SE Labs

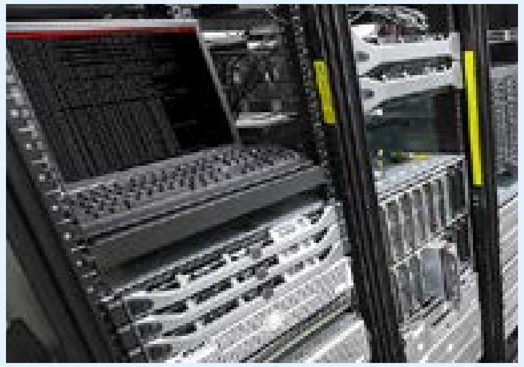
Enterprise Endpoint Protection

January - March 2016

SE Labs tested a range 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 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 4th April 2016

SIMON EDWARDS
Director

Website www.SELabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Phone 0203 875 5000
Post ONE Croydon, London, CR0 0XT

INTRODUCTION

Endpoint products are considered by almost every security software vendor to be an essential level of protection in a business network. Headlines that proclaim anti-virus to be dead are usually making a too-subtle point about signature-reliant technologies rather than writing off a whole segment of the IT security market. All the products here combine signature-based protection with other, more advanced, technologies.

Ideally an endpoint product will require no management, protect against every threat that it encounters and allow access to all non-malicious applications and websites that match the organisation's policy. That's a pretty tall order and one that is unlikely to exist, despite various claims from newly arrived companies that offer alternatives to 'anti-virus'.

This test shows the results of three months of research during which time the SE Labs team located live web-based threats that internet users in the real world were encountering at the time of testing. Crucially, we tested straight away, as soon as each threat was verified, so we could determine how well the popular anti-malware endpoints in the lab would perform against current prevalent malware threats.

There is much talk of targeted attacks in the press and strong claims by some security vendors that anti-malware technology is useless against these types of threats. We decided to test this claim and included a range of attacks in this test that are close, if not identical, to how an attacker could attempt to compromise an endpoint.

SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests, please visit our website and follow us on Twitter.

EXECUTIVE SUMMARY

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

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

Products tested

PRODUCT	PROTECTED ACCURACY	LEGITIMATE ACCURACY	TOTAL ACCURACY
Symantec Endpoint Security Enterprise Edition	99%	100%	99%
Kaspersky Endpoint Security	90%	100%	97%
Sophos Endpoint Protection	75%	100%	92%
Microsoft System Center Endpoint Protection	71%	100%	90%
Trend Micro OfficeScan, Intrusion Defense Firewall	61%	96%	85%
McAfee VirusScan, HIPS and SiteAdvisor	91%	46%	61%

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 effective at handling general threats from cyber criminals…**
All the products were capable of handling public web-based threats such as those used by criminals to attack Windows PCs and install ransomware automatically, without having to trick a user into clicking an install button.

- **…but targeted attacks posed more of a challenge**
While half of the products were also competent at blocking more targeted, exploit-based attacks, the other half were less effective. One product, from Trend Micro, failed to stop targeted attacks more often than it succeeded.

- **False positives were not an issue for most products**
With the notable exception of McAfee's product, all endpoint solutions were good at correctly classifying legitimate applications and websites. Four of the six products made no mistakes at all.

- **Which products were the most effective?**
Symantec and Kaspersky Lab 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, 4th April 2016

1. TOTAL ACCURACY RATINGS

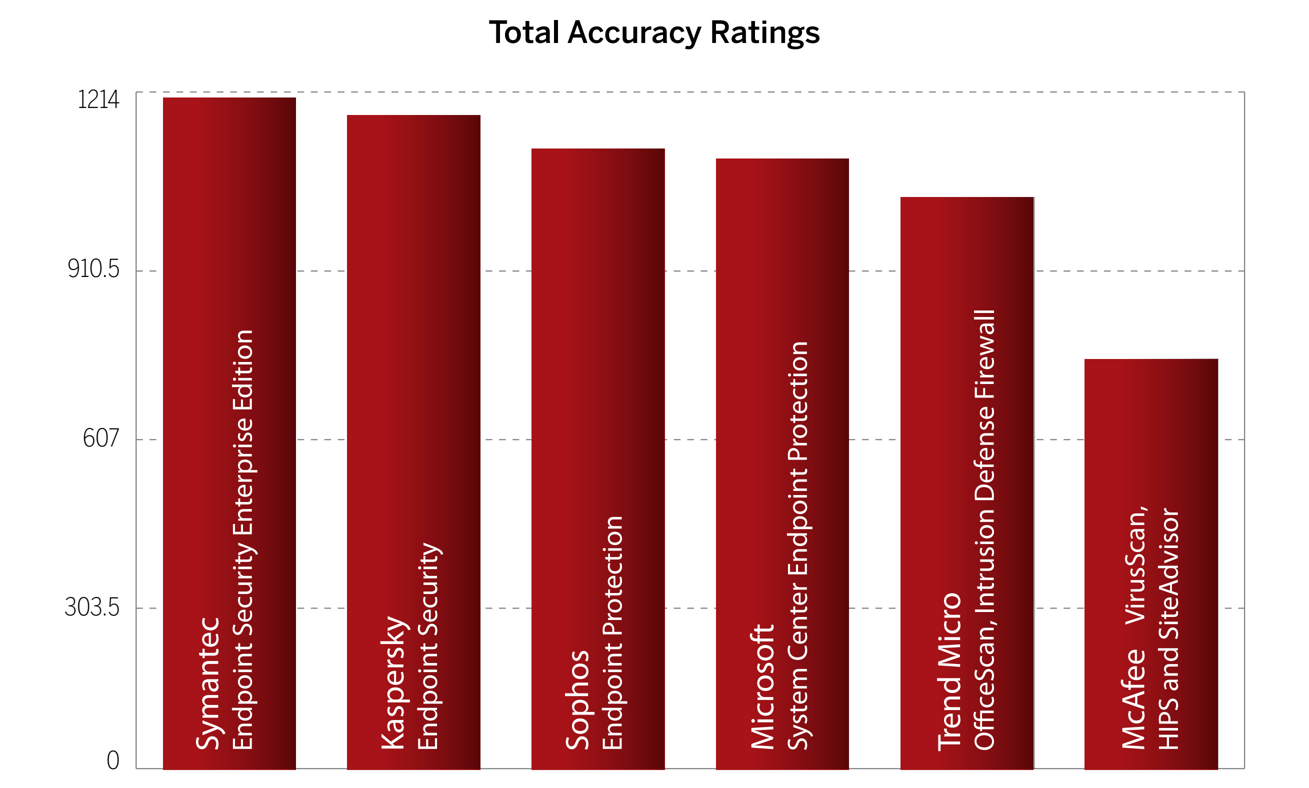
Judging the effectiveness of an endpoint security product is a subtle art, and many factors are at play when assessing how well it performs. To make things easier, we've combined all the different results from this report into one easy-to-understand graph.

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

Not all protections, or detections for that matter, are equal. A product might completely block a URL, which prevents the threat completely before it can even start its intended series of malicious events. Alternatively, the product might allow a web-based exploit to execute but prevent it from downloading any further code to the target. In another case malware might run on the target for a short while before its behaviour is detected and its code is deleted or moved to a safe 'quarantine' area for future analysis. We take these outcomes into account when attributing points that form final ratings.

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

Categorising how a product handles legitimate objects is complex, and you can find out how we do it in 5. Legitimate Software Ratings on page 12.



Total Accuracy Ratings combine protection and false positives.

Awards

The following products win SE Labs awards:

- ● Symantec Endpoint Security Enterprise Edition
- ● Kaspersky Endpoint Security

- ● Sophos Endpoint Protection
- ● Microsoft System Center Endpoint Protection

- ● Trend Micro OfficeScan, Intrusion Defense Firewall

TOTAL ACCURACY RATINGS

Product	Total Accuracy Rating	Total Accuracy (%)	Award
Symantec Endpoint Security Enterprise Edition	1206	99%	AAA
Kaspersky Endpoint Security	1174	97%	AAA
Sophos Endpoint Protection	1114	92%	AA
Microsoft System Center Endpoint Protection	1096	90%	AA
Trend Micro OfficeScan, Intrusion Defense Firewall	1027	85%	A
McAfee VirusScan, HIPS and SiteAdvisor	736.5	61%	-

2. PROTECTION RATINGS

The results below indicate how effectively the products dealt with threats. Points are earned for detecting the threat and for either blocking or neutralising it.

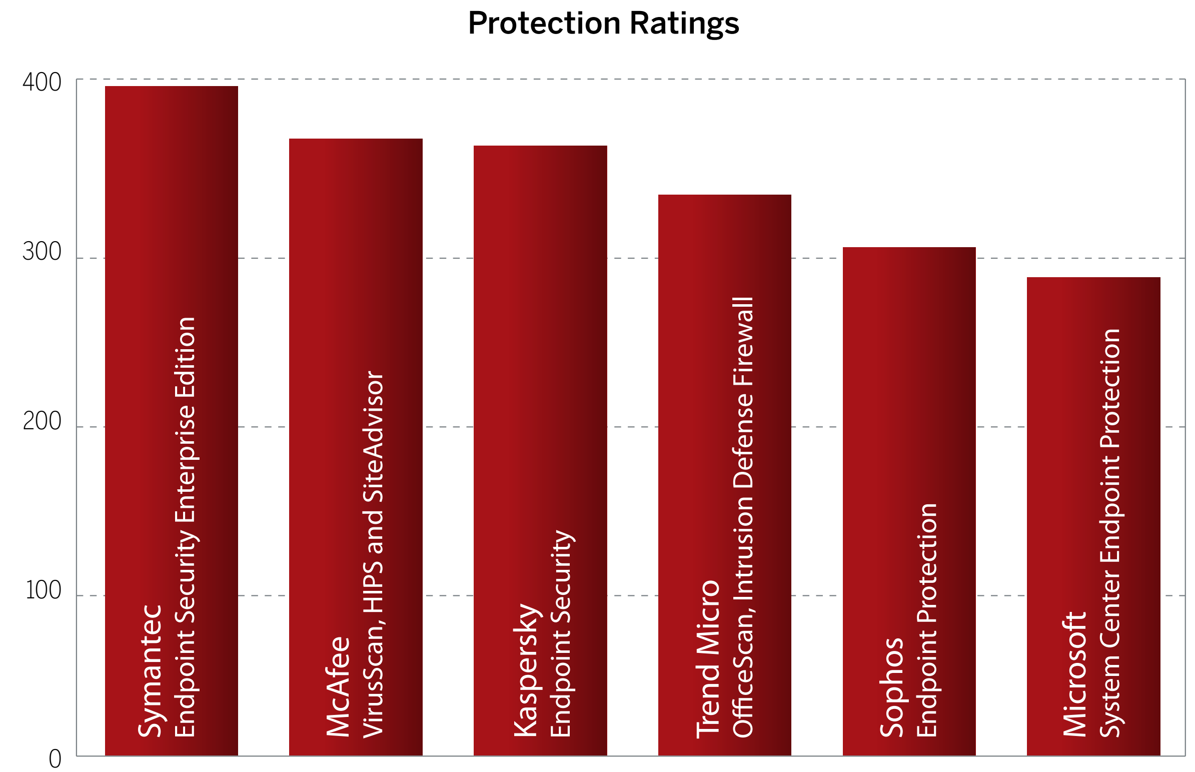
- **Detected (+1)**
If the product detected the threat with any degree of useful information, we award it one point.

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

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

- **Complete remediation (+1)**
If, in addition to neutralising a threat, the product removes all significant traces of the attack, it gains an additional one point.

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



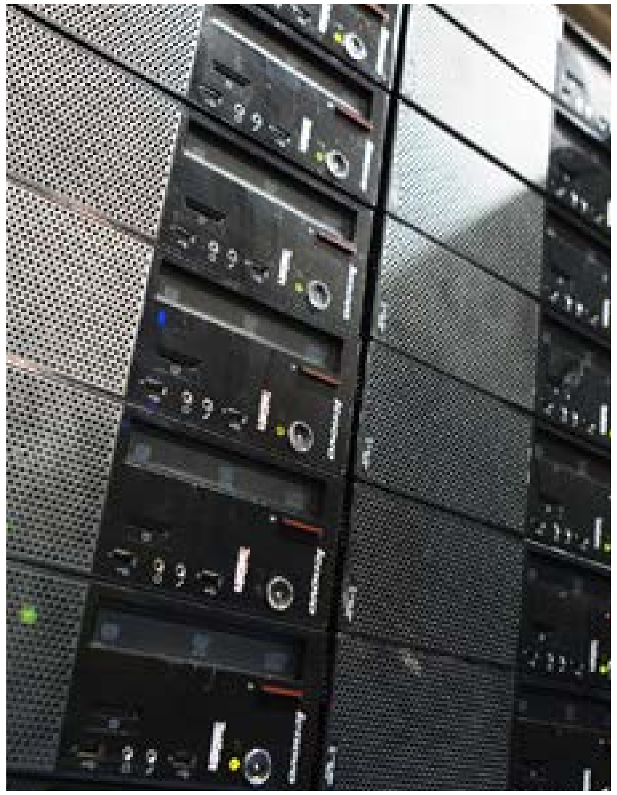
Protection ratings are weighted to show that how products handle threats can be subtler than just "win" or "lose".

Rating calculations
We calculate the protection ratings using the following formula:

Protection rating =
(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 (%)
Symantec Endpoint Security Enterprise Edition	395	99%
McAfee VirusScan, HIPS and SiteAdvisor	364	91%
Kaspersky Endpoint Security	360	90%
Trend Micro OfficeScan, Intrusion Defense Firewall	331	83%
Sophos Endpoint Protection	300	75%
Microsoft System Center Endpoint Protection	282	71%

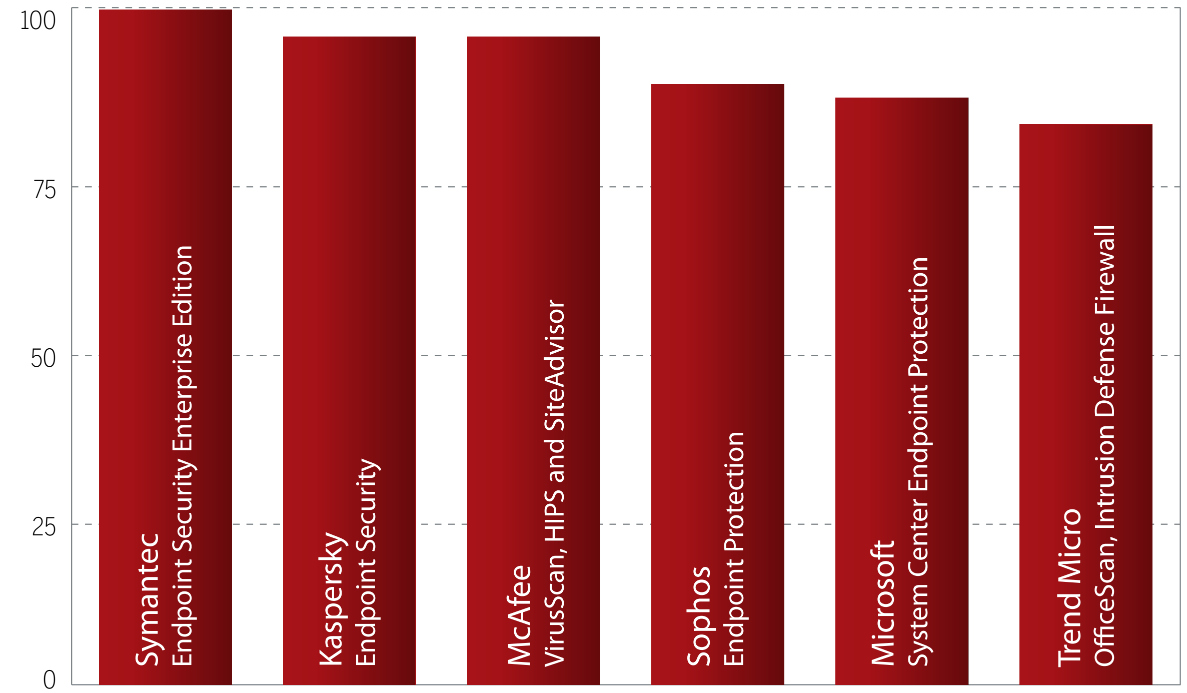
Average: 85%

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.

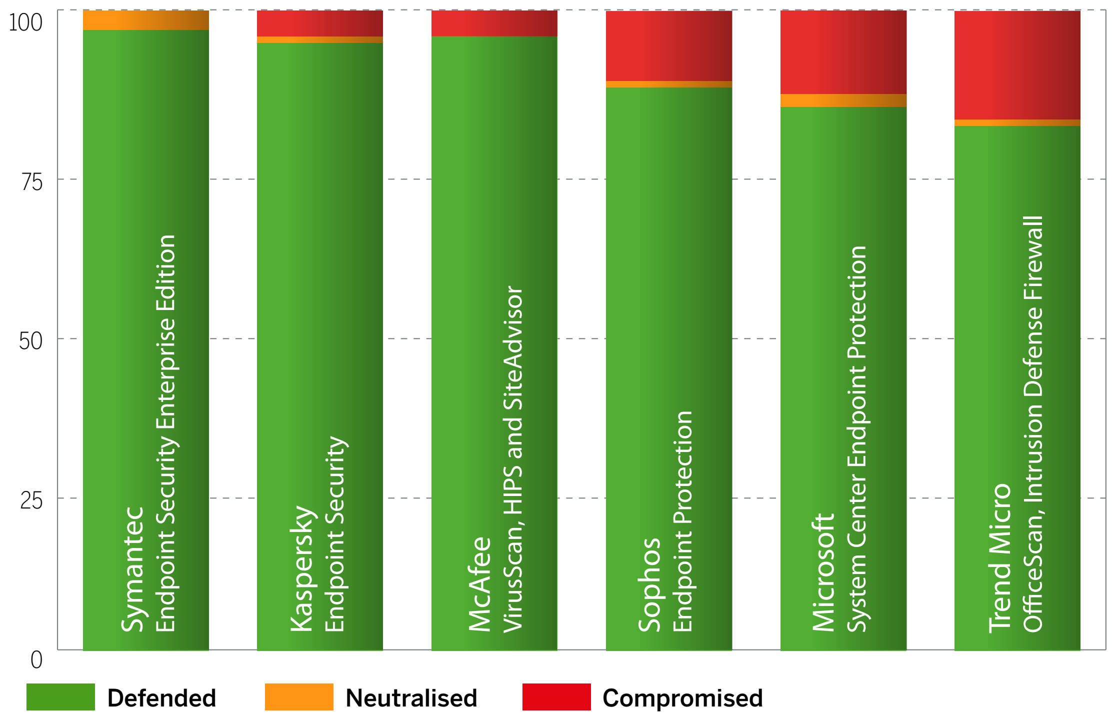
PROTECTION SCORES	
Product	**Protection Score**
Symantec Endpoint Security Enterprise Edition	100
Kaspersky Endpoint Security	96
McAfee VirusScan, HIPS and SiteAdvisor	96
Sophos Endpoint Protection	89
Microsoft System Center Endpoint Protection	87
Trend Micro OfficeScan, Intrusion Defense Firewall	83

4. PROTECTION DETAILS

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

Products sometimes detect more threats than they protect against. This can happen when they recognise an element of the threat but are not equipped to stop it. Products can also provide protection even if they don't detect certain threats. Some threats abort on detecting specific endpoint protection software.

Protection Details



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

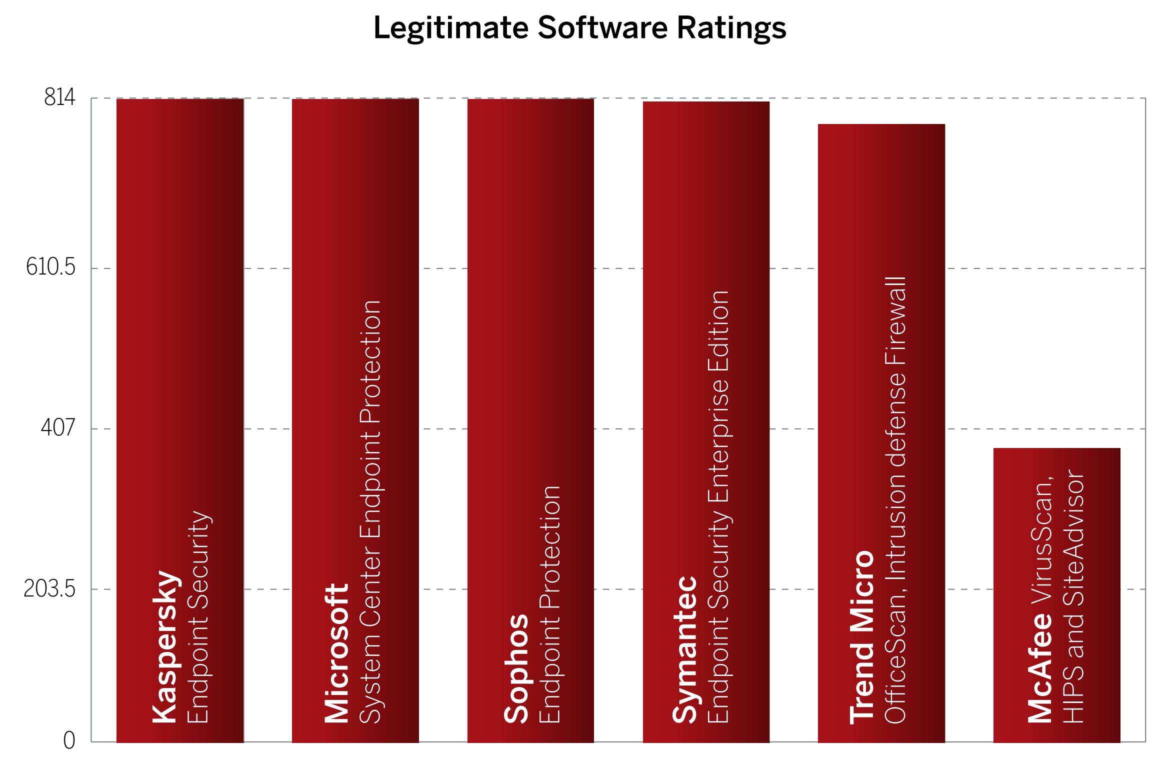
PROTECTION DETAILS					
Product	**Detected**	**Blocked**	**Neutralised**	**Compromised**	**Protected**
Symantec Endpoint Security Enterprise Edition	100	97	3	0	100
Kaspersky Endpoint Security	93	95	1	4	96
McAfee VirusScan, HIPS and SiteAdvisor	96	96	0	4	96
Sophos Endpoint Protection	90	88	1	11	89
Microsoft System Center Endpoint Protection	89	85	2	13	87
Trend Micro OfficeScan, Intrusion Defense Firewall	82	82	1	17	83

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 (%)**
Kaspersky Endpoint Security	814	100%
Microsoft System Center Endpoint Protection	814	100%
Sophos Endpoint Protection	814	100%
Symantec Endpoint Security Enterprise Edition	811	100%
Trend Micro OfficeScan, Intrusion Defense Firewall	782	96%
McAfee VirusScan, HIPS and SiteAdvisor	372.5	46%

5.1 Interaction ratings

It's crucial that anti-malware endpoint products not only stop, or at least detect, threats but that they allow legitimate applications to install and run without misclassifying them as malware. Such an error is known as a 'false positive' (FP).

In reality, genuine false positives are quite rare in testing. In our experience it is unusual for a legitimate application to be classified as "malware". More often it will be classified as "unknown", "suspicious" or "unwanted" (or terms that mean much the same thing).

We use a subtle system of rating an endpoint's approach to legitimate objects which takes into account how it classifies the application and how it presents that information to the user. Sometimes the endpoint software will pass the buck and demand that the user decide if the application is safe or not. In such cases the product may make a recommendation to allow or block. In other cases, the product will make no recommendation, which is possibly even less helpful.

If a product allows an application to install and run with no user interaction, or with simply a brief notification that the application is likely to be safe, it has achieved an optimum result. Anything else is a Non-Optimal Classification/Action (NOCA). We think that measuring NOCAs is more useful than counting the rarer FPs.

Interaction Ratings

	None (allowed)	Click to allow (default allow)	Click to allow/block (no recommendation)	Click to block (default block)	None (blocked)	
Object is safe	2	1.5	1			A
Object is unknown	2	1	0.5	0	-0.5	B
Object is not classified	2	0.5	0	-0.5	-1	C
Object is suspicious	0.5	0	-0.5	-1	-1.5	D
Object is unwanted	0	-0.5	-1	-1.5	-2	E
Object is malicious				-2	-2	F
	1	2	3	4	5	

Products that do not bother users and classify most applications correctly earn more points than those that ask questions and condemn legitimate applications.

INTERACTION RATINGS			
Product	**Click to block (default block)**	**None (allowed)**	**None (blocked)**
Kaspersky Endpoint Security		100	
Microsoft System Center Endpoint Protection		100	
Sophos Endpoint Protection		100	
Symantec Endpoint Security Enterprise Edition	1	99	
Trend Micro OfficeScan, Intrusion Defense Firewall		98	2
McAfee VirusScan, HIPS and SiteAdvisor	1	62	37

5.2 Prevalence ratings

There is a significant difference between an endpoint product blocking a popular application like 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 following table.

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 date 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

Prevelance Rating	Frequency
Very high impact	51
High impact	27
Medium impact	10
Low impact	7
Very low impact	5
Grand total	**100**

6. CONCLUSIONS

Attacks in this test included infected websites available to the general public, including sites that automatically attack visitors and attempt to infect them without any social engineering or other interaction. Some sites relied on users being fooled into installing the malware. We also included targeted attacks, which were exploit-based attempts to gain remote control of the target systems.

Symantec Endpoint Security Enterprise Edition was able to fend off the exploit-based targeted attacks fully, while also blocking most of the public web attacks, some of which were powered by criminals using exploit kits. It neutralised three attacks and handled legitimate applications and websites without error.

Kaspersky Endpoint Security pushed away the public web-based threats entirely but was compromised by four of our targeted attacks. It was particularly effective at stopping threats by blocking within the web browser, thus preventing the threat from starting its attack. This software was also entirely effective when handling legitimate objects.

McAfee VirusScan, HIPS and SiteAdvisor was just as effective as Kaspersky Lab's product when protecting the endpoint from the general web threats but was even better when dealing with targeted attacks. It didn't fare nearly so well when encountering legitimate objects and its legitimate accuracy rating was not only the worst but pulled the product's total accuracy rating down into last place, failing to secure it an award.

Sophos Endpoint Protection was similar in effectiveness as the products above when exposed to web threats, but the targeted attacks were a significant challenge and it was compromised by 10 of the 25 deployed in the test. It was, however, perfect when handling legitimate applications and websites.

Microsoft System Center Endpoint Protection had similar problems with the targeted attacks, failing to prevent 10 compromises. However, it was strong when handling public web threats and its accurate assessment of the legitimate applications and websites gave it a good total accuracy rating.

Trend Micro OfficeScan, Intrusion Defense Firewall was the worst when tackling the targeted attacks. We were able to compromise the target with 15 exploit-based attacks. However, it did well when faced with public web-based threats, missing only a couple. It wasn't perfect when legitimate applications were installed, though, blocking two without giving the user a chance to permit the installation.

The products from Symantec and Kaspersky Lab both win AAA awards for their strong overall performance. Those from Sophos and Microsoft achieved solid AA awards, while Trend Micro's product is awarded an A. McAfee's suite of solutions failed to reach an award by a significant margin, solely down to its harsh blocking of legitimate applications and websites.

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 21st January 2016 and 18th March 2016.
- All products had full internet access and were confirmed to have access to any required or recommended back-end systems. This was confirmed, where possible, using the Anti-Malware Testing Standards Organization (AMTSO) **Cloud Lookup Features Setting Check.**
- Malicious URLs and legitimate applications and URLs were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs. They were created and managed by Metasploit Framework Edition using default settings. The choice of exploits was advised by public information about ongoing attacks. One notable source was the **2015 Data Breach Investigations Report** from Verizon.
- Malicious and legitimate data was provided to partner organisations once the full test was complete.
- SE Labs conducted this endpoint security testing on physical PCs, not virtual machines.

Q **I am a security vendor. How can I include my product in your test?**

A Please contact us at info@SELabs.uk. We will be happy to arrange a phone call to discuss our methodology and the suitability of your product for inclusion.

Q **I am a security vendor. Does it cost money to have my product tested?**

A We do not charge directly for testing products in public tests. We do charge for private tests.

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

A Partner organisations support our tests by paying for access to test data after each test has completed but before publication. Partners can dispute results and use our award logos for marketing purposes. We do not share data on one partner with other partners. We do not currently partner with organisations that do not engage in our testing.

Q **So you don't share threat data with test participants before the test starts?**

A No, this would bias the test and make the results unfair and unrealistic.

Q **I am a security vendor and you tested my product without permission. May I access the threat data to verify that your results are accurate?**

A We are willing to share small subsets of data with non-partner participants at our discretion. A small administration fee is applicable.

APPENDIX C: PRODUCT VERSIONS

A product's update mechanism may upgrade the software to a new version automatically so the version used at the start of the test may be different to that used at the end.

PRODUCT VERSIONS

Vendor	Product	Build
Kaspersky	Endpoint Security	10.2.4.674(mr2)
McAfee	VirusScan, HIPS and SiteAdvisor Agent	MHIP Build number: 8.0.0.2919 Security Content Version: 8.0.0.6894; MA Version Number: 4.8.0.641; MSA Verison Number: 3.5.0.1228; MVE Version number: 8.8.0.1247 Scan engine version: 5800.7501 DAT version 8111.0000
Microsoft	System Center Endpoint Protection	4.7.2114.0
Sophos	Endpoint Protection	10.3
Symantec	Endpoint Security Enterprise Edition	12.1.6
Trend Micro	OfficeScan	Agent Version: 11.0.1028

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	Public web attack	Protected (total)
Symantec Endpoint Security Enterprise Edition	25	75	100
Kaspersky Endpoint Security	21	75	96
McAfee VirusScan, HIPS and SiteAdvisor	22	74	96
Sophos Endpoint Protection	15	74	89
Microsoft System Center Endpoint Protection	15	72	87
Trend Micro OfficeScan, Intrusion Defense Firewall	10	73	83