

SE Labs

Home Anti-Malware Protection

January - March 2016





SE Labs tested a range 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

Introduction	04
Executive Summary	05
1. Total Accuracy Ratings	06
2. Protection Ratings	08
3. Protection Scores	10
4. Protection Details	11
5. Legitimate Software Ratings	12
6. Conclusions	16
Appendix A: Terms used	17
Appendix B: FAQs	18
Appendix C: Product versions	19
Appendix D: Attack types	19

Document version 1.0. Written 4th April 2016


SIMON EDWARDS

Director

Website www.SELabs.uk
Twitter @SELabsUK

Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Phone 0203 875 5000

Post ONE Croydon, London, CR0 0XT

INTRODUCTION

Anti-malware products are considered by almost every security expert to be an essential level of protection for Windows PCs. Headlines that proclaim anti-virus to be dead are usually making a too-subtle point about signature-reliant technologies rather than writing off a whole segment of the IT security market. All the products here combine signature-based protection with other, more advanced technologies.

Ideally an anti-malware product will require no management, protect against every threat that it encounters and allow access to all of the non-malicious applications and websites that you want to download. That's a pretty tall order and one that is unlikely to exist, despite various claims from newly arrived companies that offer alternatives to 'anti-virus'.

This test shows the results of three months of research during which time the SE Labs team located live web-based threats that internet users in the real world were encountering at the time of testing. Crucially we tested straight away, as soon as each threat was verified, so we could determine how well the popular anti-malware endpoints in the lab would perform against current prevalent malware threats.

There is much talk of targeted attacks in the press and strong claims by some security vendors that anti-malware technology is useless against these types of threats. We decided to test this claim and included a range of attacks in this test that are close, if not identical, to how an attacker could attempt to compromise an endpoint.

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 19.

Products tested

PRODUCT	PROTECTION ACCURACY	LEGITIMATE ACCURACY	TOTAL ACCURACY
ESET Smart Security 9	100%	100%	100%
Norton Security	99%	99%	99%
Avast Free Antivirus	91%	100%	97%
Kaspersky Internet Security	89%	100%	96%
Trend Micro Internet Security 10	87%	96%	93%
Microsoft Security Essentials	73%	100%	91%
AVG AntiVirus Free Edition	72%	100%	91%
McAfee Internet Security	62%	100%	87%

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.

- **Most endpoints were effective at handling general threats from cyber criminals...**

All but the McAfee product were capable of handling most 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**

While two of the products were also very competent at blocking more targeted, exploit-based attacks, the others were less effective. Products from AVG and Microsoft were particularly weak in this area.

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

All endpoint solutions were good at correctly classifying legitimate applications and websites. Six of the eight products made no mistakes at all.

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

The ESET, Symantec (Norton), Avast 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, 4th April 2016

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.

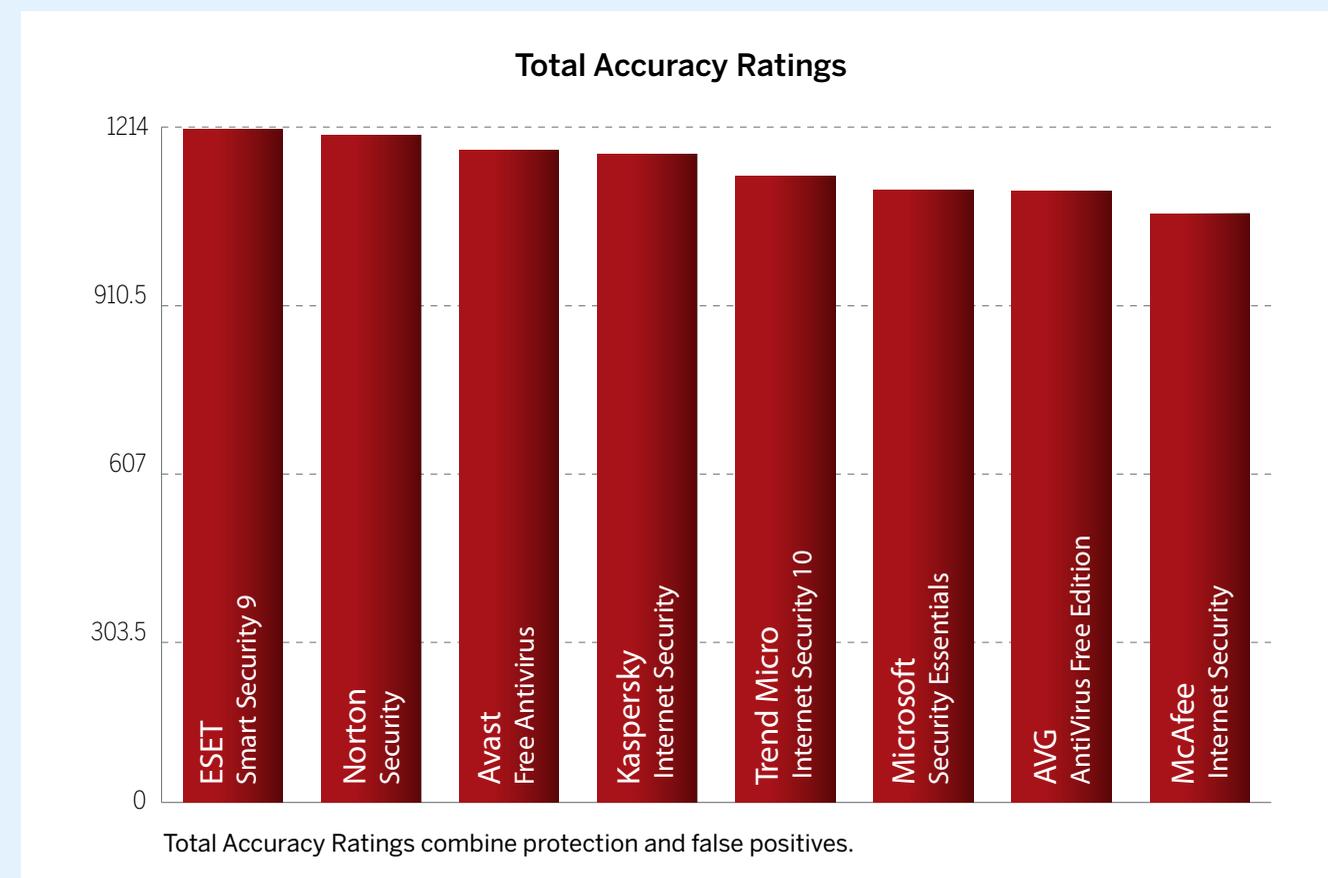
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

Not all protections, or detections for that matter, are equal. A product might completely block a URL, which prevents the threat completely 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.

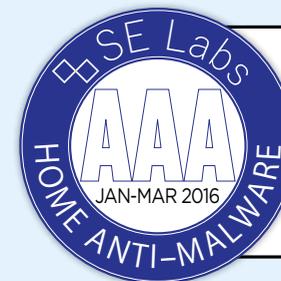
For example, a product that completely blocks a threat is rated more highly than one which allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

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.

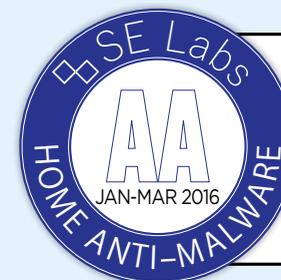


Awards

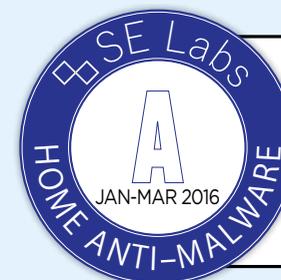
The following products win SE Labs awards:



- ESET Smart Security 9
- Norton Security
- Avast Free Antivirus
- Kaspersky Internet Security



- Trend Micro Internet Security 10
- Microsoft Security Essentials
- AVG AntiVirus Free Edition



- McAfee Internet Security

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
ESET Smart Security 9	1214	100%	AAA
Norton Security	1203	99%	AAA
Avast Free Antivirus	1176	97%	AAA
Kaspersky Internet Security	1169	96%	AAA
Trend Micro Internet Security 10	1129	93%	AA
Microsoft Security Essentials	1105	91%	AA
AVG AntiVirus Free Edition	1102	91%	AA
McAfee Internet Security	1062	87%	A

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.

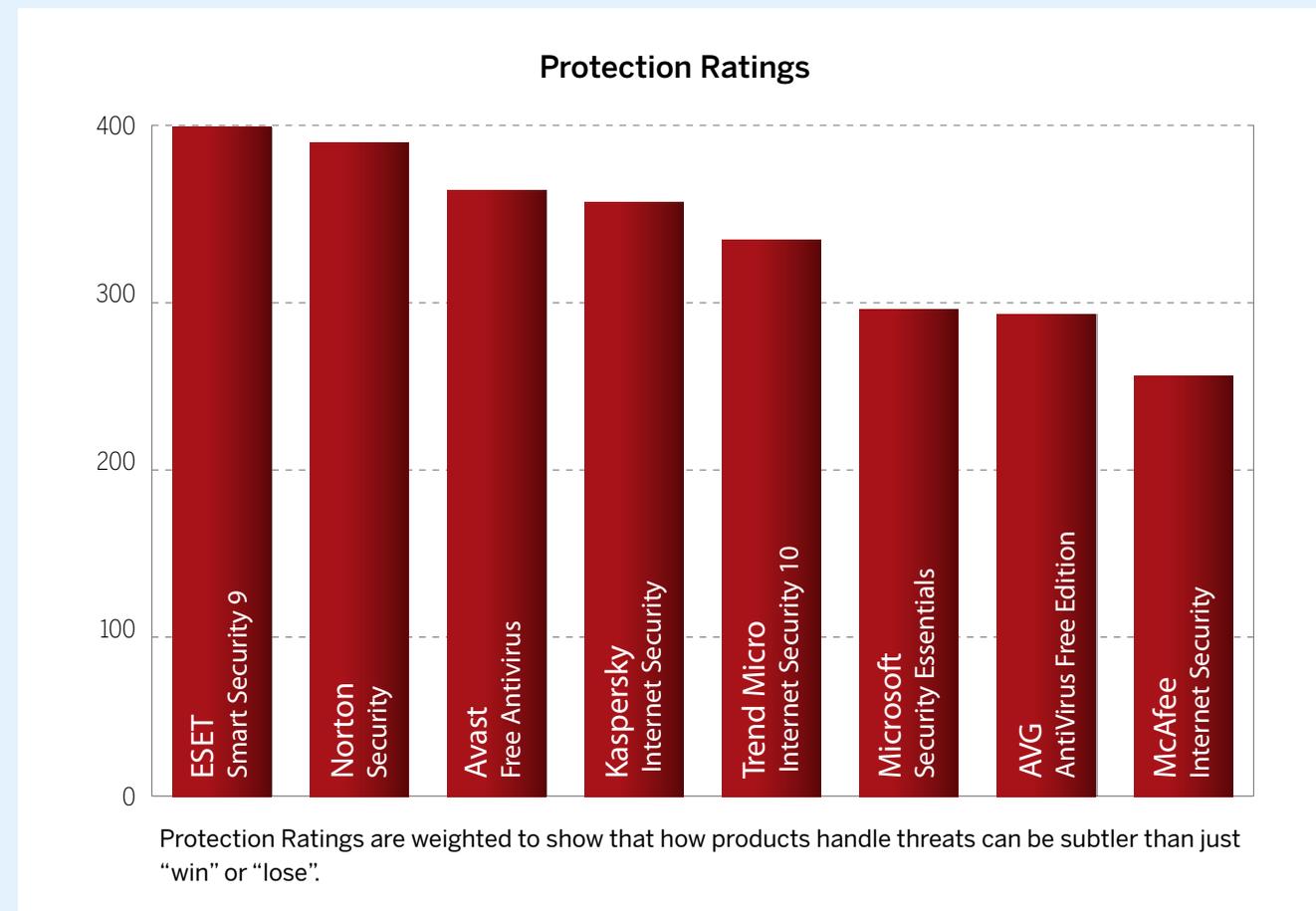
Rating calculations

We calculate the protection ratings using the following formula:

$$\text{Protection rating} = (2 \times \text{number of Blocked}) + (\text{1x number of Neutralised}) + (\text{1x number of Complete remediation}) + (-5 \times \text{number of Compromised})$$

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.



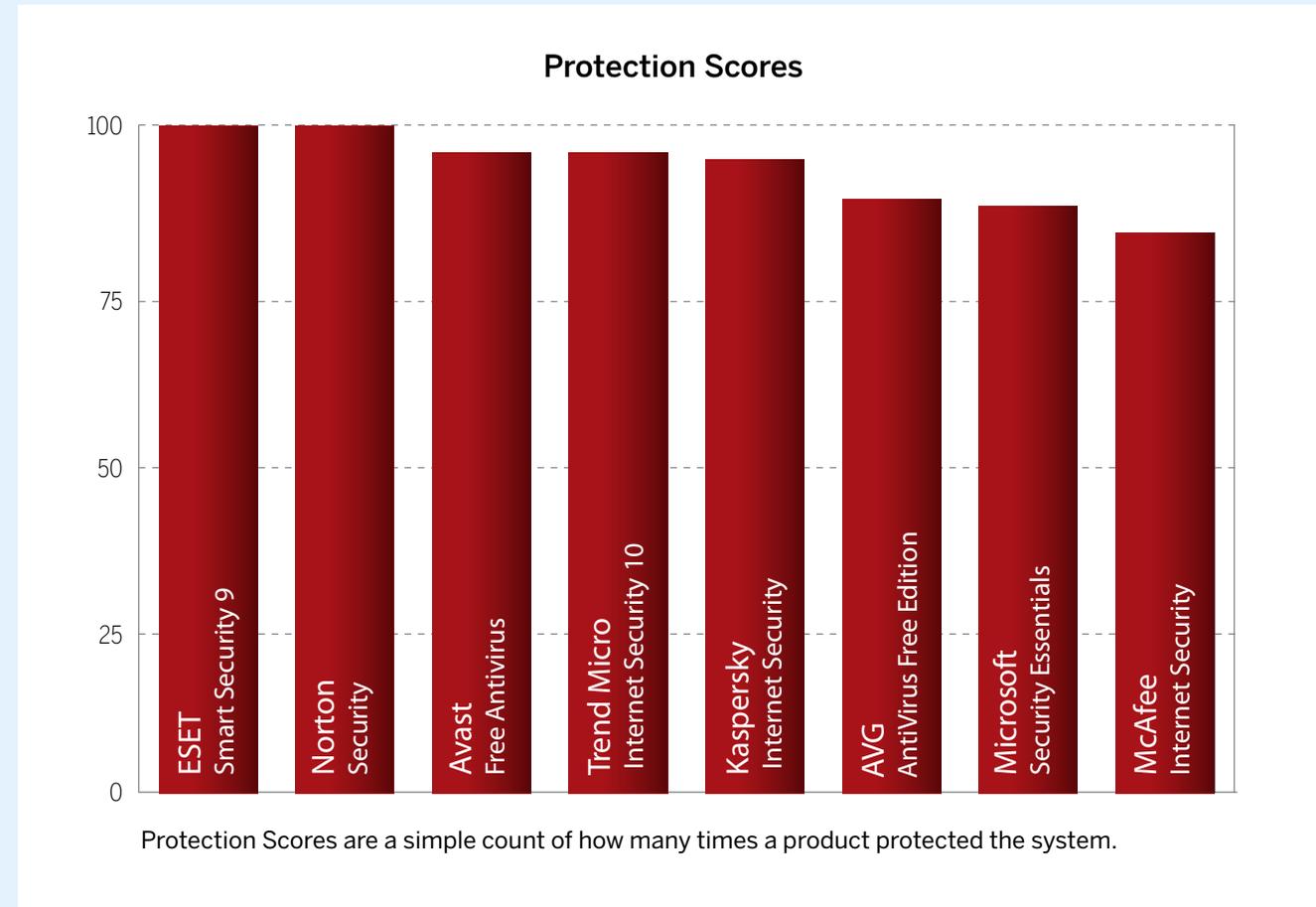
PROTECTION RATINGS		
Product	Protection Rating	Protection Rating (%)
ESET Smart Security 9	400	100%
Norton Security	395	99%
Avast Free Antivirus	362	91%
Kaspersky Internet Security	355	89%
Trend Micro Internet Security 10	347	87%
Microsoft Security Essentials	291	73%
AVG AntiVirus Free Edition	288	72%
McAfee Internet Security	251	63%

Average: 83%

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.



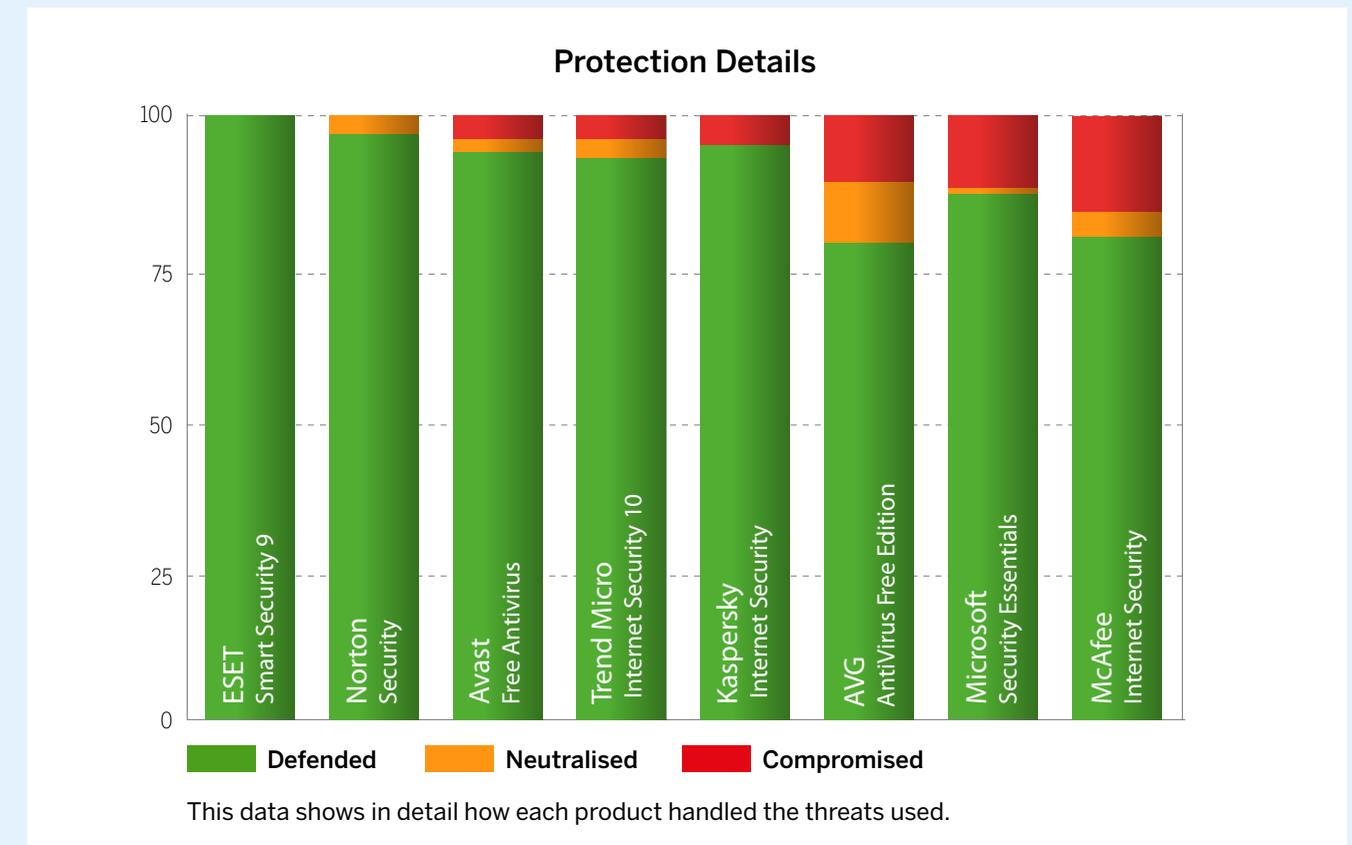
PROTECTION SCORES	
Product	Protection Score
ESET Smart Security 9	100
Norton Security	100
Avast Free Antivirus	96
Trend Micro Internet Security 10	95
Kaspersky Internet Security	89
AVG AntiVirus Free Edition	89
Microsoft Security Essentials	88
McAfee Internet Security	84

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 can also provide protection even if they don't detect certain threats. Some threats abort on detecting specific endpoint protection software.

Products sometimes detect more threats than they



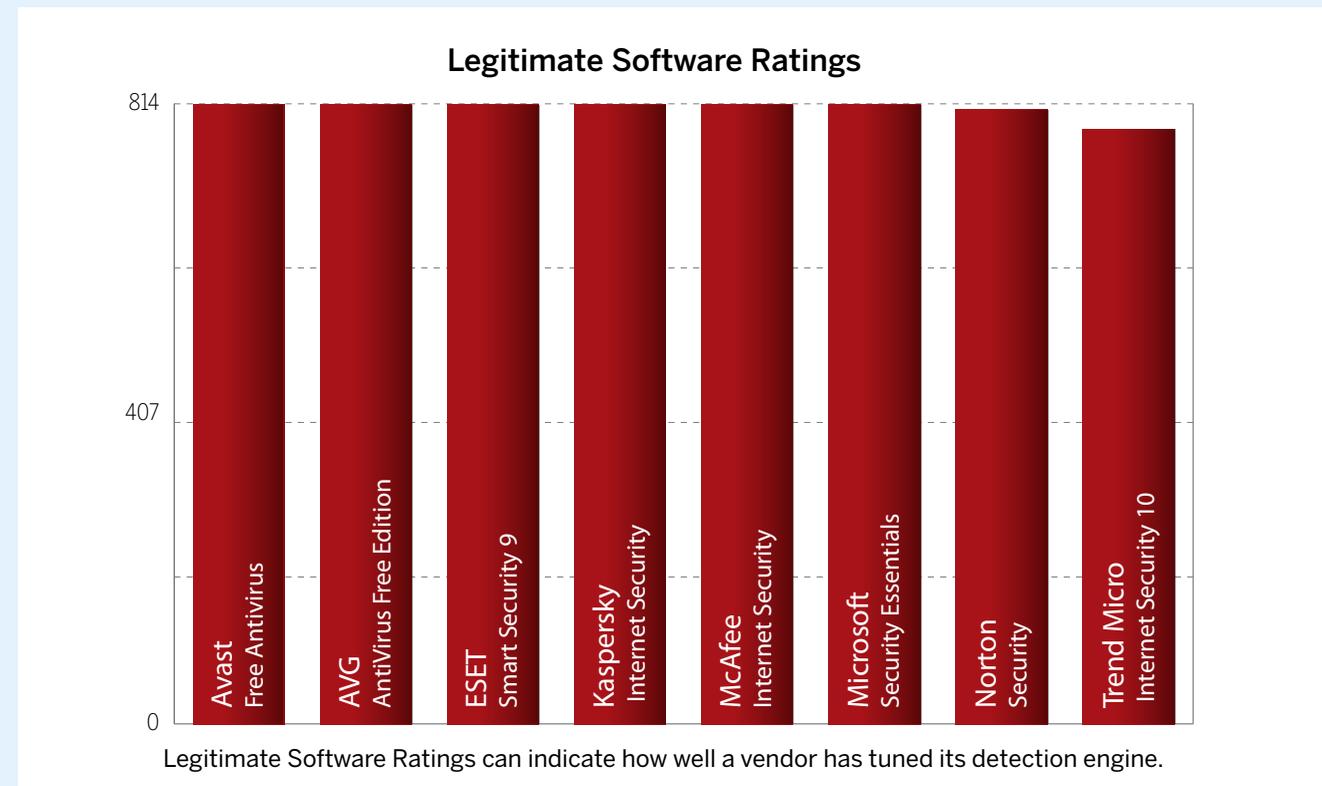
PROTECTION DETAILS					
Product	Detected	Blocked	Neutralised	Compromised	Protected
ESET Smart Security 9	100	100	0	0	100
Norton Security	100	97	3	0	100
Avast Free Antivirus	97	94	2	4	96
Trend Micro Internet Security 10	82	93	3	4	96
Kaspersky Internet Security	95	95	0	5	95
AVG AntiVirus Free Edition	89	79	10	11	89
Microsoft Security Essentials	89	87	1	12	88
McAfee Internet Security	82	80	4	16	84

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		
Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Avast Free Antivirus	814	100%
AVG AntiVirus Free Edition	814	100%
ESET Smart Security 9	814	100%
Kaspersky Internet Security	814	100%
McAfee Internet Security	814	100%
Microsoft Security Essentials	814	100%
Norton Security	808	99%
Trend Micro Internet Security 10	782	96%

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 false positives 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.

COUNT OF INTERACTION		
Product	Click to block (default block)	None (allowed)
Avast Free Antivirus		100
AVG AntiVirus Free Edition		100
ESET Smart Security 9		100
Kaspersky Internet Security		100
McAfee Internet Security		100
Microsoft Security Essentials		100
Norton Security	1	99
Trend Micro Internet Security 10	2	98

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 following table.

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

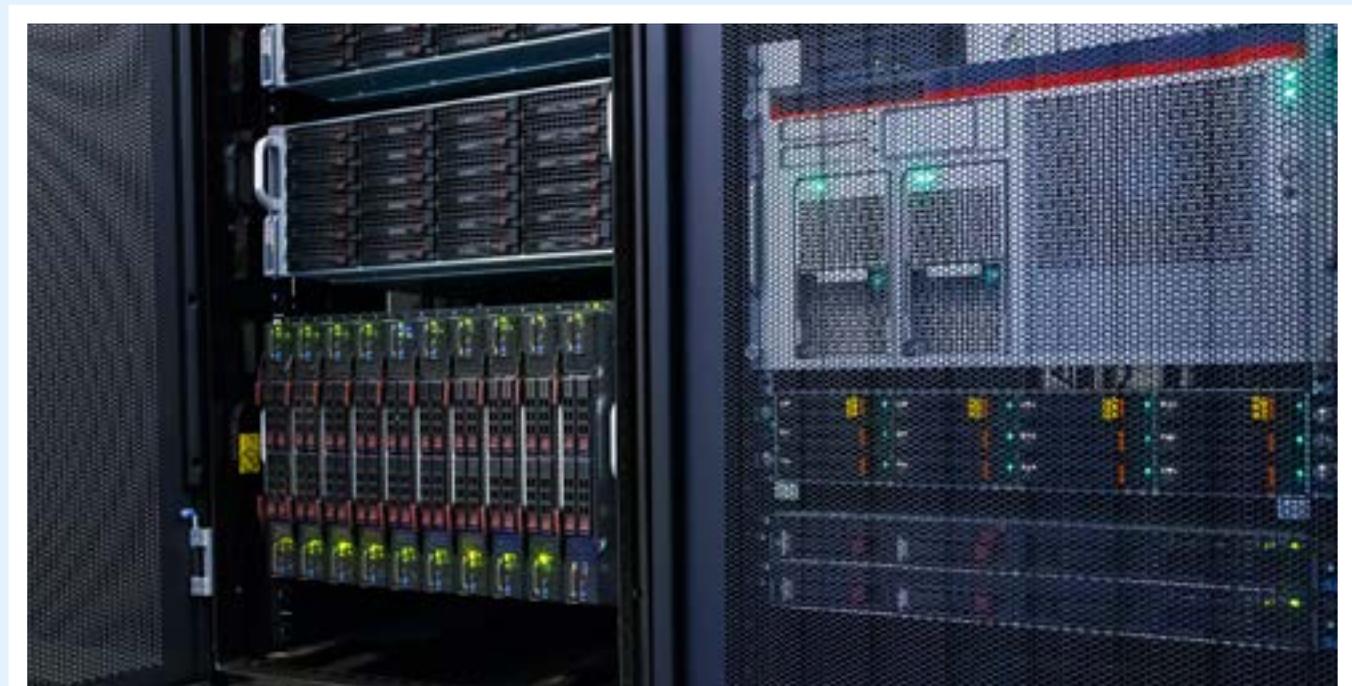
This same calculation is made for each legitimate application/site in the test and the results are summed and used to populate the graph and table shown under 5. Legitimate Software Ratings on page 12.

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	51
High impact	27
Medium impact	10
Low impact	7
Very low impact	5
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.

ESET Smart Security stands out as the one product that blocked every threat, including the targeted attacks. It was not compromised once and handled the legitimate applications and sites without error.

Symantec Norton Security was able to fend off the exploit-based targeted attacks fully, while also blocking most of the public web attacks, some of which were powered by criminals using exploit kits. It neutralised three attacks and handled legitimate applications and websites almost without error.

Avast Free Antivirus was the strongest free product in this test. It protected against all but one of the public web attacks and lost out to only three of the targeted attacks. It made no mistakes when handling legitimate objects.

Kaspersky Endpoint Security pushed away all but one of the public web-based threats entirely but was

compromised by four of our targeted attacks. It was particularly effective at stopping threats by blocking within the web browser, thus preventing the threat from starting its attack. This software was also entirely effective when handling legitimate objects.

Microsoft and **AVG** struggled with the targeted attacks, each allowing 10 to succeed. However, they were largely effective against the public attacks. While **Trend Micro's** product was slightly less accurate when handling legitimate objects, it scored higher ratings than the other two because it blocked more threats than AVG's product and protected more often than Microsoft's.

McAfee Internet Security scored the weakest ratings in this test. Perhaps surprisingly, this was not related to the targeted attacks, against which it worked quite well. It allowed 11 web attacks to compromise the target system, although its perfect handling of legitimate applications and websites helped it achieve an A award.

Four products performed very well and achieved AAA awards. These were from **ESET**, **Symantec (Norton)**, **Avast** and **Kaspersky Lab**. Their strong overall performance is to be commended. Those from **Trend Micro**, **AVG** and **Microsoft** achieved solid AA awards, while **McAfee's** product is awarded an A.

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 21st January 2016 and 18th March 2016.
- 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 [2015 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	11.1.2245
AVG	AntiVirus Free Edition	16.51.7497
ESET	Smart Security	9.0.375.0
Kaspersky	Internet Security	15.0.2.361 (d)
McAfee	Internet Security	18.0.6014
Microsoft	Security Essentials	4.8.204.0
Symantec	Norton Security	22.6.0.142
Trend Micro	Internet Security	10.0.1186

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	Public web attack	Protected (total)
Avast Free Antivirus	22	74	96
AVG AntiVirus Free Edition	15	74	89
ESET Smart Security 9	25	75	100
Kaspersky Internet Security	21	74	95
McAfee Internet Security	20	64	84
Microsoft Security Essentials	15	73	88
Norton Security	25	75	100
Trend Micro Internet Security 10	22	74	96