SE Labs

INTELLIGENCE-LED TESTING

HOME ANTI-MALWARE PROTECTION

APR - JUN 2018

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
Director Simon Edwards
Operations Director Marc Briggs
Office Manager Magdalena Jurenko
Technical Lead Stefan Dumitrascu

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Liam Fisher
Gia Gorbold
Pooja Jain
Ivan Merazchiev
Jon Thompson
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 ONE Croydon, London, CR0 0XT

CONTENTS

Document version 1.0 Written 22nd July 2018
Document version 1.01 Updated 24th July 2018, due to a minor typographical error.

INTRODUCTION

Detected, blocked, quarantined, cleaned?

What happens when your choice of security software handles an attack?

It should be simple. You've clicked on the wrong link, opened a malicious email or installed something inadvisable. A threat is now attacking your PC and it's up to your choice of anti-malware product to handle things. But what does it actually do under the hood?

Detection is important. The product should recognise that a threat exists, even if it can't fully handle it. At least you can receive an alert and seek help (or an alternative anti-malware program!)

Blocking threats is also very important. Ideally the protection system will prevent the malware from running. Sometimes that doesn't happen and the malware runs. In that case one hopes that the security software would recognise that bad things are happening and stop them. This is what we call 'neutralisation'.

Following a neutralisation your computer might not be completely clean. There could be some rogue code still on your hard disk, possibly even on your Desktop. There might also be entries in the Registry and elsewhere that will try to run this code (or code that has been deleted or quarantined).

You probably want your system to be protected by having threats blocked and, in cases where they are not, that they be removed as fast as possible and all significant traces removed. We call this happy state 'complete remediation'.

In SE Labs tests we measure all of these outcomes, including the worst one: *compromise*.

If you want to know how the different products tested in this report handled threats in detail, check out the ***Protection Details*** *table and graph on page 10*. We don't show details of which products completely remediated threats and which did not when neutralising but the ***Protection Ratings*** *on page 8* take these into account.

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.

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 16.*

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Norton Security	99%	100%	100%
ESET Smart Security	98%	100%	99%
McAfee Internet Security	98%	100%	99%
Kaspersky Internet Security	97%	100%	99%
Trend Micro Internet Security	95%	98%	97%
Windows Defender	89%	100%	96%
Bitdefender Internet Security	88%	100%	96%
F-Secure Safe	96%	94%	94%
Avira Free Security Suite	86%	99%	94%
AVG Antivirus Free Edition	82%	100%	94%
Check Point ZoneAlarm	78%	100%	92%
Avast Free Antivirus	76%	100%	91%
Webroot Antivirus	24%	99%	72%

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 endpoints 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. **ZoneAlarm** and **Webroot Antivirus** were notably weaker than the competition.

■ **False positives were not an issue for most products**
Most of the endpoint solutions were good at correctly classifying legitimate applications and websites. The vast majority allowed all of the legitimate websites and applications. **F-Secure's** was the least accurate in this part of the test.

■ **Which products were the most effective?**
Products from **Symantec (Norton)**, **McAfee**, **ESET**, **Kaspersky Lab**, **Trend Micro**, **Bitdefender** 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.

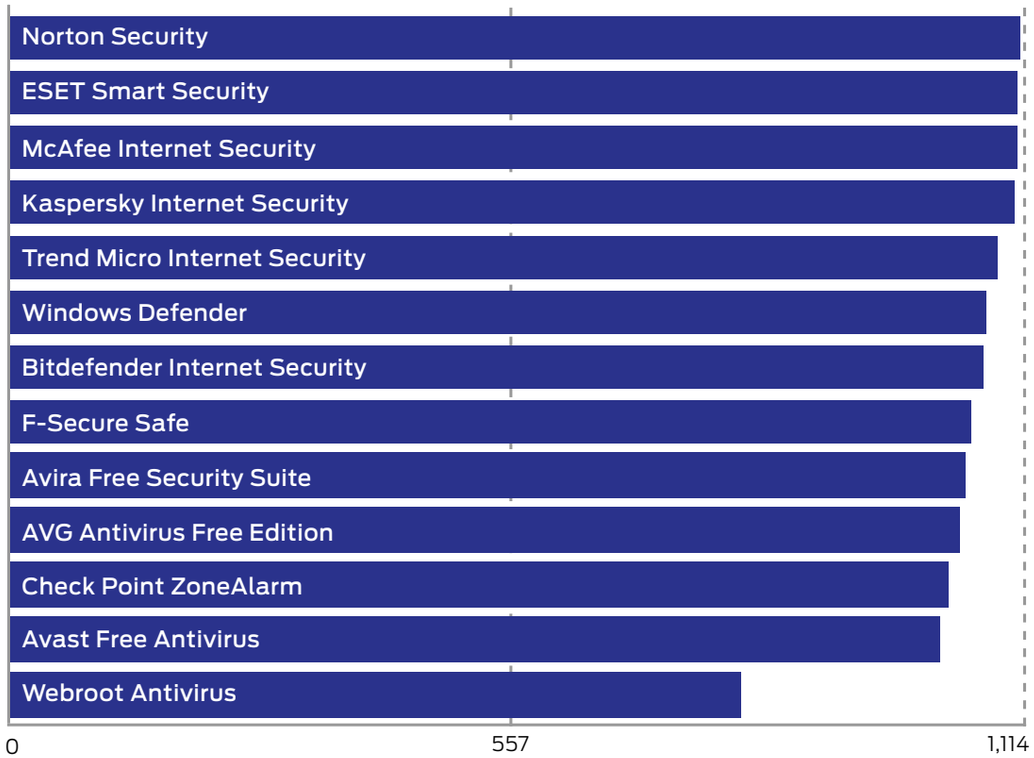
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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 11.

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Norton Security	1,109	100%	AAA
ESET Smart Security	1,104	99%	AAA
McAfee Internet Security	1,104	99%	AAA
Kaspersky Internet Security	1,102	99%	AAA
Trend Micro Internet Security	1,082	97%	AAA
Windows Defender	1,069	96%	AAA
Bitdefender Internet Security	1,067	96%	AAA
F-Secure Safe	1,052	94%	AA
Avira Free Security Suite	1,047	94%	AA
AVG Antivirus Free Edition	1,042	94%	AA
Check Point ZoneAlarm	1,027	92%	AA
Avast Free Antivirus	1,017	91%	AA
Webroot Antivirus	802.5	72%	



Total Accuracy Ratings combine protection and false positives.

Home Anti-Malware Protection Awards

The following products win SE Labs awards:

- **Norton** Security
- **ESET** Smart Security
- **McAfee** Internet Security
- **Kaspersky** Internet Security
- **Trend Micro** Internet Security
- **Windows** Defender
- **Bitdefender** Internet Security

- **F-Secure** Safe
- **Avira** Free Security Suite
- **AVG** Antivirus Free Edition
- **Check Point** ZoneAlarm
- **Avast** Free Antivirus

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.

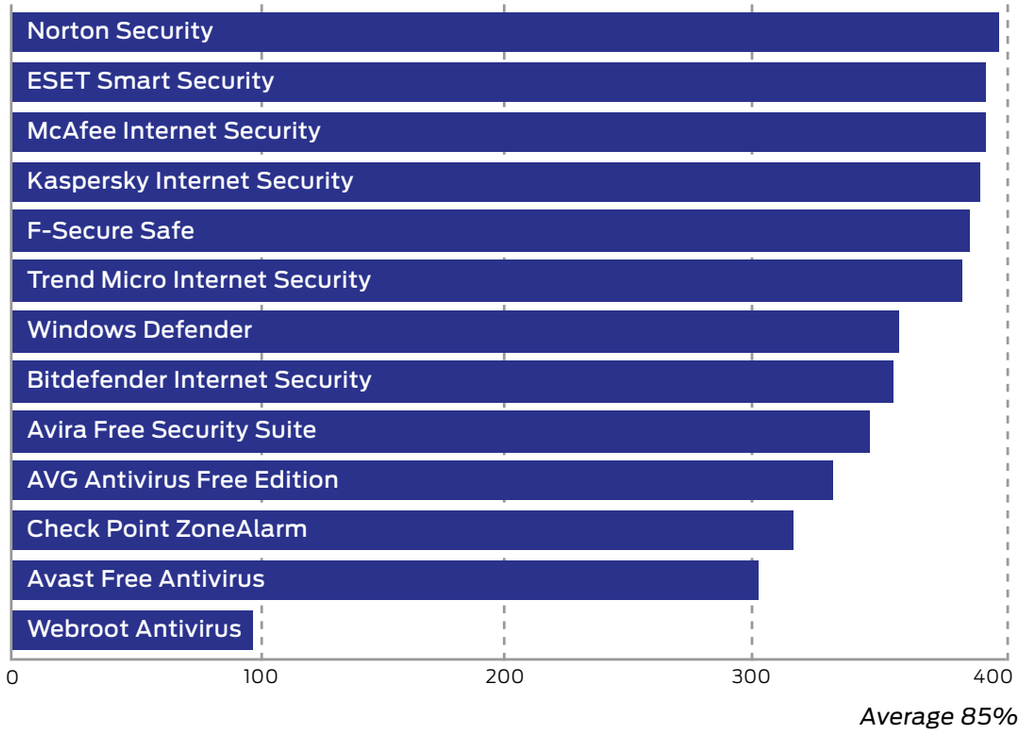
Complete Remediation (+1)
If, in addition to neutralising a threat, the product removes all significant traces of the attack, it gains an additional one point.

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

PROTECTION RATINGS		
Product	Protection Rating	Protection Rating (%)
Norton Security	395	99%
ESET Smart Security	390	98%
McAfee Internet Security	390	98%
Kaspersky Internet Security	388	97%
F-Secure Safe	383	96%
Trend Micro Internet Security	380	95%
Windows Defender	355	89%
Bitdefender Internet Security	353	88%
Avira Free Security Suite	343	86%
AVG Antivirus Free Edition	328	82%
Check Point ZoneAlarm	313	78%
Avast Free Antivirus	303	76%
Webroot Antivirus	96	24%

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



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.

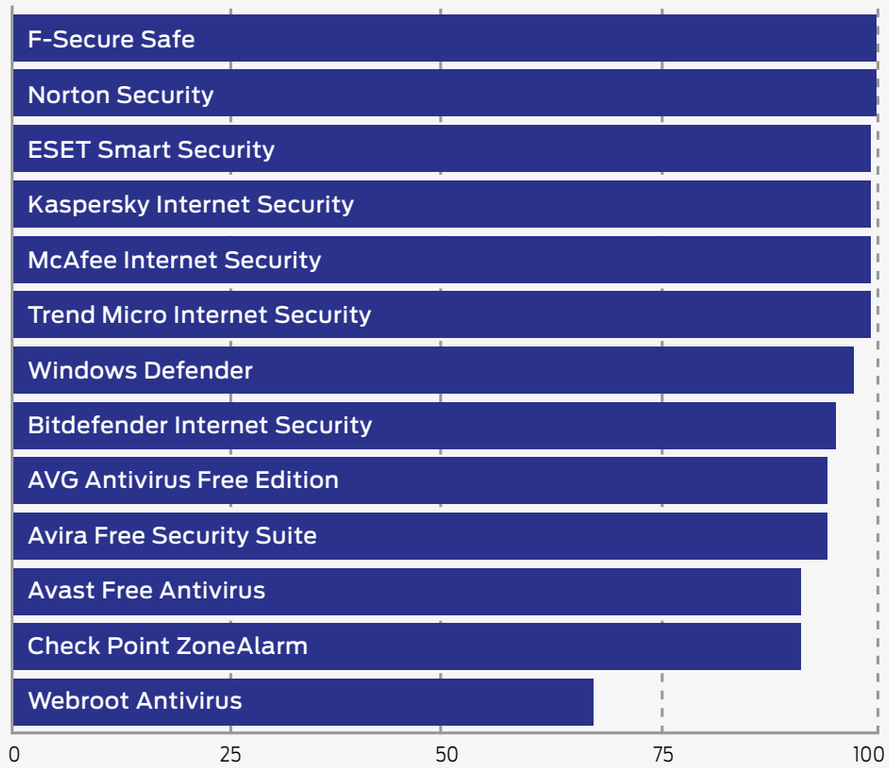
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how seriously you treat a 'Compromise' or 'Neutralisation without complete remediation'. If you want to create your own rating system, you can use the raw data from ***4. Protection Details*** *on page 10 to roll your own set of personalised ratings.*

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
Norton Security	100
ESET Smart Security	99
Kaspersky Internet Security	99
McAfee Internet Security	99
Trend Micro Internet Security	99
Windows Defender	97
Bitdefender Internet Security	95
AVG Antivirus Free Edition	94
Avira Free Security Suite	94
Avast Free Antivirus	91
Check Point ZoneAlarm	91
Webroot Antivirus	67

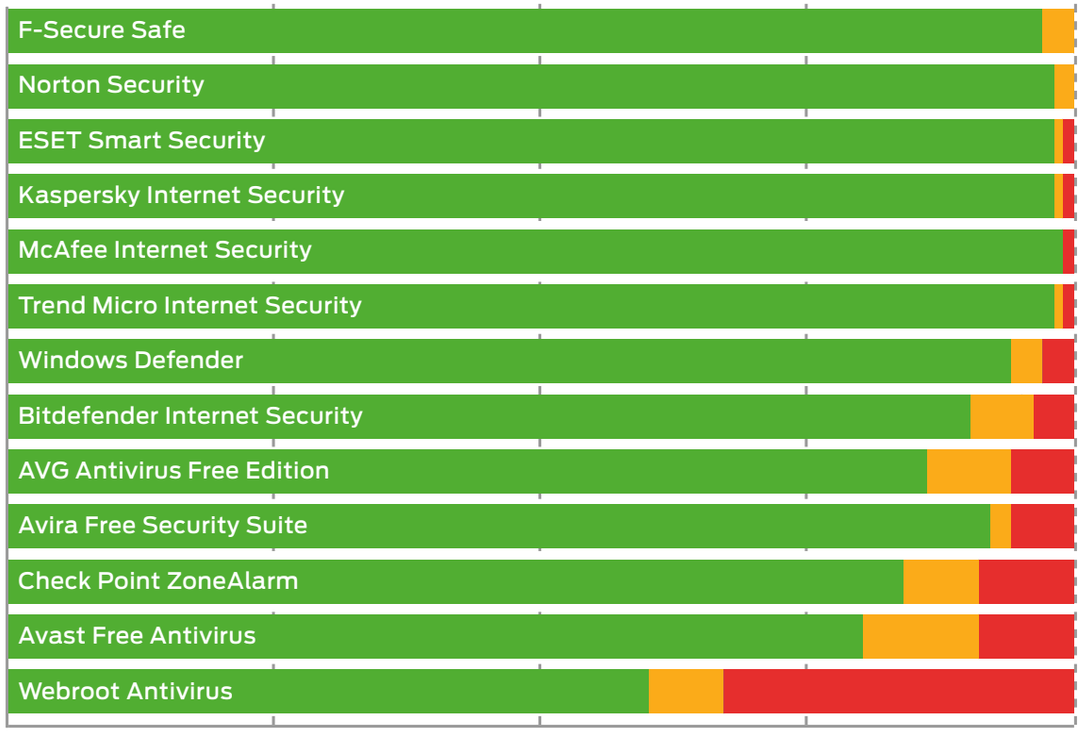


Protection Scores are a simple count of how many times a product protected the system.

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.



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

PROTECTION DETAILS

Product	Detected	Blocked	Neutralised	Persistent Neutralisation	Compromised	Protected
F-Secure Safe	100	97	3	0	0	100
Norton Security	100	98	2	0	0	100
ESET Smart Security	100	98	1	0	1	99
Kaspersky Internet Security	100	98	1	0	1	99
McAfee Internet Security	100	99	0	0	1	99
Trend Micro Internet Security	100	98	1	0	1	99
Windows Defender	100	94	3	0	3	97
Bitdefender Internet Security	100	90	6	0	4	95
AVG Antivirus Free Edition	99	86	8	0	6	94
Avira Free Security Suite	99	92	2	0	6	94
Check Point ZoneAlarm	100	84	7	0	9	91
Avast Free Antivirus	95	80	11	0	9	91
Webroot Antivirus	90	60	7	0	33	67

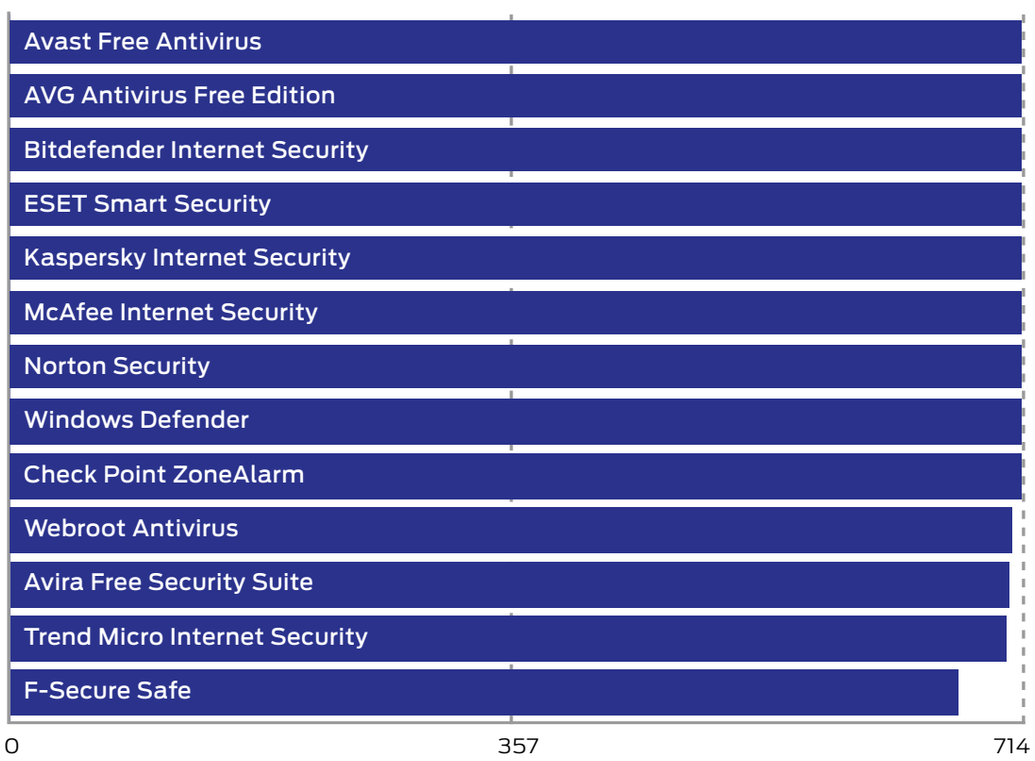
5. Legitimate Software Ratings

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 13.*

LEGITIMATE SOFTWARE RATINGS		
Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Avast Free Antivirus	714	100%
AVG Antivirus Free Edition	714	100%
Bitdefender Internet Security	714	100%
Check Point ZoneAlarm	714	100%
ESET Smart Security	714	100%
Kaspersky Internet Security	714	100%
McAfee Internet Security	714	100%
Norton Security	714	100%
Windows Defender	714	100%
Webroot Antivirus	706.5	99%
Avira Free Security Suite	704	99%
Trend Micro Internet Security	702	98%
F-Secure Safe	669	94%



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)	None (blocked)
Avast Free Antivirus	100	0
AVG Antivirus Free Edition	100	0
Avira Free Security Suite	100	0
Bitdefender Internet Security	100	0
Check Point ZoneAlarm	100	0
ESET Smart Security	100	0
Kaspersky Internet Security	100	0
McAfee Internet Security	100	0
Norton Security	100	0
Webroot Antivirus	100	0
Windows Defender	100	0
Trend Micro Internet Security	99	1
F-Secure Safe	97	3

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 CATEGORY FREQUENCY	
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 11.*

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	25
High impact	37
Medium impact	17
Low impact	12
Very low impact	9
GRAND 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 every vendor being tested should do poorly.

Consequently, it's not a shock to see all products handle the public threats very effectively. **Webroot Antivirus** was a little weaker than the competition here, though. Targeted attacks were also handled well by most but caused some significant problems for the products from **Check Point** (**ZoneAlarm**) and **Webroot**. **Webroot** notes that testing occurred before it released its script and anti-exploit protection.

The **Symantec** and **F-Secure** products blocked all of the public and targeted attacks. **Norton** handled all of the legitimate applications correctly, while **F-Secure** Safe did not. **McAfee Internet Security**, **Kaspersky Internet Security** and **ESET Smart Security** each missed one targeted attack but did correctly handle all legitimate software.

Products from **Bitdefender** and **Microsoft** follow up close behind, handling legitimate applications with similar accuracy and fighting off the vast majority of threats.

ZoneAlarm Free Antivirus allowed a number of targeted attacks to infect the system. **Webroot** missed a few public threats and all but one of the targeted threats. The **Webroot** product scored the lowest, failing to achieve a rating.

The leading products from **Symantec** (**Norton**), **McAfee**, **ESET**, **Kaspersky Lab**, **Trend Micro**, **Bitdefender** and **Microsoft** 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 3rd April and 5th June 2018.
- 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.

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	Avast Free Antivirus	18.2.2328 (build 18.2.3827.307)	Program version: 18.4.2338 (build 18.4.3895.325); virus definitions versions: 180603-4
AVG	AVG Antivirus Free Edition	Software: 18.2.3046	Software version: 18.4.3056, Virus definitions version: 180605-4
Avira	Avira Free Security Suite	1.2.106.18629/ 15.0.34.27	15.0.36.180
Bitdefender	Internet Security	Build: 22.0.19.242	Build: 22.0.21.297, Virus signatures: 12135188, Engine version: 7.76264
Check Point	ZoneAlarm	Firewall: 15.1.522.17528; Vsmon 15.1.522.17528; Driver: 15.1.29.17237; Antivirus Engine: 8.7.1.99; Antivirus signature DAT file: 1282821344	15.1.522.17528; Vsmon: 15.1.522.17528; Driver version: 15.1.29.17237; Antivirus engine version: 8.7.1.99; Antivirus signature DAT file version: 1288004416
ESET	ESET Smart Security	10.1.235.0	ESET Version: 11.1.54.0, Windows 10 Version: 10.0.16299
F-Secure	F-Secure Safe	Antivirus: 17.204.106; Family Rules: 2.204.7118.12; Common Component Framework 3.04.148	F-Secure SAFE 17.3; Antivirus 17.211.122; Family Rules 2.221.7392.4091; Common Component Framework 3.11.269
Kaspersky Lab	Kaspersky Internet Security	18.0.0.405 (g)	18.0.0.405 (h)
McAfee	McAfee Internet Security	16	McAfee Internet Security - Version: 16.0, Release Name: 16.0 R6, McAfee SecurityCenter - Version: 16.6, Build: 16.6.149, McAfee VirusScan - Version: 20.6, Build: 20.6.170, Engine version: 3366.0, McAfee Personal Firewall - Version: 17.6, Build: 17.6.135, McAfee WebAdvisor - Version: 4.0, Build: 4.0.7.141
Microsoft	Windows Defender	4.12.17007.18022 (Antimalware Client Version) 1.263.870.0 (Antivirus Version)	4.16.17656.18052 (Antimalware Client Version), 1.269.615.0 (Antivirus Version), 1.269.615.0 (Antispyware Version), 1.1.14901.4 (Engine Version)
Symantec	Norton Security	22.12.1.15	22.14.0.54
Trend Micro	Trend Micro Internet Security	12	12.0.1226
Webroot	Webroot Antivirus	9.0.19.43	9.0.20.31

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
Norton Security	75	25	100
ESET Smart Security	75	24	99
Kaspersky Internet Security	75	24	99
McAfee Internet Security	75	24	99
Trend Micro Internet Security	75	24	99
Windows Defender	72	25	97
Bitdefender Internet Security	74	21	95
AVG Antivirus Free Edition	74	20	94
Avira Free Security Suite	72	22	94
Check Point ZoneAlarm	75	16	91
Avast Free Antivirus	73	18	91
Webroot Antivirus	66	1	67