SE Labs

INTELLIGENCE-LED TESTING

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

ENTERPRISE ENDPOINT PROTECTION

APR - JUN 2017

SE Labs tested a variety of 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 7th July 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

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Stefan Dumitrascu
Gia Gorbold
Magdalena Jurenko
Alexandru Statie
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

Can anti-malware be 100 per cent effective?

There are a lot of threats on the web, and going online without protection is very risky. We need good, consistently effective anti-malware products to reduce our risk of infection. And the ones included in this report look great – in fact, some score 100 per cent. That means they stopped all the threats that we exposed them to, and didn't block anything legitimate.

But wait a minute! Those in the security industry know full well that there is no such thing as 100 per cent security. There is always a way past every security measure, and this is as true in the anti-malware world as with any other measures for threat protection.

This test includes some of the very best anti-malware products in the world, and pits them against prevalent threats, be they ones that affect hundreds of thousands of users worldwide, or those that could be used to target individuals and organisations. It's a tough test, but a fair one. You could argue that any anti-malware product worth its salt would score 100 per cent or thereabouts.

Products can score 100 per cent in our tests because we don't choose thousands of weird and wonderful rare pieces of malware to test. Regular users are extremely unlikely to encounter those in the real world. We're looking at the threats that could affect *you*.

Our mission is to help improve computer security through testing, both publicly and privately. We also want to help customers choose the best products by publishing some of those test results. But don't forget that success today is not a guarantee of success tomorrow. It's important to keep monitoring test results.

If you spot a detail in this report that 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.

We have removed the Microsoft System Center Endpoint Protection results from this report as we accidentally tested an older build than the current version.

EXECUTIVE SUMMARY

Product names

It is good practice to stay up to date with the latest version of your chosen endpoint security product. We made best efforts to ensure that each product tested was the very latest version running with the most recent updates to give the best possible outcome.

For specific build numbers, see Appendix C: Product versions on page 19.

Products tested

PRODUCT	PROTECTION ACCURACY RATING	LEGITIMATE ACCURACY RATING	TOTAL ACCURACY RATING
Kaspersky Endpoint Security	100%	100%	100%
ESET Endpoint Security	100%	100%	100%
Symantec Endpoint Security Enterprise Edition	100%	100%	100%
Sophos Central Endpoint	100%	98%	99%
Trend Micro OfficeScan, Intrusion Defense Firewall	98%	99%	99%

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 generally effective at handling general threats from cyber criminals...**
All products were capable of handling public threats such as those used by criminals to attack Windows PCs and install ransomware.

- **...and targeted attacks were thoroughly thwarted**
All of the products were also very competent at blocking more targeted, exploit-based attacks.

- **False positives were not an issue for most products**
Most of the endpoint solutions were good at correctly classifying legitimate applications and websites. The vast majority allowed all legitimate websites and apps.

- **Which products were the most effective?**
Kaspersky Lab, Sophos, ESET, Trend Micro and Symantec products all 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, 7th July 2017

1. TOTAL ACCURACY RATINGS

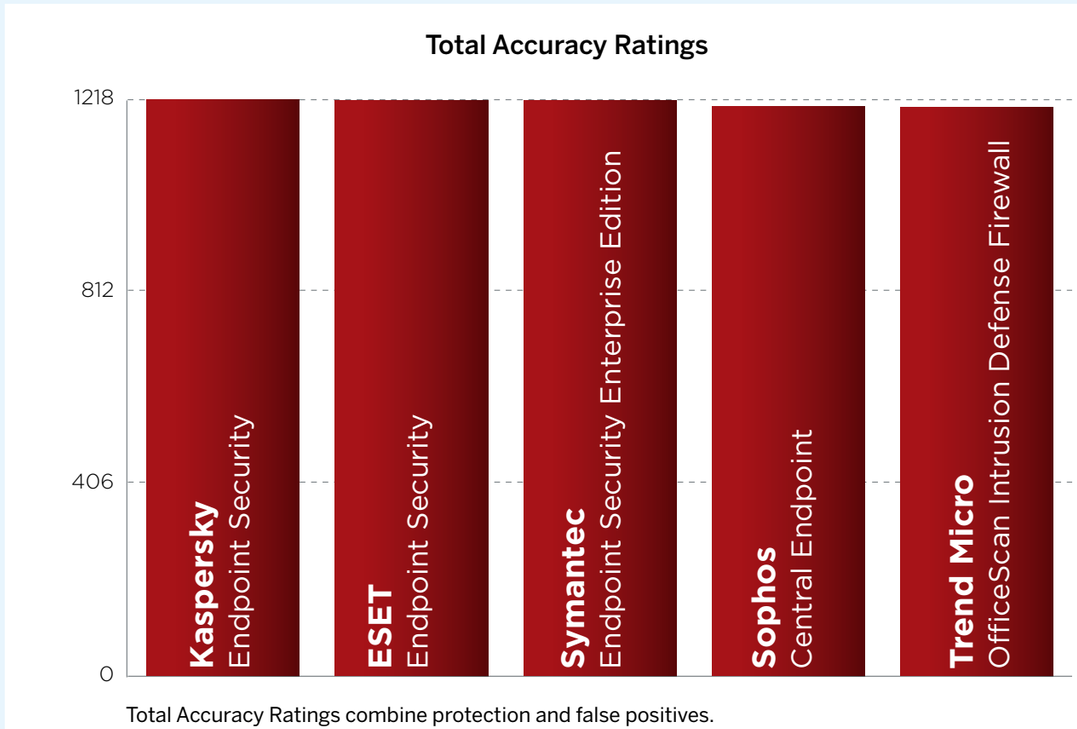
Judging the effectiveness of an endpoint security product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier, we've combined all the different results from this report into one easy-to-understand graph.

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 Endpoint Security
- ESET Endpoint Security
- Symantec Endpoint Security Enterprise Edition
- Sophos Central Endpoint
- Trend Micro OfficeScan, Intrusion Defense Firewall

TOTAL ACCURACY RATINGS			
Product	**Total Accuracy Rating**	**Total Accuracy (%)**	**Award**
Kaspersky Endpoint Security	1218	100%	AAA
ESET Endpoint Security	1216	100%	AAA
Symantec Endpoint Security Enterprise Edition	1216	100%	AAA
Sophos Central Endpoint	1202	99%	AAA
Trend Micro OfficeScan, Intrusion Defense Firewall	1201	99%	AAA

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.

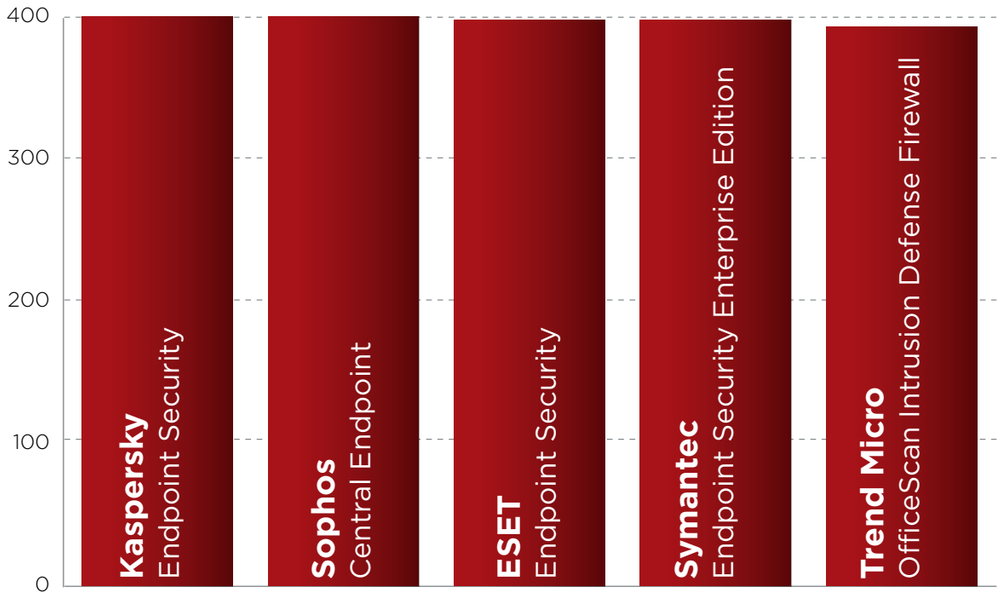
- **Blocked (+2)**
Threats that are disallowed from even starting their malicious activities are blocked. Blocking products score two points.

- **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



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 simple and 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.

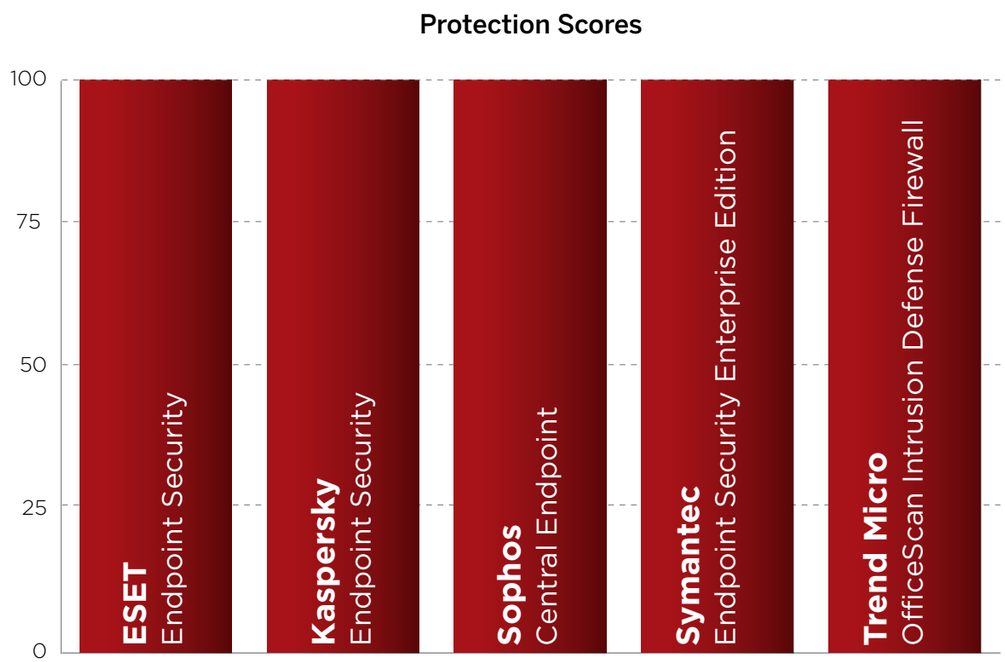
PROTECTION RATINGS		
Product	**Protection Rating**	**Protection Rating (%)**
Kaspersky Endpoint Security	400	100%
Sophos Central Endpoint	400	100%
ESET Endpoint Security	398	100%
Symantec Endpoint Security Enterprise Edition	398	100%
Trend Micro OfficeScan, Intrusion Defense Firewall	393	98%

Average: 99%

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.



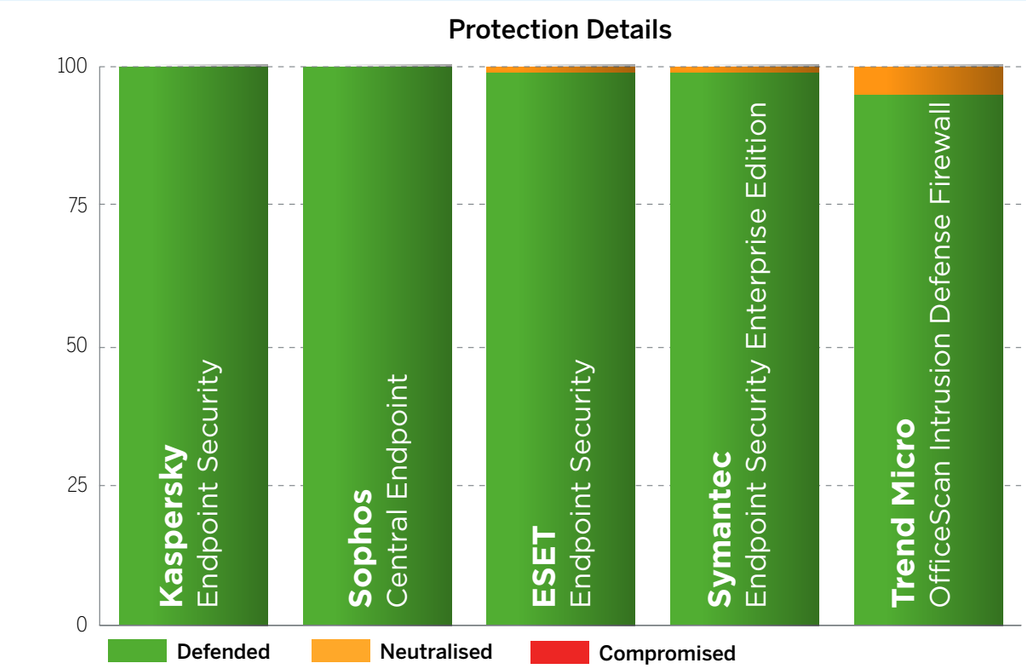
Protection Scores are a simple count of how many times a product protected the system.

PROTECTION SCORES	
Product	**Protection Score**
ESET Endpoint Security	100
Kaspersky Endpoint Security	100
Sophos Central Endpoint	100
Symantec Endpoint Security Enterprise Edition	100
Trend Micro OfficeScan, Intrusion Defense Firewall	100

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.



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

PROTECTION DETAILS					
Product	**Detected**	**Blocked**	**Neutralised**	**Compromised**	**Protected**
Kaspersky Endpoint Security	100	100	0	0	100
Sophos Central Endpoint	100	100	0	0	100
ESET Endpoint Security	100	99	1	0	100
Symantec Endpoint Security Enterprise Edition	100	99	1	0	100
Trend Micro OfficeScan, Intrusion Defense Firewall	100	95	5	0	100

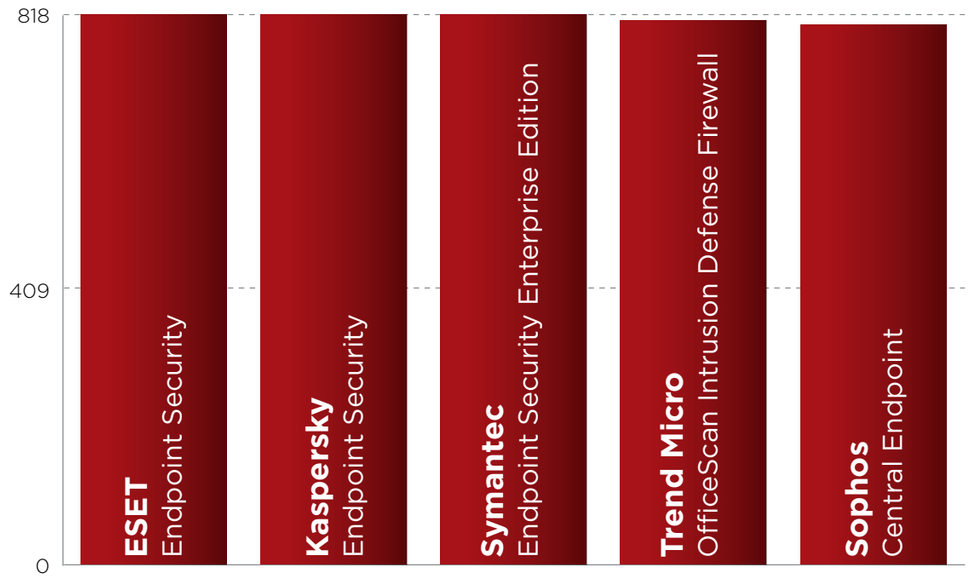
5. LEGITIMATE SOFTWARE RATINGS

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 (%)**
ESET Endpoint Security	818	100%
Kaspersky Endpoint Security	818	100%
Symantec Endpoint Security Enterprise Edition	818	100%
Trend Micro OfficeScan, Intrusion Defense Firewall	808	99%
Sophos Central Endpoint	802	98%

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)**	**None (blocked)**
ESET Endpoint Security	100	0
Kaspersky Endpoint Security	100	0
Symantec Endpoint Security Enterprise Edition	100	0
Sophos Central Endpoint	99	1
Trend Micro OfficeScan, Intrusion Defense Firewall	99	1

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 being 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	44
High impact	36
Medium impact	9
Low impact	7
Very low impact	4
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.

URLs were introduced to the targets directly and, in relevant cases, via email. We also included targeted attacks, which were exploit-based attempts to gain remote control of the target systems.

When a product failed to protect its user in this test, the chances are the attack used an exploit. Most products handled web downloads very effectively. Targeted attacks were also handled well.

Kaspersky Endpoint Security blocked all of the public and targeted attacks. It also allowed 100 per cent of the legitimate software and websites. It achieved the rare privilege of a 100 per cent total accuracy rating.

ESET Endpoint Security and Symantec Endpoint Security Enterprise Edition take joint second place, coming in a hair's breadth away from Kaspersky Lab. The only difference was that they each neutralised one threat. The practical difference is negligible and the table shows a 100 per cent totally accuracy, a figure that is rounded up from 99.8 per cent.

Sophos Central Endpoint protected against all of the threats, blocking them completely. However, it dropped some points because it blocked one legitimate website, which had previously hosted malware some time before the test was run.

Trend Micro OfficeScan, Intrusion Defense Firewall also performed strongly, detecting all threats and blocking 95 per cent of them. It neutralised the remaining five threats and blocked only one legitimate application.

In an unprecedented set of results, all the products tested (from Kaspersky Lab, ESET, Symantec, Sophos and Trend Micro) win 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 27th March and 26th May 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		
Vendor	**Product**	**Build**
ESET	**Endpoint Security**	Version: 6.4.2014.0 Database: 15517
Kaspersky	**Endpoint Security**	10.2.5.3201 (mr3)
Sophos	**Central Endpoint**	11.5.4; Intercept X
Symantec	**Endpoint Security Enterprise Edition**	Version 14 build 1904 (14.0.1904.0000)
Trend Micro	**OfficeScan, Intrusion Defense Firewall**	12.0.1850

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 drive-by**	**Web download**	**Protected (total)**
ESET Endpoint Security	25	25	27	23	**100**
Kaspersky Endpoint Security	25	25	27	23	**100**
Sophos Central Endpoint	25	25	27	23	**100**
Symantec Endpoint Security Enterprise Edition	25	25	27	23	**100**
Trend Micro OfficeScan, Intrusion Defense Firewall	25	25	27	23	**100**