SE Labs

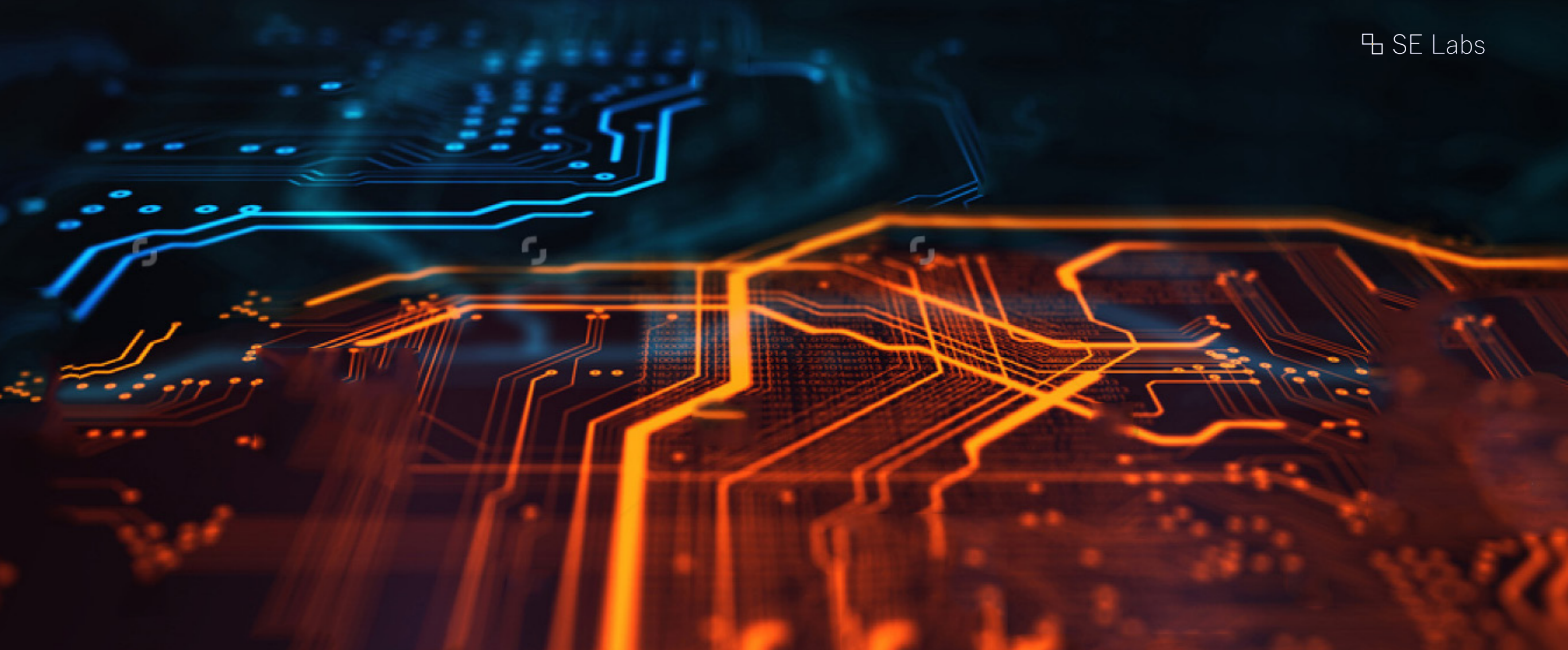## INTELLIGENCE-LED TESTING

HOME ANTI-MALWARE PROTECTION

JAN - MAR 2019

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

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

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

CONTENTS

INTRODUCTION

How can you tell if a security test is useful or not?

How to tell if security test results are useful, misleading or just rubbish

In security testing circles there is a theoretical test used to illustrate how misleading some test reports can be.

For this test you need three identical chairs, packaging for three anti-virus products (in the old days products came on discs in a cardboard box) and an open window on a high floor of a building.

The methodology of this test is as follows:
1. Tape each of the boxes to a chair. Do so carefully, such that each is fixed in exactly the same way.
2. Throw each of the chairs out of the window, using an identical technique.
3. Examine the chairs for damage and write a comparative report, explaining the differences found.
4. Conclude that the best product was the one attached to the least damaged chair.

The problem with this test is obvious: the conclusions are not based on any useful reality.

The good part about this test is that the tester created a methodology and tested each product in exactly the same way.* And at least this was an 'apples to apples' test, in which similar products were tested in the same manner. Hopefully any tester running the chair test publishes the methodology so that readers realise what a stupidly meaningless test has been performed, but that is not a given. Sometimes test reports come with very vague statements about, "how we tested".

When evaluating a test report of anything, not only security products, we advise that you check how the testing was performed and to check

whether or not it has been found compliant with a testing Standard, such as the Anti-Malware Testing Standards Organization's Standard (see below).

Headline-grabbing results (e.g. Anti-virus is Dead!) catch the eye, but we need to focus on the practical realities when trying to find out how best to protect our systems from cyber threats. And that means having enough information to be able to judge a test report's value rather than simply trusting blindly that the test was conducted correctly.

*Although some pedants might require that each chair be released from the window at exactly the same time – possibly from windows far enough apart that the chairs would not entangle mid-air and skew the results in some way.

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 v1.0. 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 *17*.

EXECUTIVE SUMMARY			
Products Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
McAfee Internet Security	100%	100%	100%
Symantec Norton Security	100%	100%	100%
ESET Internet Security	97%	100%	99%
F-Secure Safe	98%	99%	99%
Microsoft Windows Defender	96%	100%	99%
Avast Free Antivirus	95%	100%	98%
Kaspersky Internet Security	94%	100%	98%
Trend Micro Internet Security	94%	100%	98%
AVG Antivirus Free Edition	91%	100%	97%
Avira Free Security Suite	93%	98%	96%
Bullguard Internet Security	76%	99%	91%
G-Data Internet Security	75%	98%	90%
eScan Internet Security Suite	80%	91%	87%
K7 Antivirus Premium	55%	98%	83%

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.

■ **.. and targeted attacks were prevented in many cases.**
Many products were also competent at blocking more targeted, exploit-based attacks. However, while some did very well in this part of the test, others were very much weaker. Products from **K7** and **G-Data** 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. **eScan's** was the least accurate in this part of the test.

■ **Which products were the most effective?**
Products from **McAfee**, **Symantec** (**Norton**), **ESET**, **F-Secure** 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.
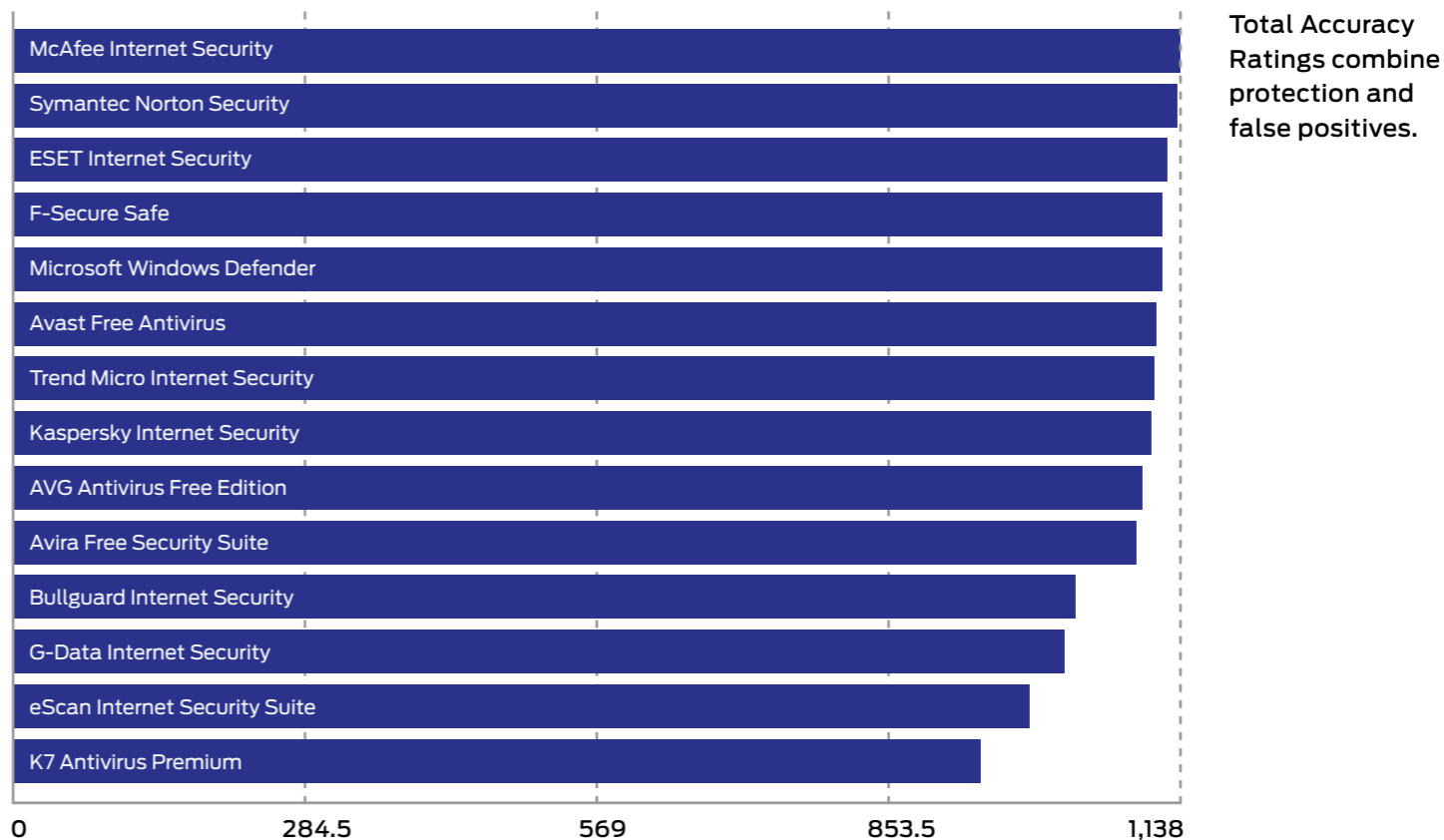
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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
5. Legitimate Software Ratings on page 12.

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
McAfee Internet Security	1,138	100%	AAA
Symantec Norton Security	1,136	100%	AAA
ESET Internet Security	1,126	99%	AAA
F-Secure Safe	1,121	99%	AAA
Microsoft Windows Defender	1,121	99%	AAA
Avast Free Antivirus	1,116	98%	AAA
Trend Micro Internet Security	1,114	98%	AAA
Kaspersky Internet Security	1,112	98%	AAA
AVG Antivirus Free Edition	1,102	97%	AAA
Avira Free Security Suite	1,095.5	96%	AAA
Bullguard Internet Security	1,036	91%	AA
G-Data Internet Security	1,026	90%	AA
eScan Internet Security Suite	991	87%	A
K7 Antivirus Premium	943	83%	B

Total Accuracy Ratings combine protection and false positives.

McAfee Internet Security
Symantec Norton Security
ESET Internet Security
F-Secure Safe
Microsoft Windows Defender
Avast Free Antivirus
Trend Micro Internet Security
Kaspersky Internet Security
AVG Antivirus Free Edition
Avira Free Security Suite
Bullguard Internet Security
G-Data Internet Security
eScan Internet Security Suite
K7 Antivirus Premium

0   284.5   569   853.5   1,138

Home Anti-Malware Protection Awards

The following products win SE Labs awards:

- **McAfee** Internet Security

- **Symantec** Norton Security

- **ESET** Internet Security

- **F-Secure** Safe

- **Microsoft** Windows Defender

- **Avast** Free Antivirus

- **Trend Micro** Internet Security

- **Kaspersky** Internet Security

- **Avira** Free Security Suite

- **AVG** Antivirus Free Edition

SE Labs — AAA — HOME ANTI-MALWARE PROTECTION — JAN-MAR 2019

- **Bullguard** Internet Security

- **G-Data** Internet Security

SE Labs — AA — HOME ANTI-MALWARE PROTECTION — JAN-MAR 2019

- **eScan** Internet Security Suite

SE Labs — A — HOME ANTI-MALWARE PROTECTION — JAN-MAR 2019

- **K7** Antivirus Premium

SE Labs — B — HOME ANTI-MALWARE PROTECTION — JAN-MAR 2019
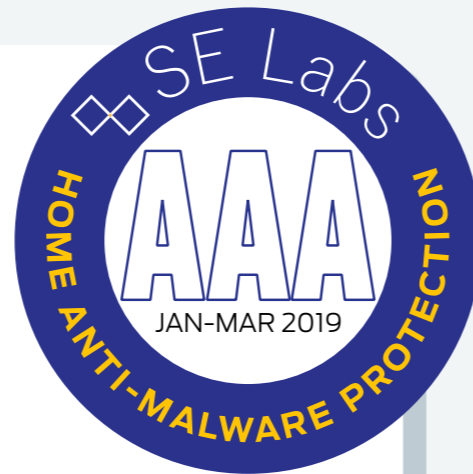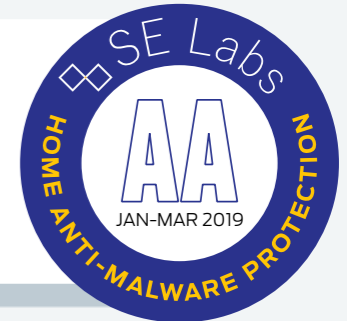
2. Protection Ratings

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.

■ **Neutralised (+1)**

Products that kill all running malicious processes 'neutralise' the threat and win one point.

■ **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.

■ **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 *4. Protection Details* on page *11* 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 RATINGS

Product	Protection Rating	Protection Rating (%)
McAfee Internet Security	400	100%
Symantec Norton Security	398	100%
F-Secure Safe	390	98%
ESET Internet Security	388	97%
Microsoft Windows Defender	383	96%
Avast Free Antivirus	378	95%
Trend Micro Internet Security	376	94%
Kaspersky Internet Security	374	94%
Avira Free Security Suite	370	93%
AVG Antivirus Free Edition	364	91%
eScan Internet Security Suite	321	80%
Bullguard Internet Security	305	76%
G-Data Internet Security	300	75%
K7 Antivirus Premium	220	55%

McAfee Internet Security

Symantec Norton Security

F-Secure Safe

ESET Internet Security

Microsoft Windows Defender

Avast Free Antivirus

Trend Micro Internet Security

Kaspersky Internet Security

Avira Free Security Suite

AVG Antivirus Free Edition

eScan Internet Security Suite

Bullguard Internet Security

G-Data Internet Security

K7 Antivirus Premium

0   100   200   300   400

Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.
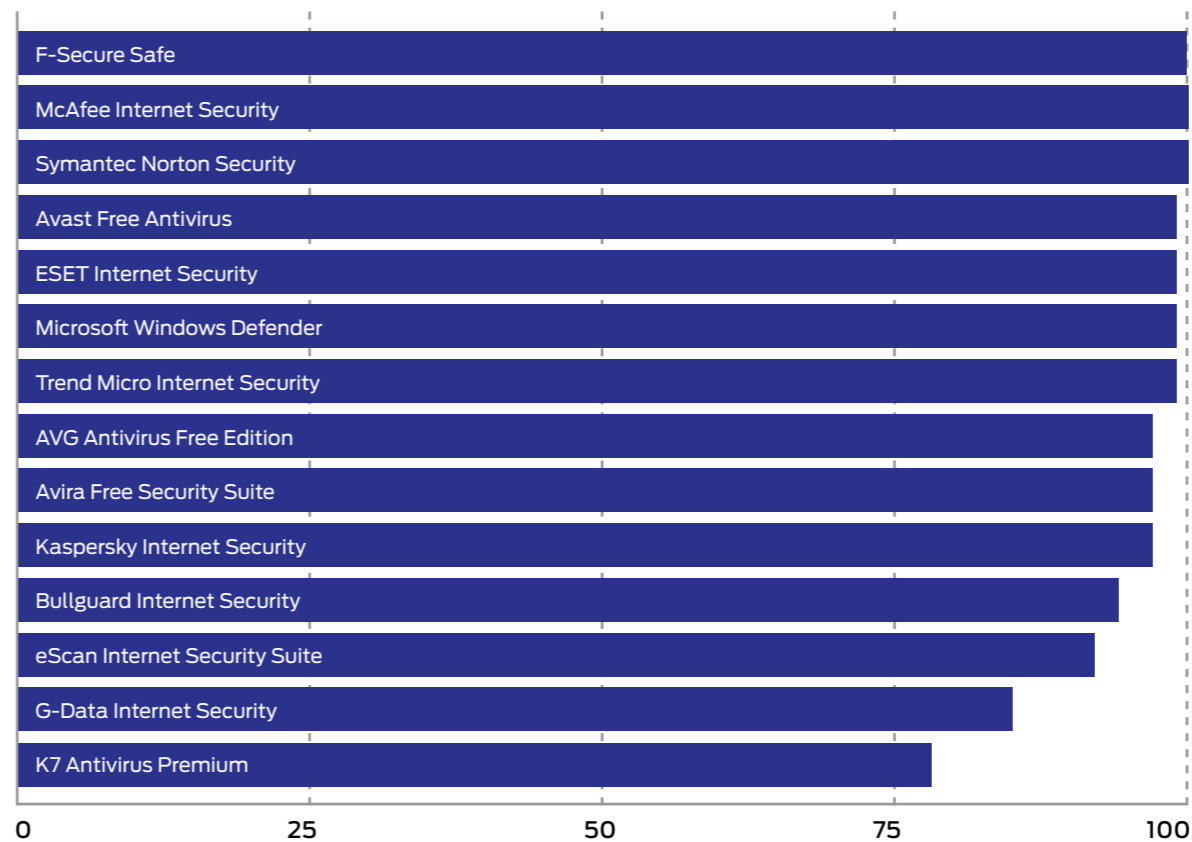
Average 87%
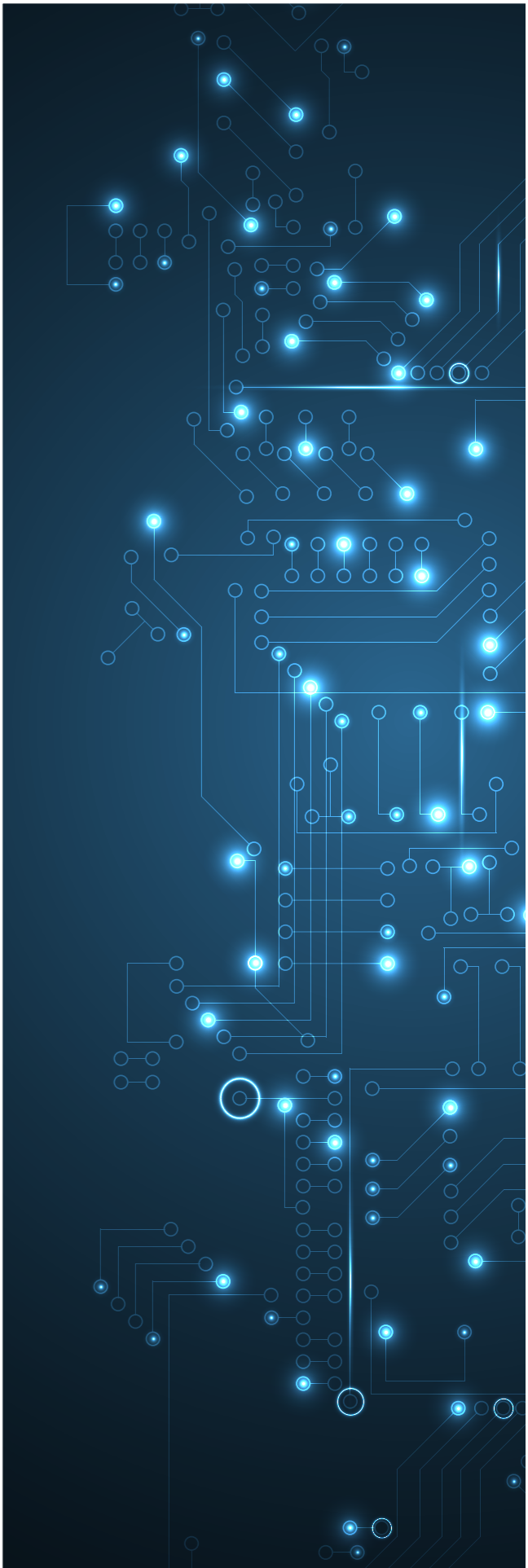
3. Protection Scores

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
F-Secure Safe	100
McAfee Internet Security	100
Symantec Norton Security	100
Avast Free Antivirus	99
ESET Internet Security	99
Microsoft Windows Defender	99
Trend Micro Internet Security	99
AVG Antivirus Free Edition	97
Avira Free Security Suite	97
Kaspersky Internet Security	97
Bullguard Internet Security	94
eScan Internet Security Suite	92
G-Data Internet Security	85
K7 Antivirus Premium	78

F-Secure Safe
McAfee Internet Security
Symantec Norton Security
Avast Free Antivirus
ESET Internet Security
Microsoft Windows Defender
Trend Micro Internet Security
AVG Antivirus Free Edition
Avira Free Security Suite
Kaspersky Internet Security
Bullguard Internet Security
eScan Internet Security Suite
G-Data Internet Security
K7 Antivirus Premium

0   25   50   75   100

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

4. 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
F-Secure Safe	100	100	0	0	100
McAfee Internet Security	100	100	0	0	100
Symantec Norton Security	100	100	0	0	100
Trend Micro Internet Security	100	99	0	1	99
ESET Internet Security	99	98	1	1	99
Microsoft Windows Defender	99	97	2	1	99
Avast Free Antivirus	100	93	6	1	99
Kaspersky Internet Security	100	97	0	3	97
Avira Free Security Suite	99	97	0	3	97
AVG Antivirus Free Edition	100	89	8	3	97
Bullguard Internet Security	96	74	20	6	94
eScan Internet Security Suite	94	81	11	8	92
G-Data Internet Security	95	82	3	15	85
K7 Antivirus Premium	95	63	15	22	78

This data shows in detail how each product handled the threats used.
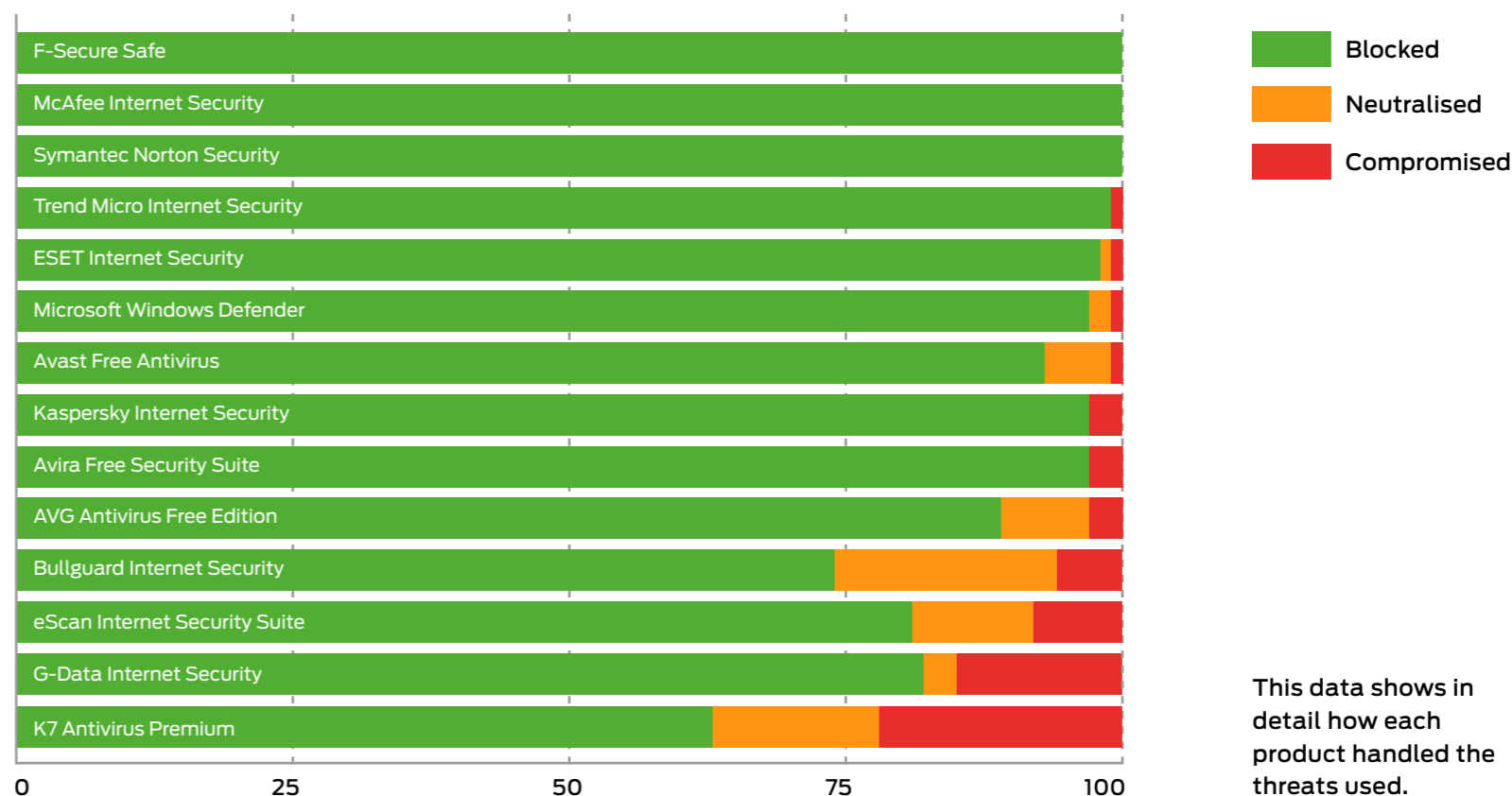
5. Legitimate Software Ratings

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 *5.3 Accuracy Ratings* on page *14.*

LEGITIMATE SOFTWARE RATINGS		
Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Avast Free Antivirus	738	100%
AVG Antivirus Free Edition	738	100%
ESET Internet Security	738	100%
Kaspersky Internet Security	738	100%
Microsoft Windows Defender	738	100%
McAfee Internet Security	738	100%
Symantec Norton Security	738	100%
Trend Micro Internet Security	738	100%
Bullguard Internet Security	731	99%
F-Secure Safe	731	99%
G-Data Internet Security	726	98%
Avira Free Security Suite	725.5	98%
K7 Antivirus Premium	723	98%
eScan Internet Security Suite	670	91%

Avast Free Antivirus

AVG Antivirus Free Edition

ESET Internet Security

Kaspersky Internet Security

Microsoft Windows Defender

McAfee Internet Security

Symantec Norton Security

Trend Micro Internet Security

Bullguard Internet Security

F-Secure Safe

G-Data Internet Security

Avira Free Security Suite

K7 Antivirus Premium

eScan Internet Security Suite

0   369   738
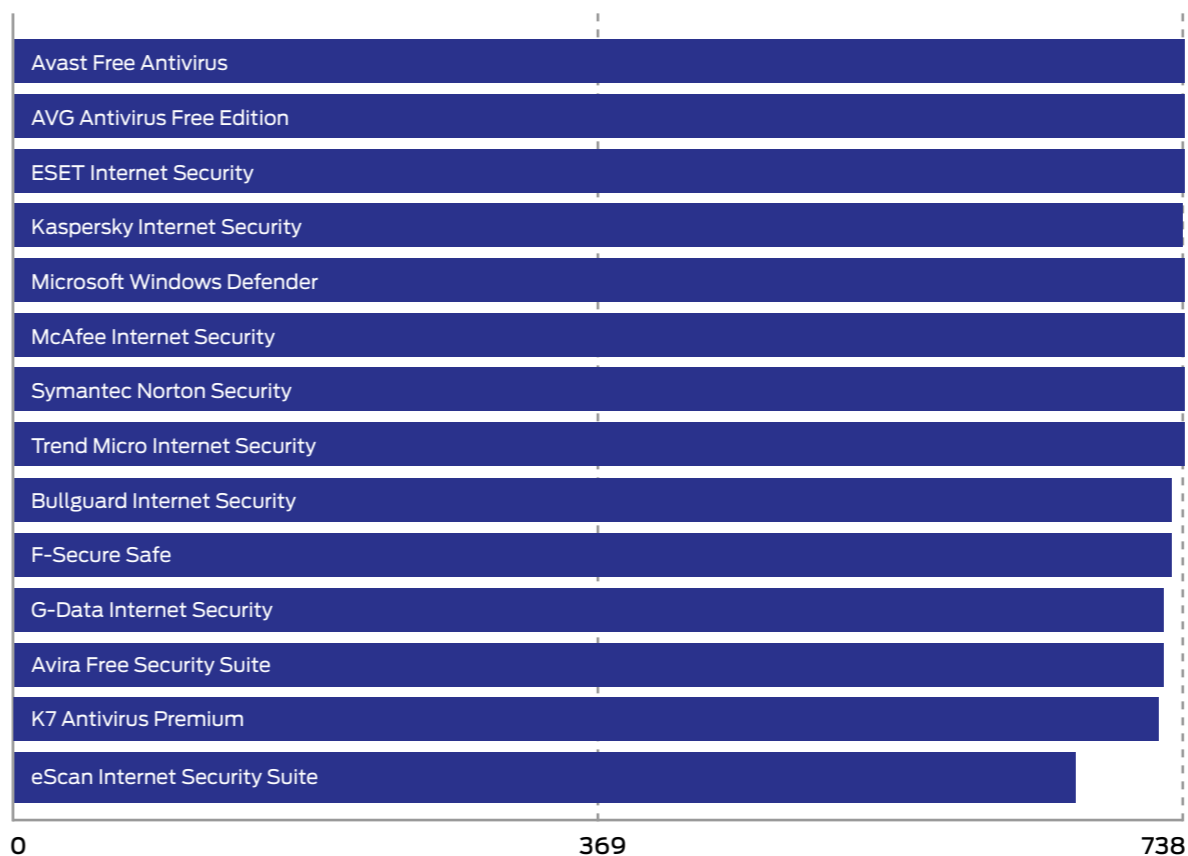
Legitimate Software Ratings can indicate how well a vendor has tuned its detection engine.

5.1 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)	Click to Allow (Default Allow)	Click to Block (Default Block)
Avast Free Antivirus	100	0	0
AVG Antivirus Free Edition	100	0	0
Avira Free Security Suite	100	0	0
ESET Internet Security	100	0	0
Kaspersky Internet Security	100	0	0
McAfee Internet Security	100	0	0
Microsoft Windows Defender	100	0	0
Symantec Norton Security	100	0	0
Trend Micro Internet Security	100	0	0
Bullguard Internet Security	99	1	0
F-Secure Safe	99	1	0
G-Data Internet Security	98	0	2
K7 Antivirus Premium	98	2	0
eScan Internet Security Suite	95	5	0

5.2 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.

5.3 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 *5. Legitimate Software Ratings* on page *12*.

5.4 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	33
High Impact	32
Medium Impact	15
Low Impact	11
Very Low Impact	9
TOTAL	100

6. 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 K7's product struggled a little. Targeted attacks were also handled well by most but caused some significant problems for the products from K7 and G-Data. K7 believes that its Total Security product is better suited to this type of testing and would have performed more strongly.

The McAfee, F-Secure and Symantec (Norton) products blocked all of the public and targeted attacks. Those same McAfee and Symantec products also handled all of the legitimate applications correctly.

Products from Microsoft, Avast, Trend Micro and Kaspersky Lab follow up close behind. Microsoft Defender missed one public threat; Avast's and Trend Micro's missed one targeted attack; while Kaspersky Labs' missed one public threat and two targeted attacks.

G-Data Internet Security stopped only 10 of the 25 targeted attacks, while K7 Antivirus Premium missed six public attacks and a rather concerning 16 targeted attacks.

The leading products from McAfee, Symantec (Norton), ESET, F-Secure, Microsoft, Avast, Trend Micro, Kaspersky Labs, Avira and AVG 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 8th January to 8th March 2019.
- 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			
Provider	Product Name	Build Version (start)	Build Version (end)
Avast	Free Antivirus	19.1.2360 (build 19.1.4142.0)	19.2.2364 (build 19.2.2364)
AVG	Antivirus Free Edition	19.1.3075	19.2.3079
Avira	Free Security Suite	15.0.43.24	15.0.43.24
Bullguard	Internet Security	19.0.360.4	19.0.362.5
eScan	Internet Security Suite	14.0.1400.2117 DB	14.0.1400.2117 DB
ESET	Internet Security	12.0.31.0	12.1.31.0
F-Secure	Safe	17.215.129	17.5
G-Data	Internet Security	25.4.0.4	25.5.2.7
K7	Antivirus Premium	15.1.0337	15.1.0341
Kaspersky Lab	Internet Security	19.0.0.1088(d)	19.0.0.1088(d)
Microsoft	Windows Defender	Antimalware Client Version: 4.12.17007.18022 Antivirus Version: 1.263.870.0	Antimalware Client Version: 4.18.1810.5 Engine Version: 1.1.15400.5, Antivirus Version: 1.281.899.0
McAfee	Internet Security	16.0. R17	16.0
Symantec	Norton Security	22.16.3.21	22.17.0.183
Trend Micro	Internet Security	15.0.1212	15.0.1212

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
F-Secure Safe	75	25	100
McAfee Internet Security	75	25	100
Symantec Norton Security	75	25	100
Avast Free Antivirus	75	24	99
ESET Internet Security	74	25	99
Microsoft Windows Defender	74	25	99
Trend Micro Internet Security	75	24	99
AVG Antivirus Free Edition	75	22	97
Avira Free Security Suite	72	25	97
Kaspersky Internet Security	74	23	97
Bullguard Internet Security	73	21	94
eScan Internet Security Suite	73	19	92
G-Data Internet Security	75	10	85
K7 Antivirus Premium	69	9	78