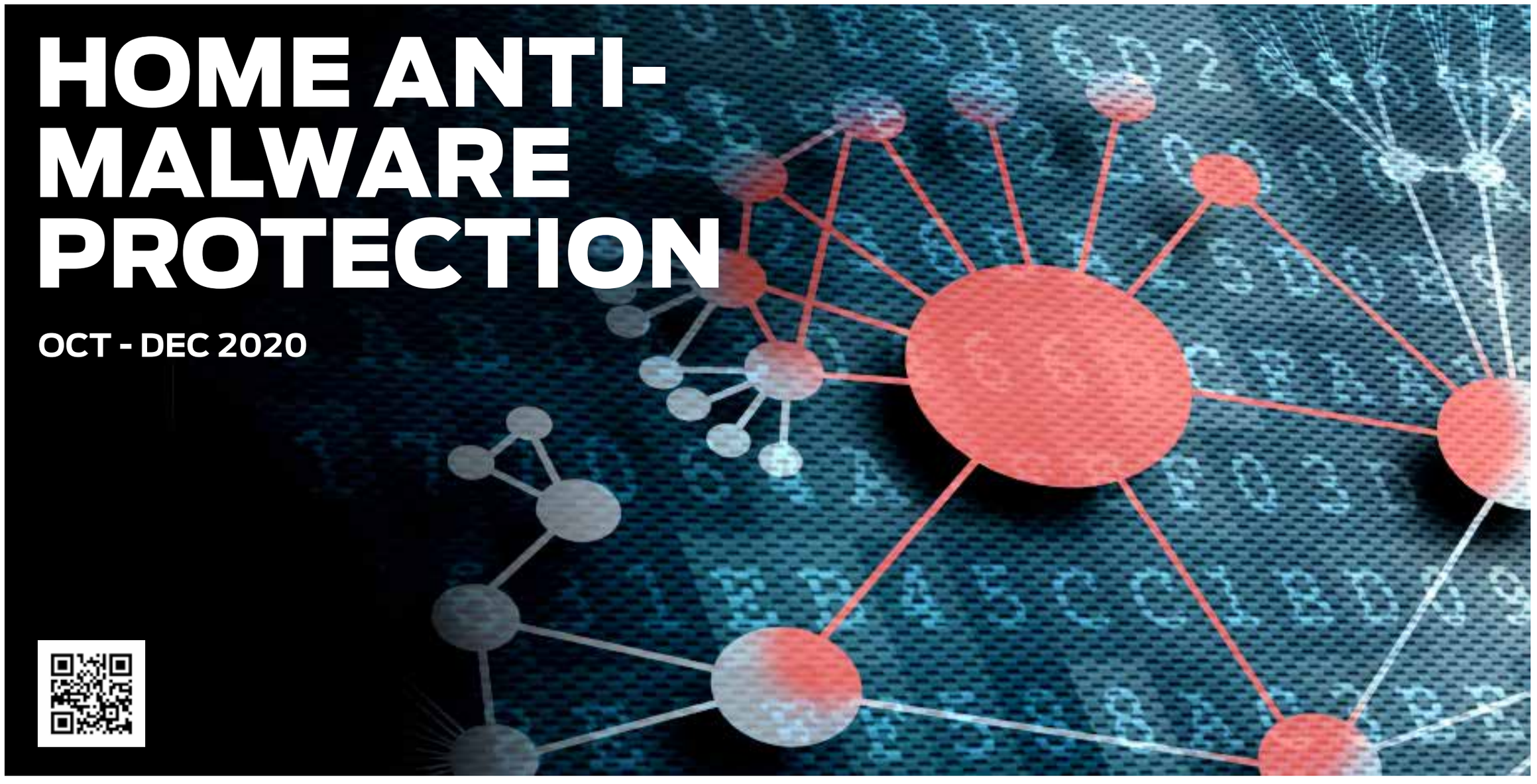
SE Labs

INTELLIGENCE-LED TESTING

HOME ANTI-MALWARE PROTECTION



OCT - DEC 2020

selabs.uk info@SELabs.uk @SELabsUK www.facebook.com/selabsuk blog.selabs.uk

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.

MANAGEMENT
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Chief Technical Officer Stefan Dumitrascu

TESTING TEAM
Nikki Albesa
Zaynab Bawa
Thomas Bean
Solandra Brewster
Liam Fisher
Gia Gorbold
Joseph Pike
Dave Togneri
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Blog blog.selabs.uk
Phone +44 (0)203 875 5000
Post SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2013 certified and BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

AMTSO Standard Reference:
selabs.uk/amtso20q4

CONTENTS

Document version 1.0 Written 22nd December 2020

INTRODUCTION

2020: year of the breach

Solid endpoint protection is a bare minimum

If it feels like new breaches are reported every week it's because they are. Attackers are taking no prisoners and are successfully breaking into businesses, political organisations and systems belonging to individuals.

It's not like a bank robbery, where the bad guys have to spend lots of time and effort to put themselves at physical risk for the sake of one big score. Ransomware extortions can happen in parallel, with the criminal sat in front of a screen watching piles of victims become compromised.

Ransomware attackers can wait as long as they want, in direct contrast to kidnappers in the physical world. Those criminals want to conclude the ransom payment as quickly as possible. In his book Never Split The Difference: Negotiating As If Your Life Depended On It, the ex-FBI author Chris Voss talks about handling kidnappers and pirates. There are some interesting insights, including the observation that they often become more amenable to lower ransom sums the closer they get to the weekend. They want to finish the job, relax and party.

This does not apply to digital crooks, who can scale their attacks to a different level. They are also far less likely to get caught or shot. They can relax and watch the money come rolling in over days, weeks and months.

Backups are important but, as we noted recently, they are not always the perfect solution. Recent attackers have been deleting backups and there are ways to damage offline backups held securely on tape, as we discussed in our article.

You can't rely on just one type of security solution. However, having solid endpoint protection in place is one of a few bare-minimum measures you need to take. Most of the products in this report are excellent at providing a much-needed level of protection on personal and business computers. We recommend you read through the results in detail and consider how confident you are that your current choice will stand up against real-world security threats.

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us via our Twitter or Facebook accounts. 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 Twitter.

This test report was funded by post-test consultation services provided by SE Labs to security vendors. Vendors of all products included in this report were able to request early access to results and the ability to dispute details for free. SE Labs has submitted the testing process behind this report for compliance with the AMTSO Testing Protocol Standard v1.3. To verify its compliance please check the AMTSO reference link at the bottom of page three of this report or here.

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 (%)
Kaspersky Internet Security	100%	100%	100%
McAfee Internet Security	100%	100%	100%
Avast Free Antivirus	99%	100%	100%
AVG Antivirus Free Edition	99%	100%	100%
Microsoft Defender Antivirus (consumer)	97%	100%	99%
Norton LifeLock Security	100%	94%	96%
Avira Free Security Suite	89%	100%	96%
Trend Micro Internet Security	92%	96%	94%
Comodo Internet Security	87%	97%	94%
Sophos Home Premium	86%	98%	94%
Webroot Antivirus	84%	100%	94%
F-Secure Safe	91%	93%	92%
Malwarebytes Premium	49%	98%	81%

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 security software products were generally effective at handling general threats from cyber criminals...**
Most products were largely capable of handling public 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 only half were completely effective.

- **.. and targeted attacks were prevented in most cases.**
All but one of the products were competent at blocking more targeted, exploit-based attacks. This was an unusually strong result for the vendors involved.

- **False positives were not a serious issue for most products.**
Most of the products were good at correctly classifying legitimate applications and websites.

- **Which products were the most effective?**
Products from **Kaspersky**, **McAfee**, **Avast** and **AVG** produced extremely good results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites. Others from **Microsoft**, **Avira** and **Norton LifeLock** were also exceptional.

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.

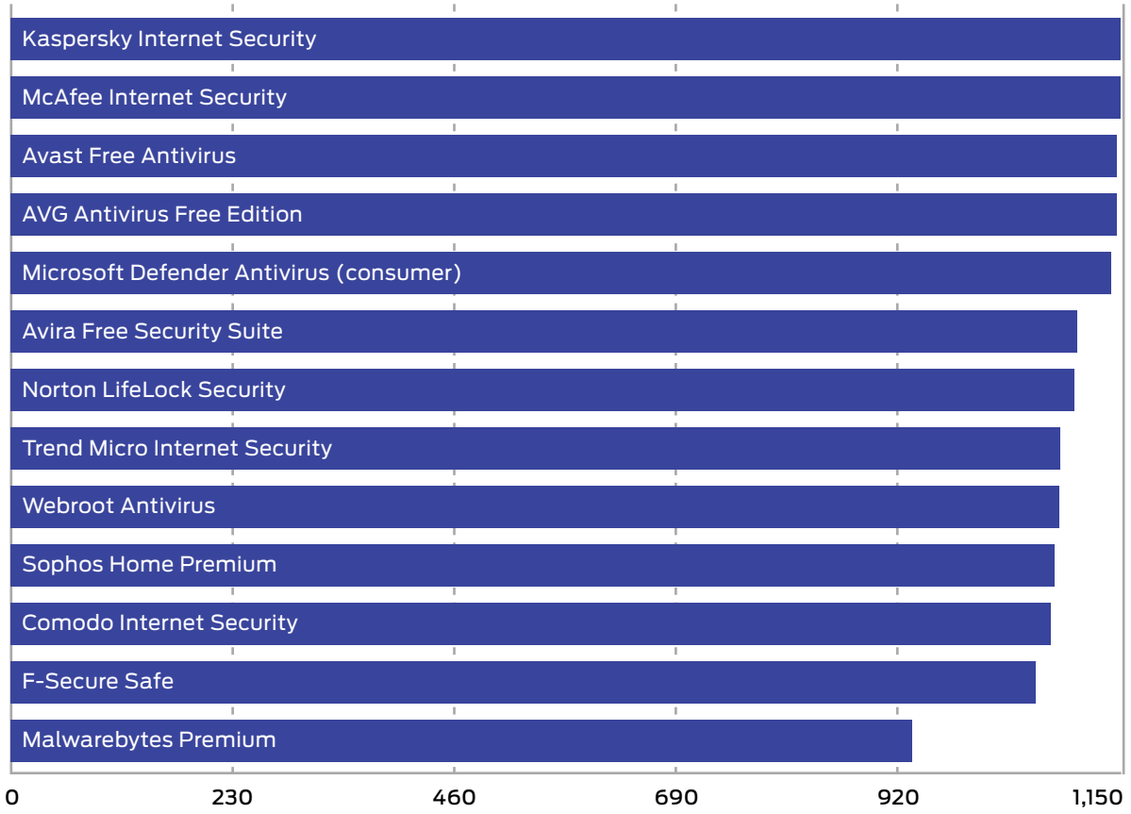
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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**
Kaspersky Internet Security	1,149	100%	AAA
McAfee Internet Security	1,149	100%	AAA
Avast Free Antivirus	1,145	100%	AAA
AVG Antivirus Free Edition	1,145	100%	AAA
Microsoft Defender Antivirus (consumer)	1,139	99%	AAA
Avira Free Security Suite	1,104	96%	AAA
Norton LifeLock Security	1,101	96%	AAA
Trend Micro Internet Security	1,086.5	94%	AA
Webroot Antivirus	1,085	94%	AA
Sophos Home Premium	1,080	94%	AA
Comodo Internet Security	1,077	94%	AA
F-Secure Safe	1,061	92%	AA
Malwarebytes Premium	933	81%	B



Total Accuracy Ratings combine protection and false positives.

Home Anti-Malware Protection Awards

The following products win SE Labs awards:

- **Kaspersky** Internet Security
- **McAfee** Internet Security
- **Avast** Free Antivirus
- **AVG** Antivirus Free Edition
- **Microsoft** Defender Antivirus (consumer)
- **Avira** Free Security Suite
- **Norton** LifeLock Security

- **Trend Micro** Internet Security
- **Webroot** Antivirus
- **Sophos** Home Premium
- **Comodo** Internet Security
- **F-Secure** Safe

- **Malwarebytes** Premium

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 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.

Attack Chain: How Hackers Progress

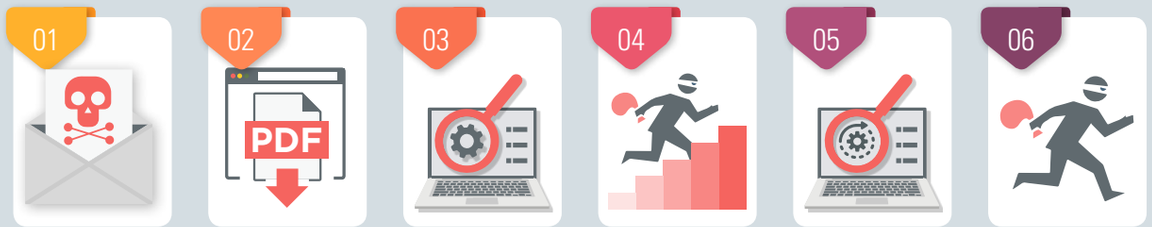


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

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.

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. Such traces should not exist if the threat was 'Blocked' and so Blocked results imply Complete remediation.

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.

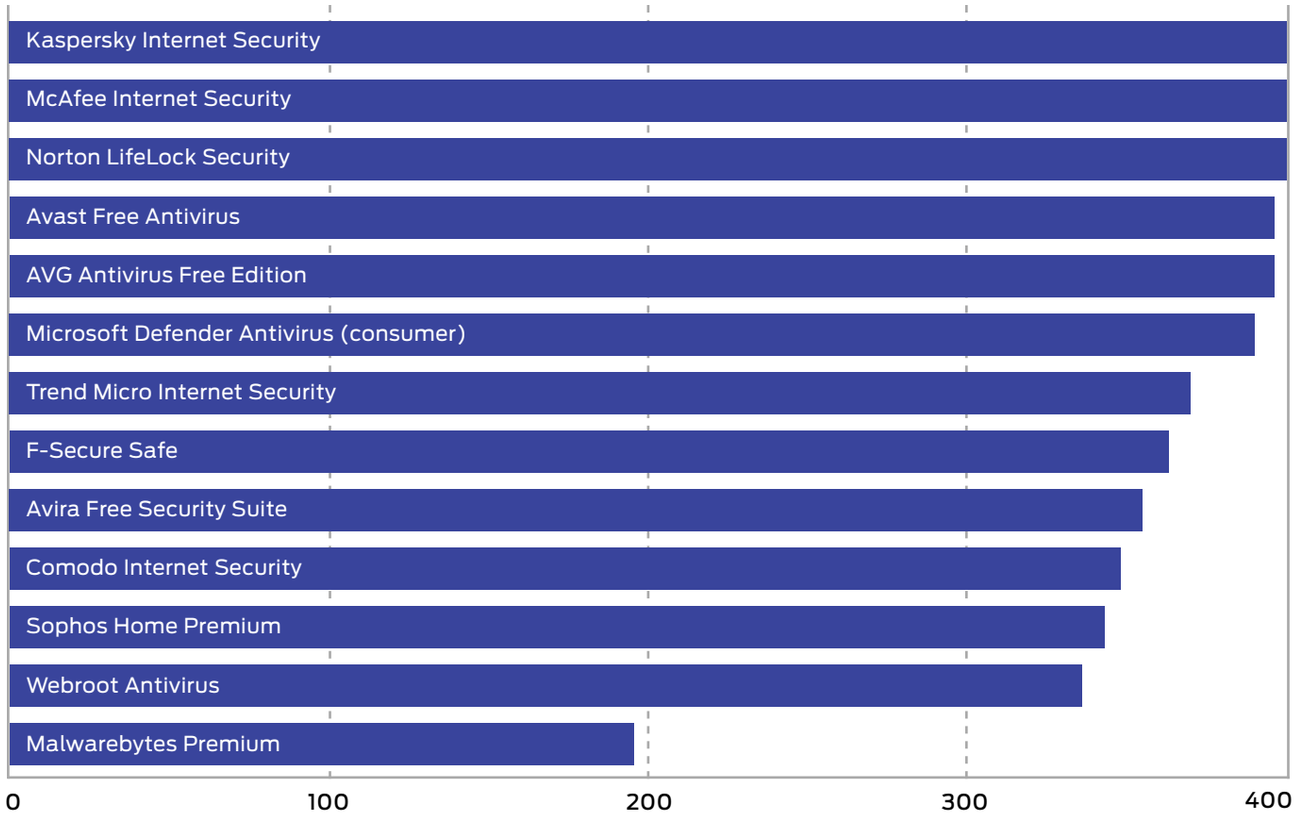
Action (-1)
If the attacker is able to exfiltrate a document from the target's Desktop of the currently logged in user then an 'action' has been successfully taken.

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 (%)
Kaspersky Internet Security	399	100%
McAfee Internet Security	399	100%
Norton LifeLock Security	399	100%
Avast Free Antivirus	395	99%
AVG Antivirus Free Edition	395	99%
Microsoft Defender Antivirus (consumer)	389	97%
Trend Micro Internet Security	369	92%
F-Secure Safe	362	91%
Avira Free Security Suite	354	89%
Comodo Internet Security	347	87%
Sophos Home Premium	342	86%
Webroot Antivirus	335	84%
Malwarebytes Premium	195	49%

Average 90%



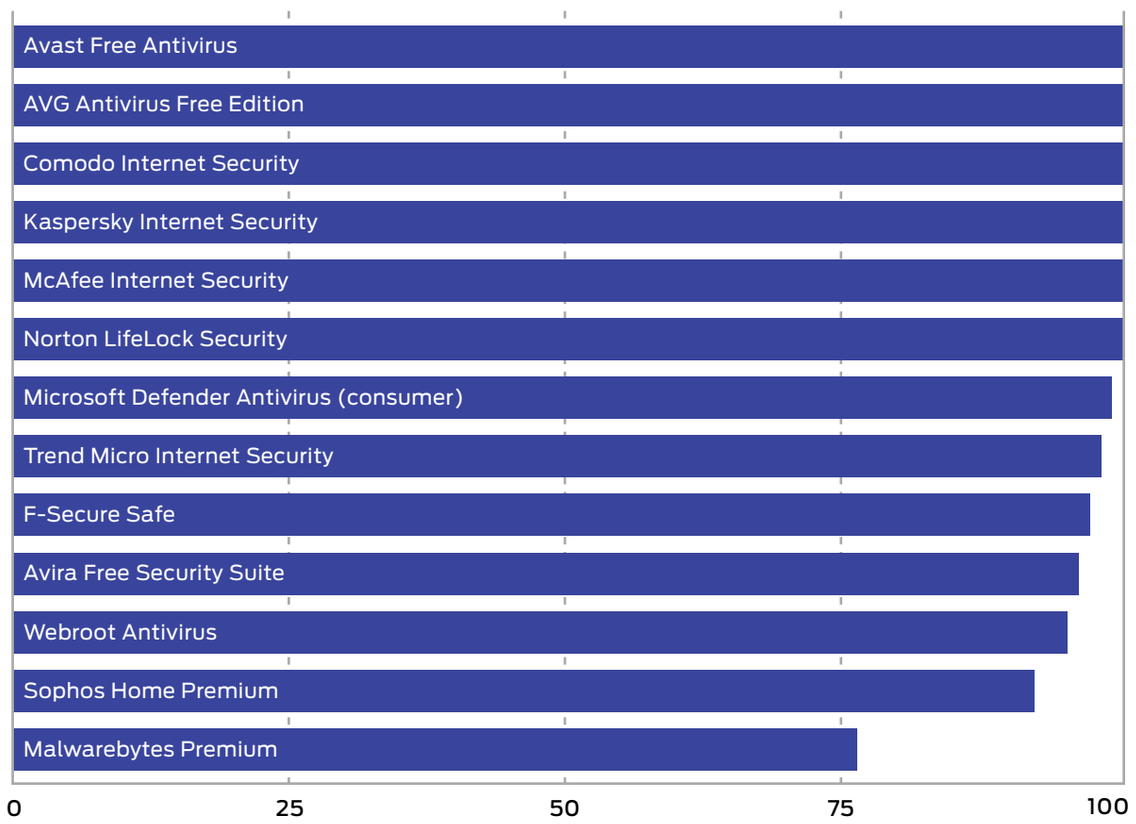
Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

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**
Avast Free Antivirus	100
AVG Antivirus Free Edition	100
Comodo Internet Security	100
Kaspersky Internet Security	100
McAfee Internet Security	100
Norton LifeLock Security	100
Microsoft Defender Antivirus (consumer)	99
Trend Micro Internet Security	98
F-Secure Safe	97
Avira Free Security Suite	96
Webroot Antivirus	95
Sophos Home Premium	92
Malwarebytes Premium	76



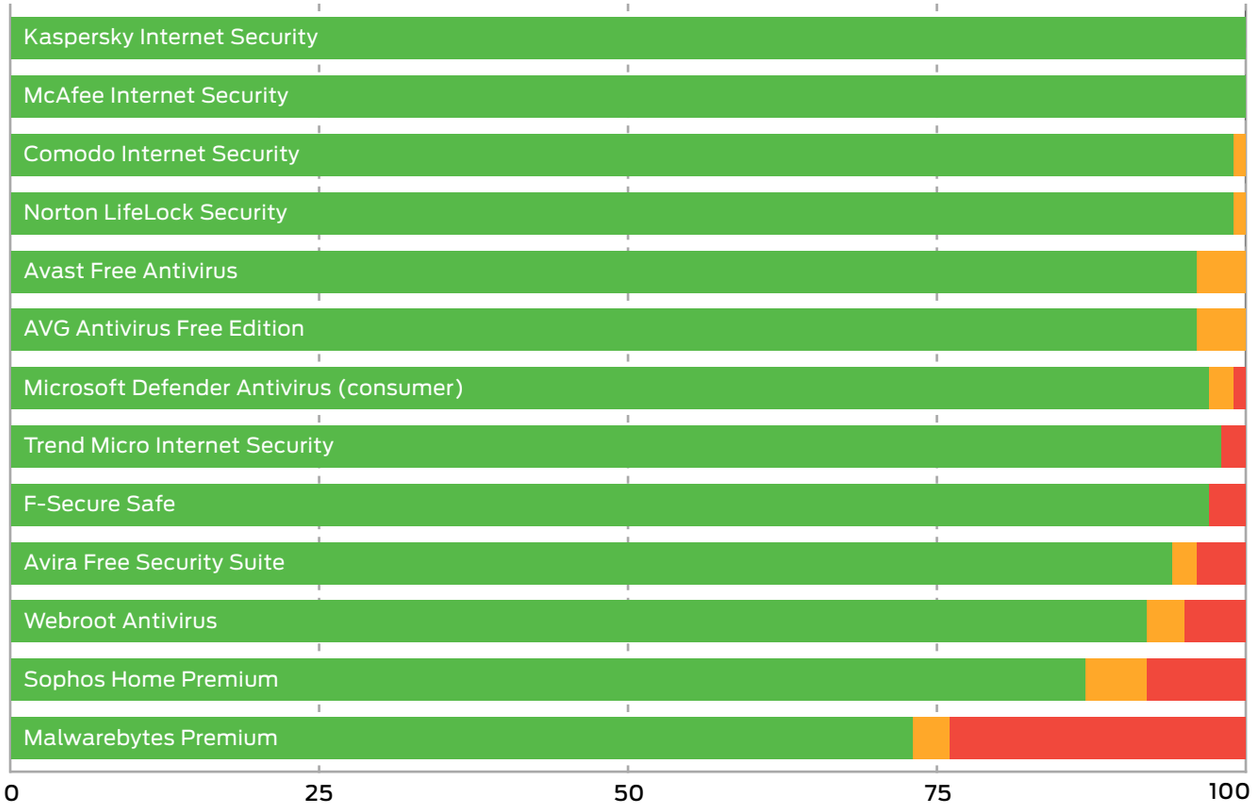
Protection Scores are a simple count of how many times a product protected the system.

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**
Kaspersky Internet Security	100	100	0	0	100
McAfee Internet Security	100	100	0	0	100
Comodo Internet Security	100	99	1	0	100
Norton LifeLock Security	100	99	1	0	100
Avast Free Antivirus	100	96	4	0	100
AVG Antivirus Free Edition	100	96	4	0	100
Microsoft Defender Antivirus (consumer)	99	97	2	1	99
Trend Micro Internet Security	98	98	0	2	98
F-Secure Safe	97	97	0	3	97
Avira Free Security Suite	96	94	2	4	96
Webroot Antivirus	97	92	3	5	95
Sophos Home Premium	99	87	5	8	92
Malwarebytes Premium	88	73	3	24	76



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

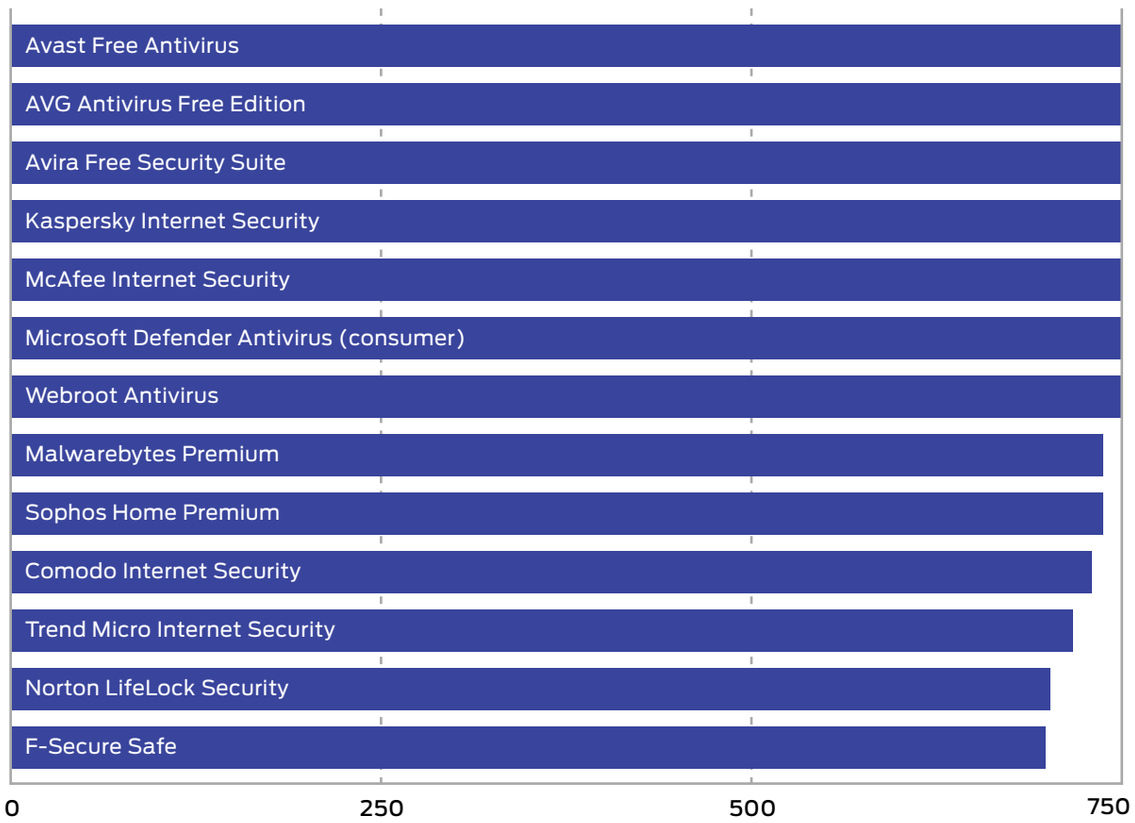
6. Legitimate Software Ratings

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	750	100%
AVG Antivirus Free Edition	750	100%
Avira Free Security Suite	750	100%
Kaspersky Internet Security	750	100%
McAfee Internet Security	750	100%
Microsoft Defender Antivirus (consumer)	750	100%
Webroot Antivirus	750	100%
Malwarebytes Premium	738	98%
Sophos Home Premium	738	98%
Comodo Internet Security	730	97%
Trend Micro Internet Security	717.5	96%
Norton LifeLock Security	702	94%
F-Secure Safe	699	93%



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)	Click to allow/block (no recommendation)	None (blocked)
Avast Free Antivirus	100	0	0
AVG Antivirus Free Edition	100	0	0
Avira Free Security Suite	100	0	0
Kaspersky Internet Security	100	0	0
McAfee Internet Security	100	0	0
Microsoft Defender Antivirus (consumer)	100	0	0
Webroot Antivirus	100	0	0
Malwarebytes Premium	99	0	0
Sophos Home Premium	99	0	1
Trend Micro Internet Security	97	2	1
F-Secure Safe	97	0	3
Norton LifeLock Security	97	0	3
Comodo Internet Security	95	0	0

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 Alexa.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	33
Medium Impact	17
Low Impact	14
Very Low Impact	4

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 don't write unique malware so there is no technical reason why any vendor being tested should do poorly.

However, half of the products tested failed to handle 100 per cent of the public threats effectively. While, in most cases, the numbers of 'misses' are not out of this world, it's disappointing to see well-known products miss well-known threats. **Malwarebytes** was particularly worrying in this regard, missing ten per cent of them.

Targeted attacks were handled well by all but two of the products. 11 of the 13 products tested were 100 per cent accurate. **Malwarebytes** disappointed by failing to protect against over 60 per cent of them. **Sophos** missed around 25 per cent.

Sophos notes that each of its targeted attack misses used the same evasion kit with the same root cause for the miss. **Sophos** has since updated detection accordingly. Additionally, customers will be protected against variants of this attack technique with a new feature due for release in early January.

Some products blocked all of the public and targeted attacks. These included those from **Norton LifeLock**, **Comodo**, **Avast**, **AVG**, **Kaspersky** and **McAfee**. **Microsoft's** handled all well, except for one public threat, while **Trend Micro** missed two.

The products handled most legitimate objects correct, with only three making three mistakes each and one making one mistake. **Sophos** blocked one object while **Norton LifeLock** and **F-Secure** blocked three objects each, while **Trend Micro** blocked one and questioned a further two without making any recommendations.

The leading products from **Kaspersky**, **McAfee**, **Avast**, **AVG**, **Microsoft**, **Avira** and **Norton LifeLock** all win AAA 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 21st September to 10th November 2020.
- 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.
- SE Labs conducted this endpoint security testing on physical PCs, not virtual machines.
- 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**).

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	200922-12	20.9.2437
AVG	Antivirus Free Edition	200922-12	20.9.3152
Avira	Free Security Suite	1.0.37.11666	1.0.40.12944
Comodo	Internet Security	Product Version: 12.2.2.7036 Database Version: 32772	Product Version: 12.2.2.7036 Database Version: 32836
F-Secure	Safe	17.8	17.9
Kaspersky	Internet Security	21.1.15.500 (b)	21.1.15.500 (c)
Malwarebytes	Premium	4.2.1	4.2.3.96
McAfee	Internet Security	16.0	16.0
Microsoft	Defender Antivirus (consumer)	1.327.1238.0	1.327.1238.0
Norton	LifeLock Security	22.20.5.39	22.20.5.39
Sophos	Home Premium	3.1.2	3.2.0
Trend Micro	Internet Security	16.0.1405	16.0.1411
Webroot	Antivirus	9.0.29.51	9.0.29.51

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	**Web-Download**	**Targeted Attack**	**Protected**
Avast Free Antivirus	75	25	100
AVG Antivirus Free Edition	75	25	100
Comodo Internet Security	75	25	100
Kaspersky Internet Security	75	25	100
McAfee Internet Security	75	25	100
Norton LifeLock Security	75	25	100
Microsoft Defender Antivirus (consumer)	74	25	99
Trend Micro Internet Security	73	25	98
F-Secure Safe	72	25	97
Avira Free Security Suite	71	25	96
Webroot Antivirus	70	25	95
Sophos Home Premium	74	18	92
Malwarebytes Premium	67	9	76

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 his 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.