SE Labs

INTELLIGENCE-LED TESTING

www.SELabs.uk info@SELabs.uk @SELabsUK www.facebook.com/selabsuk blog.selabs.uk

HOME ANTI-MALWARE PROTECTION

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

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

CONTENTS

Document version 1. 0. Written 29th September 2017

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

MANAGEMENT
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

SE Labs is BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

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

INTRODUCTION

100% Certifiable

Whether you're in the market for a car, hamburger or computer security product, certifications are useful. They don't tell you how smooth the car drives, how tasty the sandwich is or how completely accurate the anti-virus software will be, but certifications indicate a general level of competence.

In the UK new cars must be certified by the Vehicle Certification Agency (VCA), restaurants are checked for hygiene by the Food Standards Agency (FSA) and various independent testing organisations, including SE Labs, test IT security products for basic functionality.

A certification emphatically does not indicate the overall quality of a product, though. The FSA specifically states that, "The food hygiene rating is not a guide to food quality." In other words, the food won't make you ill, but you might not like it! Similarly, the VCA cares more about cars being made according to specification rather than how nice they look.

SE Labs has a range of available testing services. We consider certification to be the most basic type of testing. If a product claims to be able to detect malware then we can test that, but we don't claim it can detect all types. For a higher level of understanding about a product's capabilities so-called 'real-world' testing is necessary.

The report you are reading now is based on our more advanced testing, which exposes real products to live threats in a realistic environment, running on real computers on an internet-connected network.

But how can you be sure that we're really doing that, and not just making up the figures or giving some products an unfair advantage? After all, some companies contribute financially to supporting the tests, while others do not.

To go some way to addressing this concern, as well as to improve generally and continue to evolve the business, **SE Labs has achieved ISO 9001:2015 certification** for "The Provision of IT Security Product Testing". We think it's fair for the testers to be tested and we're very proud to have passed!

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 19.

EXECUTIVE SUMMARY

Products tested	Protection Accuracy (%)	Legitimate Accuracy (%)	Total Accuracy (%)
ESET Smart Security	100%	100%	100%
Kaspersky Internet Security	100%	100%	100%
Norton Security	100%	99%	99%
Bitdefender Internet Security	91%	100%	97%
AVG AntiVirus Free Edition	90%	100%	97%
Avast Free Antivirus	88%	100%	96%
Trend Micro Internet Security 10	88%	100%	96%
Microsoft Security Essentials	81%	100%	94%
Avira Free Security Suite	65%	95%	85%
360 Total Security	31%	95%	74%

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 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.

- **... but targeted attacks posed more of a challenge**

Less than half of the products were very competent at blocking more targeted, exploit-based attacks. 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. Six out of the 10 products made no mistakes at all and products that blocked them did so sparingly.

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

Kaspersky Lab, ESET, Symantec (Norton), Bitdefender, AVG, Avast 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, 29th September 2017

1. TOTAL ACCURACY RATINGS

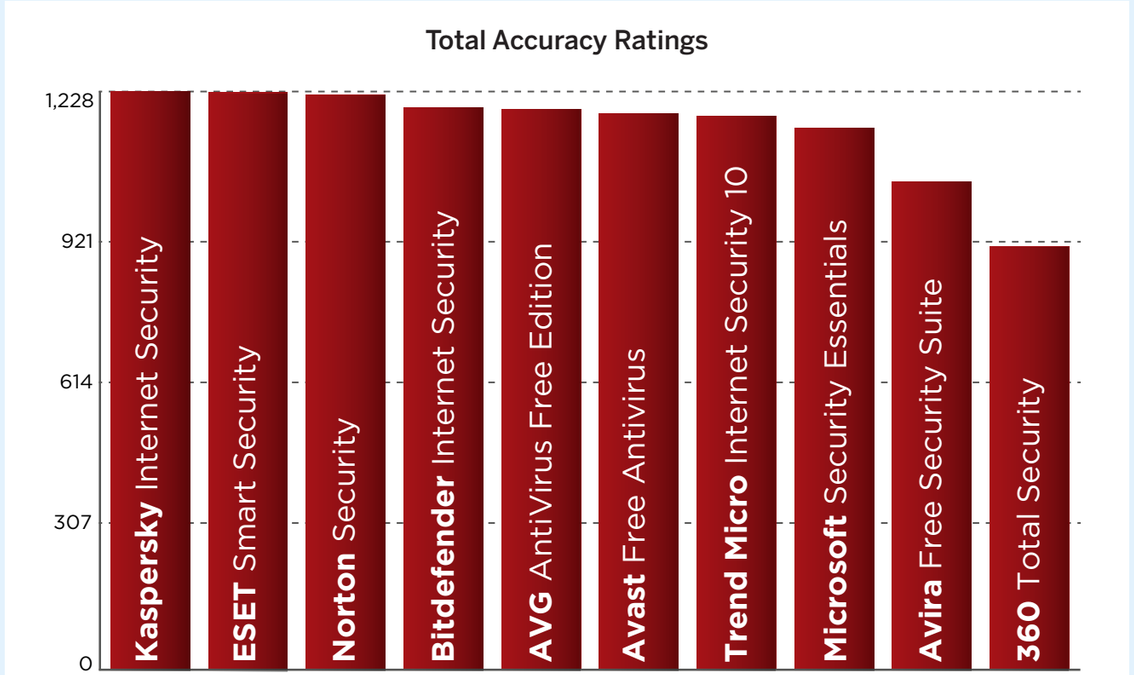
Judging the effectiveness of an endpoint security product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier we've combined all the different results from this report into one easy-to-understand graph.

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 combine protection and false positives.

AWARDS

The following products win SE Labs awards:

- Kaspersky Internet Security
- ESET Smart Security
- Norton Security
- AVG AntiVirus Free Edition
- Bitdefender Internet Security
- Avast Free Antivirus
- Trend Micro Internet Security 10

- Microsoft Security Essentials

- Avira Free Security Suite

TOTAL ACCURACY RATINGS			
Product	**Total Accuracy Rating**	**Total Accuracy (%)**	**Award**
Kaspersky Internet Security	1,228	100%	AAA
ESET Smart Security	1,226	100%	AAA
Norton Security	1,220	99%	AAA
Bitdefender Internet Security	1,193	97%	AAA
AVG AntiVirus Free Edition	1,189	97%	AAA
Avast Free Antivirus	1,181	96%	AAA
Trend Micro Internet Security 10	1,176	96%	AAA
Microsoft Security Essentials	1,150	94%	AA
Avira Free Security Suite	1,034	84%	B
360 Total Security	913	74%	

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.

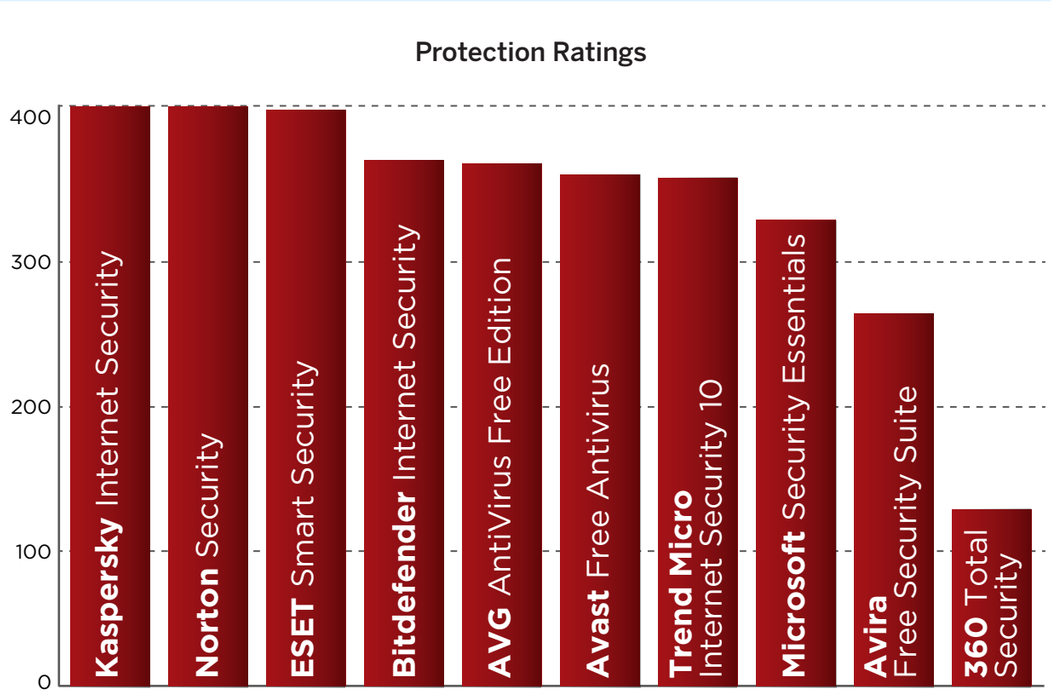
- **Detected (+1)**
If the product detects the threat with any degree of useful information, we award it one point.

- **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.

- **Compromised (-5)**
If the threat compromises the system, the product loses five points. This loss may be reduced to four points if it manages to detect the threat (see Detected, above), as this at least alerts the user, who may now take steps to secure the system.



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

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.

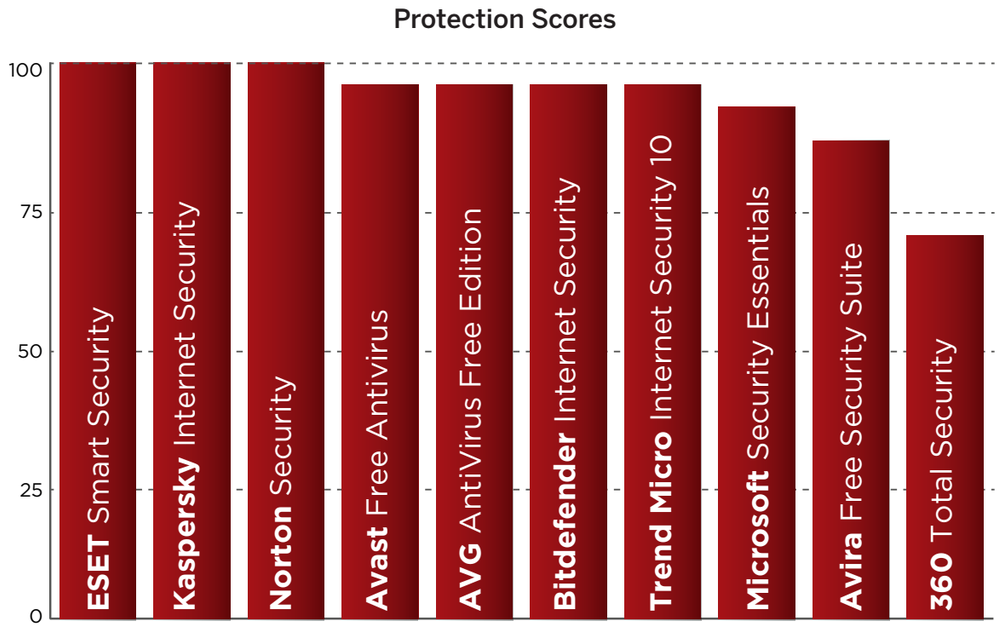
PROTECTION RATINGS		
Product	**Protection Rating**	**Protection Rating (%)**
Kaspersky Internet Security	400	100%
Norton Security	400	100%
ESET Smart Security	398	100%
Bitdefender Internet Security	365	91%
AVG AntiVirus Free Edition	361	90%
Avast Free Antivirus	353	88%
Trend Micro Internet Security 10	352	88%
Microsoft Security Essentials	322	81%
Avira Free Security Suite	256	64%
360 Total Security	123	31%

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.



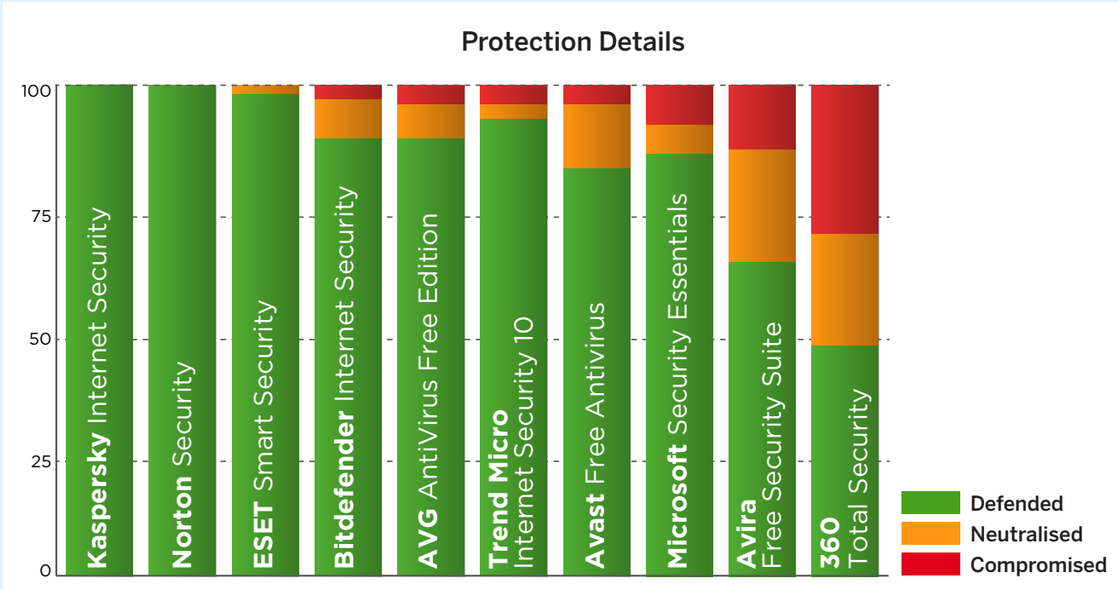
Protection Scores are a simple count of how many times a product protected the system.

PROTECTION SCORES	
Product	**Protection Score**
ESET Smart Security	100
Kaspersky Internet Security	100
Norton Security	100
Bitdefender Internet Security	97
Avast Free Antivirus	96
AVG AntiVirus Free Edition	96
Trend Micro Internet Security 10	96
Microsoft Security Essentials	92
Avira Free Security Suite	86
360 Total Security	70

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.

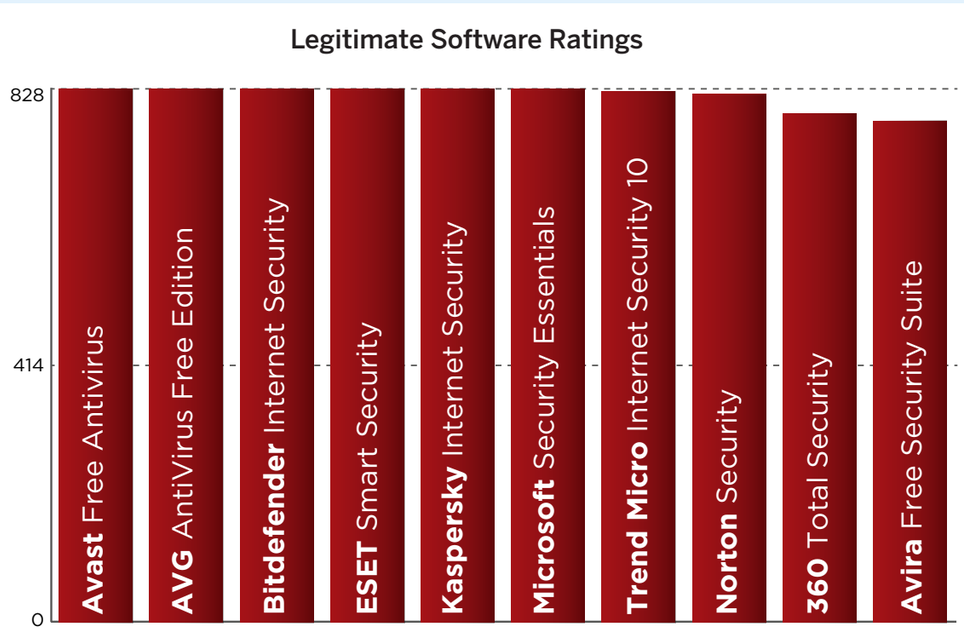
PROTECTION DETAILS					
Product	**Detected**	**Blocked**	**Neutralised**	**Compromised**	**Protected**
Kaspersky Internet Security	100	100	0	0	100
Norton Security	100	100	0	0	100
ESET Smart Security	100	98	2	0	100
Bitdefender Internet Security	97	89	8	3	97
AVG AntiVirus Free Edition	97	93	3	4	96
Trend Micro Internet Security 10	97	83	13	4	96
Avast Free Antivirus	96	89	7	4	96
Microsoft Security Essentials	94	86	6	8	92
Avira Free Security Suite	87	64	23	13	87
360 Total Security	90	47	23	30	70

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 can indicate how well a vendor has tuned its detection engine.

LEGITIMATE SOFTWARE RATINGS		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy (%)**
Avast Free Antivirus	828	100%
AVG AntiVirus Free Edition	828	100%
Bitdefender Internet Security	828	100%
ESET Smart Security	828	100%
Kaspersky Internet Security	828	100%
Microsoft Security Essentials	828	100%
Trend Micro Internet Security 10	824	100%
Norton Security	820	99%
360 Total Security	790	95%
Avira Free Security Suite	778	94%

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.

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

5.2 Prevalence Ratings

There is a significant difference between an endpoint product blocking a popular application such as the latest version of Microsoft Word and condemning a rare Iranian dating toolbar for Internet Explorer 6. One is very popular all over the world and its detection as malware (or something less serious but still suspicious) is a big deal. Conversely, the outdated toolbar won't have had a comparably large user base even when it was new. Detecting this application as malware may be wrong, but it is less impactful in the overall scheme of things.

With this in mind, we collected applications of varying popularity and sorted them into five separate categories, as follows:

1. Very high impact
2. High impact
3. Medium impact
4. Low impact
5. Very low impact

Incorrectly handling any legitimate application will invoke penalties, but classifying Microsoft Word as malware and blocking it without any way for the user to override this will bring far greater penalties than doing the same for an ancient niche toolbar. In order to calculate these relative penalties, we assigned each impact category with a rating modifier, as shown in the table above.

LEGITIMATE SOFTWARE PREVALENCE RATING MODIFIERS	
Impact Category	**Rating Modifier**
Very high impact	5
High impact	4
Medium impact	3
Low impact	2
Very low impact	1

Applications were downloaded and installed during the test, but third-party download sites were avoided and original developers' URLs were used where possible. Download sites will sometimes bundle additional components into applications' install files, which may correctly cause anti-malware products to flag adware. We remove adware from the test set because it is often unclear how desirable this type of code is.

The prevalence for each application and URL is estimated using metrics such as third-party download sites and the data from Alexa.com's global traffic ranking system.

5.3 Accuracy Ratings

We calculate legitimate software accuracy ratings by multiplying together the interaction and prevalence ratings for each download and installation:

Accuracy rating = Interaction rating x Prevalence rating

If a product allowed one legitimate, Medium impact application to install with zero interaction with the user, then its Accuracy rating would be calculated like this:

Accuracy rating = 2 x 3 = 6

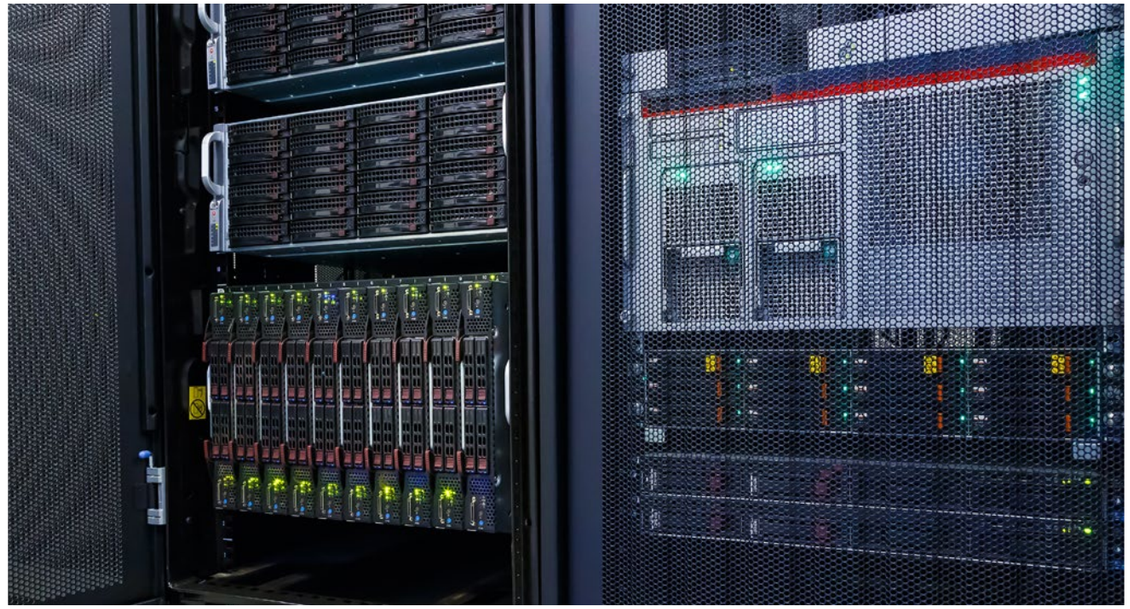
This same calculation is made for each legitimate application/site in the test and the results are summed and used to populate the graph and table shown under 5. Legitimate Software Ratings on page 12.

5.4 Distribution of Impact Categories

Endpoint products that were most accurate in handling legitimate objects achieved the highest ratings. If all objects were of the highest prevalence, the maximum possible rating would be 1,000 (100 incidents x (2 interaction rating x 5 prevalence rating)).

In this test there was a range of applications with different levels of prevalence. The table below shows the frequency:

LEGITIMATE SOFTWARE CATEGORY FREQUENCY	
Prevalence Rating	**Frequency**
Very high impact	53
High impact	24
Medium impact	12
Low impact	6
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.

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 place. It neutralised two threats, which fractionally reduced its overall score, which is rounded up to 100 per cent in our table.

Norton Security blocked all of the threats, but also blocked a legitimate application, which penalised its final rating. It came very close to the leading two products, though.

Bitdefender Internet Security was able to fend off all of the exploit-based targeted attacks fully but missed three web attacks.

AVG and Avast Free Antivirus were the most effective free products in this test, earning AAA awards. AVG failed to stop three targeted attacks but one public web threat. Avast handled all of the web threats but missed four targeted attacks. An accurate handling of legitimate software helped boost their ratings.

360 Total Security was the weakest product in the test by far. It was compromised by all but one of the targeted attacks and missed six of the web-based attacks. It allowed all but two of the legitimate applications and sites and failed to achieve an award.

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

SE Labs

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 27th June and 29th August 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 awards 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.

SE Labs

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
Qihoo	360 Total Security	9.2.0.1164
Avast	Free Antivirus	17.5.2303
AVG	AntiVirus Free Edition	17.5.3022
Avira	Free Security Suite	15.0.28.28
Bitdefender	Internet Security	7.72972 (9959764)
ESET	Smart Security	10.1.210.0 (15999)
Kaspersky	Internet Security	18.0.0.405 (c)
Microsoft	Security Essentials	4.10.209.0
Symantec	Norton Security	22.10.0.85
Trend Micro	Internet Security 10	11.1.1045

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	Email attack	Web download	Protected (total)
Norton Security	25	25	50	100
ESET Smart Security	25	25	50	100
Kaspersky Internet Security	25	25	50	100
Bitdefender Internet Security	25	25	47	97
Avast Free Antivirus	21	25	50	96
AVG AntiVirus Free Edition	22	25	49	96
Trend Micro Internet Security 10	24	25	47	96
Microsoft Security Essentials	21	24	47	92
Avira Free Security Suite	16	24	46	86
360 Total Security	1	25	44	70