SE Labs

INTELLIGENCE-LED TESTING

HOME ANTI-MALWARE PROTECTION

OCT - DEC 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

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)

While every effort is made to ensure the accuracy of the information published in this document, no guarantee is expressed or implied and SE Labs Ltd does not accept liability for any loss or damage that may arise from any errors or omissions.

INTRODUCTION

WILL YOUR ANTI-MALWARE PROTECT YOU FROM TARGETED ATTACKS?

The news isn't good. Discover your best options in our latest report.

Criminals routinely create ingenious scams and indiscriminate attacks designed to compromise the unlucky and, occasionally, foolish. But sometimes they focus on a specific target rather than casting a net wide in the hope of landing something interesting.

Targeted attacks can range from basic, like an email simply asking you to send some money to an account, through to extremely devious and technical. If you received an email from your accountant with an attached PDF or Excel spreadsheet would you open it? Most would and all that then stands between them and a successful hack (because the email was a trick and contained a dodgy document that gives remote control to the attacker) is the security software running on their PC.

In this test we've included indiscriminate, public attacks that come at victims from the web and via email, but we've also included some devious targeted attacks to see how well-protected potential victims would be.

We've not created any new types of threat and we've not discovered and used 'zero day' attacks. Instead we took tools that are freely distributed online and are well-known to penetration testers and criminals alike. We used these to generate threats that are realistic representations of what someone could quite easily put together to attack you or your business.

The results are extremely worrying. While a few products were excellent at detecting and protecting against these threats many more were less useful. We will continue this work and report any progress that these companies make in improving their products.

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.

We continue to test Microsoft and McAfee business products privately and plan to produce results in the first report of 2018.

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.

EXECUTIVE SUMMARY			
Products Tested	**Protection Accuracy (%)**	**Legitimate Accuracy (%)**	**Total Accuracy (%)**
Norton Security	94%	98%	96%
Kaspersky Internet Security	88%	100%	96%
ESET Smart Security	79%	100%	93%
Avira Free Security Suite	77%	100%	92%
Avast Free Antivirus	75%	100%	91%
Trend Micro Internet Security	78%	96%	89%
AVG Antivirus Free Edition	70%	100%	89%
ZoneAlarm Free Antivirus	61%	100%	86%
F-Secure Safe Internet Security	76%	89%	84%
Bitdefender Internet Security	72%	90%	83%
Cisco Immunet	52%	100%	83%
Microsoft Security Essentials	41%	99%	78%
Qihoo 360 Total Security	27%	95%	70%

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.

● **There was a wide spread in how effectively the anti-malware products were able to handle general threats from cyber criminals...**
Most products were largely capable of handling public web-based threats such as those used by criminals to attack Windows PCs, tricking users into running malicious files or running scripts that download and run malicious files.

● **.. and targeted attacks were prevented in many cases.**
A few were particularly competent at blocking more targeted, exploit-based attacks. However, the majority struggled.

● **False positives were not an issue for most products**
Most of the products were good at correctly classifying legitimate applications and websites. A slim majority allowed all of the legitimate websites and applications.

● **Which products were the most effective?**
Symantec and **Kaspersky Lab** products achieved extremely good 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, 1st February 2018

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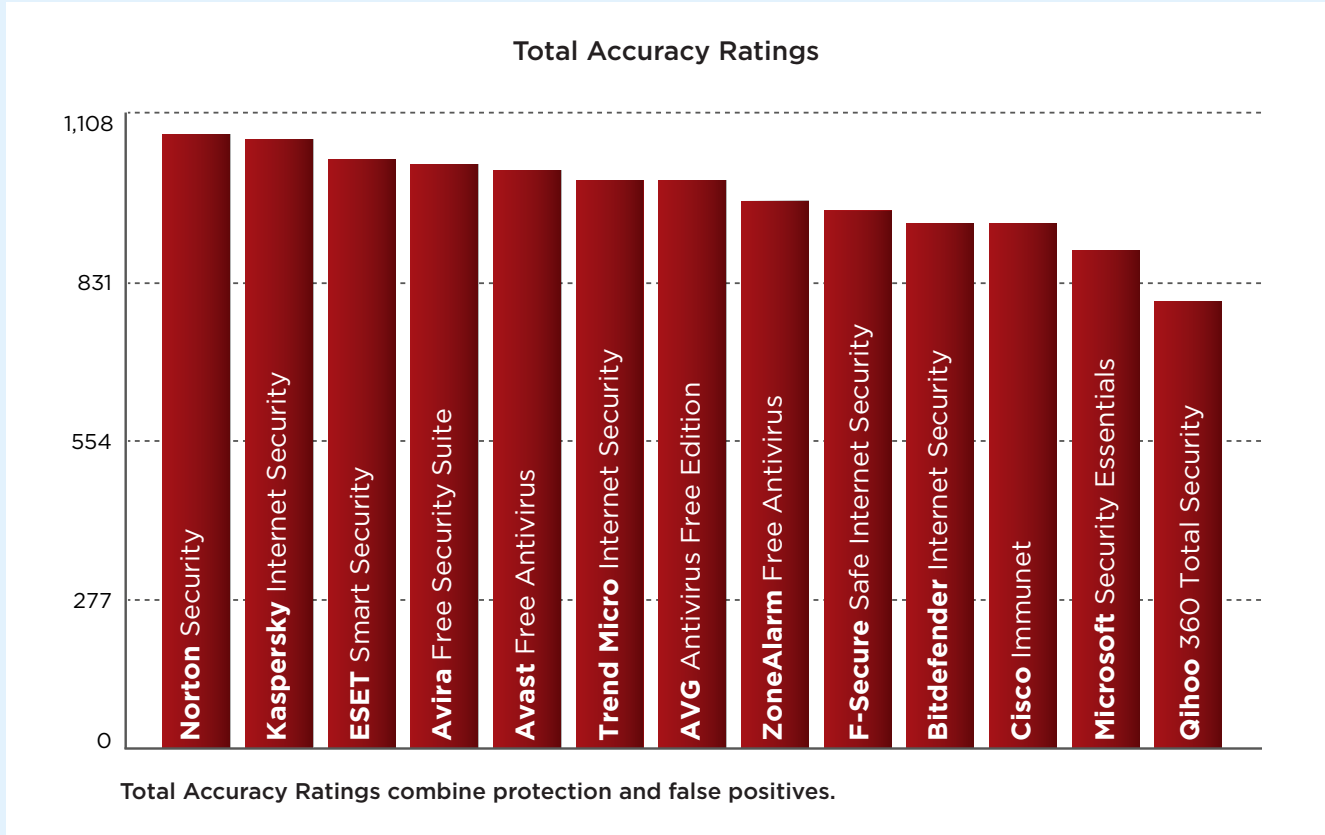
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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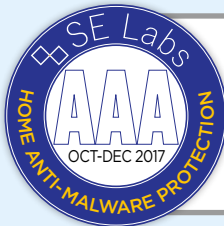
For example, a product that completely blocks a threat is rated more highly than one that allows a threat to run for a while before eventually evicting it. Products that allow all malware infections, or that block popular legitimate applications, are penalised heavily.

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.
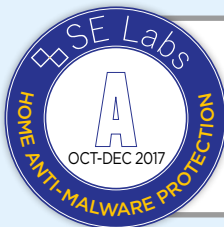
Total Accuracy Ratings

Total Accuracy Ratings combine protection and false positives.

AWARDS

The following products win SE Labs awards:

AAA (OCT-DEC 2017 · HOME ANTI-MALWARE PROTECTION)
- Norton Security
- Kaspersky Internet Security

AA (OCT-DEC 2017 · HOME ANTI-MALWARE PROTECTION)
- ESET Smart Security
- Avira Free Security Suite
- Avast Free Antivirus

A (OCT-DEC 2017 · HOME ANTI-MALWARE PROTECTION)
- Trend Micro Internet Security
- AVG Antivirus Free Edition
- ZoneAlarm Free Antivirus
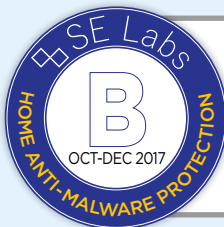
B (OCT-DEC 2017 · HOME ANTI-MALWARE PROTECTION)
- F-Secure Safe Internet Security
- Bitdefender Internet Security
- Cisco Immunet
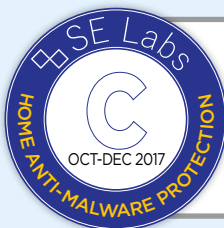
C (OCT-DEC 2017 · HOME ANTI-MALWARE PROTECTION)
- Microsoft Security Essentials

TOTAL ACCURACY RATINGS

Product	Total Accuracy Rating	Total Accuracy (%)	Award
Norton Security	1,069	96%	AAA
Kaspersky Internet Security	1,060	96%	AAA
ESET Smart Security	1,025	93%	AA
Avira Free Security Suite	1,017	92%	AA
Avast Free Antivirus	1,007	91%	AA
Trend Micro Internet Security	988.5	89%	A
AVG Antivirus Free Edition	988	89%	A
ZoneAlarm Free Antivirus	953	86%	A
F-Secure Safe Internet Security	936	84%	B
Bitdefender Internet Security	924	83%	B
Cisco Immunet	915	83%	B
Microsoft Security Essentials	867	78%	C
Qihoo 360 Total Security	778	70%	

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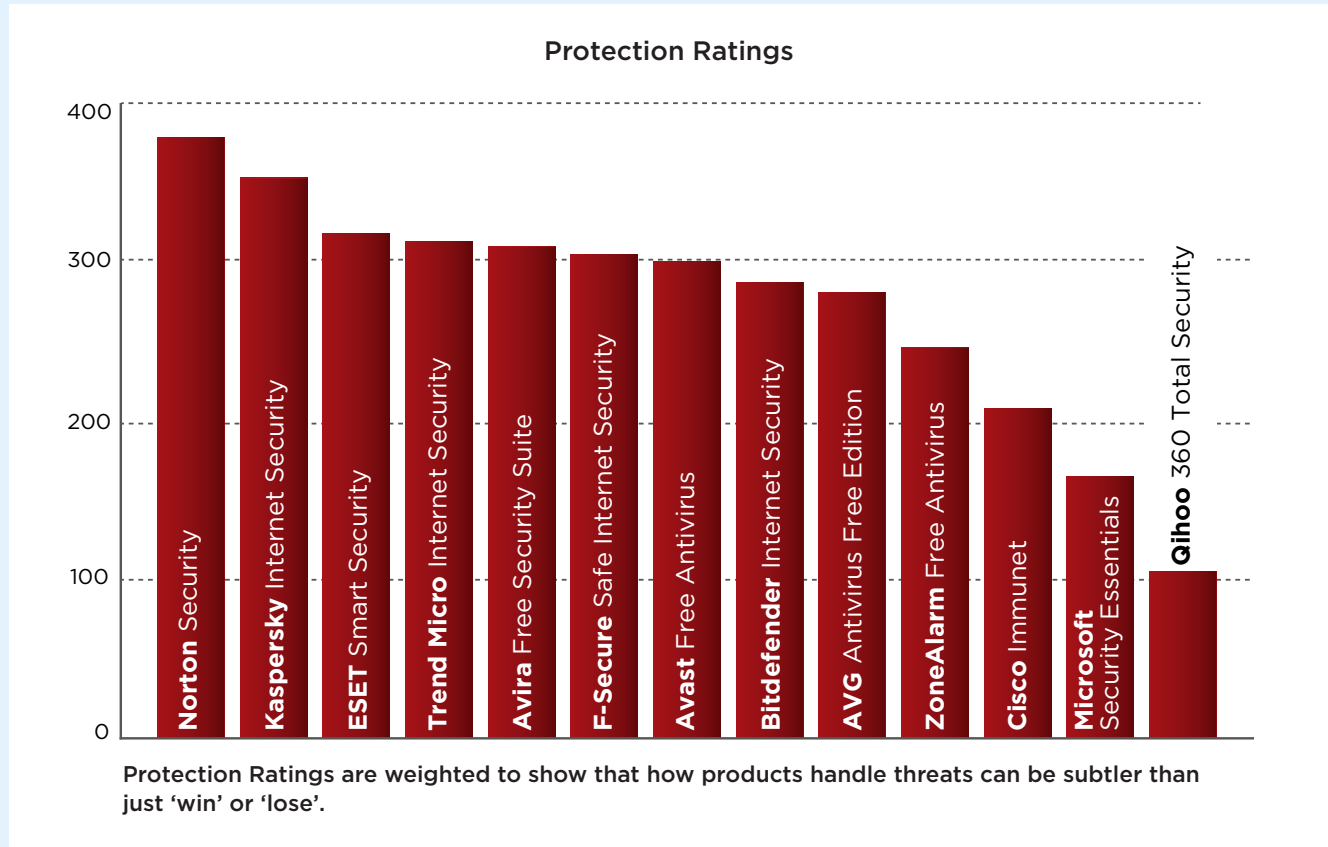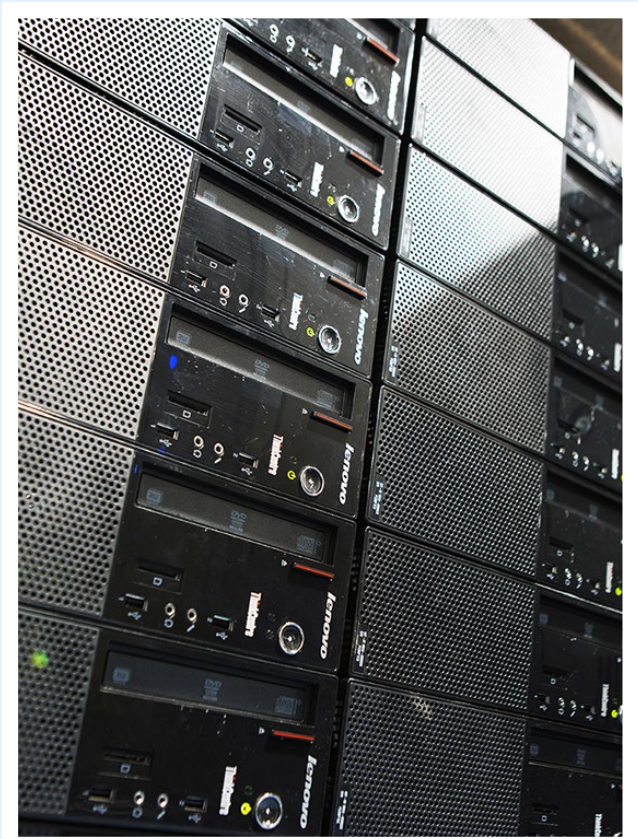
- **Neutralised (+1)**
Products that kill all running malicious processes 'neutralise' the threat and win one point.

- **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.

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 (%)**
Norton Security	377	94%
Kaspersky Internet Security	352	88%
ESET Smart Security	317	79%
Trend Micro Internet Security	312	78%
Avira Free Security Suite	309	77%
F-Secure Safe Internet Security	304	76%
Avast Free Antivirus	299	75%
Bitdefender Internet Security	288	72%
AVG Antivirus Free Edition	280	70%
ZoneAlarm Free Antivirus	245	61%
Cisco Immunet	207	52%
Microsoft Security Essentials	164	41%
Qihoo 360 Total Security	106	27%

Average: 69%

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.
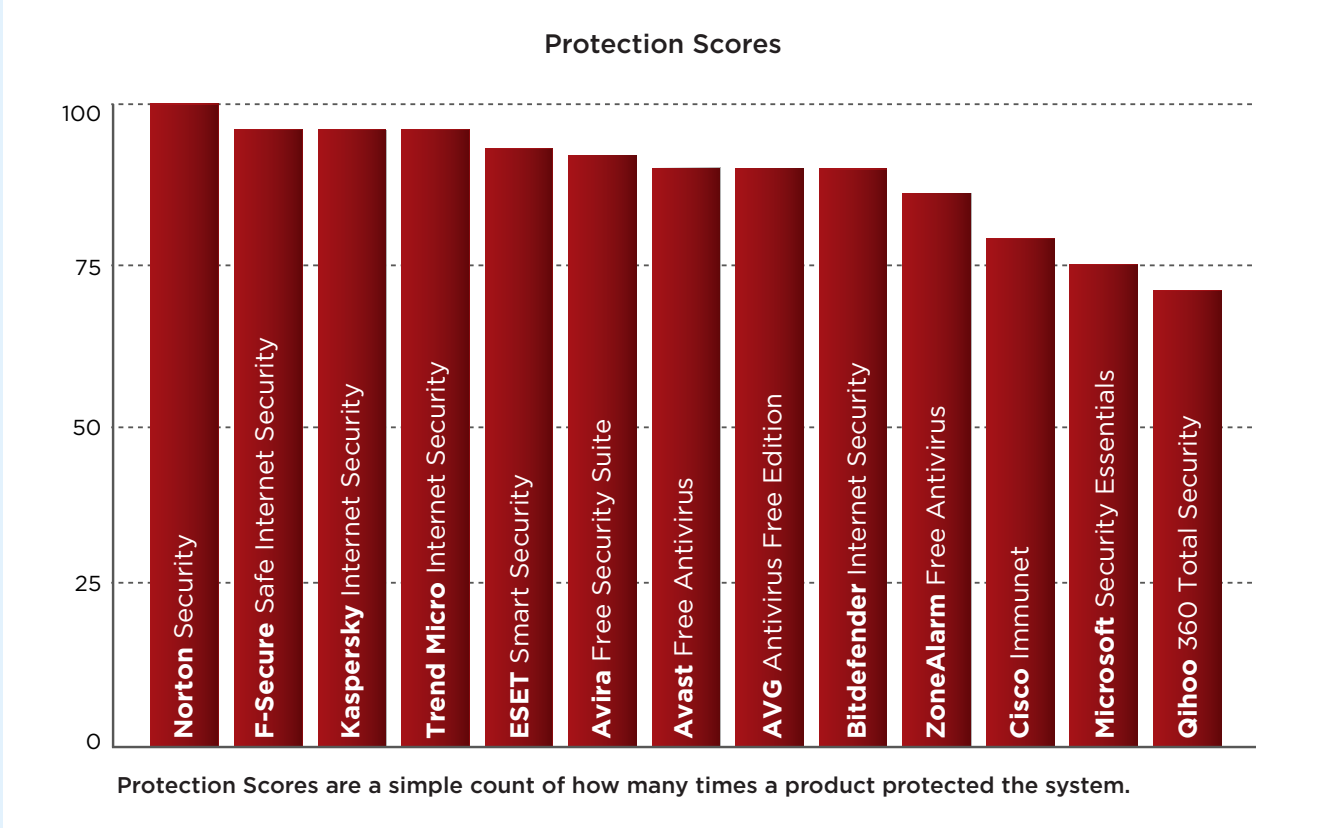
PROTECTION SCORES	
Product	Protection Score
Norton Security	100
F-Secure Safe Internet Security	96
Kaspersky Internet Security	96
Trend Micro Internet Security	96
ESET Smart Security	93
Avira Free Security Suite	92
Avast Free Antivirus	90
AVG Antivirus Free Edition	90
Bitdefender Internet Security	90
ZoneAlarm FreeAntivirus	86
Cisco Immunet	79
Microsoft Security Essentials	75
Qihoo 360 Total Security	72

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.

Protection Details

This data shows in detail how each product handled the threats used.
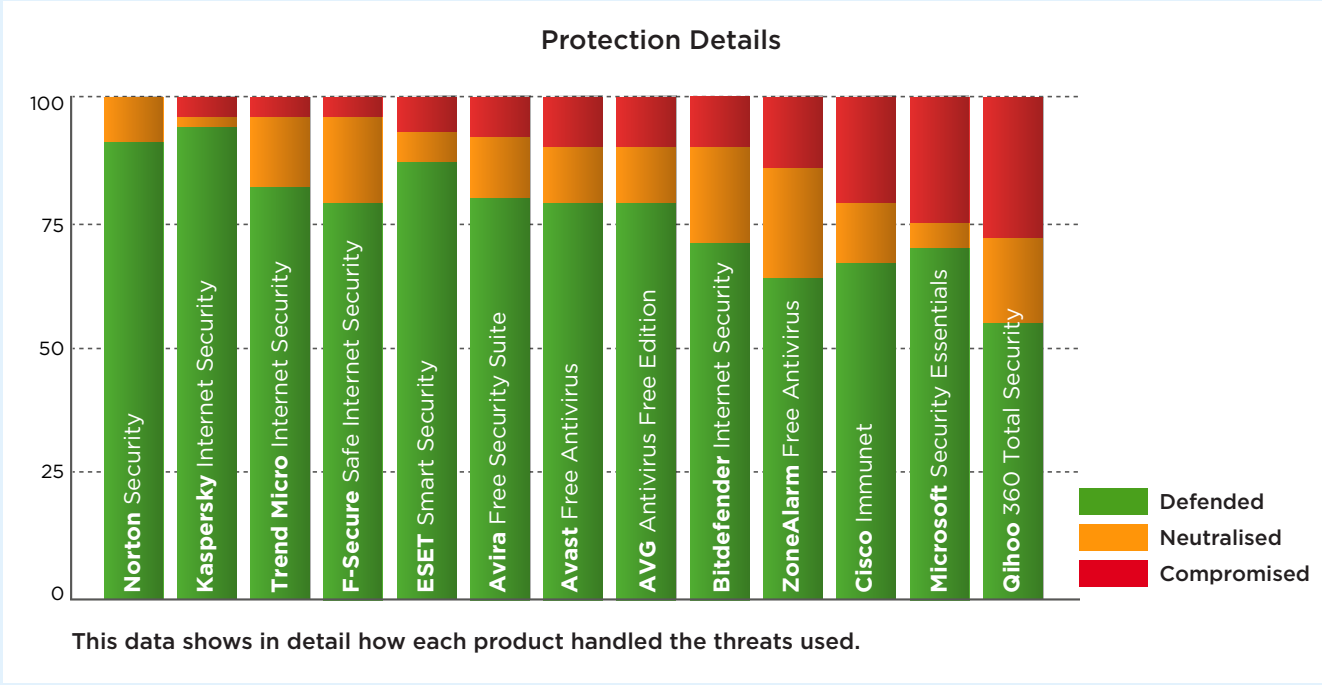
PROTECTION DETAILS					
Product	Detected	Blocked	Neutralised	Compromised	Protected
Norton Security	100	91	9	0	100
Kaspersky Internet Security	91	94	2	4	96
Trend Micro Internet Security	97	82	14	4	96
F-Secure Safe Internet Security	98	79	17	4	96
ESET Smart Security	94	87	6	7	93
Avira Free Security Suite	96	80	12	8	92
Avast Free Antivirus	100	79	11	10	90
AVG Antivirus Free Edition	92	79	11	10	90
Bitdefender Internet Security	99	71	19	10	90
ZoneAlarm Free Antivirus	97	64	22	14	86
Cisco Immunet	92	67	12	21	79
Microsoft Security Essentials	74	70	5	25	75
Qihoo 360 Total Security	73	55	17	28	72

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.
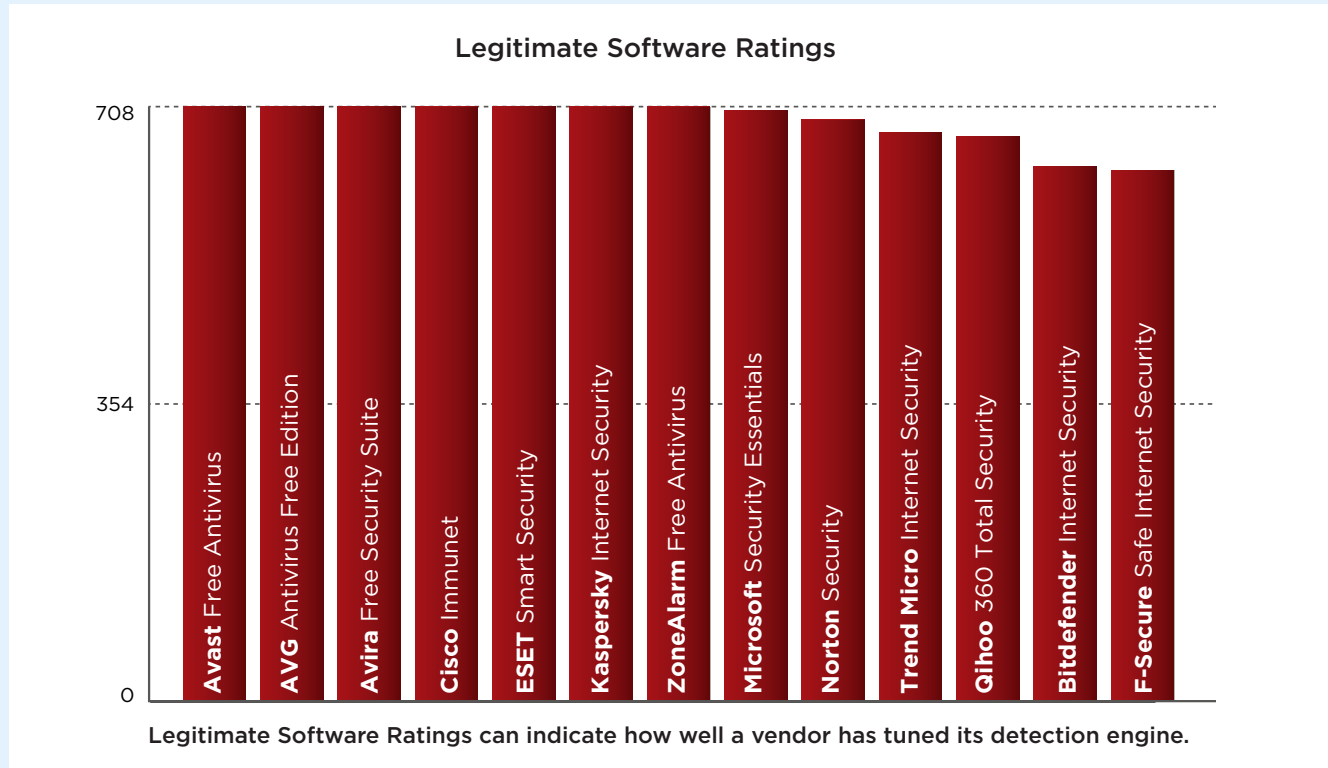
LEGITIMATE SOFTWARE RATINGS

Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
Avast Free Antivirus	708	100%
AVG Antivirus Free Edition	708	100%
Avira Free Security Suite	708	100%
Cisco Immunet	708	100%
ESET Smart Security	708	100%
Kaspersky Internet Security	708	100%
ZoneAlarm Free Antivirus	708	100%
Microsoft Security Essentials	703	99%
Norton Security	692	98%
Trend Micro Internet Security	676.5	96%
Qihoo 360 Total Security	672	95%
Bitdefender Internet Security	636	90%
F-Secure Safe Internet Security	632	89%

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)	Click to allow (Default Allow)
Avast Free Antivirus	100	0	0	0
AVG Antivirus Free Edition	100	0	0	0
Avira Free Security Suite	100	0	0	0
Cisco Immunet	100	0	0	0
ESET Smart Security	100	0	0	0
Kaspersky Internet Security	100	0	0	0
ZoneAlarm Free Antivirus	100	0	0	0
Microsoft Security Essentials	98	0	0	2
Norton Security	98	1	1	0
Trend Micro Internet Security	98	0	2	0
Qihoo 360 Total Security	96	2	2	0
F-Secure Safe Internet Security	94	0	6	0
Bitdefender Internet Security	92	8	0	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	23
High impact	39
Medium impact	17
Low impact	11
Very low impact	10
Grand total	**100**
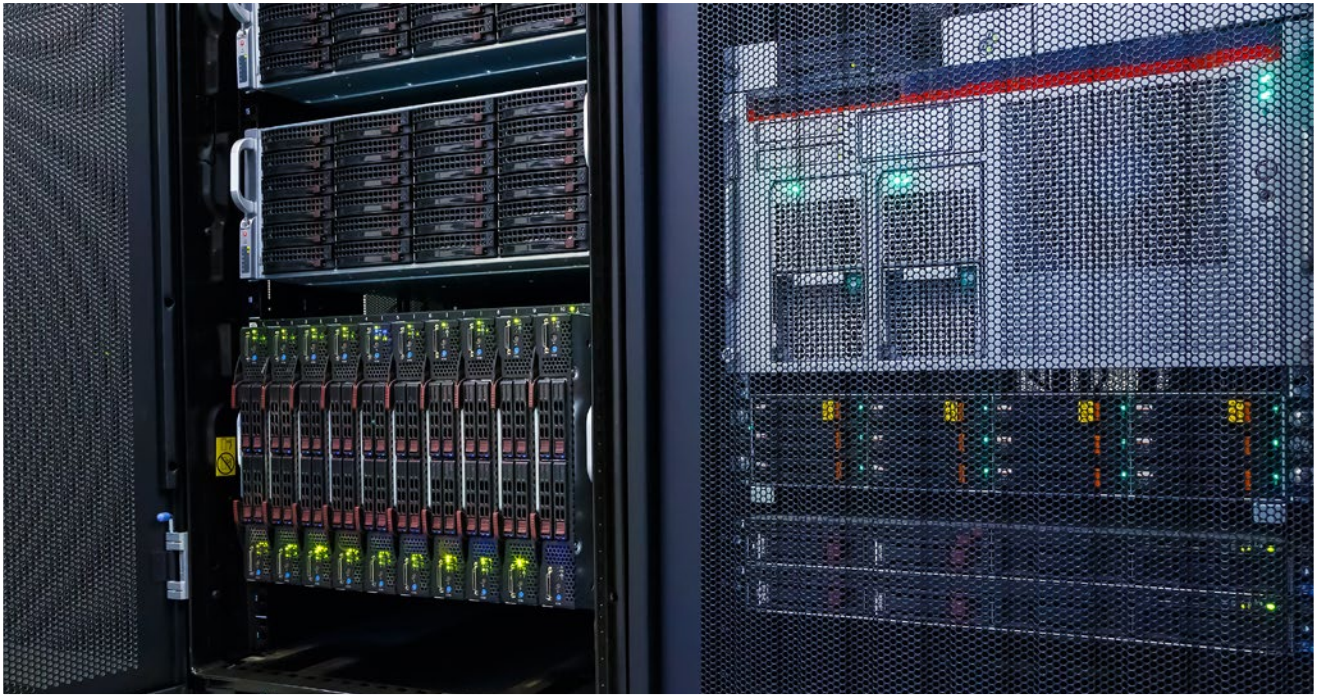
6. CONCLUSIONS

Attacks in this test included threats that affect the wider public and more closely-targeted individuals and organisations. You could say that we tested the products with 'public' malware and full-on hacking attacks. We introduced the threats in a realistic way such that threats seen in the wild on websites were downloaded from those same websites, while threats caught spreading through email were delivered to our target systems as emails.

All of the products tested are well-known and should do well in this test. While we do 'create' threats by using publicly available free hacking tools, we don't write unique malware so there is no technical reason why any vendor being tested should do poorly.

Consequently, it's not a shock to see all products handle the email threats very effectively. By and large the malicious websites were also ineffective, although there were a few that evaded detection. **360 Total Security** was particularly weak in handling these in comparison to the competition. Targeted attacks were handled well by the leaders in this test, but most products missed a lot and those from **Cisco**, **Microsoft** and **Qihoo 360** (**360 Total Security**) were significantly weaker than the others.

Norton Security blocked all of the public and targeted attacks. It blocked two legitimate applications, though, so it lost a few points – but not enough to move it from the number one spot.

Kaspersky Internet Security came a very close second. This is because it made no mistakes with the legitimate software and protected against 96 per cent of the threats. In the cases where it was compromised (with targeted attacks), it detected the attack and removed the threat, although we were still able to hack the system even after the initial malicious file was removed.

ESET Smart Security takes third place. It was compromised more often than **Kaspersky's** product but detected more of the threats. It scores just ahead of two of the free products in this test, those from **Avast** and **Avira**. The other free products scored more humbly in this test.

Products were awarded the full range of ratings, from **AAA** at the top down through **AA**, **A**, **B** and **C**. **360 Total Security** scored the lowest and failed to achieve a rating. It tended to neutralise, rather than block threats, and missed nearly all of the targeted attacks.

The leading products from **Symantec** and **Kaspersky Lab** win **AAA** awards. **AAA** awards for their strong overall performance.

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 26th September and 6th December 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.

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

Provider	Product Name	Build Version
Avast	Avast Free Antivirus	17.8.2318
AVG	AVG Antivirus Free Edition	17.8.3036
Avira	Avira Free Security Suite	15.0.33.24
Bitdefender Internet Security	Bitdefender Internet Security	22.0.15.189
CISCO	Cisco Immunet	6.0.6.106.00
ESET	ESET Smart Security	10.1.219.0
F-Secure	F-Secure Safe Internet Security	2.93 build 175
Kaspersky Lab	Kaspersky Internet Security	18.0.0405 (c)
Microsoft	Microsoft Security Essentials	4.10.209.0
Symantec	Norton Security	22.11.2.7
Trend Micro	Trend Micro Internet Security	12.0.1191
Qihoo	360 Total Security	9.6.0.1017
ZoneAlarm	ZoneAlarm Free Antivirus	15.1.504.17269

APPENDIX D: Attack Types

The table below shows how each product protected against the different types of attacks used in the test.

ATTACK TYPES

Product	Web Download	Targeted Attack	Email Attack	Protected (Total)
Norton Security	50	25	25	100
Trend Micro Internet Security	50	23	23	96
F-Secure Safe Internet Security	50	24	22	96
Kaspersky Internet Security	50	21	25	96
ESET Smart Security	50	20	23	93
Avira Free Security Suite	50	18	24	92
AVG Antivirus Free Edition	50	17	23	90
Avast Free Antivirus	49	17	24	90
Bitdefender Internet Security	50	16	24	90
ZoneAlarm Free Antivirus	49	14	23	86
Cisco Immunet	49	5	25	79
Microsoft Security Essentials	47	3	25	75
Qihoo 360 Total Security	45	3	23	71