SE LABS ®

EPS
PROTECTION

Security Evaluation Test Report
Home Anti-Malware

ONLINE REPORT

JULY-SEPTEMBER 2026

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

Introduction	04
Executive Summary	05
Security Evaluation EPS Protection Home Awards	06
Threat Responses	07
1. Protection and Legitimate Handling Accuracy	08
1.1 Protection Details	08
1.2 Attack Types	08
1.3 Total Accuracy Ratings	09
1.4 Protection Accuracy	09
1.5 Protection Scores	10
1.6 Legitimate Accuracy Ratings	10
2. Conclusion	11
Appendices	12
Appendix A: Protection Ratings	12
Appendix B: Legitimate Interaction Ratings	13
Appendix C: Terms Used	15
Appendix D: FAQs	15
Appendix E: Product Versions	16

Document version 1.0 Written 2nd November 2026

SE LABS

Management
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Technical Director Thomas Bean

Testing Team
Nikki Albesa
Daniel Botez
Solandra Brewster
Billy Coyne
Jarred Earlington
Gia Gorbold
Anila Johny
Cameron Love
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Enejda Torba

Marketing
Sara Claridge
Isobel Edwards
Tessa Welsh

Publication
Rahat Hussain
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

Website selabs.uk
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog https://selabs.uk/blog/
Post SE Labs Ltd,
55A High Street,
Wimbledon,
SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2022 certified and BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

amtso
CONFIRMED COMPLIANT

© 2026 SE Labs Ltd



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.

Testing the hard way

Anything less is unacceptable

SE Labs has been testing anti-malware products for a decade and, despite the chaos caused by cyber attacks over that time, one thing has remained constant. The way we test is still the most robust, consistent and accurate available. A bold claim! How can we be sure?

Our approach has always been to assume nothing about how attackers and defenders will behave. We don't decide how a product should work, and we don't guess how attackers will operate. We built a way of testing that takes a completely unbiased, evidence-based view of how systems react to attacks. This has proved to be solid over the last ten years. When products change their approach, such as adopting AI, the testing still works. When attackers use new approaches (or, more likely, readopt old ones), we copy them and the testing still works.

It is tempting to get clever in the name of efficiency. It might be cheaper to heavily automate the tests, pulling in random attacks from the internet and pushing them onto targets without human intervention. The advent of competent AI would make this even easier. But, in our experience of testing and talking to other testers (and the businesses that they test), the more 'clever' you get with testing, the more you run into unforeseen problems. And if these problems compromise the accuracy and usefulness of the test, then they are unacceptable.

Over the last 10 years the SE Labs testing team has stuck to its core principles of testing with real humans, who monitor the threat landscape and ensure that the attacks used in the tests are fully comprehensive, realistic and viable. This approach ensures that the report you are about to read gives you the strongest evidence to help when you come to invest in a cyber security product.

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.

Products Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
McAfee Total Protection	100%	100%	100%
Kaspersky Premium	100%	100%	100%
Sophos Home Premium	100%	100%	100%
Avast Free Antivirus	98%	100%	99%
Microsoft Defender Antivirus (consumer)	97%	100%	99%
NortonLifeLock Norton360	95%	100%	98%
Panda Dome	95%	100%	98%
Webroot Antivirus	94%	100%	97%
Malwarebytes Premium	98%	92%	94%
Scanguard Essential Antivirus	83%	100%	94%
TotalAV Premium	81%	100%	93%

- 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 public threats from cyber criminals...**

However, only 4 out 11 products handled email- and web-based threats perfectly. The others missed anywhere from a single to several of the kind of public threat that criminals use to attack Windows PCs, tricking users into running malicious files or running scripts that download and run malicious files.

- **...and targeted attacks likewise caused problems for some of the products.**

Less than half of the products provided completed protection against the targeted attacks used in this test. Some were unable to prevent only one such attack, others missed as many as three. This is a concerning result since it only takes a single targeted attack to breach an organisation.

- **False positives were not an issue for the products.**

Almost all of the products were perfectly good at correctly classifying legitimate applications and websites. Only **Malwarebytes Premium** blocked or restricted access to a few legitimate objects.

- **Which products were the most effective?**

The products from **McAfee**, **Sophos** and **Kaspersky** produced the best results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites. Products from **Avast**, **Microsoft**, **Norton**, **Panda** and **Webroot** that achieved Total Accuracy Ratings in the high 90s also received AAA awards. AA awardees **Malwarebytes Premium**, **Scanguard Essential Antivirus** and **TotalAV Premium** also achieved Total Accuracy Ratings in the 90s.

Security Evaluation
EPS Protection Home Awards

The following products win SE Labs awards:

SE LABS
AAA
October 2026
Security Evaluation
Home
Anti-Malware

McAfee Total Protection
Kaspersky Premium
Sophos Home Premium
Avast Free Antivirus
Microsoft Defender Antivirus (consumer)
NortonLifeLock Norton360
Panda Dome
Webroot Antivirus

SE LABS
AA
October 2026
Security Evaluation
Home
Anti-Malware

Malwarebytes Premium
Scanguard Essential Antivirus
TotalAV Premium



SE LABS
WORKSHOP
2027

Beyond the test results

Meet the people behind SE Labs testing, discover what our research is revealing and join the conversation about what security testing should tackle next.

17th June 2027 | Wimbledon, London

For security vendors and enterprise security leaders. By invitation only.

Request an invitation:
workshop@selabs.uk

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.

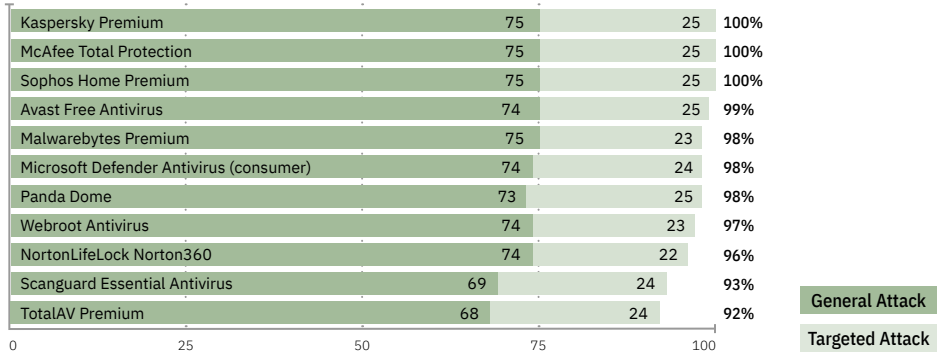
Products sometimes detect more threats than they protect against. This can happen when they recognise an element of the threat but aren't equipped to stop it. Products can also provide protection even if they don't detect certain threats. Some threats abort on detecting specific endpoint protection software.

Product	Detected	Blocked	Neutralised	Compromised	Protected
McAfee Total Protection	100	100	0	0	100
Sophos Home Premium	100	100	0	0	100
Kaspersky Premium	100	99	1	0	100
Avast Free Antivirus	100	99	0	1	99
Malwarebytes Premium	99	98	0	2	98
Microsoft Defender Antivirus (consumer)	99	98	0	2	98
Panda Dome	98	97	1	2	98
Webroot Antivirus	98	96	1	3	97
NortonLifeLock Norton360	100	96	0	4	96
Scanguard Essential Antivirus	93	87	6	7	93
TotalAV Premium	93	86	6	8	92

- **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.

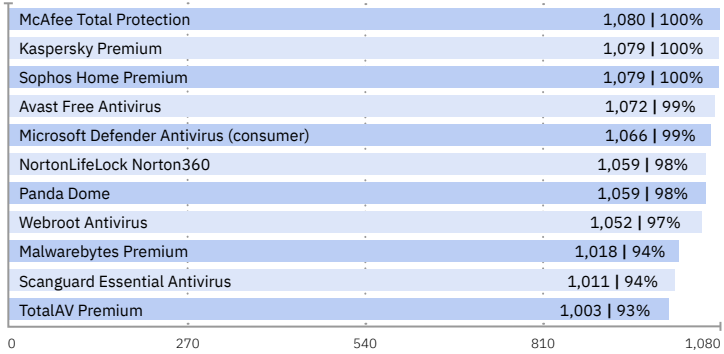


1.3. Total Accuracy Ratings

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.



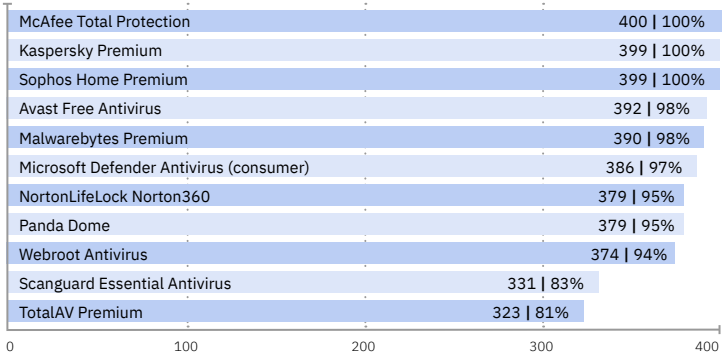
- Categorising how a product handles legitimate objects is complex, and you can find out how we do it in **Legitimate Accuracy Ratings** on page 10.
- Total Accuracy Ratings combine protection and false positives

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.



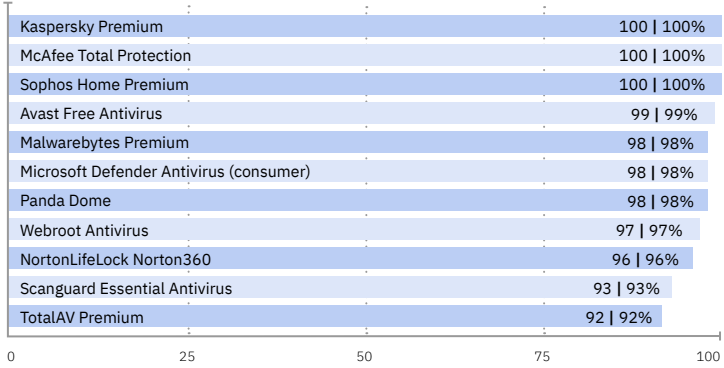
- Protection Accuracy Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

Average 95%

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.



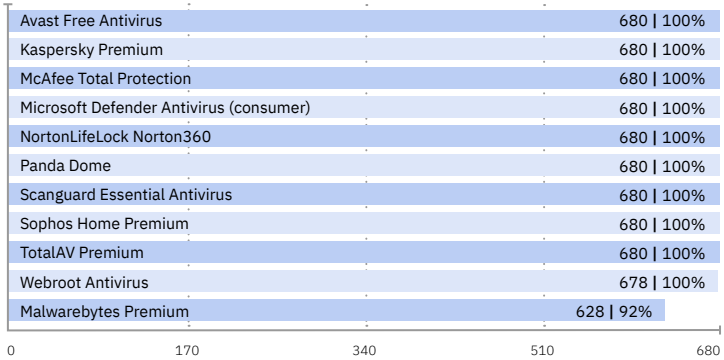
- **Protection Scores are a simple count of how many times a product protected the system.**

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.



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

2. Conclusion

Attacks in this test include 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 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 in the way the products handled both public threats and targeted attacks, with most of the products stopping most of the attacks. Although only **Sophos Home Premium**, **McAfee Total Protection** and **Kaspersky Premium** achieved a 100% Protection Accuracy rating, the five other AAA awardees posted scores in the high 90s. These were **Avast Free Antivirus**, **Microsoft Defender Antivirus (consumer)**, **Panda Dome**, **NortonLifeLock**, and **Webroot Antivirus**.

This quarter, less than half of the endpoints detected against 100% of the public malware used in test. Public malware test a product's familiarity with common threats and its ability to keep its databases current since the samples are downloaded from the Internet on the day that the products are tested. Five products missed only one or two of the public threats, while **Scanguard Essential Antivirus** missed six and **TotalAV Premium** missed seven.

This overall result is concerning since the typical user for home security products is more vulnerable to the widespread threats from the web. Unlike organisations that employ security professionals who can mitigate the damage caused by a public threat, the home user often relies only on endpoint protection.

More than half the products also missed targeted attacks this quarter. Those from **Microsoft**, **Scanguard** and **TotalAV** only missed one targeted attack each, while **Malwarebytes Premium** and **Webroot Antivirus** missed two and **NortonLifeLock Norton360** missed three.

In most of these cases, the targeted attacks progressed unimpeded all the way up to the post-escalation stage, providing the attacker with access and control over the entire system. In a few instances, however, late detection could prompt rear guard action. **Microsoft Defender Antivirus (consumer)** and **NortonLifeLock Norton360** tried to prevent escalation and remove the initial malicious file.

All but one of the products posted 100% Legitimate Accuracy Ratings. **Malwarebytes Premium's** overly strict treatment of some legitimate files and one website pulled down its Total Accuracy score, making it miss an AAA rating by a sliver.

In contrast, the perfect Legitimate Accuracy scores of the products from **Avast**, **Microsoft**, **Norton**, **Panda** and **Webroot** allowed them to offset the few points that were shaved off from their Protection Accuracy Ratings. They, as well as the strongest performers **McAfee**, **Sophos** and **Kaspersky** are AAA Awardees. Like **Malwarebytes Premium**, the products from **Scanguard** and **TotalAV** won AA awards for achieving Total Accuracy Ratings in the 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 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	

Legitimate Software Prevalence Rating Modifiers

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

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)	Click to allow/block (No Recommendation)	None (blocked)
Avast Free Antivirus	100	0	0
Kaspersky Premium	100	0	0
McAfee Total Protection	100	0	0
Microsoft Defender Antivirus (consumer)	100	0	0
NortonLifeLock Norton360	100	0	0
Panda Dome	100	0	0
Scanguard Essential Antivirus	100	0	0
Sophos Home Premium	100	0	0
TotalAV Premium	100	0	0
Webroot Antivirus	99	1	0
Malwarebytes Premium	97	3	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
High Impact	40
Medium Impact	40
Low Impact	20

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 13th July and 9th September 2026.
- 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)
Avast	Free Antivirus	Program Version: 26.3.10886g (Build 26.3.10886.973) Virus Definitions Version: 260331-0 UI version: 1.0.858	Program Version: 26.6.11050g (build 26.6.11050.0) Virus Definitions Version: 260624-2
Kaspersky	Premium	21.24.8.522	21.25.7.504(a)
Malwarebytes	Premium	Product Version: 5.5.3.246 Update Package Version: 1.0.108672 Component Package Version: 153.1.5565	Product Version: 5.5.7.255 Update Package Version: 1.0.111361 Component Package Version: 157.0.5633
McAfee	Total Protection	Version: 1.37.173.1 Antivirus Build: 1.37.144.0	Version: 1.37.173.1 Antivirus Build: 1.37.144.0
Microsoft	Defender Antivirus (consumer)	Antimalware Client Version: 4.18.26020.6 Engine Version: 1.1.26020.3 Antivirus Version: 1.447.231.0 Antispyware Version: 1.447.231.0	Antimalware Client Version: 4.18.26050.15 Engine Version: 1.1.26050.11 Antivirus Version: 1.453.259.0 Antispyware Version: 1.453.259.0
NortonLifeLock	Norton360	Program Version: 26.3.10886 (build 26.3.10886.0) Virus Definitions Version: 260331-0	Program Version: 26.6.11050 (build 26.6.11050.0) Virus Definitions version: 260624-2
Panda	Dome	23.0.0	23.0.0
Scanguard	Essential Antivirus	ScanGuard v6.6.51 Virus Definition: 8.20.74.242 Remediation Definition Version: 1.0.2512.2988	ScanGuard: v6.6.51 Virus Definition: 8.21.2.54 Remediation Definition Version: 1.0.2512.2988
Sophos	Home Premium	2024.3.3.1.0	2025.2.3.67.0
TotalAV	Premium	App Version: 6.6.51 Antivirus Engine Version: 1.0.2601.7834 Remediation Definitions Version: 1.0.2512.2988 Virus Definitions Version: 8.20.75.102	App Version: 6.6.51 Antivirus Engine Version: 1.0.2601.7834 Remediation Definitions Version: 1.0.2512.2988 Virus Definitions Version: 8.21.2.54
Webroot	Antivirus	9.0.42.42	9.0.44.46

SE LABS

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising from this report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.