SE Labs

INTELLIGENCE-LED TESTING

SMALL BUSINESS ENDPOINT PROTECTION

JAN - MAR 2018

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

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.

MANAGEMENT
Director Simon Edwards
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

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

CONTENTS

Document version 1.0 *Written 27th April 2018.*

Document version 1.1 *Updated 25th April 2019 to reflect correct name for Microsoft product.*

INTRODUCTION

Are you buying solid protection or snake oil?

Sometimes testers need to be tested too. We're always up for a challenge!

How do you know which security products to buy? Many rely on independent tests to help in the decision-making process. But how do you know if a test is any good or not?

The Anti-Malware Testing Standards Organization (**AMTSO**) has been working to create a Standard that will give you, the customer, some assurance that the test was conducted fairly.

Earlier this year AMTSO has been trying out its Standard, which it has been working on for many months. SE Labs is proud to be involved in this initiative and the testing for this report has been assessed for compliance with the Standard.

If that sounds a bit dry, what it means is that there are experimental rules about how a tester should behave and we have put ourselves up for judgment by AMTSO.

Did participating in this process change the way we worked? Yes, but not in the technical ways that we test. Instead we turned the testing world's business model on its head.

Many testers charge vendors money to be tested. Some will test regardless, but charge money if the vendors want to see their results before publication (and have the opportunity to make requests for corrections).

We think that the dispute process should be free for all. SE Labs has not charged any vendor for its participation in this test and we provided a free dispute process to any vendor that requested it. In this way every vendor is treated as equally as possible, for the fairest possible test.

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 16.*

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Kaspersky Small Office Security	100%	100%	100%
ESET Endpoint Security	98%	100%	99%
Sophos Central Endpoint	95%	100%	98%
Symantec Endpoint Protection Cloud	96%	98%	97%
Trend Micro Worry Free Security Services	91%	98%	96%
Panda Endpoint Protection	60%	100%	86%
Microsoft Windows Defender ATP's Antivirus	49%	91%	76%
Webroot SecureAnywhere Endpoint Protection	23%	98%	71%
Malwarebytes Endpoint Security	-16%	98%	57%

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…**

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. **Malwarebytes** was notably weaker than the competition.

■ **.. and targeted attacks were prevented in many cases.**

Many products were also competent at blocking more targeted, exploit-based attacks. However, while some did very well in this part of the test, others were very much weaker. **Malwarebytes** and **Webroot** were largely incapable of stopping the targeted 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 of the legitimate websites and applications. **Microsoft's** was the least accurate in this part of the test.

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

Products from **Kaspersky Lab**, **ESET**, **Sophos**, **Symantec** and **Trend Micro** achieved extremely good results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites.

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 11.

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Kaspersky Small Office Security	1,116	100%	AAA
ESET Endpoint Security	1,111	99%	AAA
Sophos Central Endpoint	1,099	98%	AAA
Symantec Endpoint Protection Cloud	1,085	97%	AAA
Trend Micro Worry Free Security Services	1,071	96%	AAA
Panda Endpoint Protection	957	86%	A
Microsoft Windows Defender ATP's Antivirus	848.5	76%	C
Webroot SecureAnywhere Endpoint Protection	794	71%	
Malwarebytes Endpoint Security	639	57%	

Total Accuracy Ratings combine protection and false positives.

SE Labs

Small Business Endpoint Protection Awards

The following products win SE Labs awards:

- **Kaspersky** Small Office Security
- **ESET** Endpoint Security
- **Sophos** Central Endpoint
- **Symantec** Endpoint Protection Cloud
- **Trend Micro** Worry Free Security Services

- **Panda** Endpoint Protection

- **Microsoft** Windows Defender ATP's Antivirus

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:

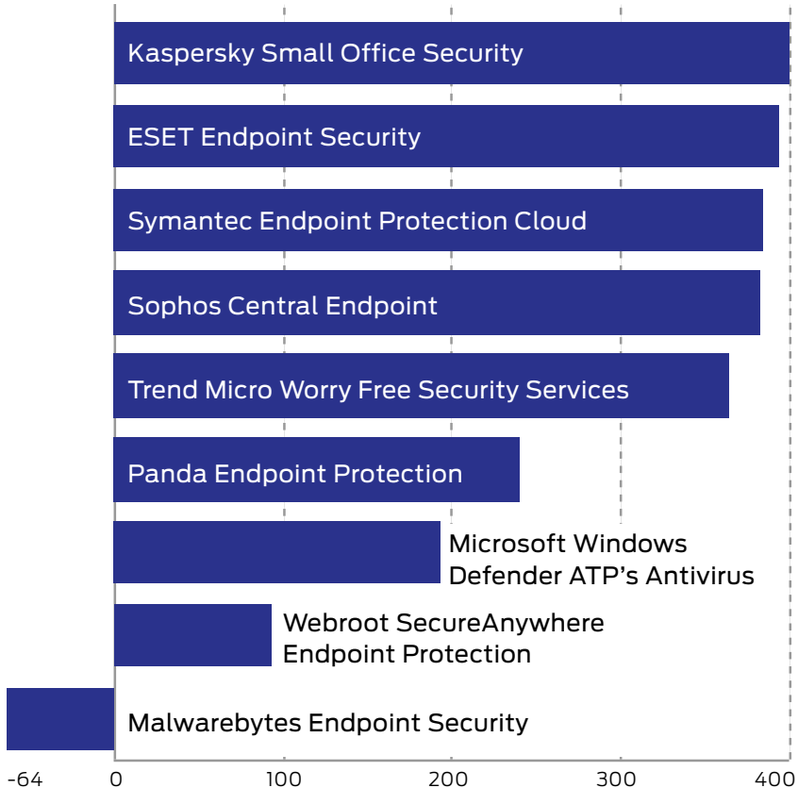
Protection rating =
(1x number of Detected) +
(2x number of Blocked) +
(1x number of Neutralised) +
(1x number of Complete remediation) +
(-5x number of Compromised)

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		
Product	**Protection Rating**	**Protection Rating (%)**
Kaspersky Small Office Security	398	100%
ESET Endpoint Security	393	98%
Symantec Endpoint Protection Cloud	383	96%
Sophos Central Endpoint	381	95%
Trend Micro Worry Free Security Services	365	91%
Panda Endpoint Protection	239	60%
Microsoft Windows Defender ATP's Antivirus	194	49%
Webroot SecureAnywhere Endpoint Protection	92	23%
Malwarebytes Endpoint Security	-64	-16%

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



Average 66%

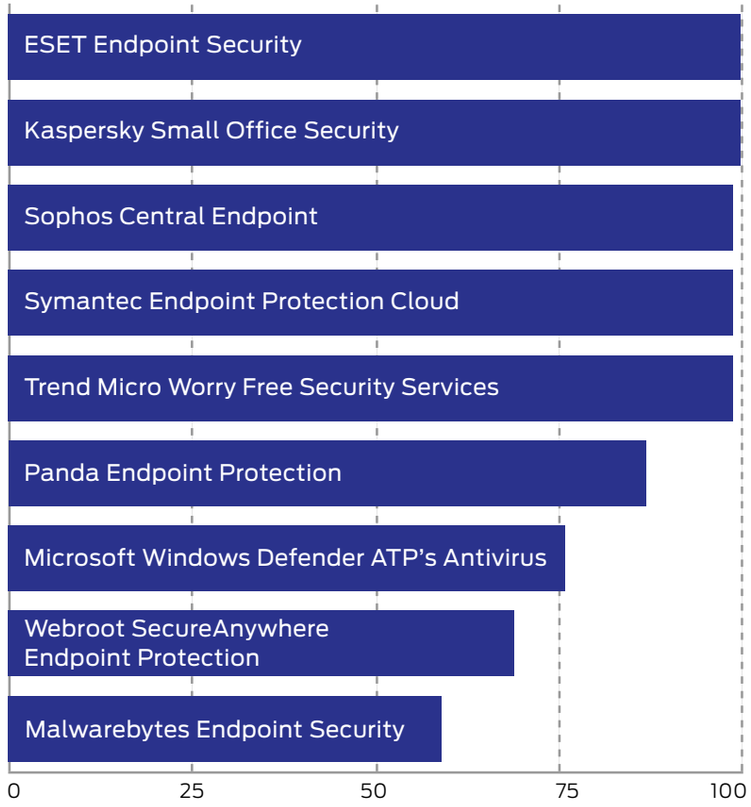
3. Protection Scores

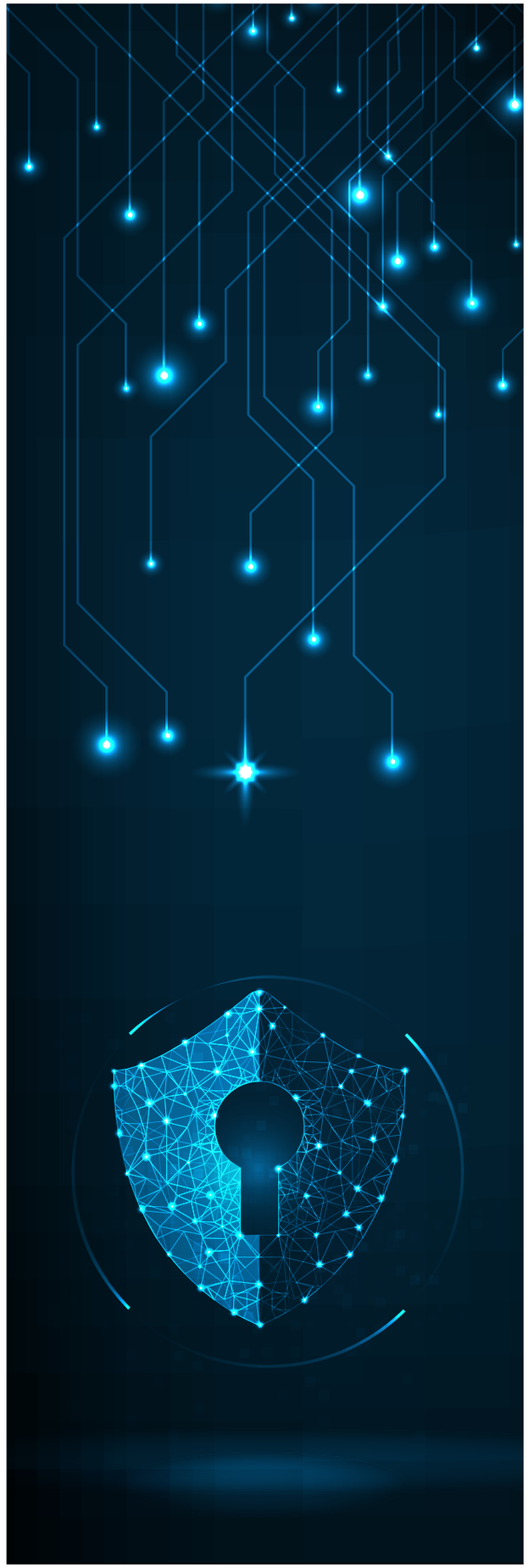
This graph shows the overall level of protection, making no distinction between neutralised and blocked incidents.

For each product we add Blocked and Neutralised cases together to make one simple tally.

PROTECTION SCORES	
Product	**Protection Score**
ESET Endpoint Security	100
Kaspersky Small Office Security	100
Sophos Central Endpoint	99
Symantec Endpoint Protection Cloud	99
Trend Micro Worry Free Security Services	99
Panda Endpoint Protection	87
Microsoft Windows Defender ATP's Antivirus	76
Webroot SecureAnywhere Endpoint Protection	69
Malwarebytes Endpoint Security	59

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





4. Protection Details

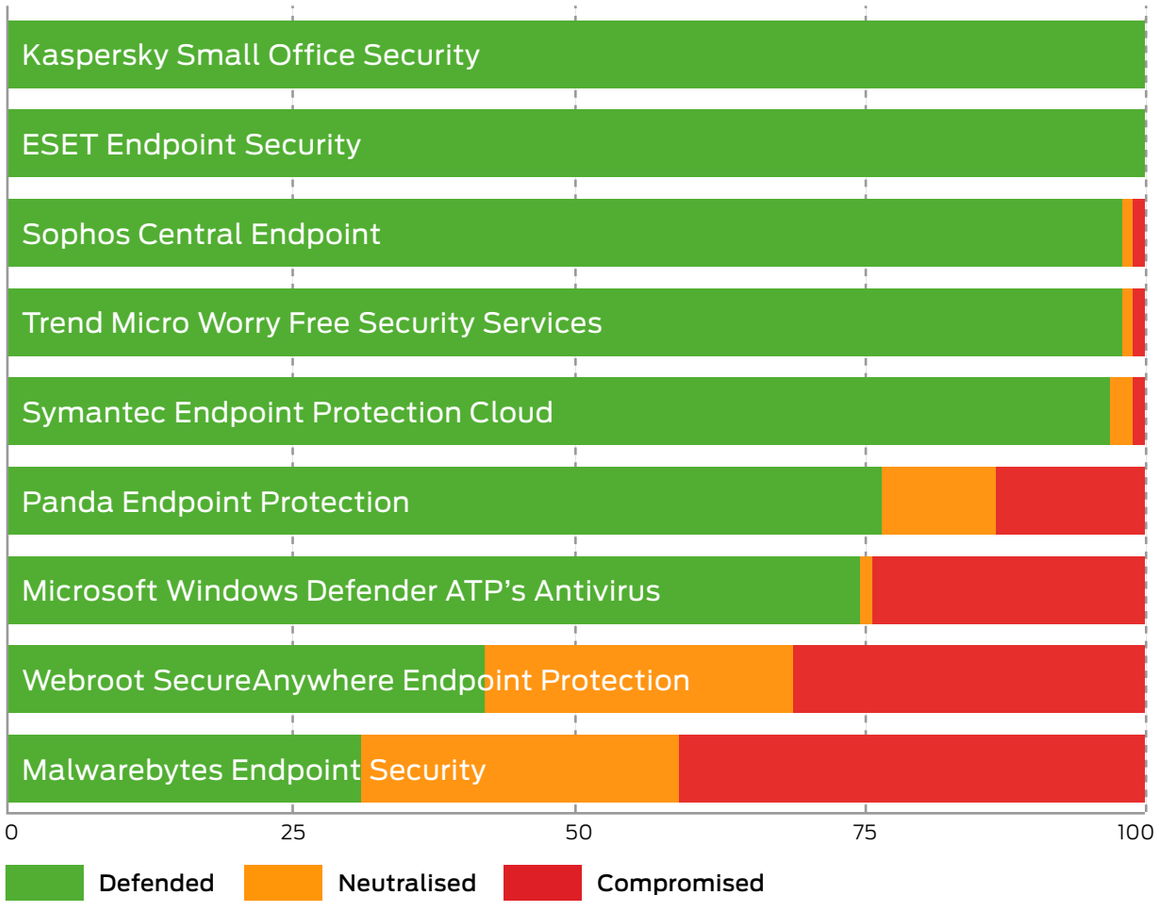
These results break down how each product handled threats into some detail. You can see how many detected a threat and the levels of protection provided.

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

Product	Detected	Blocked	Neutralised	Compromised	Protected
Kaspersky Small Office Security	100	100	0	0	100
ESET Endpoint Security	100	100	0	0	100
Sophos Central Endpoint	99	98	1	1	99
Trend Micro Worry Free Security Services	100	98	1	1	99
Symantec Endpoint Protection Cloud	100	97	2	1	99
Panda Endpoint Protection	93	77	10	13	87
Microsoft Windows Defender ATP's Antivirus	95	75	1	24	76
Webroot SecureAnywhere Endpoint Protection	97	42	27	31	69
Malwarebytes Endpoint Security	32	31	28	41	59

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



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 13.*

LEGITIMATE SOFTWARE RATINGS		
Product	Legitimate Accuracy Rating	Legitimate Accuracy (%)
ESET Endpoint Security	718	100%
Kaspersky Small Office Security	718	100%
Panda Endpoint Protection	718	100%
Sophos Central Endpoint	718	100%
Trend Micro Worry Free Security Services	706	98%
Malwarebytes Endpoint Security	703	98%
Symantec Endpoint Protection Cloud	702	98%
Webroot SecureAnywhere Endpoint Protection	702	98%
Microsoft Windows Defender ATP's Antivirus	654.5	91%

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

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.

	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 Small Office Security	100	0
Panda Endpoint Protection	100	0
Sophos Central Endpoint	100	0
Malwarebytes Endpoint Security	99	1
Symantec Endpoint Protection Cloud	99	1
Trend Micro Worry Free Security Services	99	1
Webroot SecureAnywhere Endpoint Protection	99	1
Microsoft Windows Defender ATP's Antivirus	96	4

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 CATEGORY FREQUENCY	
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 11.

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	25
High impact	38
Medium impact	17
Low impact	11
Very low impact	9
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 every vendor being tested should do poorly.

Consequently, it's not a shock to see all products handle the public threats very effectively. **Malwarebytes** was notable in its struggle at handling these. Targeted attacks were also handled well by most but caused some significant problems for the products from **Malwarebytes** and **Webroot**. **Webroot** notes that testing occurred before it released its script and anti-exploit protection.

The **Kaspersky Lab** and **ESET** products blocked all of the public and targeted attacks. They also handled the legitimate applications correctly.

Kaspersky Small Office Security fully remediated attacked systems a few more times than did **ESET Endpoint Security** and so gained a slightly higher protection rating.

Products from **Symantec**, **Sophos** and **Trend Micro** follow up close behind, handling legitimate applications with similar accuracy and fighting off the vast majority of threats. Each product only missed one threat.

Panda Endpoint Protection allowed a number of threats to infect the system, particularly the targeted attacks. It also neutralised more threats than most of the other products, which pulled its ratings down. **Microsoft** was even less successful when protecting against targeted attacks.

The **Webroot** and **Malwarebytes** products scored the lowest, both failing to achieve a rating. They were accurate with legitimate applications but both tended to neutralise, rather than block threats, and they also missed most of the targeted attacks.

The leading products from **Kaspersky Lab**, **ESET**, **Sophos**, **Symantec** and **Trend Micro** win AAA awards.

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 unsponsored.
- The test was conducted between January and March 2018.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Malicious URLs and legitimate applications and URLs were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- SE Labs conducted this email security services protection test using real email accounts running on popular commercial services.

Q What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

A Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

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 a certain level of test data with non-partner participants for free. The intention is to provide sufficient data to demonstrate that the results are accurate. For more in-depth data suitable for product improvement purposes we recommend becoming a partner.

APPENDIX C: Product Versions

The table below shows the service's name as it was being marketed at the time of the test.

PRODUCT VERSIONS		
Provider	**Product name**	**Build version**
ESET	Endpoint Security	6.4.2014.0
Kaspersky Lab	Small Office Security	17.0.0.611 (j)
Malwarebytes	Endpoint Security	1.80.2.1012
Microsoft	Windows Defender ATP's Antivirus	4.12.17007.18022 (Antimalware Client Version) 1.263.824.0 (Antivirus Version)
Panda	Endpoint Protection	7.70.0 Agent: 7.80.0
Sophos	Central Endpoint	2.0.2
Symantec	Endpoint Protection Cloud	22.12.1.15
Trend Micro	Worry Free Security Services	6.3.1194
Webroot	SecureAnywhere Endpoint Protection	9.0.19.43

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**	**Protected**
ESET Endpoint Security	75	25	**100**
Kaspersky Small Office Security	75	25	**100**
Trend Micro Worry Free Security Services	74	25	**99**
Sophos Central Endpoint	74	25	**99**
Symantec Endpoint Protection Cloud	74	25	**99**
Panda Endpoint Protection	70	17	**87**
Microsoft Windows Defender ATP's Antivirus	69	7	**76**
Webroot SecureAnywhere Endpoint Protection	68	1	**69**
Malwarebytes Endpoint Security	58	1	59