SE Labs

INTELLIGENCE-LED TESTING

HOME ANTI-MALWARE PROTECTION

JAN - MAR 2020

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
Thomas Bean
Solandra Brewster
Dimitar Dobrev
Liam Fisher
Gia Gorbold
Dave Togneri
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Steve Haines
Colin Mackleworth

Website www.SELabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Blog blog.selabs.uk
Phone 0203 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:
https://tinyurl.com/sel2020q1

CONTENTS

Document version 1.0 Written 4th May 2020
1.01 Updated 14th May 2020 to correct ESET's results.
1.02 Updated 27th May 2020 to correct the NortonLifeLock product's name.

INTRODUCTION

Strong protection in uncertain times

A hacker mentality is keeping (computer) virus testing on track

This is the first in our series of 2020 endpoint protection reports. And it is unique, for all the usual reasons but also a new one.

We would normally highlight the latest new threats that we've discovered on the internet and discuss how we test them against the security software you use in your business and at home in the most realistic ways possible. And we've done that. But these reports are different to any we've produced before, for another reason.

We started testing shortly after the first signs of the COVID-19 virus were reported in China. By the time we were halfway through the work, London and the rest of the UK was in lock-down. So were large parts of Europe and, towards the end, the United States of America.

The way we test involves a large team interacting directly with computer hardware, as well as software. Remote working was something we had discounted for years. As the crisis unfolded we tried to keep our staff as far from each other as possible, although still in the office. But as the seriousness of the situation grew and, despite the fact that we could have continued working in the office legally, we put our own people's wellbeing first and decided to close down the lab.

We thought our deadlines might slip; our clients would miss out on the help we provide in improving their products; and you would not receive the latest updates on the state of endpoint protection against the latest threats.

It is a testament to the tenacity, imagination and technical skill of the team that we managed to find a solution that allowed testing to continue in the lab, with the vast majority of the team working from home. This represents a true hacker mentality, in which unconventional approaches to problem solving win the day, and the whole team should be applauded for their efforts.

The good news coming from this timely (and on-time!) research is that the cohort of companies that engaged with our testing are clearly performing strongly despite the technical challenges they are also no doubt facing in these troubling times. We've never seen such a strong showing from endpoint protection products in the enterprise, small business and home user markets.

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 (%)
ESET Internet Security	100%	100%	100%
Kaspersky Internet Security	100%	100%	100%
Sophos Home Premium	100%	100%	100%
Microsoft Windows Defender Consumer	98%	100%	99%
AVG Antivirus Free Edition	100%	97%	98%
Trend Micro Internet Security	98%	98%	98%
Avast Free Antivirus	95%	100%	98%
Avira Free Security Suite	95%	100%	98%
NortonLifeLock Norton 360	95%	100%	98%
F-Secure Safe	98%	96%	97%
McAfee Total Protection	93%	99%	97%
ZoneAlarm Free Antivirus	90%	100%	96%
G-Data Internet Security	87%	98%	94%
Comodo Internet Security	80%	100%	93%
Trustport Internet Security Sphere	65%	95%	85%
Webroot Antivirus	56%	100%	85%
NANO Antivirus Pro	-47%	97%	46%

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. Products from **Trustport** and **NANO** were notably weaker than the others.

■ **.. and targeted attacks were prevented in many cases.**

Many products were also competent at blocking more targeted, exploit-based attacks. However, while nearly all did very well in this part of the test **NANO** and **Webroot** products were notably weaker than the competition.

■ **False positives were not an issue for most products**

Most of the products were good at correctly classifying legitimate applications and websites. The vast majority allowed all of the legitimate websites and applications. Products from **AVG**, **F-Secure**, **G-Data**, **Trend Micro** and **Trustport** each made one mistake.

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

Products from **Kaspersky Lab**, **Sophos** and **Microsoft** achieved extremely good results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites.

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.

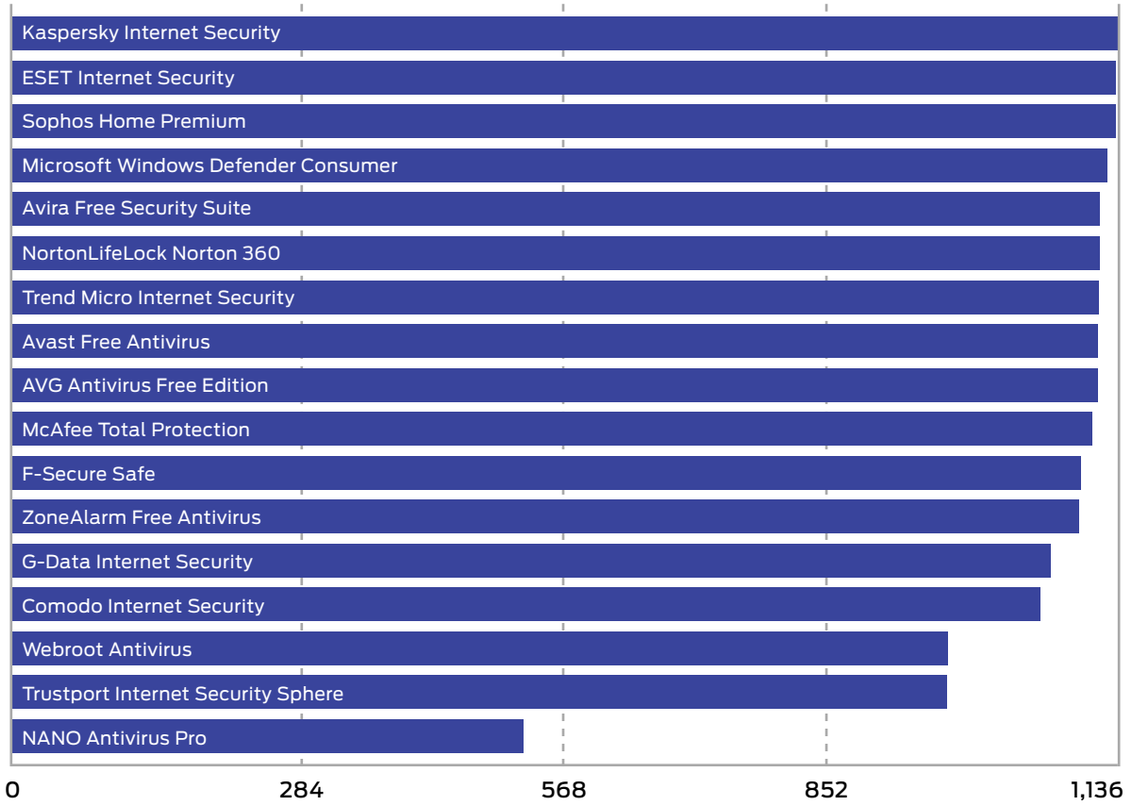
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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	1,136	100%	AAA
ESET Internet Security	1,134	100%	AAA
Sophos Home Premium	1,134	100%	AAA
Microsoft Windows Defender Consumer	1,126	99%	AAA
Avira Free Security Suite	1,117	98%	AAA
NortonLifeLock Norton 360	1,117	98%	AAA
Trend Micro Internet Security	1,116	98%	AAA
Avast Free Antivirus	1,115	98%	AAA
AVG Antivirus Free Edition	1,115	98%	AAA
McAfee Total Protection	1,100	97%	AAA
F-Secure Safe	1,098	97%	AAA
ZoneAlarm Free Antivirus	1,096	96%	AAA
G-Data Internet Security	1,067	94%	AA
Comodo Internet Security	1,056	93%	AA
Webroot Antivirus	961	85%	A
Trustport Internet Security Sphere	960	85%	A
NANO Antivirus Pro	527	46%	



Total Accuracy Ratings combine protection and false positives.

Home Anti-Malware Protection Awards

The following products win SE Labs awards:

- **ESET** Internet Security
- **Kaspersky** Internet Security
- **Sophos** Home Premium
- **Microsoft** Windows Defender Consumer
- **Avira** Free Security Suite
- **NortonLifeLock** Norton 360
- **Trend Micro** Internet Security
- **Avast** Free Antivirus
- **AVG** Antivirus Free Edition
- **McAfee** Total Protection
- **F-Secure** Safe
- **ZoneAlarm** Free Antivirus

- **G-Data** Internet Security
- **Comodo** Internet Security

- **Webroot** Antivirus
- **Trustport** Internet Security Sphere

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 contains 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.

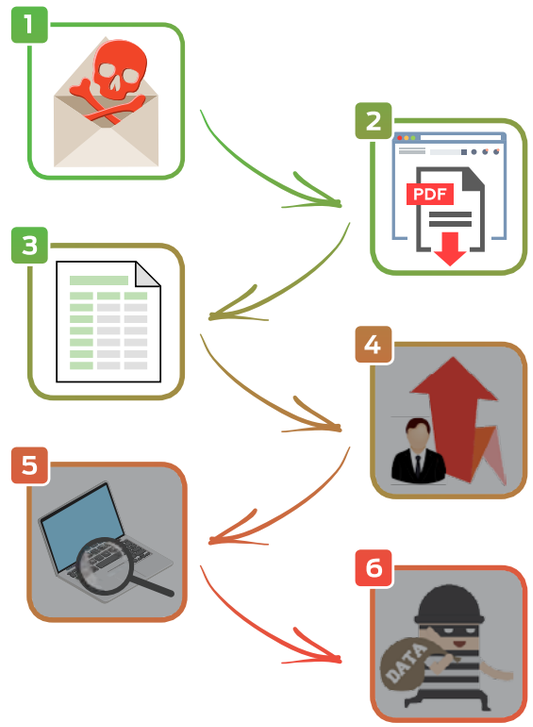


Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

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.

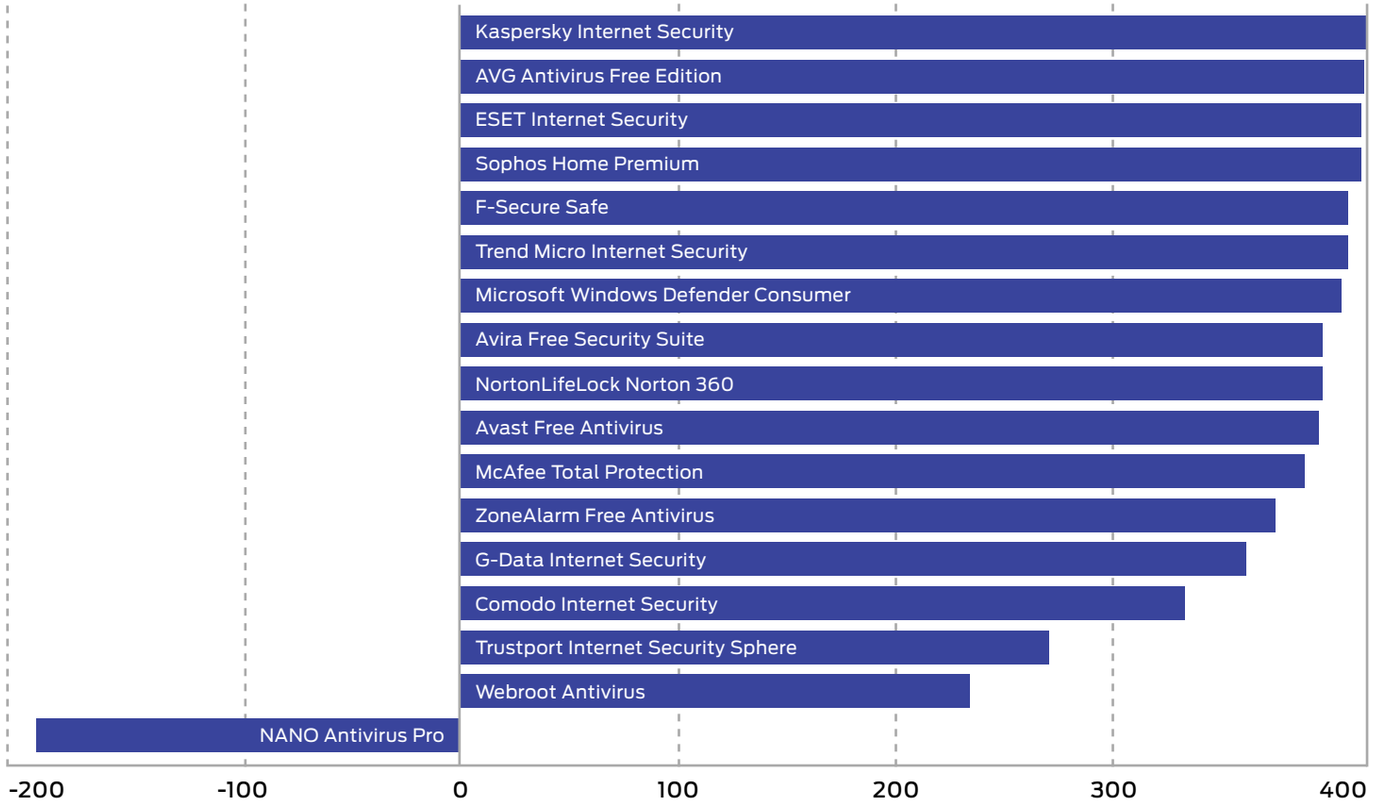
Action (-1)
If the attacker is able to exfiltrate a document from the target's Desktop of the currently logged in user then an 'action' has been successfully taken.

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

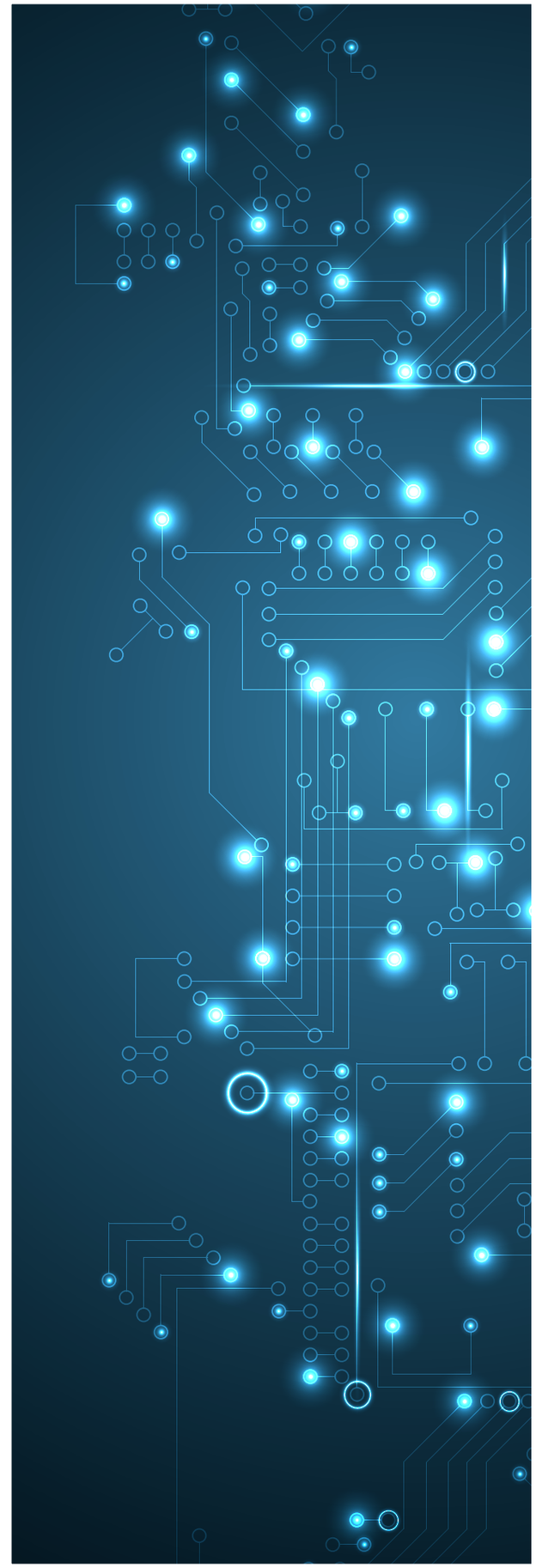
Post-Escalation Action (-1)
After escalation the attacker attempts actions that rely on escalated privileges. These include attempting to steal credentials, modifying the file system and recording keystrokes. If any of these actions are successful then a further penalty of one point deduction is applied.

PROTECTION ACCURACY		
Product	Protection Accuracy	Protection Accuracy (%)
Kaspersky Internet Security	400	100%
AVG Antivirus Free Edition	399	100%
ESET Internet Security	398	100%
Sophos Home Premium	398	100%
F-Secure Safe	392	98%
Trend Micro Internet Security	392	98%
Microsoft Windows Defender Consumer	390	98%
Avira Free Security Suite	381	95%
NortonLifeLock Norton 360	381	95%
Avast Free Antivirus	379	95%
McAfee Total Protection	373	93%
ZoneAlarm Free Antivirus	360	90%
G-Data Internet Security	347	87%
Comodo Internet Security	320	80%
Trustport Internet Security Sphere	260	65%
Webroot Antivirus	225	56%
NANO Antivirus Pro	-189	-47%

Average 82%



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

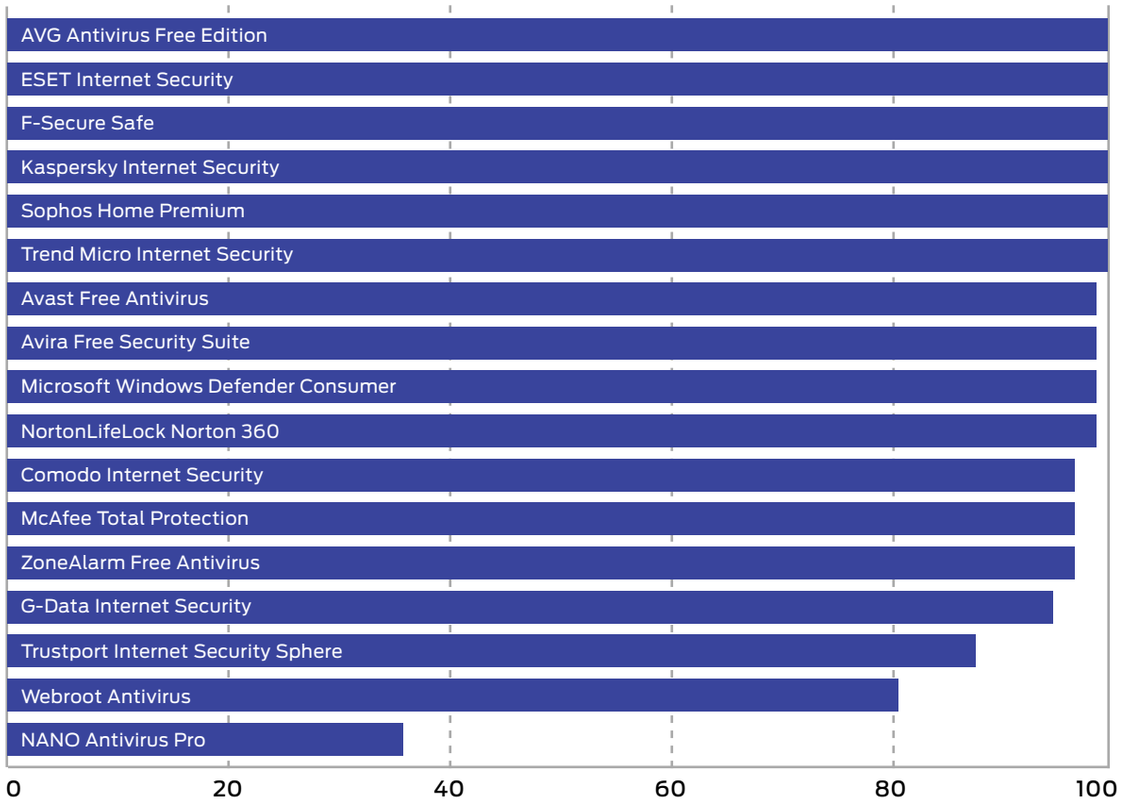


4. Protection Scores

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**
AVG Antivirus Free Edition	100
ESET Internet Security	100
F-Secure Safe	100
Kaspersky Internet Security	100
Sophos Home Premium	100
Trend Micro Internet Security	100
Avast Free Antivirus	99
Avira Free Security Suite	99
Microsoft Windows Defender Consumer	99
NortonLifeLock Norton 360	99
Comodo Internet Security	97
McAfee Total Protection	97
ZoneAlarm Free Antivirus	97
G-Data Internet Security	95
Trustport Internet Security Sphere	88
Webroot Antivirus	81
NANO Antivirus Pro	36



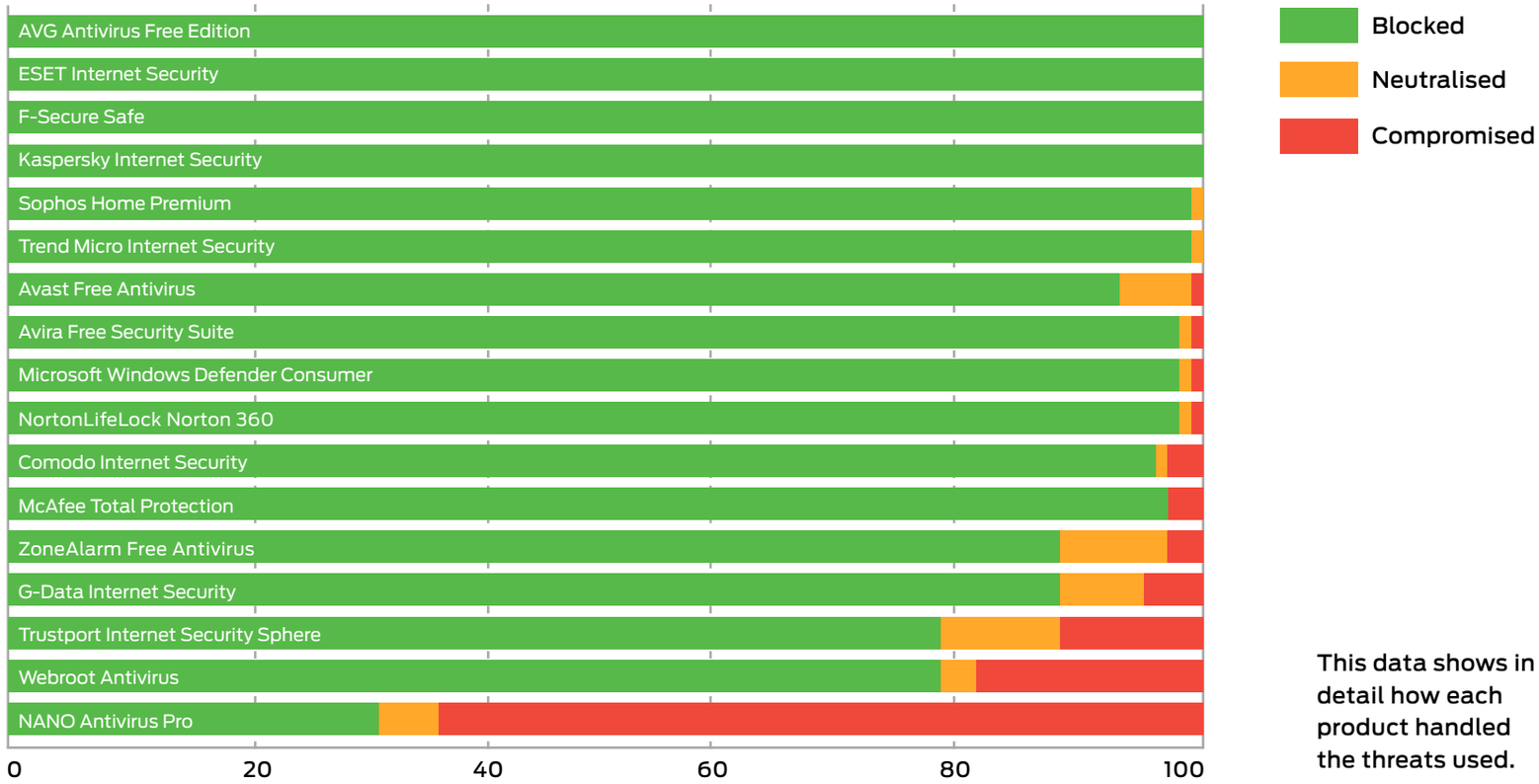
Protection Scores are a simple count of how many times a product protected the system.

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**
AVG Antivirus Free Edition	100	100	0	0	100
ESET Internet Security	100	100	0	0	100
F-Secure Safe	100	100	0	0	100
Kaspersky Internet Security	100	100	0	0	100
Sophos Home Premium	100	99	1	0	100
Trend Micro Internet Security	100	99	1	0	100
Avast Free Antivirus	99	93	6	1	99
Avira Free Security Suite	99	98	1	1	99
Microsoft Windows Defender Consumer	99	98	1	1	99
NortonLifeLock Norton 360	99	98	1	1	99
Comodo Internet Security	100	96	1	3	97
McAfee Total Protection	97	97	0	3	97
ZoneAlarm Free Antivirus	97	88	9	3	97
G-Data Internet Security	100	88	7	5	95
Trustport Internet Security Sphere	92	78	10	12	88
Webroot Antivirus	91	78	3	19	81
NANO Antivirus Pro	38	31	5	64	36



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

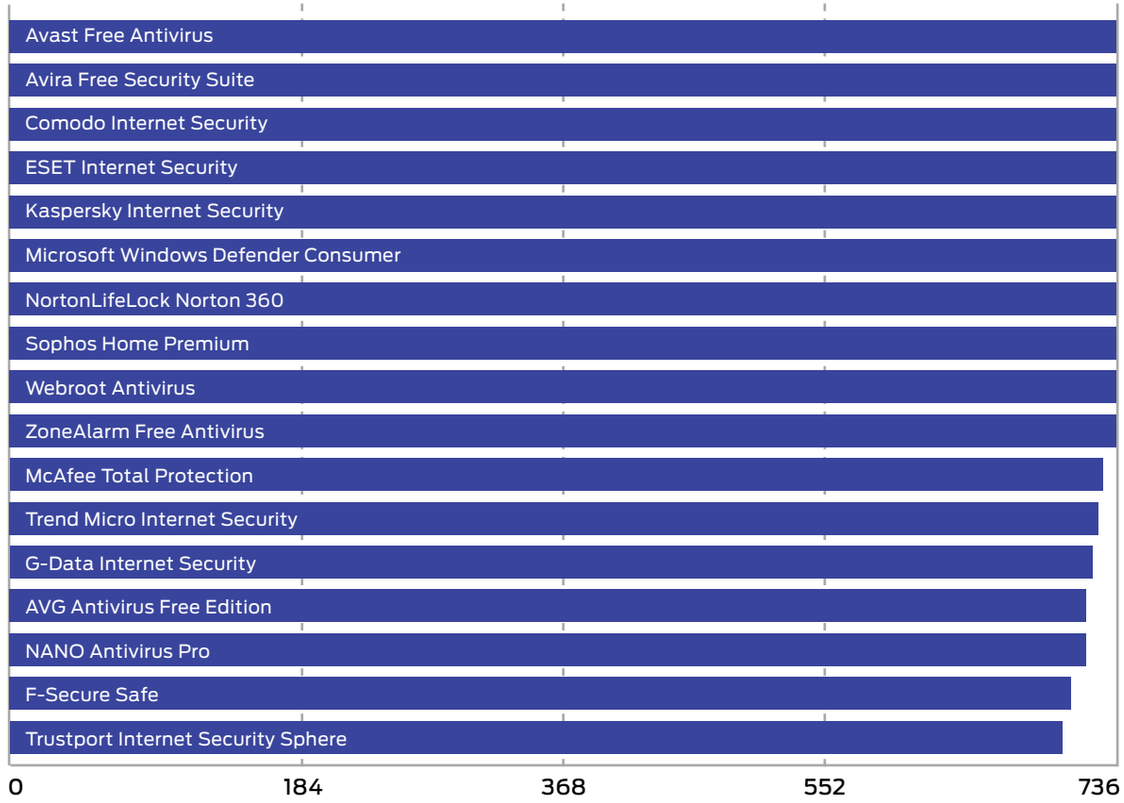
6. Legitimate Software Ratings

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	736	100%
Avira Free Security Suite	736	100%
Comodo Internet Security	736	100%
ESET Internet Security	736	100%
Kaspersky Internet Security	736	100%
Microsoft Windows Defender Consumer	736	100%
NortonLifeLock Norton 360	736	100%
Sophos Home Premium	736	100%
Webroot Antivirus	736	100%
ZoneAlarm Free Antivirus	736	100%
McAfee Total Protection	727	99%
Trend Micro Internet Security	724	98%
G-Data Internet Security	720	98%
AVG Antivirus Free Edition	716	97%
NANO Antivirus Pro	716	97%
F-Secure Safe	706	96%
Trustport Internet Security Sphere	700	95%



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	

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

INTERACTION RATINGS		
Product	None (Allowed)	None (Blocked)
Avast Free Antivirus	100	0
Avira Free Security Suite	100	0
Comodo Internet Security	100	0
ESET Internet Security	100	0
Kaspersky Internet Security	100	0
Microsoft Windows Defender Consumer	100	0
NortonLifeLock Norton 360	100	0
Sophos Home Premium	100	0
Webroot Antivirus	100	0
ZoneAlarm Free Antivirus	100	0
AVG Antivirus Free Edition	99	1
F-Secure Safe	99	1
G-Data Internet Security	99	1
McAfee Total Protection	99	0
NANO Antivirus Pro	99	0
Trend Micro Internet Security	99	1
Trustport Internet Security Sphere	97	1

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	15
Low impact	11
Very low impact	9

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.

Consequently, it's not a shock to see most of the products handle the public threats very effectively, although products from **Trustport** and **Webroot** struggled a little. **NANO Antivirus Pro** was the weakest by far in this part of the test. Targeted attacks were also handled well by most but caused some significant problems for **NANO's** product and that from **Webroot**.

The **AVG**, **ESET**, **F-Secure**, **Kaspersky Lab**, **Sophos** and **Trend Micro** products blocked all of the public and targeted attacks. With few exceptions they handled legitimate objects correctly too.

Avira's product followed up close behind, missing only one public threat but stopping all others, including targeted attacks. Products **Microsoft** and **NortonLifeLock** missed one public threat each but stopped all targeted attacks.

Webroot Antivirus stopped all but five of the public threats but fewer than half of the targeted attacks, while **NANO Antivirus Pro** missed 51 public threats and more than half of the targeted attacks.

The leading products from **Kaspersky Labs**, **Sophos**, **Microsoft**, **Avira**, **NortonLifeLock**, **Trend Micro**, **Avast**, **AVG**, **ESET**, **McAfee**, **F-Secure** and **Check Point** 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 9th January to 12th March 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	19.8.2393 (build 19.8.4257.546), Virus definitions version: 200108.4	20.1.2397 (build 20.1.5069.559)
AVG	Antivirus Free Edition	19.8.3108 (build 19.8.4257.548)	20.1.3112 (build 20.1.5069.559)
Avira	Free Security Suite	15.0.1912.1683. Virus definition file: 8.16.33.232	15.0.2002.1755
Comodo	Internet Security	Product version: 12.1.0.6914; database version: 31942	Product version: 12.1.0.6914; database version: 32191
ESET	Internet Security	13.0.24.0	13.0.24.0
F-Secure	Safe	17.7	17.7
G-Data	Internet Security	25.5.5.43	25.5.5.43
Kaspersky	Internet Security	20.0.14.1085(g)	20.0.14.1085(i)
McAfee	Total Protection	18.3 Build: 18.3.201	18.3 Build: 18.3.201
Microsoft	Windows Defender Consumer	Antimalware Client Version: 4.18.1911.3, Engine Version: 1.1.16600.7, Antivirus Version: 1.307.2266.0, Anti-spyware Version: 1.307.2266.0	Antimalware Client Version: 4.18.1911.3, Engine Version: 1.1.16800.2, Antivirus Version: 1.311.1042.0, Anti-spyware Version: 1.311.1042.0
NANO	Antivirus Pro	Antivirus engine: 1.0.134.90567, Virus base: 0.14.33.16991	Antivirus engine: 1.0.134.90568, Virus base: 0.14.33.17458
NortonLifeLock	Norton 360	22.19.9.63	22.20.1.69
Sophos	Home Premium	2.1.10	3.0.0
Trend Micro	Internet Security	16.0.1249	16.0.1302
Trustport	Internet Security Sphere	17.0.6.7106	17.0.6.7106
Webroot	Antivirus	9.0.26.64	9.0.27.64
ZoneAlarm	Free Antivirus	Zone Alarm Free Antivirus + Firewall version: 15.8.023.18219, Vsmon version: 15.8.7.18219, Driver version: 15.1.29.17237, Anti-virus engine version: 8.9.1.113, Anti-Virus engine version: 8.9.1.113, Anti-Virus signature DAT file version: 1345127936	15.8.023.18219

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
AVG Antivirus Free Edition	75	25	100
ESET Internet Security	75	25	100
F-Secure Safe	75	25	100
Kaspersky Internet Security	75	25	100
Sophos Home Premium	75	25	100
Trend Micro Internet Security	75	25	100
Avast Free Antivirus	75	24	99
Avira Free Security Suite	74	25	99
Microsoft Windows Defender Consumer	74	25	99
NortonLifeLock Norton 360	74	25	99
Comodo Internet Security	75	22	97
McAfee Total Protection	75	22	97
ZoneAlarm Free Antivirus	72	25	97
G-Data Internet Security	75	20	95
Trustport Internet Security Sphere	64	24	88
Webroot Antivirus	70	11	81
NANO Antivirus Pro	24	12	36

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.