SE Labs
INTELLIGENCE-LED TESTING

EPS PROTECTION

Endpoint Security

Home

Apr - Jun 2024

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 18th July 2024

Introduction

Is AI able to protect your Windows systems?
And are attackers using it to breach your network?

Artificial Intelligence is ruling the stock market and may be on the verge of ruling the world if you believe the business influencers. If it's as powerful as some say, surely it should be able to protect our computer systems from hackers?

The products in this test almost certainly rely on AI-related technologies to detect and protect against attacks. These technologies have been running in the background for about 20 years. We can argue that not only does anti-virus/ endpoint protection use AI, but it's been doing so for many years, and certainly before Cylance claimed to be the first.

But I did something sneaky there. I slid in the word '-related'. Because when people talk about ChatGPT and other popular 'AI' tools, they are usually talking about something else. They are amazed by the utility of Machine Learning (ML) systems, which appear to be able to mimic human thought in a rather magical way.

ML is a subset of AI, so it's related to AI but it isn't capable of thought. It cannot reason, in the way that we hope future AI systems will. It is great at recognising patterns, but it can make mistakes and it's not very good at understanding why it makes those mistakes.

As I wrote this introduction, I asked ChatGPT for a fun fact about SE Labs. It claimed we had run a cyber security 'bake-off' that involved employees

baking "virus-shaped cupcakes [and] firewall-layered cakes." That sounds fun, and maybe we should do it, but we haven't, so it's not a fact. Fun or otherwise.

(I corrected ChatGPT, which responded, "You're right, I made that up in an attempt to be fun and creative." Maybe tomorrow's robot overlords will be "fun and creative" and it won't be so bad if they take over.)

Being able to match patterns is incredibly useful for cyber security tools, because attackers behave in largely similar ways, with small variations. ML can often detect new variations. Attackers can use ML, as indeed does SE Labs when creating some new threats, to try to evade detection. It's a cat-and-mouse game, with both sides using computer brainpower to detect or escape detection.

See how well ML and other detection technologies worked for the security companies involved in this test.

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**.

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 C: Product Versions** on page 19.

Executive Summary			
Products Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Avast Free Antivirus	100%	100%	100%
Kaspersky Plus	100%	100%	100%
McAfee Total Protection	100%	100%	100%
Microsoft Defender Antivirus (consumer)	100%	100%	100%
Sophos Home Premium	100%	100%	100%
NortonLifeLock Norton360	97%	100%	99%
Webroot Antivirus	95%	100%	98%
Panda Free Antivirus	83%	97%	92%
Comodo Antivirus	76%	98%	90%

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. Total Accuracy Ratings** on page 6.

● **The products were 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. However, one product missed one general attack and another missed four.

● **… but targeted attacks caused problems for some of the products.**
Only five of the nine products provided complete protection against the targeted attacks used in this test. The number of missed attacks ranged from one to four for the rest of the products. It only takes one targeted attack to breach an organisation, so this is a concerning result.

● **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 two products blocked or restricted access to a couple of legitimate applications.

● **Which products were the most effective?**
Products from **Microsoft**, **Kaspersky**, **Avast**, **Sophos** and **McAfee** 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, except those from **Panda** and **Comodo**, performed well enough to achieve AAA awards.

1. 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 below 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. 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.

Categorising how a product handles legitimate objects is complex, and you can find out how we do it in **6. Legitimate Software Ratings** on page 14.

Total Accuracy Ratings

Product	Total Accuracy Rating	Total Accuracy (%)	Award
Avast Free Antivirus	1,140	100%	AAA
Kaspersky Plus	1,140	100%	AAA
Microsoft Defender Antivirus (consumer)	1,140	100%	AAA
Sophos Home Premium	1,138	100%	AAA
McAfee Total Protection	1,136.5	100%	AAA
NortonLifeLock Norton360	1,127	99%	AAA
Webroot Antivirus	1,118	98%	AAA
Panda Free Antivirus	1,049	92%	AA
Comodo Antivirus	1,028	90%	AA

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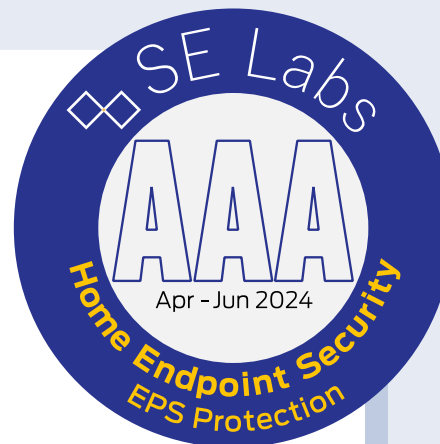Comodo Antivirus

0   285   570   855   1,140
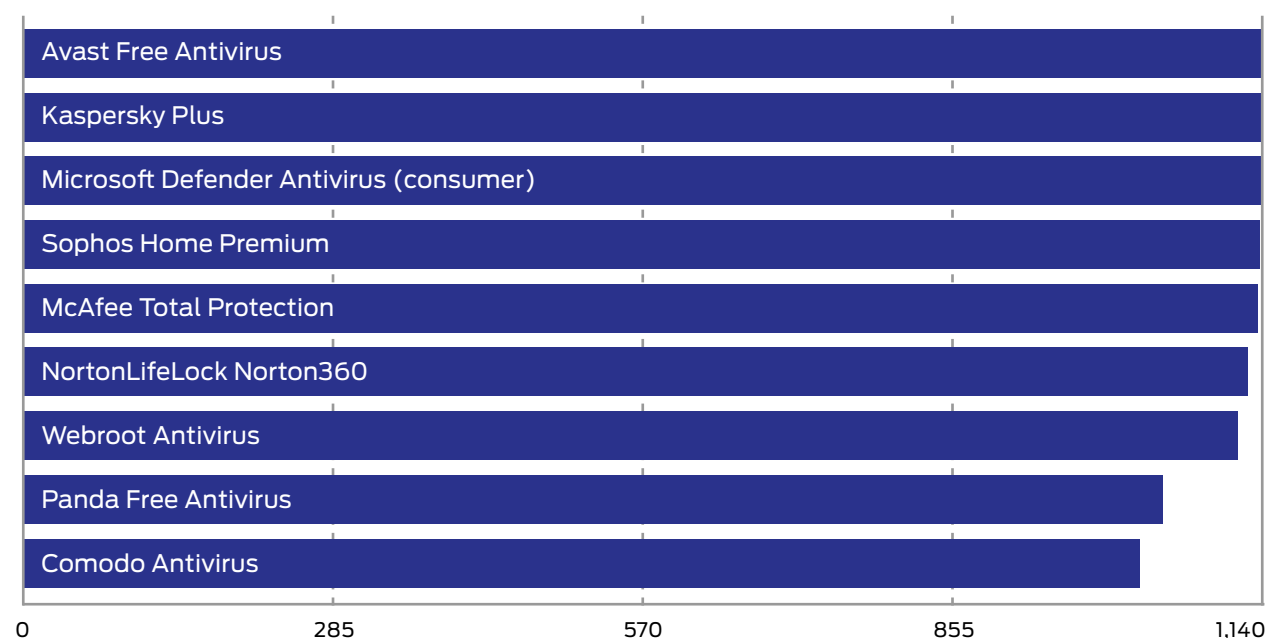
Total Accuracy Ratings combine protection and false positives.

Home Endpoint Security Awards

The following products win SE Labs awards:

- **Avast** Free Antivirus

- **Kaspersky** Plus

- **Microsoft** Defender Antivirus (consumer)

- **Sophos** Home Premium

- **McAfee** Total Protection

- **NortonLifeLock** Norton360

- **Webroot** Antivirus

SE Labs
AAA
Apr – Jun 2024
Home Endpoint Security
EPS Protection

- **Panda** Free Antivirus

- **Comodo** Antivirus

SE Labs
AA
Apr – Jun 2024
Home Endpoint Security
EPS Protection

2. 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, 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 some typical stages of an attack. In a test each of these should be

Attack Chain: 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.
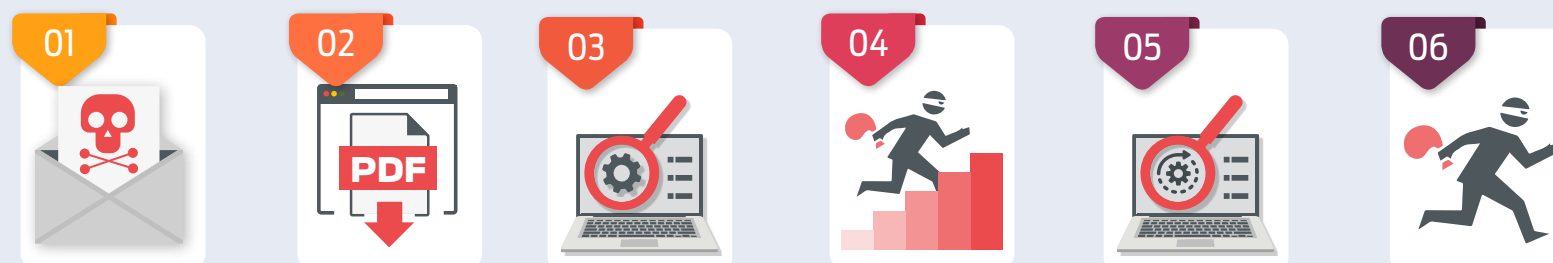
Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.
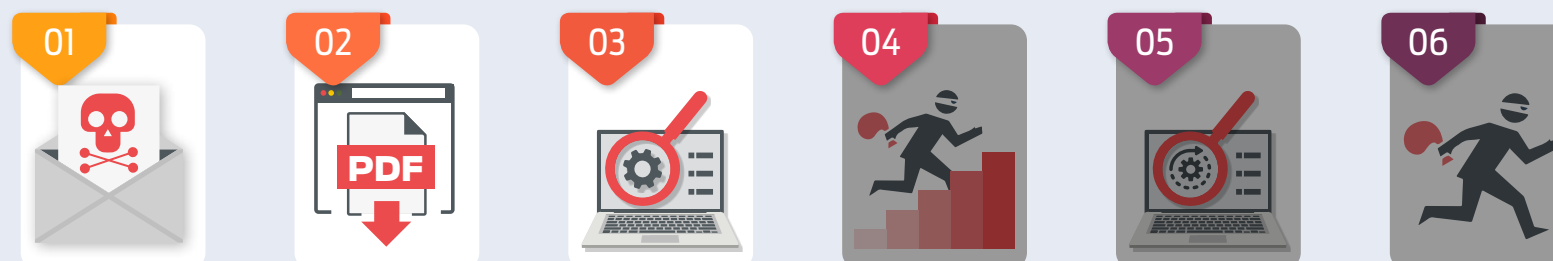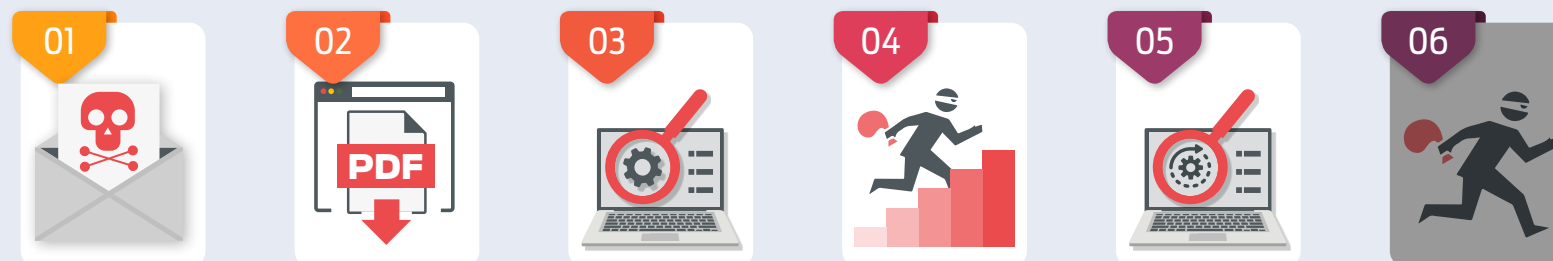
Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

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 but 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 (step 5).

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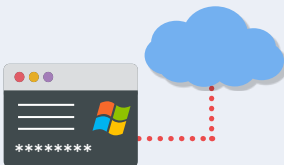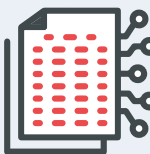
In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

It is possible that attackers will not cause noticeable damage during an attack. It may be that their goal is persistent presence on the

systems to monitor for activities, slowly steal information and other more subtle missions.

In figure 3. the attacker has managed to progress as far as stage five. This means that the system has been seriously compromised. The attacker has a high level of access and has stolen passwords. However, attempts to exfiltrate data from the target were blocked, as were attempts to damage the system.

The table below shows how a typical way in which security testers illustrate attackers' behaviour. It is largely the same as our images above, but more detailed.

MITRE Example Attack Chain Details

Initial Access	Execution	Privilege Escalation	Credential Access	Discovery	Collection	Command and Control	Exfiltration
Spear Phishing via Service	Command-Line Interface		Input Capture	File and Directory Discovery	Input Capture	Data Encoding	
Spear Phishing Link	PowerShell	Bypass UAC	OS Credential Dumping	Process Discovery	Data from Local System	Data Obfuscation	Exfiltration Over C2 Channel
	Scripting			System Information Discovery			
	User Execution						
Spear Phishing Link	Scripting	Bypass UAC	OS Credential Dumping	Process Discovery	Data from Local System	Data Obfuscation	Exfiltration Over C2 Channel

3. 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 **5. Protection Details** on page 13 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.

Protection Accuracy		
Product	Protection Accuracy	Protection Accuracy (%)
Avast Free Antivirus	400	100%
Kaspersky Plus	400	100%
McAfee Total Protection	400	100%
Microsoft Defender Antivirus (consumer)	400	100%
Sophos Home Premium	398	100%
NortonLifeLock Norton360	387	97%
Webroot Antivirus	378	95%
Panda Free Antivirus	333	83%
Comodo Antivirus	304	76%

Average 94%
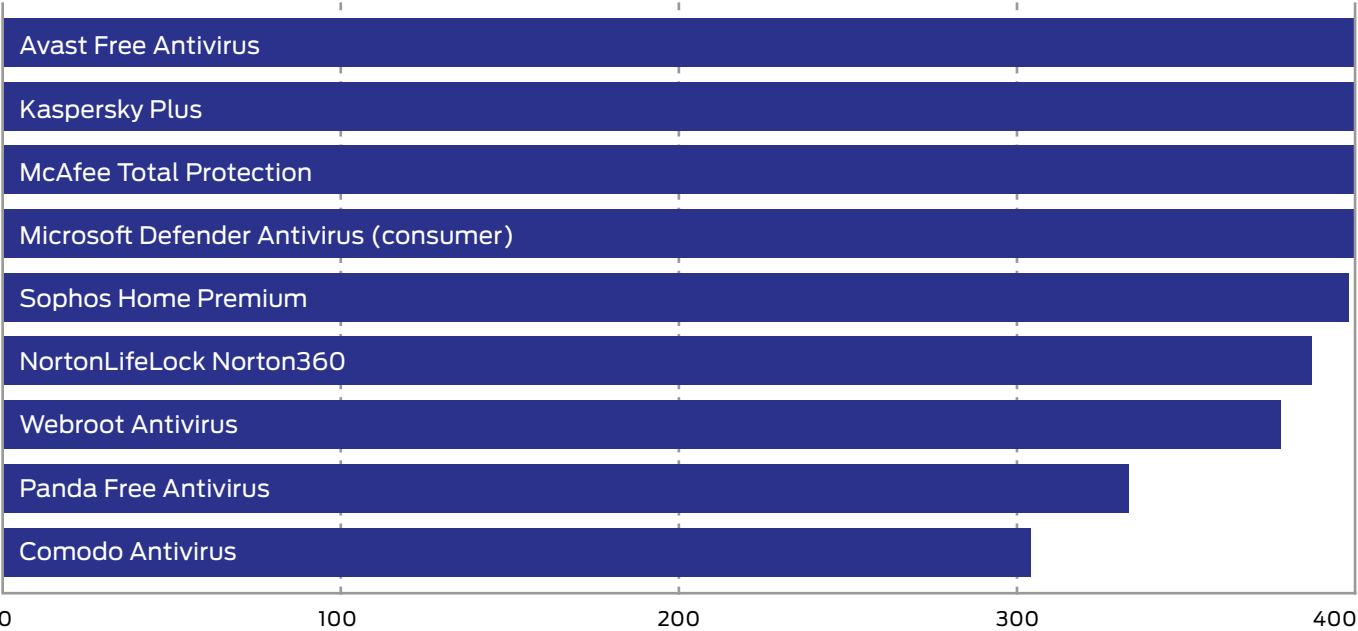
Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

4. 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	
Product	**Protection Score**
Microsoft Defender Antivirus (consumer)	100
Avast Free Antivirus	100
Sophos Home Premium	100
Kaspersky Plus	100
McAfee Total Protection	100
Webroot Antivirus	98
NortonLifeLock Norton360	98
Comodo Antivirus	94
Panda Free Antivirus	92

Microsoft Defender Antivirus (consumer)

Avast Free Antivirus

Sophos Home Premium

Kaspersky Plus

McAfee Total Protection

Webroot Antivirus

NortonLifeLock Norton360

Comodo Antivirus

Panda Free Antivirus

0   25   50   75   100
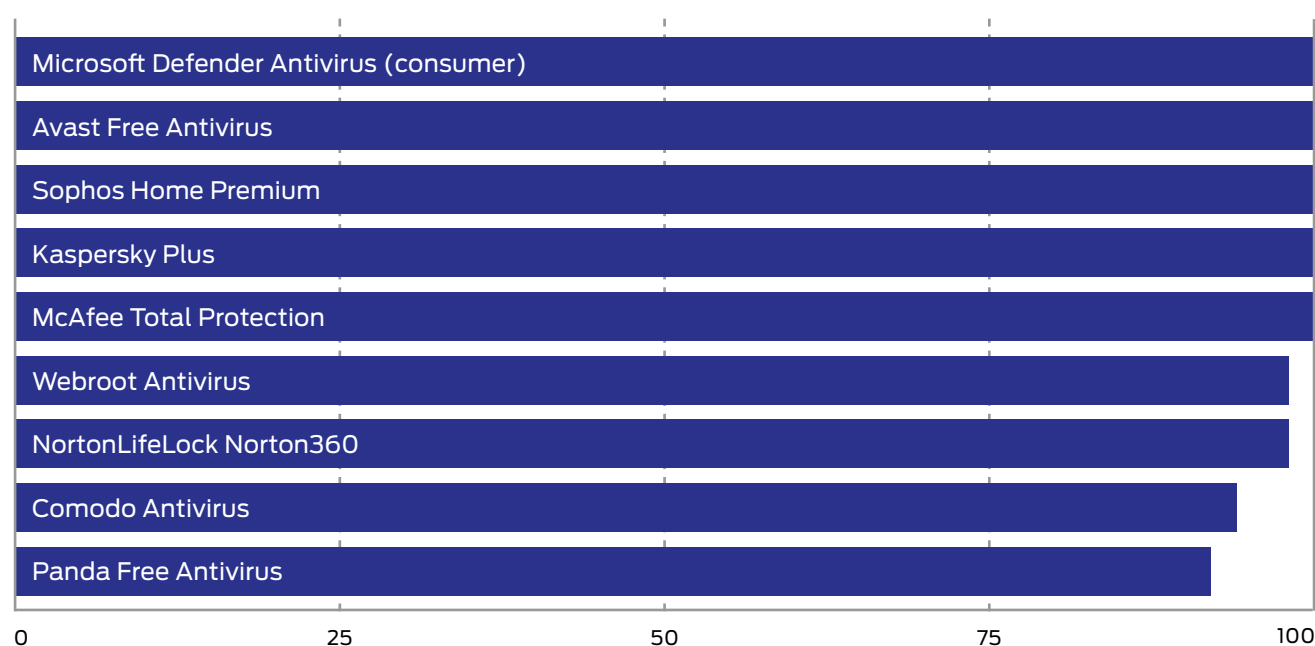
Protection Scores are a simple count of how many times a product protected the system.

5. 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.

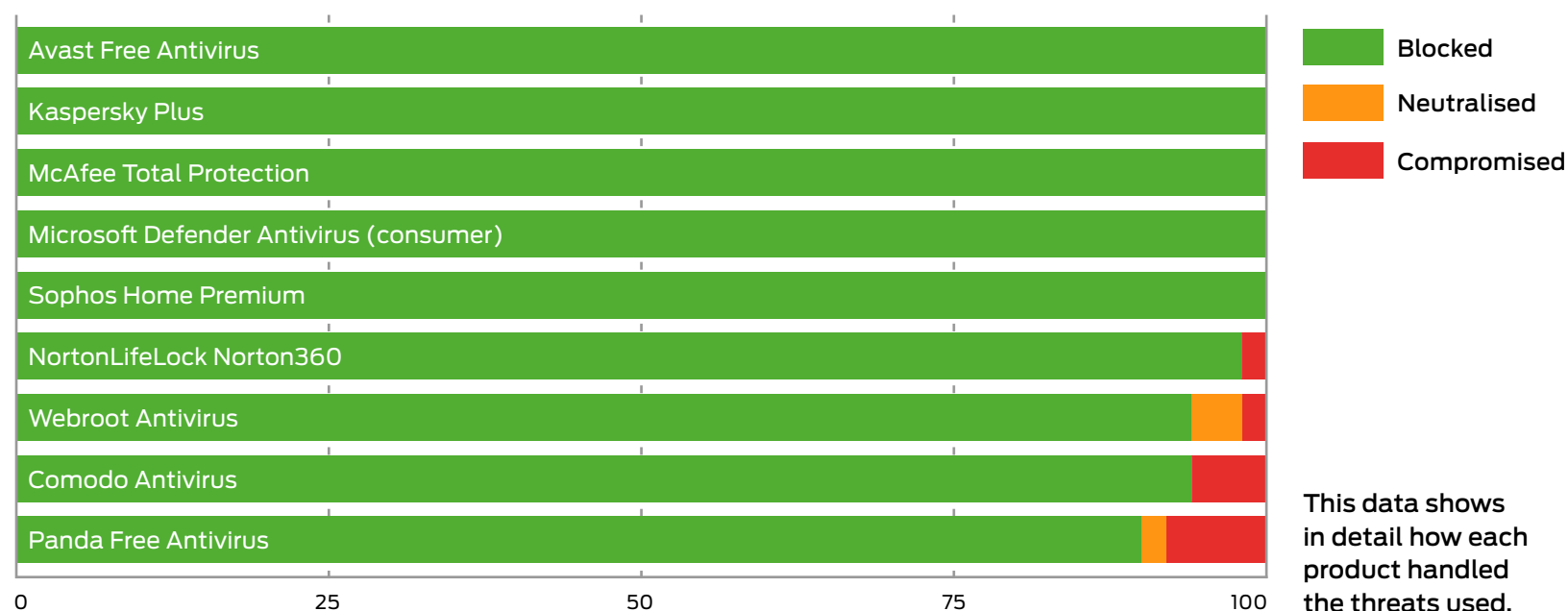| Protection Details					
Product	Detected	Blocked	Neutralised	Compromised	Protected
Avast Free Antivirus	100	100	0	0	100
Kaspersky Plus	100	100	0	0	100
McAfee Total Protection	100	100	0	0	100
Microsoft Defender Antivirus (consumer)	100	100	0	0	100
Sophos Home Premium	100	100	0	0	100
NortonLifeLock Norton360	98	98	0	2	98
Webroot Antivirus	99	94	4	2	98
Comodo Antivirus	98	94	0	6	94
Panda Free Antivirus	94	90	2	8	92

Legend:
- Blocked (green)
- Neutralised (orange)
- Compromised (red)

Chart categories: Avast Free Antivirus, Kaspersky Plus, McAfee Total Protection, Microsoft Defender Antivirus (consumer), Sophos Home Premium, NortonLifeLock Norton360, Webroot Antivirus, Comodo Antivirus, Panda Free Antivirus. Axis: 0, 25, 50, 75, 100.

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

6. Legitimate Software 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 **6.3 Accuracy Ratings** on page 16.

Legitimate Software Ratings		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy (%)**
Avast Free Antivirus	740	100%
Kaspersky Plus	740	100%
Microsoft Defender Antivirus (consumer)	740	100%
NortonLifeLock Norton360	740	100%
Sophos Home Premium	740	100%
Webroot Antivirus	740	100%
McAfee Total Protection	736.5	100%
Comodo Antivirus	724	98%
Panda Free Antivirus	716	97%

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

0   370   740
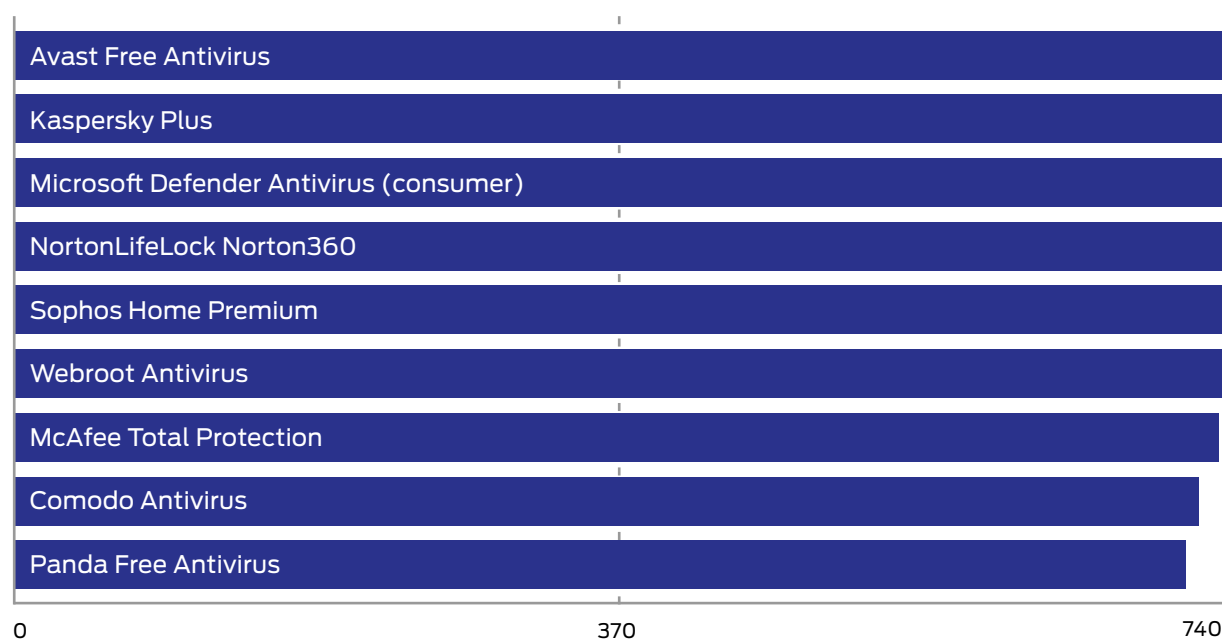
Legitimate Software Ratings can indicate how well a vendor has tuned its detection engine.

6.1 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.

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

Interaction Ratings		
Product	None (allowed)	None (blocked)
Avast Free Antivirus	100	0
Kaspersky Plus	100	0
Microsoft Defender Antivirus (consumer)	100	0
NortonLifeLock Norton360	100	0
Sophos Home Premium	100	0
Webroot Antivirus	100	0
McAfee Total Protection	99	1
Comodo Antivirus	98	2
Panda Free Antivirus	98	2

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

6.2 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

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.

Legitimate Software Prevalence Rating Modifiers	
Impact Category	Rating Modifier
Very High Impact	5
High Impact	4
Medium Impact	3
Low Impact	2
Very Low Impact	1

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.

6.3 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 **6. Legitimate Software Ratings** on page 14.

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

7. Conclusions

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 spreading through email were delivered to our target systems as emails.

All of 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.

Five of the nine products stopped all of the attacks this quarter. These belonged to **Microsoft**, **Avast**, **Sophos**, **Kaspersky** and **McAfee**. In fact, almost all of the products provided excellent protection against public email- and web-based threats by blocking them. **Webroot Antivirus** only missed one general attack while **Panda Free Antivirus** missed four.

Four products missed targeted attacks. Targeted attacks are usually more of challenge because they are not as widely known. **Webroot Antivirus** only missed one, as it failed to detect elements of the attack until ransomware was introduced. **Panda Free Antivirus** also missed the introduction of four targeted attacks, thus failing despite wrestling with the later elements of the threat sequence. **Comodo Antivirus** failed six targeted attacks after missing the initial threats when these were introduced to the system. **NortonLifeLock Norton360** missed two targeted attacks that ran unimpeded at every stage.

Almost all of the products handled the legitimate applications and websites correctly, with no mistakes. **Comodo Antivirus** and **Panda Free Antivirus** both blocked a couple of legitimate applications from running. Despite that, this is a particularly strong performance for all of the products.

Almost all the products in this test win AAA awards by virtue of scoring total accuracy ratings of either 100% or in the high 90s. The strongest, from **Microsoft**, **Kaspersky**, **Avast**, **Sophos** and **McAfee** stopped all of the threats and allowed all legitimate applications. Products from **Norton** and **Webroot** were only one or two percentage points shy of a perfect total accuracy score. **Comodo Antivirus** and **Panda Free Antivirus** performed well enough to achieve AA awards.

Appendices

Appendix A: Terms Used

Term	Meaning
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 B: FAQs

A **full methodology** for this test is available from our website.
- The products chosen for this test were selected by SE Labs.
- The test was unsponsored.
- The test was conducted between 8th April and 12th June 2024.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Malicious URLs and legitimate applications and URLs were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- The web browser used in this test was Google Chrome. When testing Microsoft products Chrome was equipped with the Windows Defender Browser Protection browser extension (**https://browserprotection.microsoft.com**). We allow other browser extensions when a tested product requests a user install one or more.

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.

Appendix C: Product Versions

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

Product Versions			
Vendor	**Product**	**Build Version (start)**	**Build Version (end)**
Avast	Free Antivirus	Program Version: 24.2.6105 (build 24.2.8918.827) Virus Definitions Version: 240402-0 UI version: 1.0.801	Program Version: 24.5.6116 (build 24.5.9153.844) Virus Definitions Version: 240612-0 UI Version: 1.0.809
Comodo	Antivirus	12.2.2.8012	12.2.2.8012
Kaspersky	Plus	21.16.6.467(c)	21.16.6.467(c)
McAfee	Total Protection	McAfee Antivirus: 1.1.3105.0 Secure VPN: 1.16 Tracker Remover: 1.14 Shredder: 1.16 Advanced Firewall: 1.16 McAfee WebAdvisor: 8.1.0.4881	McAfee Antivirus: 1.1.3105.0 Secure VPN: 1.16 Tracker Remover: 1.16 Shredder: 1.16 Advanced Firewall: 1.16 McAfee WebAdvisor: 8.1.0.4881
Microsoft	Defender Antivirus (consumer)	Antimalware Client Version: 4.18.24030.9 Engine Version: 1.1.24030.4 Antivirus Version: 1.409.7.0 Anti-spyware Version: 1.409.7.0	Antimalware Client Version: 4.18.24050.7 Engine Version: 1.1.24050.5 Antivirus Version: 1.413.234.0 Anti-spyware Version: 1.413.234.0
NortonLifeLock	Norton360	22.24.2.6	22.24.3.2
Panda	Free Antivirus	22.02.01	22.02.01
Sophos	Home Premium	2023.2.2.2	2023.2.2.2
Webroot	Antivirus	9.0.35.12	9.0.35.12

Appendix D: Attack Types

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

Attack Types			
Product	General Attack	Targeted Attack	Protected (%)
Avast Free Antivirus	75	25	100%
Kaspersky Plus	75	25	100%
McAfee Total Protection	75	25	100%
Microsoft Defender Antivirus (consumer)	75	25	100%
Sophos Home Premium	75	25	100%
NortonLifeLock Norton360	75	23	98%
Webroot Antivirus	74	24	98%
Comodo Antivirus	75	19	94%
Panda Free Antivirus	71	21	92%

DE:CODED
Deciphering Cyber Security

Understand cybersecurity and other security issues. Practical and insightful, our experts have experience in attacking and defending in the physical and digital worlds.
Peek behind the curtain with the Cyber Security **DE:CODED** podcast.

Listen on Apple Podcasts

PODCAST

DE:CODED % SE Labs

Deciphering Cyber Security