SE Labs

INTELLIGENCE-BASED TESTING

HOME ANTI-MALWARE PROTECTION

OCT - DEC 2016
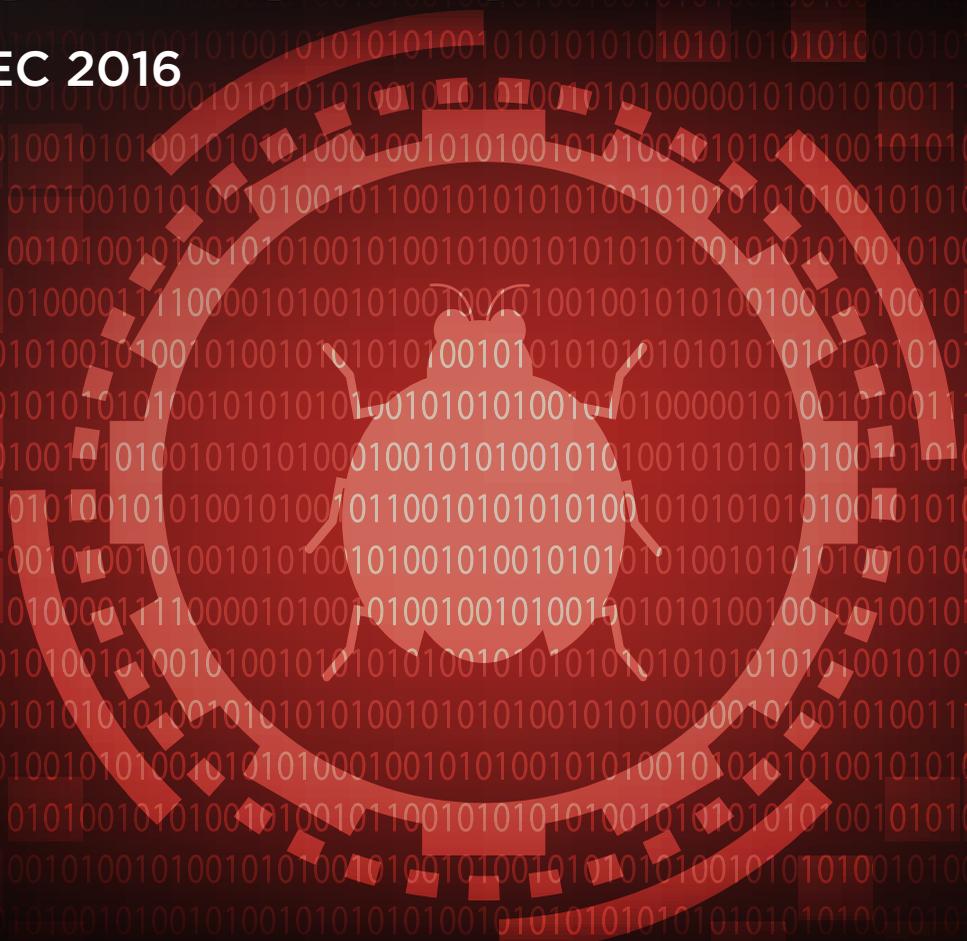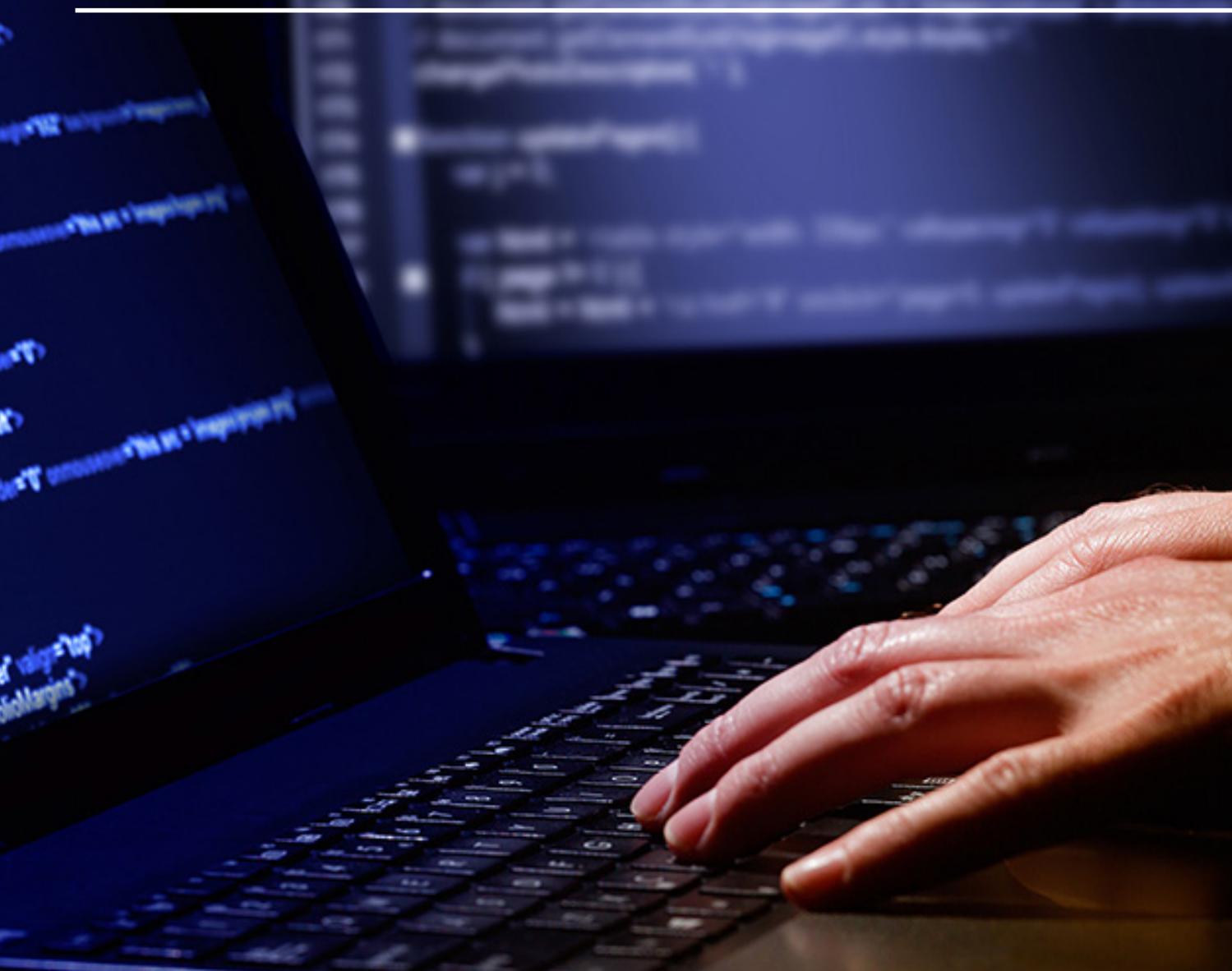
SE Labs tested a range of anti-malware (aka 'anti-virus'; aka 'endpoint security') products from a range of well-known vendors in an effort to judge which were the most effective.

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

Document version 1. 0. Written 21st December 2016

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)

INTRODUCTION

Welcome to the final set of endpoint security tests for 2016. We've spent the entire year scanning the internet for prevalent threats that affect real people and exposing popular security products to those same threats in real-time.

If you want an answer to the question, "How well does my anti-malware product protect me?" the reports we've published throughout the year should go some way to helping you either feel safe or make an informed decision on which product to change to. You can find this and earlier reports on our website

But helping you, our readers, choose the best products is only part of our mission. We want products to improve, because even the best are not perfect. We offer the developers of these products the chance to engage with us and learn where the problems lie.

At the end of each test we could say to them, "bad luck, you missed these threats. Better luck next time!" But what we do is provide a huge amount of useful data to companies that want to work with us. This includes extremely detailed analyses of the threat itself, how it worked against individual products and forensic data proving what happened.

This data provides two benefits to the security companies: the first is proof that we're not just making everything up! The second is an unbiased, third-party quality assurance service that can identify problems overlooked by in-house teams. In the end they benefit and so do you, if you use their products.

We're trying to make things better. Thanks for your support throughout the year.

If you spot a detail in this report you don't understand, or would like to discuss, please contact us via Twitter or Facebook.

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 RATING	LEGITIMATE ACCURACY RATING	TOTAL ACCURACY RATING
ESET Smart Security 9	100%	100%	100%
Kaspersky Internet Security	100%	100%	100%
Norton Security	100%	97%	98%
Trend Micro Internet Security 11	94%	100%	98%
G DATA Internet Security	84%	98%	93%
AVG AntiVirus Free Edition	79%	100%	93%
Avast Free Antivirus	79%	99%	92%
Microsoft Security Essentials	75%	95%	88%
McAfee Internet Security	45%	100%	81%

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**
Only a few of the products were very competent at blocking more targeted, exploit-based attacks. Only products from ESET, Symantec and Kaspersky 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. Five out of the nine products made no mistakes at all.

● **Which products were the most effective?**
ESET, Symantec, Kaspersky Lab and Trend Micro 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, 21st December 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.

Total Accuracy Ratings

Total Accuracy Ratings combine protection and false positives.
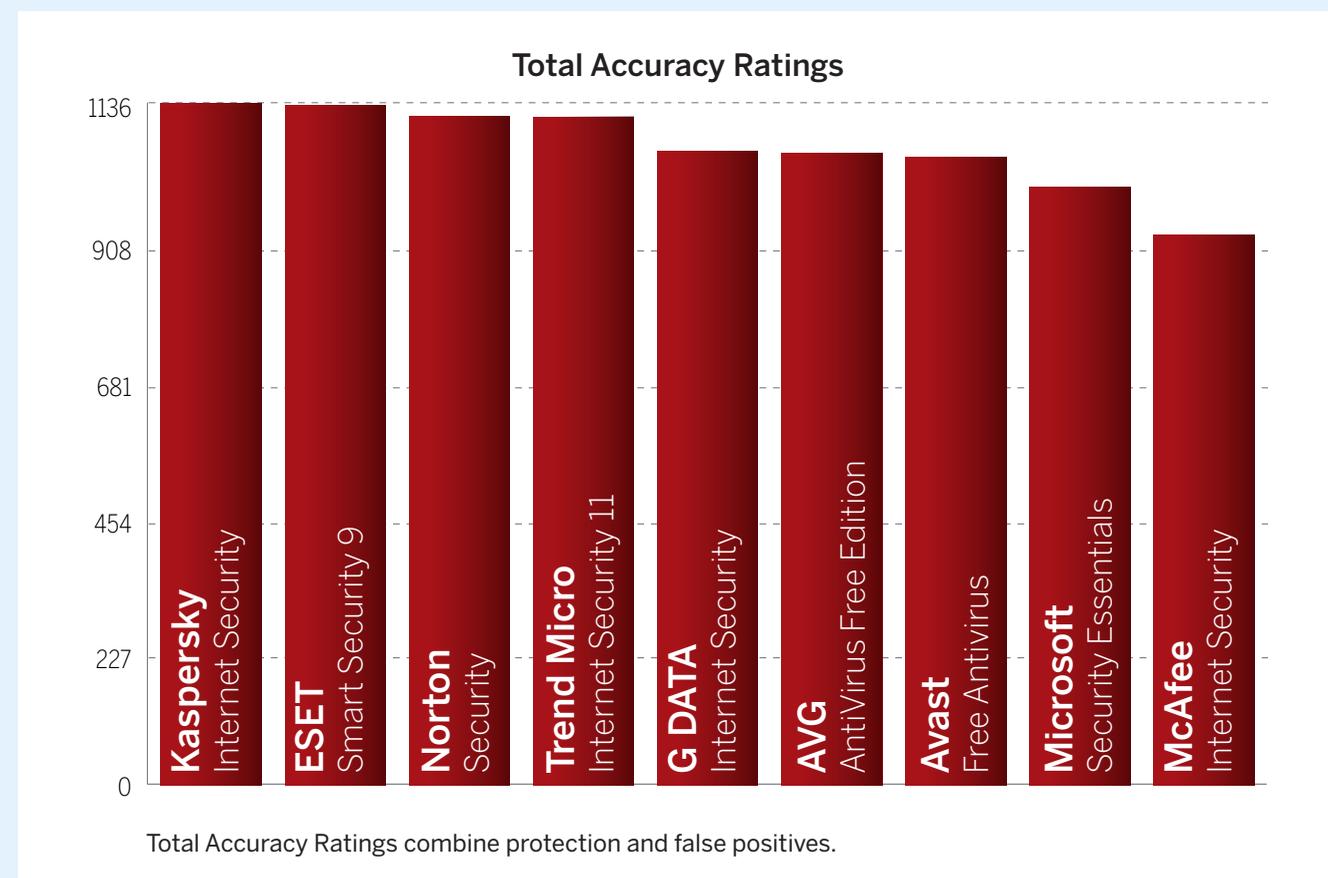
Awards

The following products win SE Labs awards:

AAA (HOME ANTI-MALWARE • OCT-DEC 2016)
- ESET Smart Security 9
- Norton Security
- Kaspersky Internet Security
- Trend Micro Internet Security 11

AA (HOME ANTI-MALWARE • OCT-DEC 2016)
- G DATA Internet security
- AVG AntiVirus Free Edition
- Avast Free Antivirus

A (HOME ANTI-MALWARE • OCT-DEC 2016)
- Microsoft Security Essentials

B (HOME ANTI-MALWARE • OCT-DEC 2016)
- McAfee Internet Security

TOTAL ACCURACY RATINGS			
Product	**Total Accuracy Rating**	**Total Accuracy (%)**	**Award**
Kaspersky Internet Security	1136	100%	AAA
ESET Smart Security 9	1135	100%	AAA
Norton Security	1115	98%	AAA
Trend Micro Internet Security 11	1113	98%	AAA
G DATA Internet Security	1055.5	93%	AA
AVG AntiVirus Free Edition	1052	93%	AA
Avast Free Antivirus	1046	92%	AA
Microsoft Security Essentials	997	88%	A
McAfee Internet Security	917	81%	B

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'.
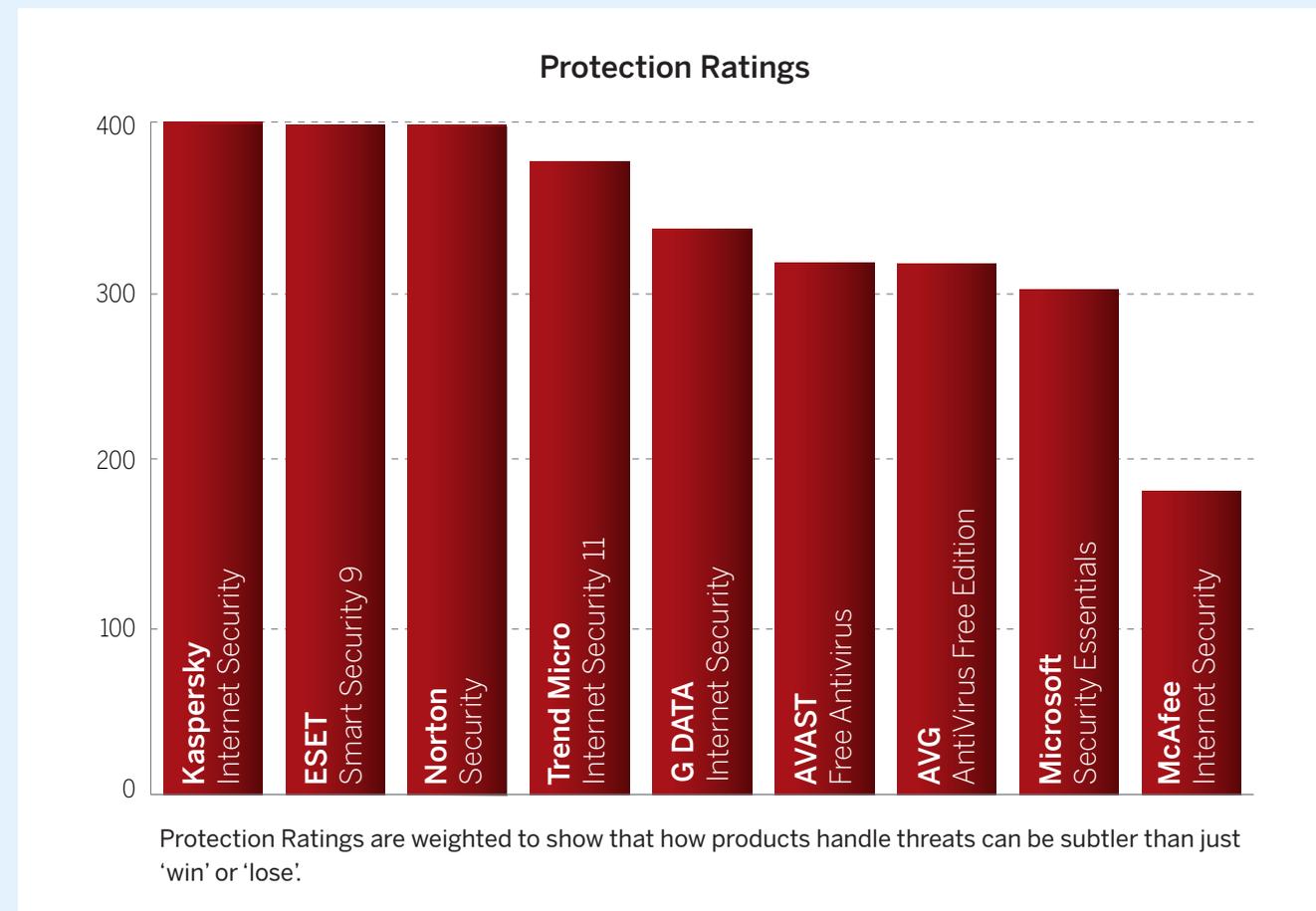
PROTECTION RATINGS		
Product	**Protection Rating**	**Protection Rating (%)**
Kaspersky Internet Security	400	100%
ESET Smart Security 9	399	100%
Norton Security	399	100%
Trend Micro Internet Security 11	377	94%
G DATA Internet Security	337	84%
Avast Free Antivirus	317	79%
AVG AntiVirus Free Edition	316	79%
Microsoft Security Essentials	301	75%
McAfee Internet Security	181	45%

Average: 84%

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.
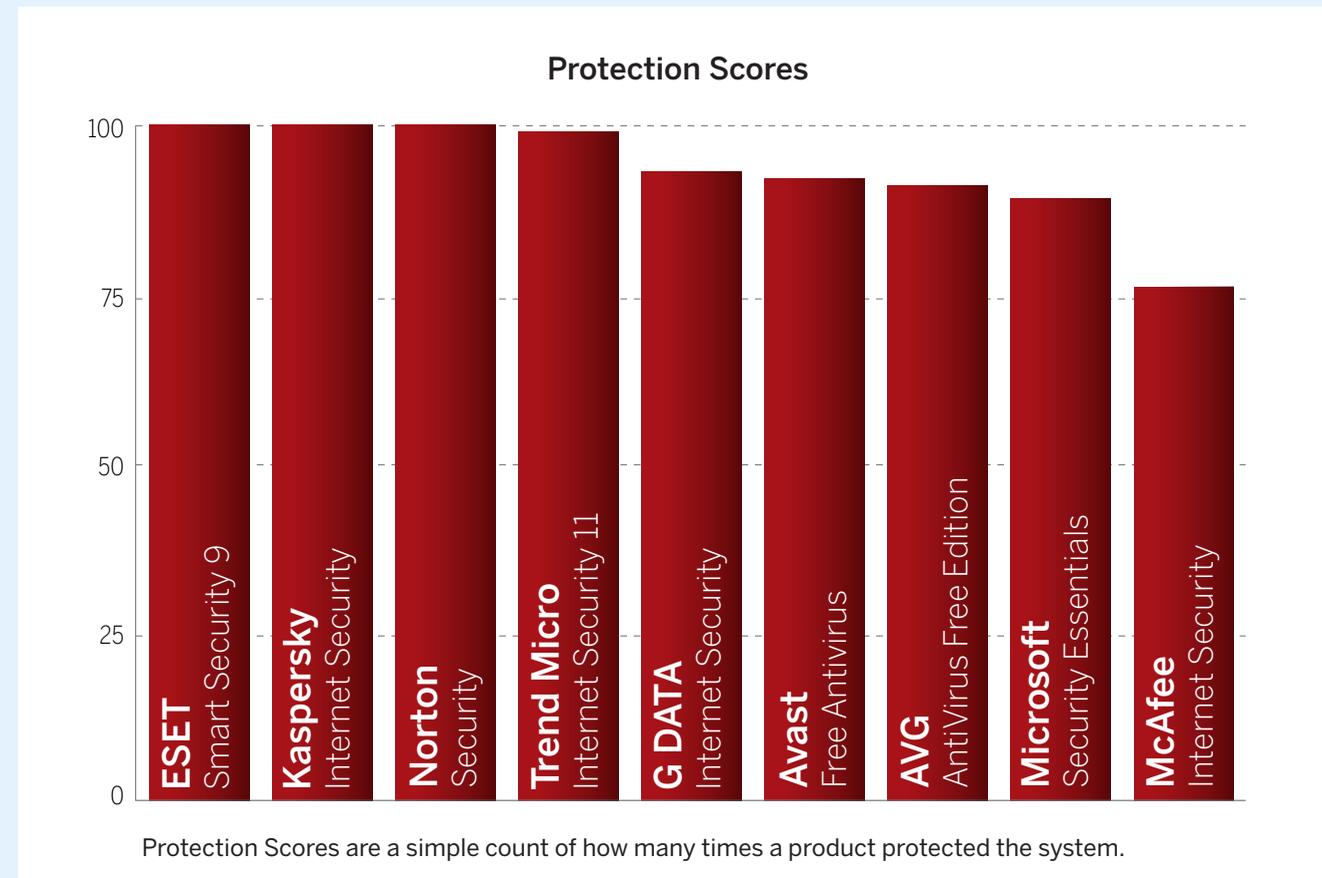
PROTECTION SCORES	
Product	Protection Score
ESET Smart Security 9	100
Kaspersky Internet Security	100
Norton Security	100
Trend Micro Internet Security 11	99
G DATA Internet Security	93
Avast Free Antivirus	92
AVG AntiVirus Free Edition	91
Microsoft Security Essentials	89
McAfee Internet Security	76

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.
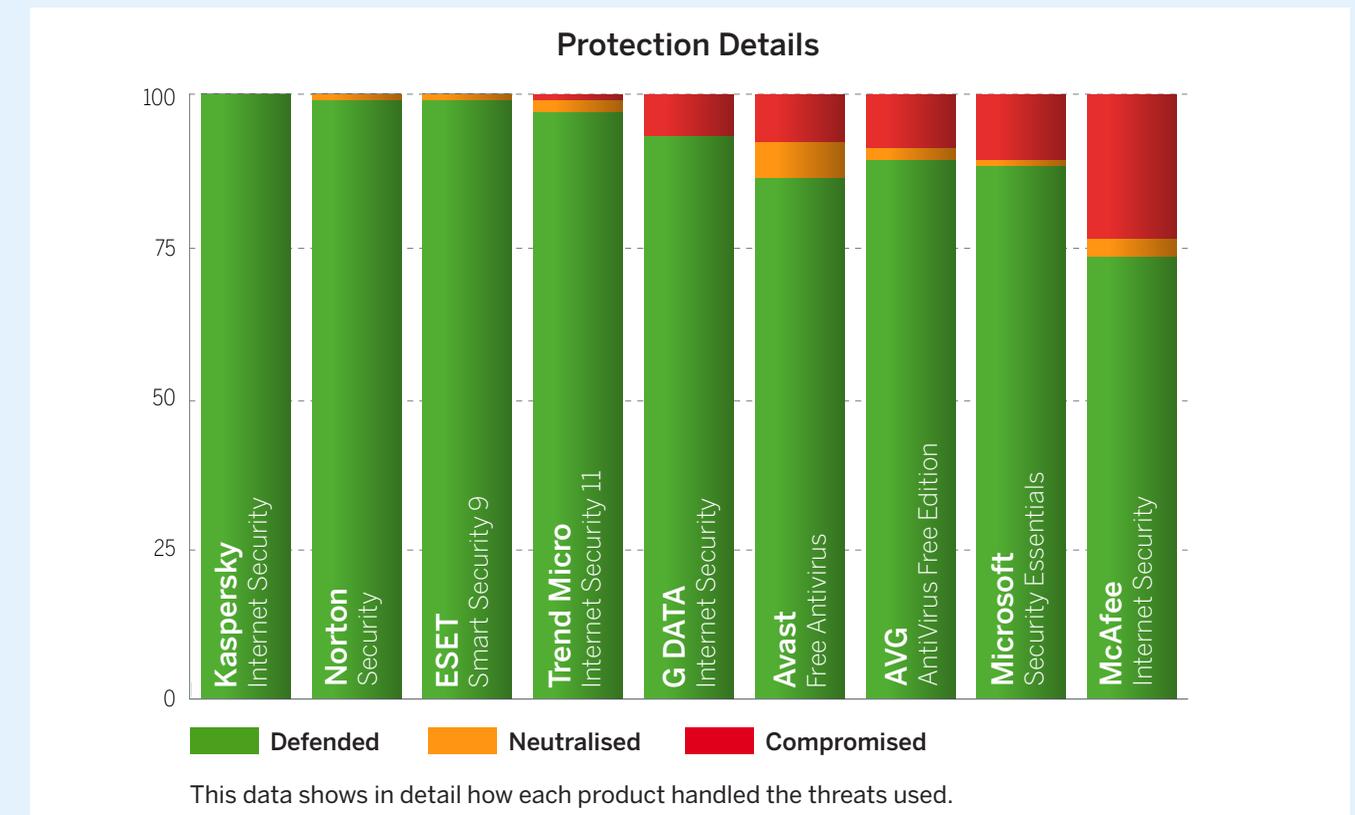
PROTECTION DETAILS					
Product	Detected	Blocked	Neutralised	Compromised	Protected
Kaspersky Internet Security	100	100	0	0	100
Norton Security	100	99	1	0	100
ESET Smart Security 9	100	99	1	0	100
Trend Micro Internet Security 11	87	97	2	1	99
G DATA Internet Security	93	93	0	7	93
Avast Free Antivirus	91	86	6	8	92
AVG AntiVirus Free Edition	90	89	2	9	91
Microsoft Security Essentials	90	88	1	11	89
McAfee Internet Security	77	73	3	24	76

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.
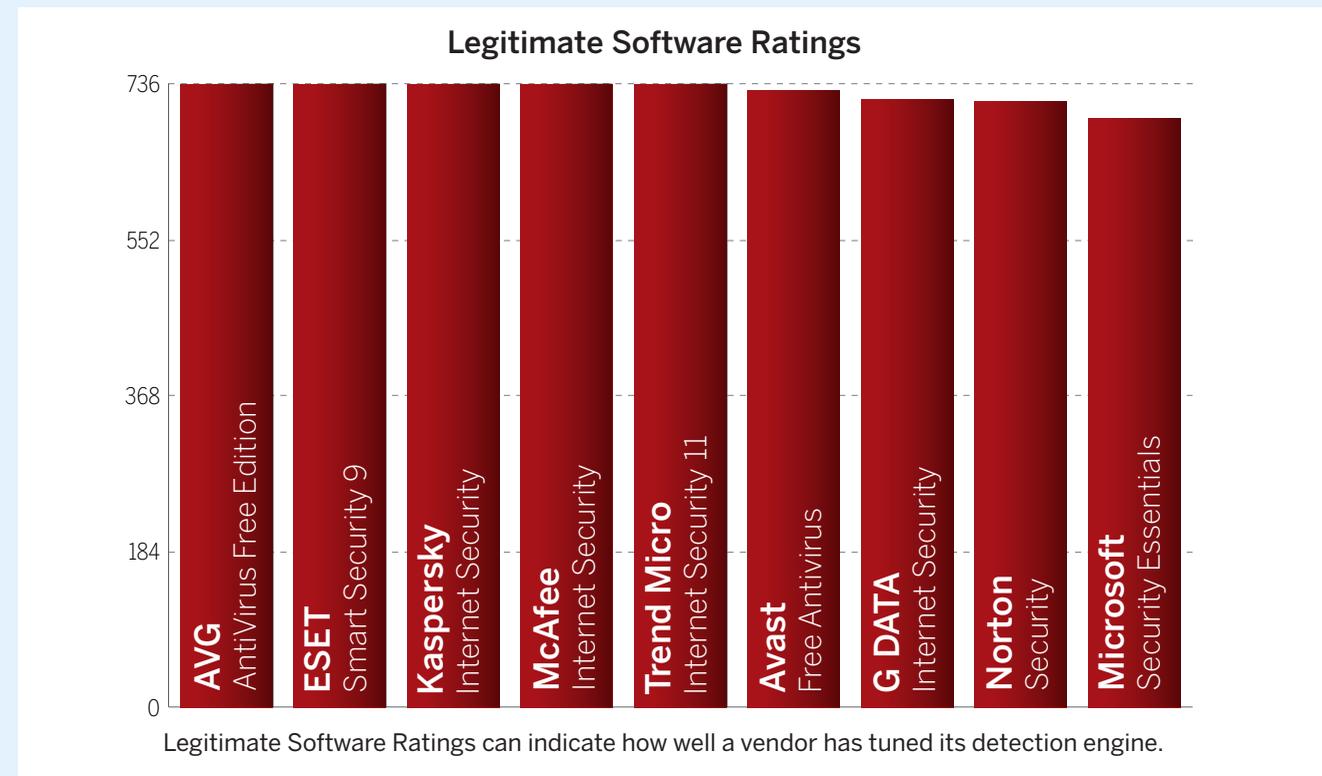
LEGITIMATE SOFTWARE RATINGS		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy (%)**
AVG AntiVirus Free Edition	736	100%
ESET Smart Security 9	736	100%
Kaspersky Internet Security	736	100%
McAfee Internet Security	736	100%
Trend Micro Internet Security 11	736	100%
Avast Free Antivirus	729	99%
G DATA Internet Security	718.5	98%
Norton Security	716	97%
Microsoft Security Essentials	696	95%

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.

INTERACTION RATINGS			
Product	**Click to block (default block)**	**None (allowed)**	**None (blocked)**
AVG AntiVirus Free Edition	0	100	0
Kaspersky Internet Security	0	100	0
McAfee Internet Security	0	100	0
ESET Smart Security 9	0	100	0
Trend Micro Internet Security 11	0	100	0
Avast Free Antivirus	0	99	1
Norton Security	0	99	1
G DATA Internet Security	1	99	0
Microsoft Security Essentials	0	98	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	51
High impact	27
Medium impact	10
Low impact	7
Very low impact	5
Grand total	100
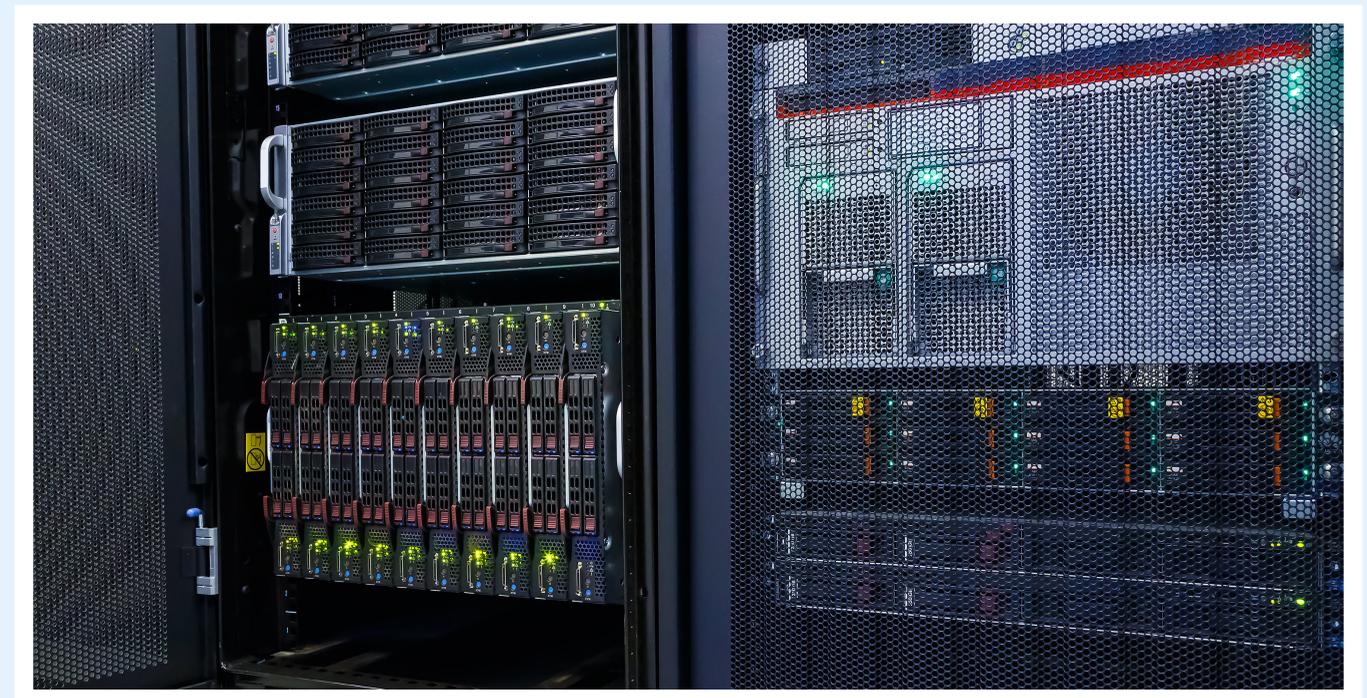
6. CONCLUSIONS

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

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.

Trend Micro Internet Security 11 was able to fend off nearly all of the exploit-based targeted attacks fully, missing just one. It blocked all of the public web attacks. It neutralised two attacks and handled legitimate applications and websites without error.

AVG AntiVirus Free Edition was the strongest free product in the test. It was compromised nine times by the targeted attacks but protected against all of the web-based drive-by attacks. It was, however, perfect when handling legitimate applications and websites.

McAfee Internet Security was the least effective product in this test. Although it stopped a fair few of the targeted attacks and all but one of the web downloads, if failed to block a significant amount of the malware delivered by drive-by websites. Its excellent handling of legitimate software was good enough to help it achieve a B rating, though.

The products from ESET, Kaspersky Lab, Symantec and Trend Micro all win AAA awards for their strong overall performance. Those from G DATA, AVG and Avast achieved solid AA awards, while Microsoft Security Essentials is awarded an A award.

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 4th October and 7th December 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 **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	12.3.2280
AVG	AntiVirus Free Edition	16.111.7797
ESET	Smart Security 9	9.0.402.0 Database: 14223 (20161004)
G DATA	Internet Security	25.2.0.2
Kaspersky	Internet Security	15.0.2.361 (f)
McAfee	Internet Security	14.0.9043 AV&AS build: 18.0.9019
Microsoft	Security Essentials	4.9.218.0
Norton	Security	22.8.0.50
Trend Micro	Internet Security 11	11.0.1158

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 Download**	**Web Drive-by**	**Protected (Total)**
Kaspersky Internet Security	25	35	40	100
Norton Security	25	35	40	100
ESET Smart Security 9	25	35	40	100
Trend Micro Internet Security 11	24	35	40	99
G DATA Internet Security	18	35	40	93
Avast Free Antivirus	19	35	38	92
AVG AntiVirus Free Edition	16	35	40	91
Microsoft Security Essentials	15	34	40	89
McAfee Internet Security	17	34	25	76