SE Labs

INTELLIGENCE-LED TESTING

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
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Chief Technical Officer Stefan Dumitrascu

TESTING TEAM
Nikki Albesa
Zaynab Bawa
Thomas Bean
Solandra Brewster
Liam Fisher
Gia Gorbold
Joseph Pike
Dave Togneri
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

Website selabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Blog blog.selabs.uk
Phone +44 (0)203 875 5000
Post SE Labs Ltd,
55A High Street, Wimbledon, SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2013 certified and BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

AMTSO Standard Reference:
selabs.uk/amtso20q3

© 2020 SE Labs Ltd

CONTENTS

Document version 1.0 Written 15th October 2020; 1.1 Updated ESET results
1.2 Updated Sophos Results 26th October 2020

INTRODUCTION

Hands up, who's been hacked?

Get ahead in the game that never ends

Have you ever been hacked? You, personally, or your business? If your answer is, "no" it would be interesting to know how you can be so sure.

I once spoke to a marketing manager at a global anti-malware company who claimed that his PC had never been infected by malware, despite him not using anti-virus. How would he know? Not all malware announces its presence as clearly as, say ransomware. "I just would," he claimed.

Why does it matter?

Years later I asked a management team at a very large media company if they had ever been breached. The head of IT claimed not. Definitely not. His lower-ranking colleague more realistically said, "probably" while the CFO responded with, "does it matter?"

Companies and individuals sometimes think that they don't have anything valuable of interest to attackers. But if your business holds any personal details of staff or customers then being breached can bring heavy fines. And if your personal PC is hacked, you can expect at best inconvenience as your computer misbehaves and shows you annoying adverts, and at worst what amounts to a bank robbery that will have your bank looking at you with considerable suspicion.

I have personally been hacked (at least) twice. I'm certain of this because in the first case I could see abnormal amounts of network traffic leaving my system and, because I am familiar with how computers work under the hood, I was then able to spot the rootkit that was hiding on my Linux server. Yes, there is malware for Linux, despite what you might have heard.

The second time was less direct, and I only found out that my British Airways account had been breached when I tried to use it. My personal email is found a number of times on the have i been pwned website, too. So clearly other companies with my personal data have been hacked too.

Game of Threats

I've nearly fallen foul of SMS phishing at least once this year, and only failed to enter my credit card details because I didn't have my wallet with me at the time. I'm looking out for this stuff and I still get tricked if you catch me on an off day. The general public will be falling for these tricks all the time. The proof is that attackers are running the same scams over and over again.

Keeping your wits about you is essential, but you can't do it all on your own. That's why a good (anti-malware) endpoint protection solution is an essential basis for your online protection. I hope this report helps you or your business get ahead in the game that never ends.

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.

This test report was funded by post-test consultation services provided by SE Labs to security vendors. Vendors of all products included in this report were able to request early access to results and the ability to dispute details for free. SE Labs has submitted the testing process behind this report for compliance with the AMTSO Testing Protocol Standard v1.3. To verify its compliance please check the AMTSO reference link at the bottom of page three of this report or here.

Executive Summary

Product Names

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

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

EXECUTIVE SUMMARY			
Products Tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Kaspersky Endpoint Security	100%	100%	100%
ESET Endpoint Security	97%	100%	99%
Sophos Intercept X	97%	100%	99%
Bitdefender Gravity Zone Endpoint Security	96%	100%	99%
Symantec Endpoint Security Enterprise Edition	99%	98%	98%
McAfee EndPoint Security	93%	100%	97%
Microsoft Defender Antivirus (enterprise)	93%	100%	97%
Crowdstrike Falcon	92%	100%	97%
FireEye Endpoint Security	81%	100%	93%

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.

- **.. and targeted attacks were prevented in nearly all cases by most products.**

Most products were competent at blocking more targeted, exploit-based attacks. Seven out of nine stopped every targeted attack. **FireEye's** product missed the most.

- **False positives were not an issue for the products**

All of the endpoint solutions were good at correctly classifying legitimate applications and websites. They allowed all of the legitimate websites and applications with the exception of products from **Symantec** and **Microsoft**, which each displayed minor numbers of mistakes in this part of the test.

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

Kaspersky's product was the only one to achieve a 100% total accuracy rating. Those from **ESET**, **Sophos**, **Bitdefender** and **Symantec** achieved extremely good results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites. **McAfee**, **Crowdstrike** and **Microsoft** products performed well enough to achieve AAA awards.

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.

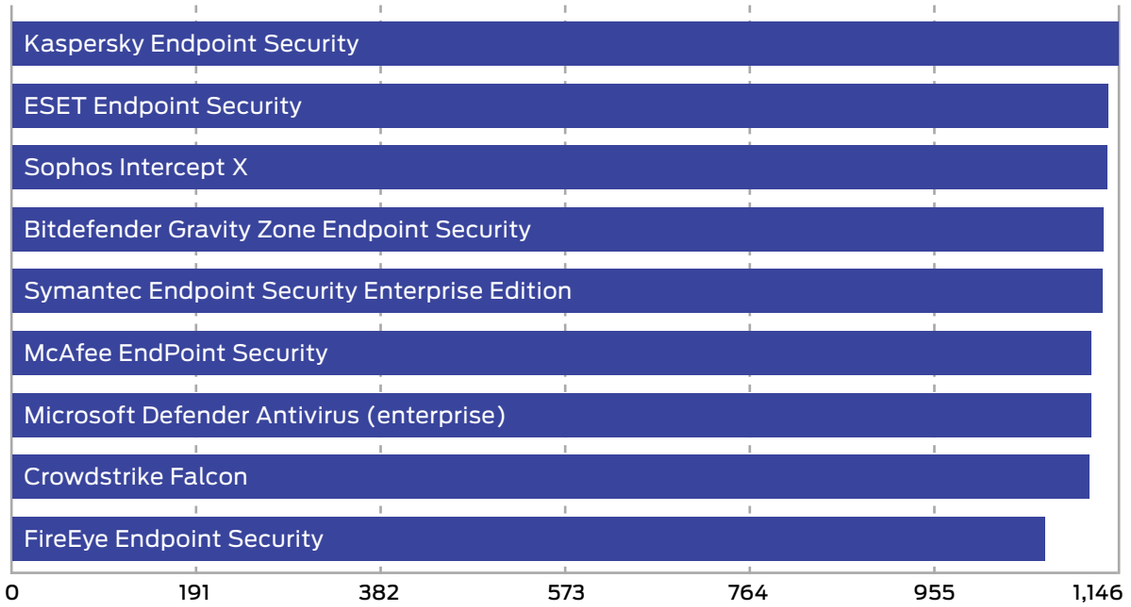
The graph below takes into account not only each product's ability to detect and protect against threats, but also its handling of non-malicious objects such as web addresses (URLs) and applications.

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 **6. Legitimate Software Ratings** on page 14.

TOTAL ACCURACY RATINGS			
Product	Total Accuracy Rating	Total Accuracy (%)	Award
Kaspersky Endpoint Security	1,146	100%	AAA
ESET Endpoint Security	1,135	99%	AAA
Sophos Intercept X	1,134	99%	AAA
Bitdefender Gravity Zone Endpoint Security	1,130	99%	AAA
Symantec Endpoint Security Enterprise Edition	1,128.5	98%	AAA
McAfee EndPoint Security	1,117	97%	AAA
Microsoft Defender Antivirus (enterprise)	1,117	97%	AAA
Crowdstrike Falcon	1,115	97%	AAA
FireEye Endpoint Security	1,069	93%	AA

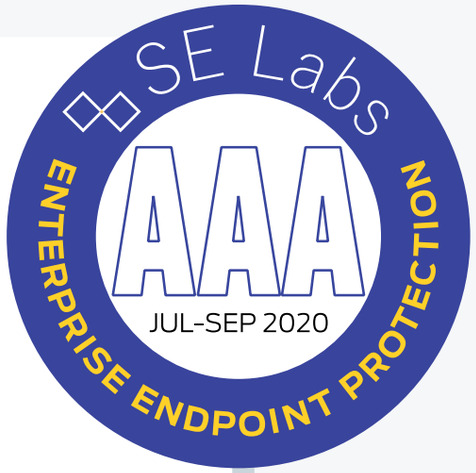


Total Accuracy Ratings combine protection and false positives.

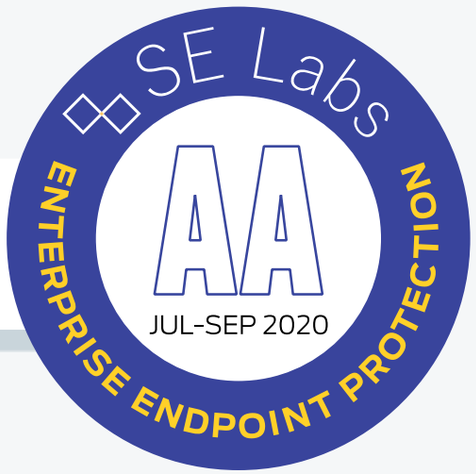
Enterprise Endpoint Protection Awards

The following products win SE Labs awards:

- **Kaspersky** Endpoint Security
- **ESET** Endpoint Security
- **Bitdefender** Gravity Zone Endpoint Security
- **Symantec** Endpoint Security Enterprise Edition
- **Sophos** Intercept X
- **McAfee** Endpoint Security
- **Crowdstrike** Falcon
- **Microsoft** Defender Antivirus (enterprise)



- **FireEye** Endpoint Security



2. Threat Responses

Full Attack Chain: Testing every layer of detection and protection

Attackers start from a certain point and don't stop until they have either achieved their goal or have reached the end of their resources (which could be a deadline or the limit of their abilities). This means, in a test, the tester needs to begin the attack from a realistic first position, such as sending a phishing email or setting up an infected website, and moving through many of the likely steps leading to actually stealing data or causing some other form of damage to the network.

If the test starts too far into the attack chain, such as executing malware on an endpoint, then many products will be denied opportunities to use the full extent of their protection and detection abilities. If the test concludes before any 'useful' damage or theft has been achieved, then similarly the product may be denied a chance to demonstrate its abilities in behavioural detection and so on.

Attack stages

The illustration below shows some typical stages of an attack. In a test each of these should be attempted to determine the security solution's effectiveness. This test's results record detection and protection for each of these stages.

We measure how a product responds to the first stages of the attack with a detection and/ or protection rating. Sometimes products allow threats to run but detect them. Other times they might allow the threat to run briefly before neutralising it. Ideally they detect and block the threat before it has a chance to run. Products may delete threats or automatically contain them in a 'quarantine' or other safe holding mechanism for later analysis.

Should the initial attack phase succeed we then measure post-exploitation stages, which are represented by steps two through to seven below. We broadly categorise these stages as: Access (step 2); Action (step 3); Escalation (step 4); and Post-escalation (step 5).

In figure 1. you can see a typical attack running from start to end, through various 'hacking' activities. This can be classified as a fully successful breach.

In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

Annual Report 2020

Our 2nd Annual Report is now available

- Annual Awards Winners
- Testing like Hackers
- The Importance of Testing with Full Attack Chains
- Testing Standards

DOWNLOAD THE REPORT NOW!

(free – no registration)

selabs.uk/ar2020

It is possible that attackers will not cause noticeable damage during an attack. It may be that their goal is persistent presence on the systems to monitor for activities, slowly steal information and other more subtle missions.

In figure 3. the attacker has managed to progress as far as stage five. This means that the system has been seriously compromised. The attacker has a high level of access and has stolen passwords. However, attempts to exfiltrate data from the target were blocked, as were attempts to damage the system.

Attack Chain: How Hackers Progress

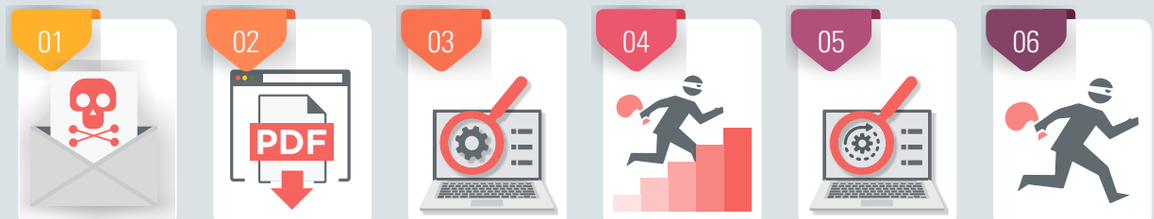


Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.

Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

Figure 3. A more successful attack manages to steal passwords but wholesale data theft and destruction was blocked.

HOME ANTI-MALWARE PROTECTION

Which services from well-known vendors are the *most* effective?

DOWNLOAD NOW!

selabs.uk/home

3. 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.

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.

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

Persistent Neutralisation (-2)
This result occurs when a product continually blocks a persistent threat from achieving its aim, while not removing it from the system.

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 **5. Protection Details** on page 13 to roll your own set of personalised ratings.

Targeted Attack Scoring

The following scores apply only to targeted attacks and are cumulative, ranging from -1 to -5.

Access (-1)
If any command that yields information about the target system is successful this score is applied. Examples of successful commands include listing current running processes, exploring the file system and so on. If the first command is attempted and the session is terminated by the product without the command being successful the score of Neutralised (see above) will be applied.

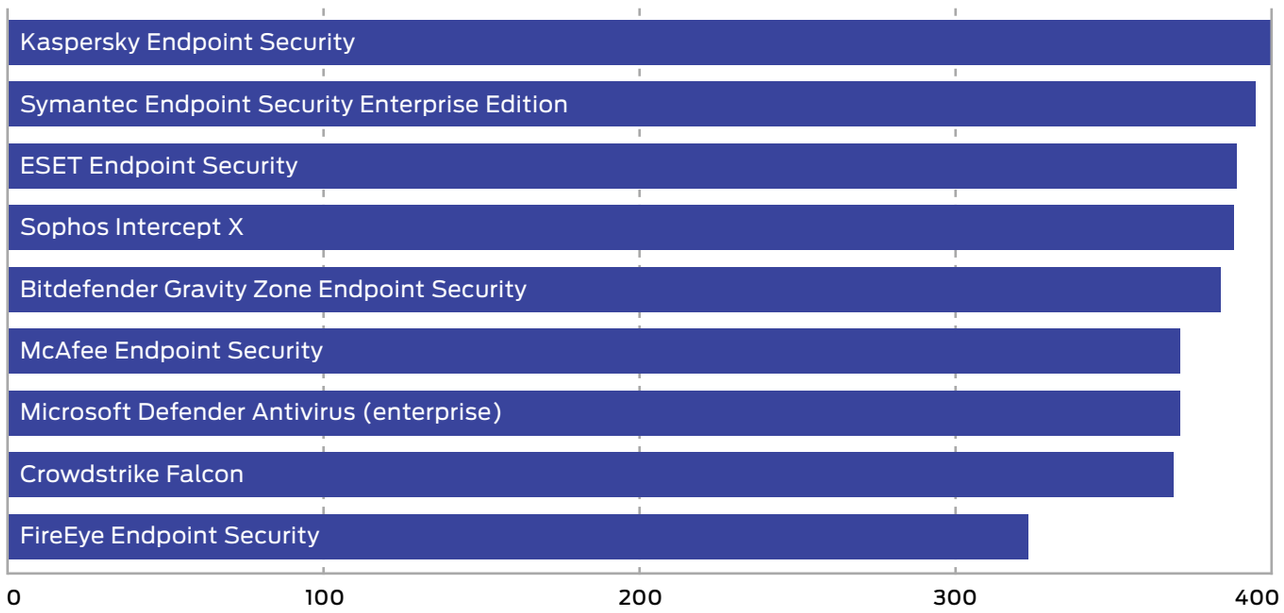
Action (-1)
If the attacker is able to exfiltrate a document from the target's Desktop of the currently logged in user then an 'action' has been successfully taken.

Escalation (-2)
The attacker attempts to escalate privileges to NT Authority/System. If successful, an additional two points are deducted.

Post-Escalation Action (-1)
After escalation the attacker attempts actions that rely on escalated privileges. These include attempting to steal credentials, modifying the file system and recording keystrokes. If any of these actions are successful then a further penalty of one point deduction is applied.

PROTECTION RATINGS		
Product	Protection Rating	Protection Rating (%)
Kaspersky Endpoint Security	400	100%
Symantec Endpoint Security Enterprise Edition	395	99%
ESET Endpoint Security	389	97%
Sophos Intercept X	388	97%
Bitdefender Gravity Zone Endpoint Security	384	96%
McAfee Endpoint Security	371	93%
Microsoft Defender Antivirus (enterprise)	371	93%
Crowdstrike Falcon	369	92%
FireEye Endpoint Security	323	81%

Average 94%



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

EMAIL SECURITY SERVICES PROTECTION

Which services from well-known vendors are the *most* effective?

DOWNLOAD NOW!

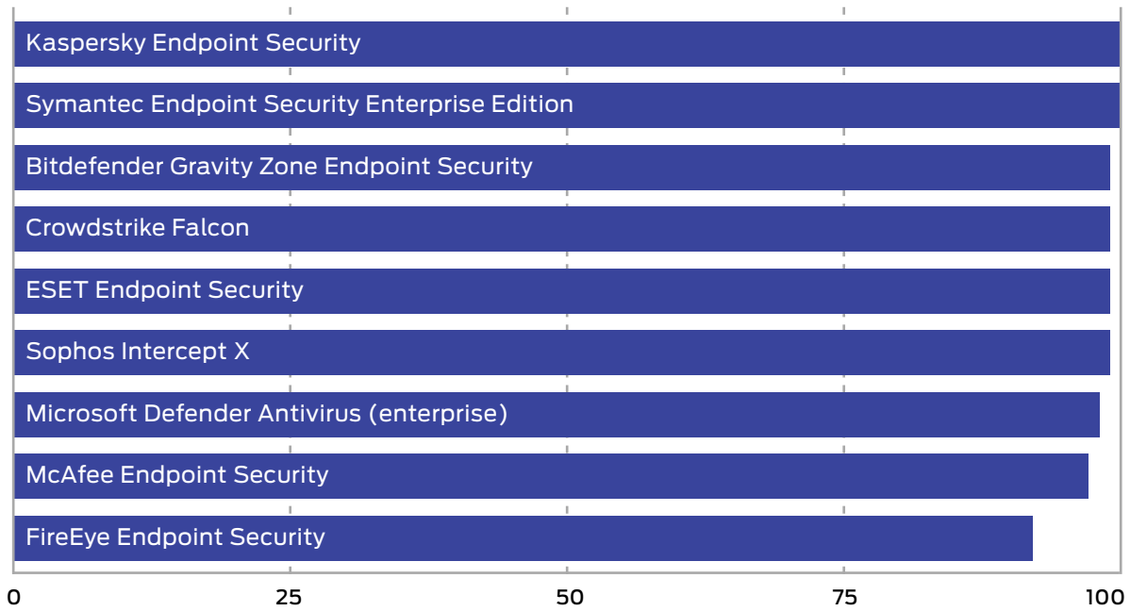
selabs.uk/essp2020

4. 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**
Kaspersky Endpoint Security	100
Symantec Endpoint Security Enterprise Edition	100
Bitdefender Gravity Zone Endpoint Security	99
Crowdstrike Falcon	99
ESET Endpoint Security	99
Sophos Intercept X	99
Microsoft Defender Antivirus (enterprise)	98
McAfee EndPoint Security	97
FireEye Endpoint Security	92



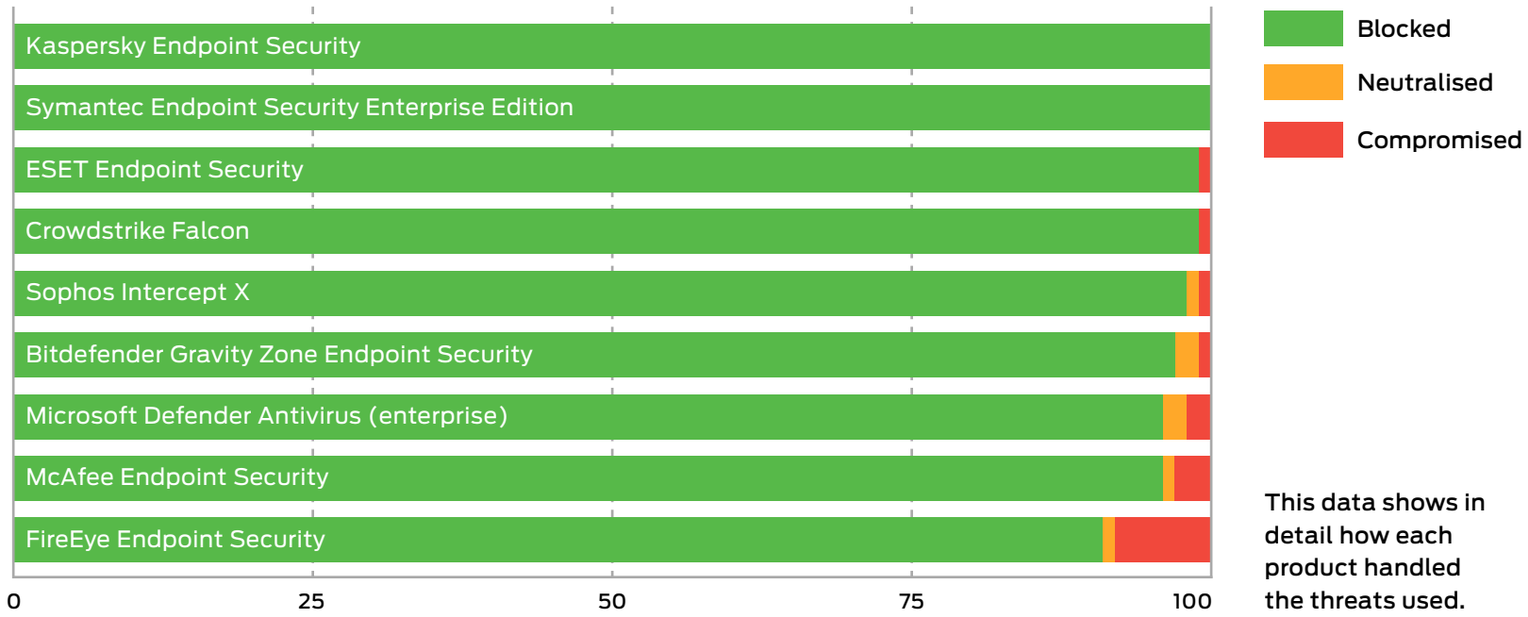
Protection Scores are a simple count of how many times a product protected the system.

5. 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 Endpoint Security	100	100	0	0	100
Symantec Endpoint Security Enterprise Edition	100	100	0	0	100
ESET Endpoint Security	100	99	0	1	99
Crowdstrike Falcon	99	99	0	1	99
Sophos Intercept X	99	98	1	1	99
Bitdefender Gravity Zone Endpoint Security	100	97	2	1	99
Microsoft Defender Antivirus (enterprise)	100	96	2	2	98
McAfee Endpoint Security	98	96	1	3	97
FireEye Endpoint Security	96	91	1	8	92



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

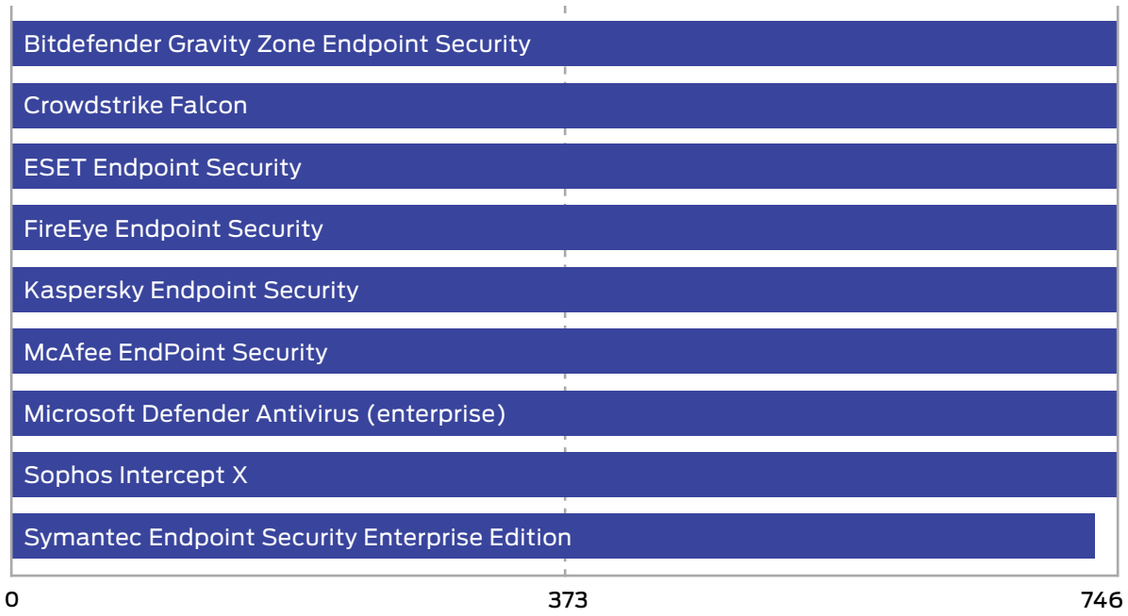
6. Legitimate Software Ratings

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 **6.3 Accuracy Ratings** on page 16.

LEGITIMATE SOFTWARE RATINGS		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy (%)**
Bitdefender Gravity Zone Endpoint Security	746	100%
Crowdstrike Falcon	746	100%
ESET Endpoint Security	746	100%
FireEye Endpoint Security	746	100%
Kaspersky Endpoint Security	746	100%
McAfee EndPoint Security	746	100%
Microsoft Defender Antivirus (enterprise)	746	100%
Sophos Intercept X	746	100%
Symantec Endpoint Security Enterprise Edition	733.5	98%



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

6.1 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	

INTERACTION RATINGS

Product	None (allowed)	Click to allow/block (no recommendation)
Bitdefender Gravity Zone Endpoint Security	100	0
Crowdstrike Falcon	100	0
ESET Endpoint Security	100	0
FireEye Endpoint Security	100	0
Kaspersky Endpoint Security	100	0
McAfee EndPoint Security	100	0
Microsoft Defender Antivirus (enterprise)	100	0
Sophos Intercept X	100	0
Symantec Endpoint Security Enterprise Edition	99	1

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

6.2 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.

6.3 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 **6. Legitimate Software Ratings** on page 14.

6.4 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	32
High Impact	33
Medium Impact	15
Low Impact	16
Very Low Impact	4

7. 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 do not write unique malware so there is no technical reason why any vendor being tested should do poorly.

Consequently, it is not a shock to see most products handle the public threats very effectively. Even the weaker products protected the target systems in the majority of cases. Targeted attacks were also handled well by most.

Products from **Kaspersky** and **Symantec (Broadcom)** protected against all of the public and targeted attacks. **Bitdefender's** missed one targeted attack, while those from **Crowdstrike**, **ESET** and **Sophos** stopped all targeted attacks, but each missed one public threat. **Microsoft** and **McAfee** products stopped all targeted attacks but missed a handful of public threats, while **FireEye** missed five public malware attacks and three targeted attacks.

Most of the products handled the legitimate applications correctly, but there were a few mistakes. **Symantec's** product was unclear on one application while **Microsoft**'s product was penalised for blocking one each.

The leading products from **Kaspersky**, **ESET**, **Sophos**, **Bitdefender**, **Symantec**, **McAfee**, **Crowdstrike** and **Microsoft** all 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 6th July to 24th August 2020.
- 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 endpoint security testing on physical PCs, not virtual machines.
- The web browser used in this test was Google Chrome. When testing Microsoft products Chrome was equipped with the Windows Defender Browser Protection browser extension (**https://browserprotection.microsoft.com**).

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			
Vendor	**Product**	**Build Version (start)**	**Build Version (end)**
Bitdefender	Gravity Zone Endpoint Security	6.6.18.261	7.85737
Crowdstrike	Falcon	5.34.11603.0	5.36.11809.0
ESET	Endpoint Security	7.2.2055.0	7.2.2055.0
FireEye	Endpoint Security	32.30.0	32.30.0
Kaspersky	Endpoint Security	11.3.0.773 AES256	11.4.0.233 AES256
McAfee	Endpoint Security	Exchange Layer: 6.0.0.204 Agent: 5.6.4.121 Endpoint Security: 10.7	Exhange Layer: 6.0.0.218 Agent: 5.6.5.165 Endpoint Security: 10.7
Microsoft	Defender Antivirus (enterprise)	Antimalware Client Versions: 4.18.2005.5 Engine Versions 1.1.17200.2 Antivirus Version: 1.319.81.0 Anti-spyware Version: 1.319.81.0	Antimalware Client Version: 4.18.2008.9 Engine Version: 1.1.17400.5 Antivirus Version: 1.323.369.0 Anti-spyware Version: 1.323.369.0
Sophos	Intercept X	Core Agent (2.7.7) Endpoint Advanced (10.8.7) Sophos Intercept X (2.0.17) Device Encryption (2.0.81)	Core Agent (2.8.6) Endpoint Advanced (10.8.8.1) Sophos Intercept X (2.0.17) Device Encryption (2.0.81)
Symantec	Endpoint Security Enterprise Edition	Version 14 (14.2 RU2) Build 5323 (14.2.5323.2000)	Version 14 (14.3) Build 558 (14.3.558.0000)

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**
Kaspersky Endpoint Security	75	25	100
Symantec Endpoint Security Enterprise Edition	75	25	100
Bitdefender Gravity Zone Endpoint Security	75	24	99
Crowdstrike Falcon	74	25	99
ESET Endpoint Security	74	25	99
Sophos Intercept X	74	25	99
Microsoft Defender Antivirus (enterprise)	73	25	98
McAfee EndPoint Security	72	25	97
FireEye Endpoint Security	70	22	92

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an “AS IS” basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.