled public threats. These are threats that are live on the internet on the day that the products are tested. Excellent results from all of the products indicate both familiarity with common threats and frequent updates to keep databases current.

Seven of the eight products stopped all of the attacks this quarter. Two, belonging to **Kaspersky** and **Broadcom**, achieved 100% Protection Accuracy Ratings by being quick to block any detected intrusion. By and large, products from **ESET**, **Sophos**, **Microsoft**, **Trellix** and **VIPRE** did the same. There were a very few instances though when some malicious files ran briefly before being neutralised. Sometimes one or two artifacts of the infection would remain in the system despite complete remediation.

CrowdStrike requested that we remove its results from this report. The company provided this statement: "**CrowdStrike** remains dedicated to delivering exceptional protection and services to our customers. Our response to a recent incident required us to focus on prioritizing customer needs, which led to an unintended impact on our SE Labs evaluation.

We are committed to transparency, and the value independent testing provides; we look forward to demonstrating the full capabilities of our technology moving forward."

Fortinet FortiEDR was compromised by two web download attacks and one targeted attack. However, it prevented the post-escalation attempt at running ransomware but missed the initial malicious file that established a remote connection to a C2 server.

No mistakes were made by any of the products in the handling of the legitimate applications and websites.

All the products in this test win AAA awards by virtue of scoring Total Accuracy Ratings of either 100% or in the very high 90s. The strongest, from **Kaspersky**, **Broadcom**, **Sophos** and **Microsoft** scored 100% Total Accuracy Ratings. Those from **Trellix**, **ESET** and **VIPRE** were only a single percentage point shy of a perfect Total Accuracy score. **Fortinet FortiEDR's** scores was also in the high 90s.

Appendices

Appendix A: Protection Ratings

The results below indicate how effectively the products dealt with threats. Points are earned for detecting the threat and for either blocking or neutralising it.

■ **Detected (+1)** If the product detects the threat with any degree of useful information, we award it one point.

■ **Blocked (+2)** Threats that are disallowed from even starting their malicious activities are blocked. Blocking products score two points.

■ **Complete Remediation (+1)** If, in addition to neutralising a threat, the product removes all significant traces of the attack, it gains an additional one point.

■ **Neutralised (+1)** Products that kill all running malicious processes 'neutralise' the threat and win one point.

■ **Persistent Neutralisation (-2)** This result occurs when a product continually blocks a persistent threat from achieving its aim, while not removing it from the system.

■ **Compromised (-5)** If the threat compromises the system, the product loses five points. This loss may

be reduced to four points if it manages to detect the threat (see Detected, above), as this at least alerts the user, who may now take steps to secure the system.

Rating Calculations

We calculate the protection ratings using the following formula:

Protection Rating =
(1x number of Detected) +
(2x number of Blocked) +
(1x number of Neutralised) +
(1x number of Complete Remediation) +
(-5x number of Compromised)

The 'Complete Remediation' number relates to cases of neutralisation in which all significant traces of the attack were removed from the target.

These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how seriously you treat a 'Compromise' or 'Neutralisation without complete remediation'. If you want to create your own rating system, you can use the raw data from **1.1 Protection Details** on page 8 to roll your own set of personalised ratings.

Targeted Attack Scoring

The following scores apply only to targeted attacks and are cumulative, ranging from -1 to -5.

■ **Access (-1)** If any command that yields information about the target system is successful this score is applied. Examples of successful commands include listing current running processes, exploring the file system and so on. If the first command is attempted and the session is terminated by the product without the command being successful the score of Neutralised (see above) will be applied.

■ **Action (-1)** If the attacker is able to exfiltrate a document from the target's Desktop of the currently logged in user then an 'action' has been successfully taken.

■ **Escalation (-2)** The attacker attempts to escalate privileges to NT Authority/System. If successful, an additional two points are deducted.

■ **Post-Escalation Action (-1)** After escalation the attacker attempts actions that rely on escalated privileges. These include attempting to steal credentials, modifying the file system and recording keystrokes. If any of these actions are successful then a further penalty of one point deduction is applied.

Appendix B: Legitimate Interaction Ratings

It's crucial that anti-malware endpoint products not only stop – or at least detect – threats, but that they allow legitimate applications to install and run without misclassifying them as malware. Such an error is known as a 'false positive' (FP).

In reality, genuine FPs are quite rare in testing. In our experience it is unusual for a legitimate application to be classified as 'malware'. More often it will be classified as 'unknown', 'suspicious' or 'unwanted' (or terms that mean much the same thing).

We use a subtle system of rating an endpoint's approach to legitimate objects, which takes into account how it classifies the application and how it presents that information to the user. Sometimes

the endpoint software will pass the buck and demand that the user decide if the application is safe or not. In such cases the product may make a recommendation to allow or block. In other cases, the product will make no recommendation, which is possibly even less helpful.

If a product allows an application to install and run with no user interaction, or with simply a brief notification that the application is likely to be safe, it has achieved an optimum result. Anything else is a Non-Optimal Classification/Action (NOCA). We think that measuring NOCAs is more useful than counting the rarer FPs.

Prevalence Ratings

There is a significant difference between an

Legitimate Software Prevalence Rating Modifiers

Very High Impact	5
High Impact	4
Medium Impact	3
Low Impact	2
Very Low Impact	1

endpoint product blocking a popular application such as the latest version of Microsoft Word and condemning a rare Iranian dating toolbar for Internet Explorer 6. One is very popular all over the world and its detection as malware (or something less serious but still suspicious) is a big deal. Conversely, the outdated toolbar won't have had a comparably large user base even when it was new. Detecting this application as malware may be wrong, but it is less impactful in the overall scheme of things.

With this in mind, we collected applications of varying popularity and sorted them into five separate categories, as follows:

1. Very High Impact
2. High Impact
3. Medium Impact
4. Low Impact
5. Very Low Impact

	None (allowed)	Click to Allow (default allow)	Click to Allow/ Block (no recommendation)	Click to Block (default block)	None (blocked)	
Safe	2	1.5	1			A
Unknown	2	1	0.5	0	-0.5	B
Not Classified	2	0.5	0	-0.5	-1	C
Suspicious	0.5	0	-0.5	-1	-1.5	D
Unwanted	0	-0.5	1	-1.5	-2	E
Malicious				2	-2	F
	1	2	3	4	5	

Incorrectly handling any legitimate application will invoke penalties, but classifying Microsoft Word as malware and blocking it without any way for the user to override this will bring far greater penalties than doing the same for an ancient niche toolbar. In order to calculate these relative penalties, we assigned each impact category with a rating modifier, as shown in the table above.

Applications were downloaded and installed during the test, but third-party download sites were avoided and original developers' URLs were used where possible. Download sites will sometimes bundle additional components into applications' install files, which may correctly cause anti-malware products to flag adware. We remove adware from the test set because it is often unclear how desirable this type of code is.

The prevalence for each application and URL is estimated using metrics such as third-party download sites and the data from Tranco.com's global traffic ranking system.

Accuracy Ratings

We calculate legitimate software accuracy ratings by multiplying together the interaction and prevalence ratings for each download and installation:

Accuracy rating = Interaction rating x Prevalence rating

If a product allowed one legitimate, Medium impact application to install with zero interaction with the user, then its Accuracy rating would be calculated like this:

Accuracy rating = 2 x 3 = 6

This same calculation is made for each legitimate application/site in the test and the results are summed and used to populate the graph and table shown under **Legitimate Accuracy Ratings** on page 10.

Distribution of Impact Categories

Endpoint products that were most accurate in handling legitimate objects achieved the highest ratings. If all objects were of the highest prevalence, the maximum possible rating would be 1,000 (100 incidents x (2 interaction rating x 5 prevalence rating)).

In this test there was a range of applications with different levels of prevalence. The table below shows the frequency:

Legitimate Interaction Ratings

Product	None (allowed)	None (blocked)
Broadcom Symantec Endpoint Security	100	0
ESET Endpoint Security	100	0
Fortinet FortiEDR	100	0
Kaspersky Endpoint Security	100	0
Microsoft Defender Antivirus (Enterprise)	100	0
Sophos Intercept X	100	0
Trellix Endpoint Security	100	0
VIPRE Endpoint Security	100	0

● **Products that do not bother users and classify most applications correctly earn more points than those that ask questions and condemn legitimate applications.**

Legitimate Software Category Frequency

Prevalence Rating	Frequency
Very High Impact	32
High Impact	32
Medium Impact	17
Low Impact	12
Very Low Impact	7

Appendix C: Terms Used

Compromised The attack succeeded, resulting in malware running unhindered on the target. In the case of a targeted attack, the attacker was able to take remote control of the system and carry out a variety of tasks without hindrance.

Blocked The attack was prevented from making any changes to the target.

False positive When a security product misclassifies a legitimate application or website as being malicious, it generates a 'false positive'.

Neutralised The exploit or malware payload ran on the target but was subsequently removed.

Complete Remediation If a security product removes all significant traces of an attack, it has achieved complete remediation.

Target The test system that is protected by a security product.

Threat A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.

Update Security vendors provide information to their products in an effort to keep abreast of the latest threats. These updates may be downloaded in bulk as one or more files, or requested individually and live over the internet.

Appendix D: FAQs

Q **What is a partner organisation? Can I become one to gain access to the threat data used in your tests?**

A Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

Q **I am a security vendor and you tested my product without permission. May I access the threat data to verify that your results are accurate?**

A We are willing to share a certain level of test data with non-partner participants for free. The intention is to provide sufficient data to demonstrate that the results are accurate. For more in-depth data suitable for product improvement purposes we recommend becoming a partner.

A **full methodology** for this test is available from our website.

- The test was conducted between 4th July and 6th September 2024.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Targeted attacks were selected and verified by SE Labs.
- Malicious emails, URLs, attachments and legitimate messages were independently located and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.

Appendix E: Product Versions

The table below shows the service's name as it was being marketed at the time of the test.

Vendor	Product	Build Version (start)	Build Version (end)
Broadcom	Symantec Endpoint Security	Version 14: (14.3RU9) Build: 11216 (14.3.11216.9000)	Version 14: (14.3RU9) Build: 11216 (14.3.11216.9000)
ESET	Endpoint Security	11.0.2044.0	11.0.2044.0
Fortinet	FortiEDR	5.2.3.0089	5.2.3.0089
Kaspersky	Endpoint Security	12.3.0.493 AES256	12.3.0.493 AES256
Microsoft	Defender Antivirus (enterprise)	Antimalware Client Version: 4.18.24050.7 Engine Version: 1.1.24050.5 Antivirus Version: 1.413.630.0 Anti-spyware Version: 1.413.630.0	Antimalware Client Version: 4.18.24070.5 Engine Version: 1.1.24070.3 Antivirus Version: 1.417.641.0 Anti-spyware Version: 1.417.641.0
Sophos	Intercept X	Core Agent: 2024.2.2.1.0 Sophos Intercept: 2024.1.1.1.0 Device Encryption: 2024.2.0.49.0	Core Agent: 2024.2.3.4.0, Sophos Intercept: 2024.1.2.1.0 Device Encryption: 2024.2.0.49.0
Trellix	Endpoint Security	Trellix Endpoint Security Platform Version: 10.7.0.6809 Adaptive Threat Protection Version: 10.7.0.6887 Threat Prevention Version: 10.7.0.6711 Firewall Version: 10.7.0.6486 Web Control Version: 10.7.0.6126	Trellix Endpoint Security Platform Version: 10.7.0.6809 Adaptive Threat Protection Version: 10.7.0.6887 Threat Prevention Version: 10.7.0.6711 Firewall Version: 10.7.0.6486 Web Control Version: 10.7.0.6126
VIPRE	Endpoint Security	109278 - 7.97133	109459 - 7.97480

SE LABS