SE Labs

INTELLIGENCE-LED TESTING

HOME ANTI-MALWARE PROTECTION

JAN - MAR 2017

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 web-based threats that were found to be live on the internet at the time of the test.

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

CONTENTS

Document version 1. 0. Written 7th April 2017

INTRODUCTION

Endpoint security is an important component of computer security, whether you are a home user, a small business or running a massive company. But it's just one layer.

Using multiple layers of security – including a firewall, anti-exploit technologies built into the operating system and virtual private networks (VPNs) when using third-party Wi-Fi – is important, too.

Many people don't realise that anti-malware software often contains its own layers of protection. Threats can come at you from many different angles, which is why security vendors try to block and stop them using a whole chain of approaches.

For example, consider a malicious website that will infect victims automatically when they visit the site. Such 'drive-by' threats are common and make up about one third of this test's set of attacks. You visit the site with your browser and it exploits a vulnerability on your computer, before installing malware – possibly ransomware, a type of malware that also features prominently in this test.

Here's how the layers of endpoint security can work. The URL (web link) filter might block you from visiting the dangerous site. If that works, you're safe and nothing else need be done. But say this layer of security crumbles, and the system is exposed to the exploit. Maybe the product's anti-exploit technology prevents the exploit from running or, at least, running fully? If so, great. If not, the threat will likely download the ransomware and try to run it.

At this stage file signatures may come into play. Additionally, the malware's behaviour can be analysed. Maybe it is tested in a virtual sandbox first. Different vendors use different approaches. Ultimately the threat has to move down through a series of layers of protection in all but the most basic of 'anti-virus' products.

The way we test endpoint security is realistic and allows all layers of its protection to be tested.

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.

SIMON EDWARDS
Director

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

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Stefan Dumitrascu
Gia Gorbold
Magdalena Jurenko
Jon Thompson
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Steve Haines
Colin Mackleworth

SE Labs Ltd is a member of the Anti-Malware Testing Standards Organization (AMTSO)

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.

Products tested

PRODUCT	PROTECTION ACCURACY RATING	LEGITIMATE ACCURACY RATING	TOTAL ACCURACY RATING
Kaspersky Internet Security	100%	100%	100%
Norton Security	100%	100%	100%
ESET Smart Security	99%	100%	100%
Bitdefender Internet Security	96%	98%	97%
Trend Micro Internet Security 10	94%	98%	97%
Microsoft Security Essentials	84%	98%	94%
AVG AntiVirus Free Edition	83%	98%	93%
Avast Free Antivirus	87%	95%	92%

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 mainly effective at handling general threats from cyber criminals...**
Most products were capable of handling public web-based threats such as those used by criminals to attack Windows PCs and install ransomware automatically, without having to trick a user into clicking an install button.

● **...but targeted attacks posed more of a challenge**
Half of the products were very competent at blocking more targeted, exploit-based attacks. Only the products from Bitdefender, ESET, Kaspersky Lab and Symantec (Norton) handled the targeted attacks comprehensively.

● **False positives were not an issue for most products**
All endpoint solutions were good at correctly classifying legitimate applications and websites. Two out of the eight products made no mistakes at all and products that blocked them did so sparingly.

● **Which products were the most effective?**
ESET, Symantec and Kaspersky Lab products achieved the best results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites.

Simon Edwards, SE Labs, 7th April 2017

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.
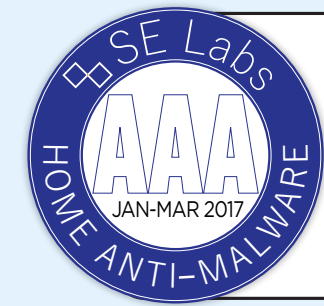
For example, a product that completely blocks a threat is rated more highly than one that allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

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

Total Accuracy Ratings combine protection and false positives.
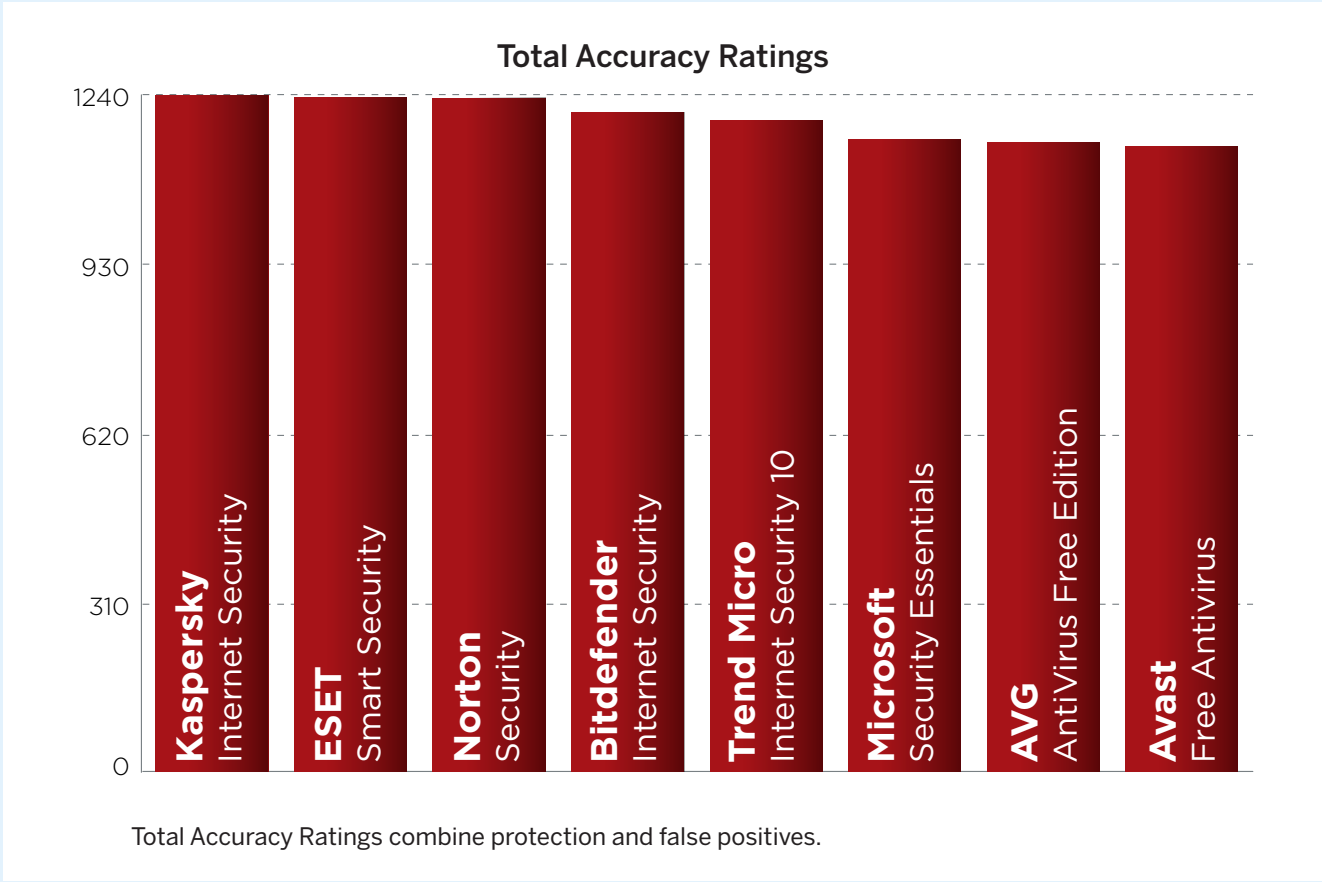
Awards

The following products win SE Labs awards:

- Kaspersky Internet Security
- ESET Smart Security
- Norton Security
- Bitdefender Internet Security
- Trend Micro Internet Security 10

- Microsoft Security Essentials
- AVG AntiVirus Free Edition
- Avast Free Antivirus

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Kaspersky Internet Security	1240	100%	AAA
ESET Smart Security	1236	100%	AAA
Norton Security	1235	100%	AAA
Bitdefender Internet Security	1208	97%	AAA
Trend Micro Internet Security 10	1197	97%	AAA
Microsoft Security Essentials	1160	94%	AA
AVG AntiVirus Free Edition	1154	93%	AA
Avast Free Antivirus	1146	92%	AA

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 detected 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.
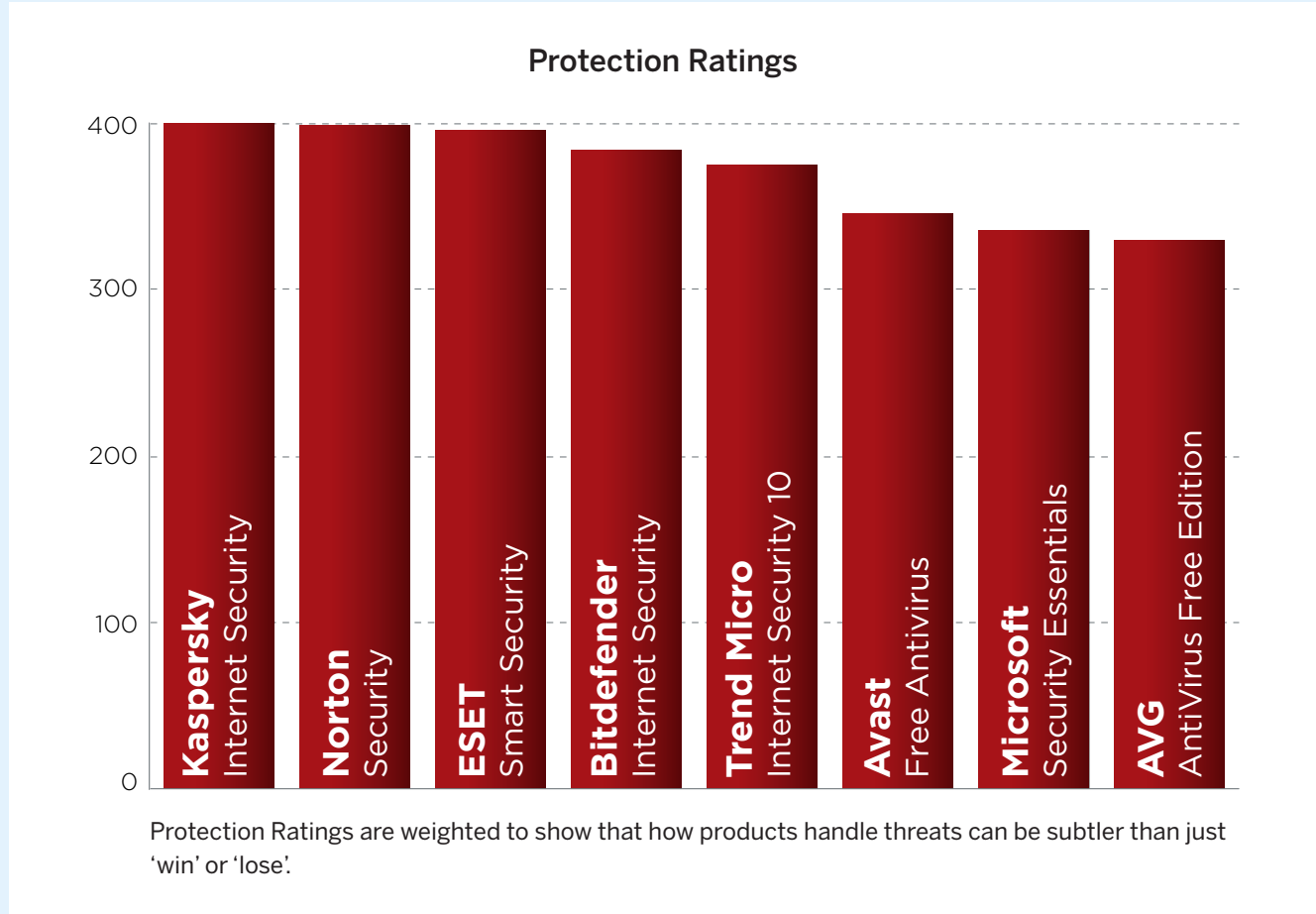
- **Neutralised (+1)**
Products that kill all running malicious processes 'neutralise' the threat and win one point.

- **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.

- **Compromised (-5)**
If the threat compromised 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.

Protection Ratings

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

PROTECTION RATINGS		
Product	**Protection Rating**	**Protection Rating %**
Kaspersky Internet Security	400	100%
Norton Security	399	100%
ESET Smart Security	396	99%
Bitdefender Internet Security	384	96%
Trend Micro Internet Security 10	377	94%
Avast Free Antivirus	346	87%
Microsoft Security Essentials	336	84%
AVG AntiVirus Free Edition	330	83%

Average: 93%

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

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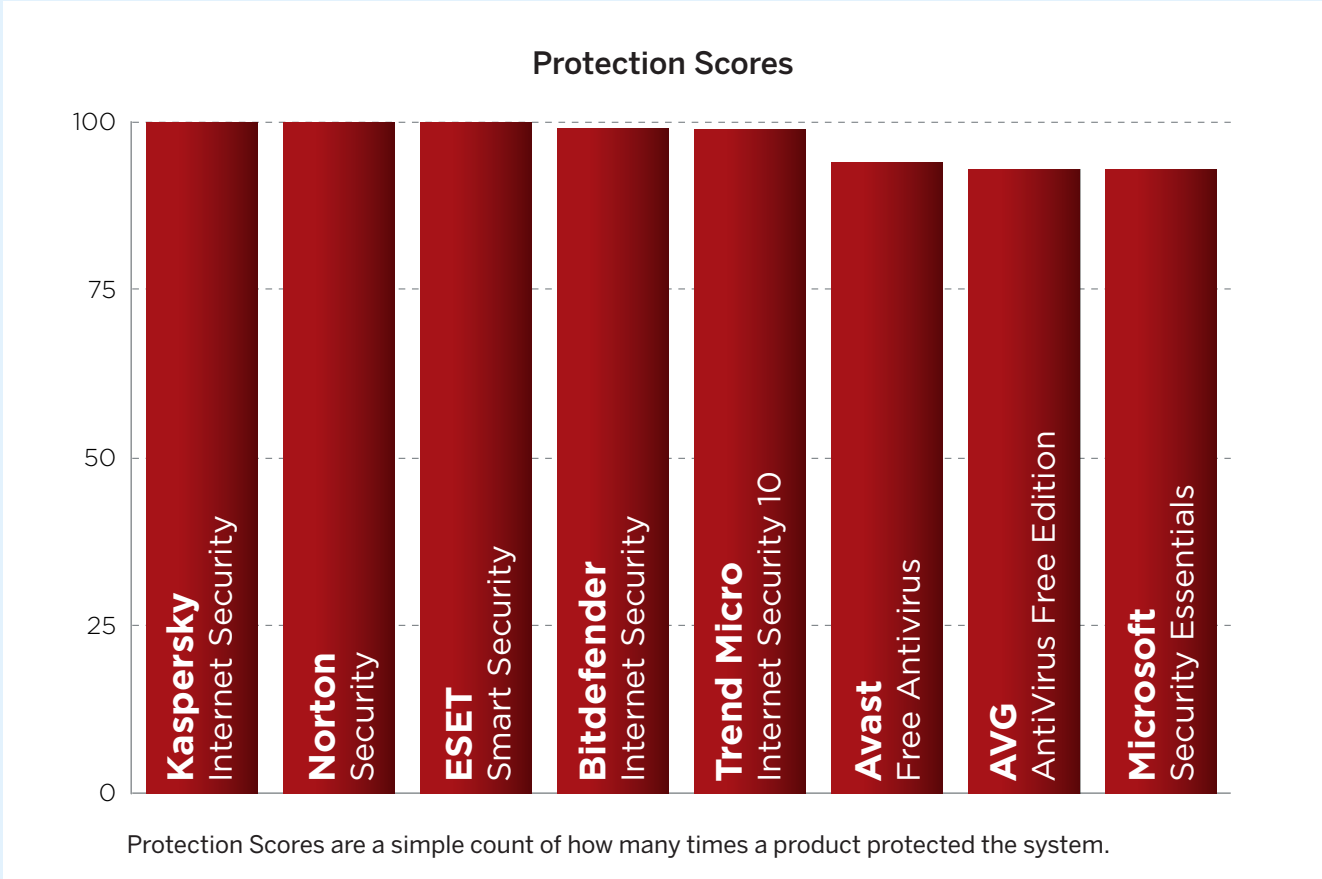
PROTECTION SCORES

Product	Protection Score
Kaspersky Internet Security	100
Norton Security	100
ESET Smart Security	100
Bitdefender Internet Security	99
Trend Micro Internet Security 10	99
Avast Free Antivirus	94
AVG AntiVirus Free Edition	93
Microsoft Security Essentials	93

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 are not 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

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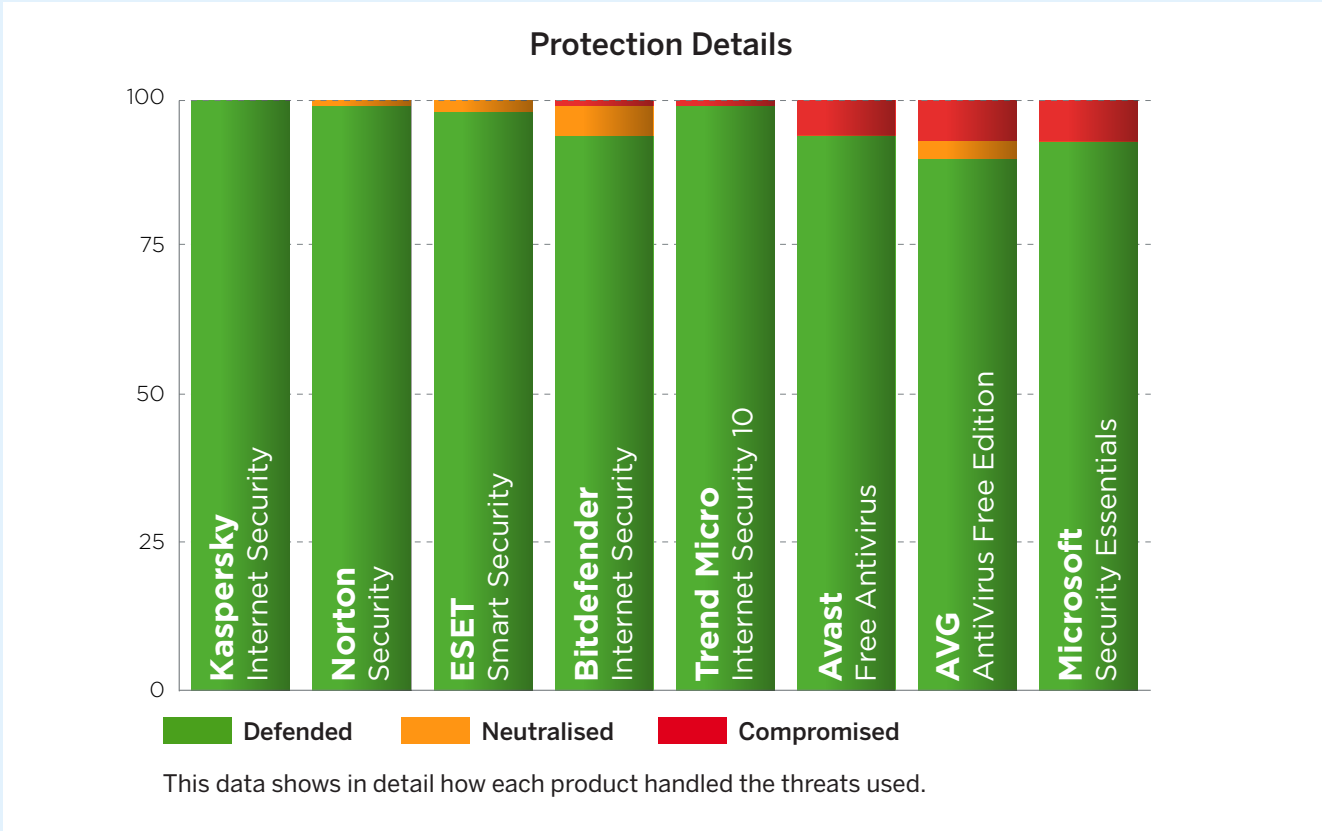
PROTECTION DETAILS

Product	Detected	Blocked	Neutralised	Compromised	Protected
Kaspersky Internet Security	100	100	0	0	100
Norton Security	100	99	1	0	100
ESET Smart Security	100	98	2	0	100
Bitdefender Internet Security	99	94	5	1	99
Trend Micro Internet Security 10	85	99	0	1	99
Avast Free Antivirus	94	94	0	6	94
AVG AntiVirus Free Edition	92	90	3	7	93
Microsoft Security Essentials	92	93	0	7	93

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 15.

Legitimate Software Ratings

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.

Interaction Ratings

	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.

LEGITIMATE SOFTWARE RATINGS

Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Kaspersky Internet Security	840	100%
ESET Smart Security	840	100%
Norton Security	836	100%
AVG AntiVirus Free Edition	824	98%
Bitdefender Internet Security	824	98%
Microsoft Security Essentials	824	98%
Trend Micro Internet Security 10	820	98%
Avast Free Antivirus	800	95%

INTERACTION RATINGS

Product	None (allowed)	Click to block (default block)	None (blocked)
ESET Smart Security	100	0	0
Kaspersky Internet Security	100	0	0
AVG AntiVirus Free Edition	99	1	0
Bitdefender Internet Security	99	0	1
Microsoft Security Essentials	99	0	1
Norton Security	99	0	1
Avast Free Antivirus	98	0	2
Trend Micro Internet Security 10	98	0	2

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	57
High impact	24
Medium impact	8
Low impact	4
Very low impact	7
Grand total	100

6. CONCLUSIONS

Attacks in this test included infected websites available to the general public, including sites that automatically attack visitors and attempt to infect them without any social engineering or other interaction. Some sites relied on users being fooled into installing the malware. We also included targeted attacks, which were exploit-based attempts to gain remote control of the target systems.

Kaspersky Internet Security protected against all of the public web-based threats and targeted attacks. It blocked 100 per cent of the threats and was also entirely effective when handling legitimate objects, giving it the rare privilege of a 100 per cent overall rating.

ESET Smart Security came an extremely close second. It neutralised two threats, which fractionally reduced its overall score, which is rounded up to 100 per cent in our table (a figure that is rounded up from 99.7 per cent).

Norton Security was just as effective when protecting the endpoint from targeted attacks and protected against all of the public threats. It neutralised one threat but was not compromised at all. It blocked one legitimate application.

Bitdefender Internet Security was able to fend off all of the exploit-based targeted attacks fully. It blocked all but one of the public web attacks. It neutralised five attacks, was compromised once and blocked one legitimate application.

Microsoft Security Essentials was the strongest free product in the test. It was compromised five times by the targeted attacks but protected against all but two of the web-based attacks. It only blocked one legitimate application.

Avast Free Antivirus was the least effective product in this test, although its performance was still strong enough to earn an AA award. It stopped a fair few of the targeted attacks and all of the public web threats, but its slightly less accurate handling of legitimate software pushed it to the bottom of the table.

The products from **ESET, Kaspersky Lab**, **Symantec (Norton)**, **Bitdefender and Trend Micro** all win AAA awards for their strong overall performance. Those from **Avast, AVG** and **Microsoft** achieved solid AA awards.

APPENDICES

APPENDIX A: TERMS USED

TERM	MEANING
Compromised	The attack succeeded, resulting in malware running unhindered on the target. In the case of a targeted attack, the attacker was able to take remote control of the system and carry out a variety of tasks without hindrance.
Blocked	The attack was prevented from making any changes to the target.
False positive	When a security product misclassifies a legitimate application or website as being malicious, it generates a 'false positive'.
Neutralised	The exploit or malware payload ran on the target but was subsequently removed.
Complete remediation	If a security product removes all significant traces of an attack, it has achieved complete remediation.
Target	The test system that is protected by a security product.
Threat	A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.
Update	Security vendors provide information to their products in an effort to keep abreast of the latest threats. These updates may be downloaded in bulk as one or more files, or requested individually and live over the internet.

APPENDIX B: FAQs

A **full methodology** for this test is available from our website.

- The products chosen for this test were selected by SE Labs.
- The test was not sponsored. This means that no security vendor has control over the report's content or its publication.
- The test was conducted between 10th January and 3rd March 2017.
- All products had full internet access and were confirmed to have access to any required or recommended back-end systems. This was confirmed, where possible, using the Anti-Malware Testing Standards Organization (AMTSO) **Cloud Lookup Features Setting Check**.
- Malicious URLs and legitimate applications and URLs were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs. They were created and managed by Metasploit Framework Edition using default settings. The choice of exploits was advised by public information about ongoing attacks. One notable source was the **2016 Data Breach Investigations Report** from Verizon.
- Malicious and legitimate data was provided to partner organisations once the full test was complete.
- SE Labs conducted this endpoint security testing on physical PCs, not virtual machines.

Q I am a security vendor. How can I include my product in your test?

A Please contact us at info@SELabs.uk. We will be happy to arrange a phone call to discuss our methodology and the suitability of your product for inclusion.

Q I am a security vendor. Does it cost money to have my product tested?

A We do not charge directly for testing products in public tests. We do charge for private tests.

Q What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

A Partner organisations support our tests by paying for access to test data after each test has completed but before publication. Partners can dispute results and use our award logos for marketing purposes. We do not share data on one partner with other partners. We do not currently partner with organisations that do not engage in our testing.

Q So you don't share threat data with test participants before the test starts?

A No, this would bias the test and make the results unfair and unrealistic.

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 small subsets of data with non-partner participants at our discretion. A small administration fee is applicable.

APPENDIX C: PRODUCT VERSIONS

A product's update mechanism may upgrade the software to a new version automatically so the version used at the start of the test may be different to that used at the end.

PRODUCT VERSIONS		
Vendor	**Product**	**Build**
Avast	Free Antivirus	17.2.2288
AVG	AntiVirus Free Edition	16.141.7998
Bitdefender	Internet Security	Signatures: 8066609 Engine: 7.70071
ESET	Smart Security	10.0.390.0 Database: 15058
Kaspersky	Internet Security	17.0.0.611 (c)
Microsoft	Security Essentials	4.10.209.0
Norton	Security	22.9.0.71
Trend Micro	Internet Security 10	11.0.1186

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	**Targeted attack**	**Web drive-by**	**Web download**	**Protected (total)**
Kaspersky Internet Security	25	31	44	100
Norton Security	25	31	44	100
ESET Smart Security	25	31	44	100
Bitdefender Internet Security	25	30	44	99
Trend Micro Internet Security 10	24	31	44	99
Avast Free Antivirus	19	31	44	94
AVG AntiVirus Free Edition	19	31	43	93
Microsoft Security Essentials	20	31	42	93