SE Labs

INTELLIGENCE-LED TESTING

ENTERPRISE ENDPOINT PROTECTION

APR - JUN 2021

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
Rory Brown
Solandra Brewster
Liam Fisher
Gia Gorbold
Jeremiah Morgan
Joseph Pike
Sarah Sargeant
Dave Togneri
Dimitrios Tsarouchas
Stephen Withey
Liangyi Zhen

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Sara Claridge
Colin Mackleworth

CONTENTS

Endpoint protection needs your attention
How to get out more than you put in

Technology gives us tools to achieve sometimes amazing things. But no matter how advanced, it usually requires humans to make an effort.

We've all heard the terms, "fire and forget" or "plug and play" but these are usually marketing dreams. In security, as with any other area, you can buy tools, but you need to understand how to use them if you are going to succeed.

Adding security to a business or home isn't (or shouldn't be) a box-ticking exercise. General advice or even official standards highlight 'endpoint security' as a must-have. Having seen plenty of good and bad deployments, we advise that choosing an endpoint security product is just the start.

You need to understand not only the strengths and weaknesses of endpoint security, but the specific abilities of the products you are considering. And your specific needs. One size does not fit all.

Sometimes understanding your tools can save you money. They might be able to do things you hadn't realised previously. Buying new tools and add-ons can become expensive, particularly if they are not necessary.

Your own expertise (or your team's) is also important. A good basic endpoint security product might be good enough if you have thought through other security layers on your network. The latest and greatest AI-powered start-up rock star product might not do everything it claims, and almost certainly won't be everything you need. And if you need a PhD to use it, so much the worse.

If you were going to buy a new security fence, burglar alarm or CCTV system you would research the various options and consider how to deploy it in your very specific situation. The same should follow for endpoint protection systems. What do you really need? Are the candidates basically capable? And can you get the best out of them in your environment. We hope this report helps you answer some of these important questions.

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 LinkedIn 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 (%)
Broadcom Endpoint Security Enterprise Edition	100%	100%	100%
Kaspersky Endpoint Security	100%	100%	100%
McAfee Endpoint Security	100%	100%	100%
Microsoft Defender Antivirus (enterprise)	100%	100%	100%
Sophos Intercept X	100%	100%	100%
Crowdstrike Falcon	98%	100%	99%
Deep Instinct D-Client	98%	100%	99%
FireEye Endpoint Security	98%	100%	99%
VIPRE Endpoint Security	98%	100%	99%
ESET Endpoint Security	96%	100%	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 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 all cases by most products.**
All products were competent at blocking more targeted, exploit-based attacks.

- **False positives were not an issue for any product**
All of the endpoint solutions were good at correctly classifying legitimate applications and websites. With no exceptions they allowed all of the legitimate websites and applications.

- **Which products were the most effective?**
Products from **Broadcom, Kaspersky, McAfee, Microsoft** and **Sophos** achieved 100% total accuracy ratings. Those from **Crowdstrike, FireEye, Deep Instinct, VIPRE** and **ESET** achieved extremely good results due to a combination of their ability to block malicious URLs, handle exploits and correctly classify legitimate applications and websites. All 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
Broadcom Endpoint Security Enterprise Edition	1,136	100%	AAA
Kaspersky Endpoint Security	1,136	100%	AAA
McAfee Endpoint Security	1,136	100%	AAA
Microsoft Defender Antivirus (enterprise)	1,136	100%	AAA
Sophos Intercept X	1,135	100%	AAA
Crowdstrike Falcon	1,130	99%	AAA
FireEye Endpoint Security	1,127	99%	AAA
Deep Instinct D-Client	1,126	99%	AAA
VIPRE Endpoint Security	1,126	99%	AAA
ESET Endpoint Security	1,122	99%	AAA

Broadcom Endpoint Security Enterprise Edition
Kaspersky Endpoint Security
McAfee Endpoint Security
Microsoft Defender Antivirus (enterprise)
Sophos Intercept X
Crowdstrike Falcon
FireEye Endpoint Security
Deep Instinct D-Client
VIPRE Endpoint Security
ESET Endpoint Security

0   284   568   852   1,136
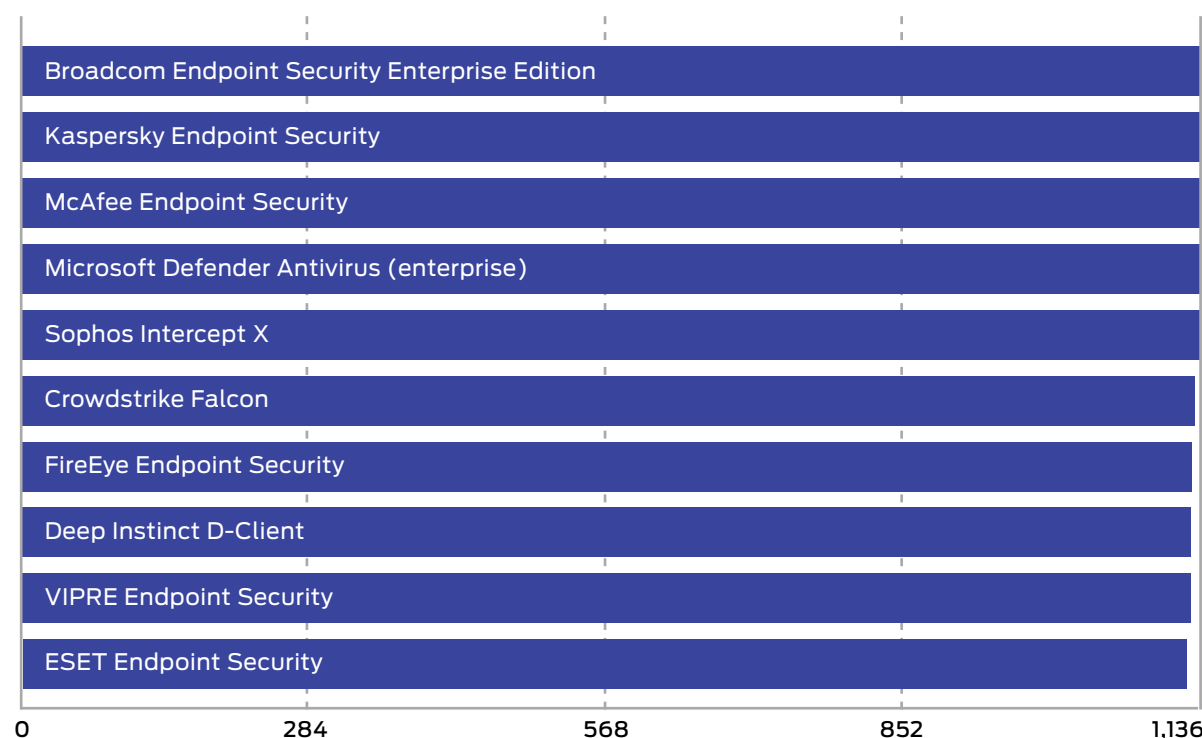
Total Accuracy Ratings combine protection and false positives.

Enterprise Endpoint Protection Awards

The following products win SE Labs awards:

- **Broadcom** Endpoint Security Enterprise Edition

- **Kaspersky** Endpoint Security

- **McAfee** Endpoint Security

- **Microsoft** Defender Antivirus (enterprise)

- **Sophos** Intercept X

- **Crowdstrike** Falcon

- **FireEye** Endpoint Security

- **Deep Instinct** D-Client

- **VIPRE** Endpoint Security

- **ESET** Endpoint Security

SE Labs
AAA
APR-JUN 2021
ENTERPRISE ENDPOINT PROTECTION

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

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.
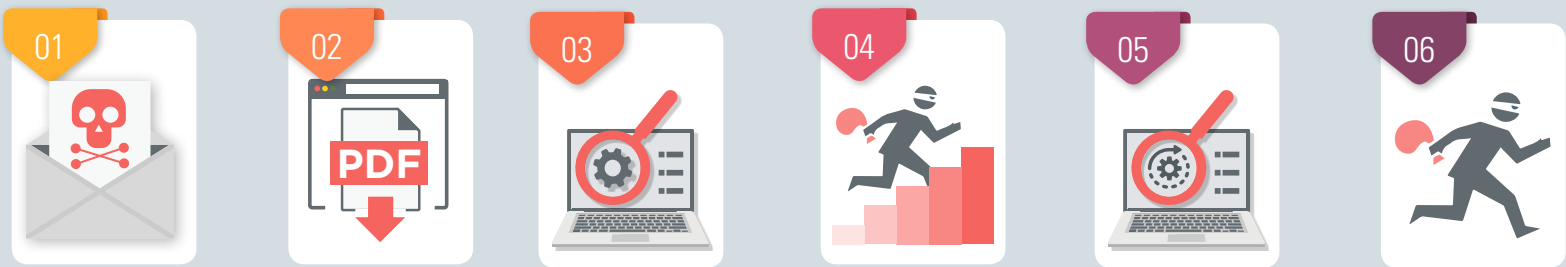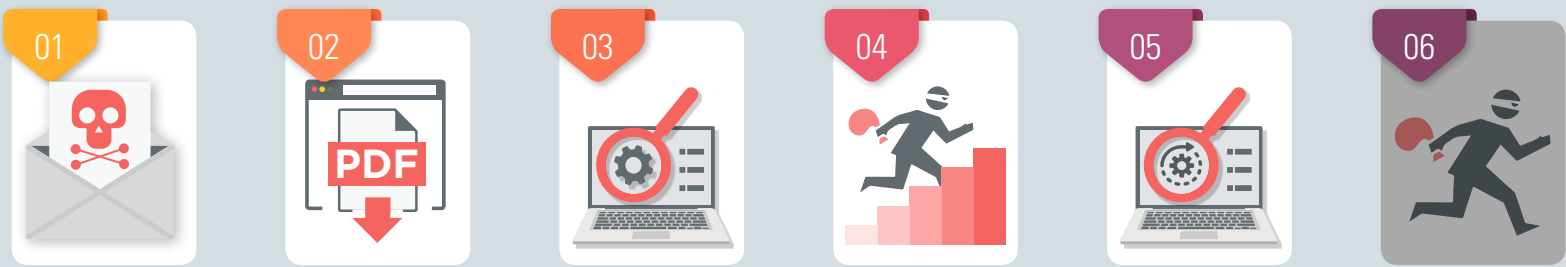

Figure 2. This attack was initially successful but only able to progress as far as the reconnaissance phase.

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

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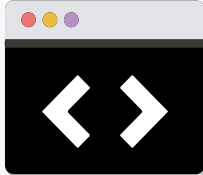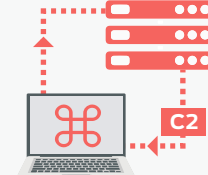
In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

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.

The table below shows how a typical way in which security testers illustrate attackers' behaviour. It is largely the same as our images above, but more detailed.

MITRE Example Attack Chain Details							
Initial Access	**Execution**	**Privilege Escalation**	**Credential Access**	**Discovery**	**Collection**	**Command and Control**	**Exfiltration**
Spearphishing via Service	Command-Line Interface	Bypass UAC	Input Capture	File and Directory Discovery	Input Capture	Data Encoding	Exfiltration Over C2 Channel
Spearphishing Link	Powershell		OS Credential Dumping	Process Discovery	Data from Local System	Data Obfuscation	
	Scripting			System Information Discovery			
	User Execution						
Spearphishing Link	Scripting	Bypass UAC	Input Capture	System Information Discovery	Input Capture	Data Encoding	Exfiltration Over C2 Channel

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.

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 (%)
Broadcom Endpoint Security Enterprise Edition	400	100%
Kaspersky Endpoint Security	400	100%
McAfee Endpoint Security	400	100%
Microsoft Defender Antivirus (enterprise)	400	100%
Sophos Intercept X	399	100%
Crowdstrike Falcon	394	98%
FireEye Endpoint Security	391	98%
Deep Instinct D-Client	390	98%
VIPRE Endpoint Security	390	98%
ESET Endpoint Security	386	96%

Average 99%
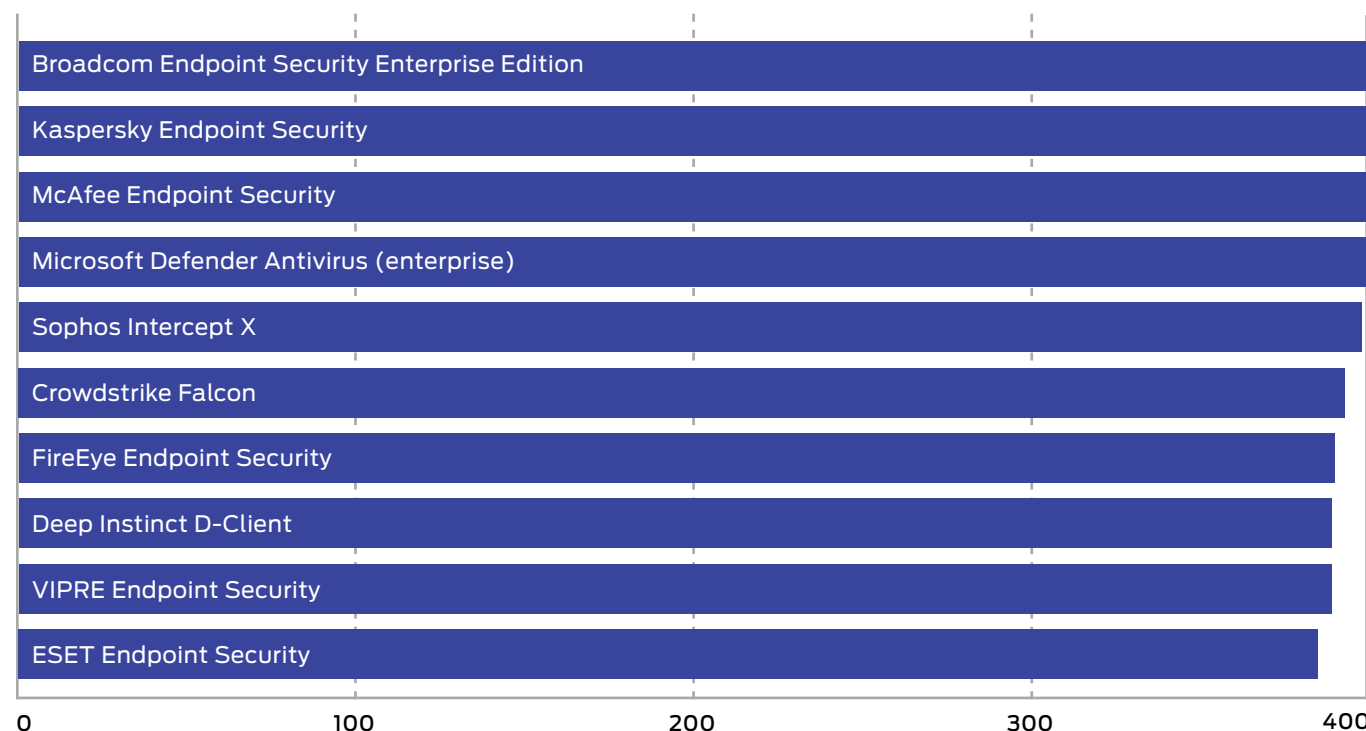
Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

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
Broadcom Endpoint Security Enterprise Edition	100
Crowdstrike Falcon	100
Deep Instinct D-Client	100
Kaspersky Endpoint Security	100
McAfee Endpoint Security	100
Microsoft Defender Antivirus (enterprise)	100
Sophos Intercept X	100
VIPRE Endpoint Security	100
FireEye Endpoint Security	99
ESET Endpoint Security	98
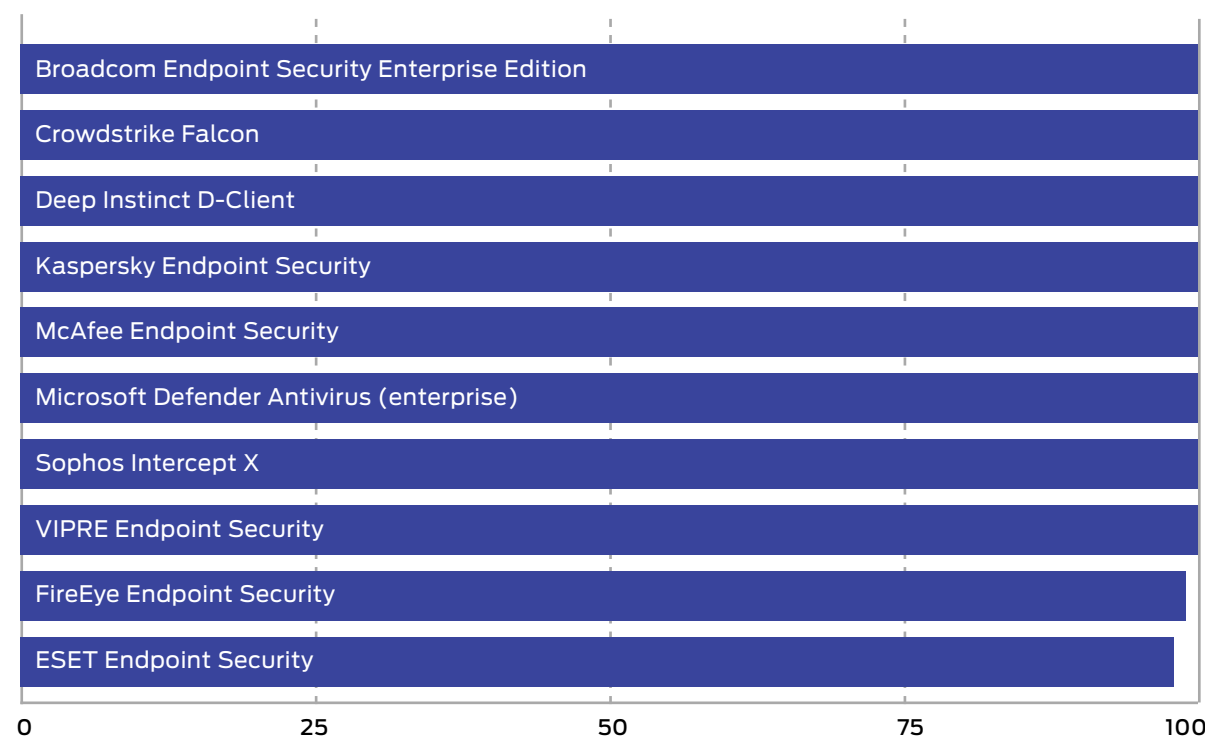
Protection Scores are a simple count of how many times a product protected the system.

5. Protection Details

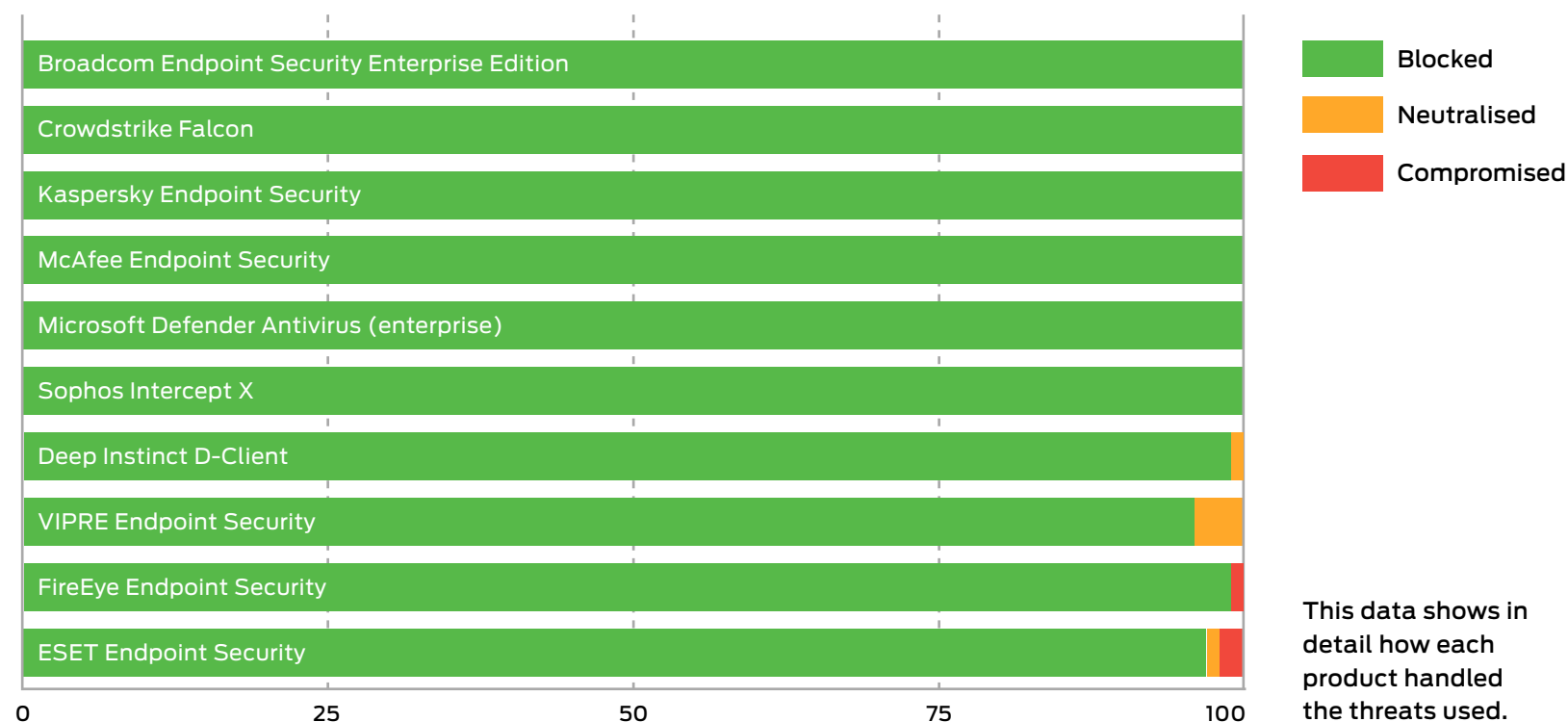These results break down how each product handled threats into some detail. You can see how many detected a threat and the levels of protection provided.

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
Broadcom Endpoint Security Enterprise Edition	100	100	0	0	100
Crowdstrike Falcon	100	100	0	0	100
Kaspersky Endpoint Security	100	100	0	0	100
McAfee Endpoint Security	100	100	0	0	100
Microsoft Defender Antivirus (enterprise)	100	100	0	0	100
Sophos Intercept X	100	100	0	0	100
Deep Instinct D-Client	100	99	1	0	100
VIPRE Endpoint Security	100	96	4	0	100
FireEye Endpoint Security	99	99	0	1	99
ESET Endpoint Security	98	97	1	2	98

Legend: ■ Blocked ■ Neutralised ■ Compromised

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 (%)
Broadcom Endpoint Security Enterprise Edition	736	100%
Crowdstrike Falcon	736	100%
Deep Instinct D-Client	736	100%
ESET Endpoint Security	736	100%
FireEye Endpoint Security	736	100%
Kaspersky Endpoint Security	736	100%
McAfee Endpoint Security	736	100%
Microsoft Defender Antivirus (enterprise)	736	100%
Sophos Intercept X	736	100%
VIPRE Endpoint Security	736	100%

Broadcom Endpoint Security Enterprise Edition

Crowdstrike Falcon

Deep Instinct D-Client

ESET Endpoint Security

FireEye Endpoint Security

Kaspersky Endpoint Security

McAfee Endpoint Security

Microsoft Defender Antivirus (enterprise)

Sophos Intercept X

VIPRE Endpoint Security

0   184   368   552   736
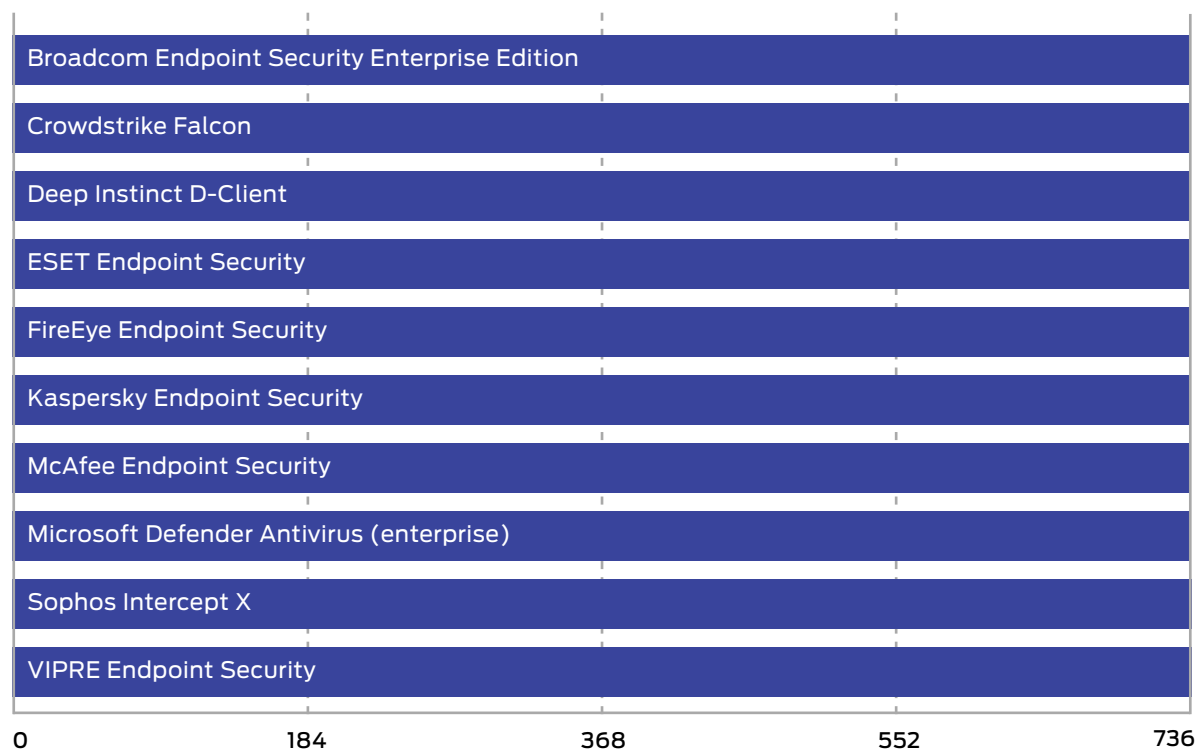
Legitimate Software Ratings can indicate how well a vendor has tuned its detection engine.

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)
Broadcom Endpoint Security Enterprise Edition	100
Crowdstrike Falcon	100
Deep Instinct D-Client	100
ESET Endpoint Security	100
FireEye Endpoint Security	100
Kaspersky Endpoint Security	100
McAfee Endpoint Security	100
Microsoft Defender Antivirus (enterprise)	100
Sophos Intercept X	100
VIPRE Endpoint Security	100

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	32
Medium Impact	16
Low Impact	12
Very Low Impact	8

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. With only a handful of threats missed, all-round performance was excellent. Targeted attacks were also handled well by all, although not perfectly.

Products from **Broadcom**, **Crowdstrike**, **Kaspersky**, **Deep Instinct**, **McAfee**, **Microsoft**, **Sophos** and **VIPRE** protected against all of the public and targeted attacks. Those from **FireEye** and **ESET** missed one or two public attacks. Each product stopped all targeted attacks.

All of the products handled the legitimate applications correctly, with no mistakes. This is an exceptionally good performance.

The leading products from **Broadcom**, **Crowdstrike**, **Deep Instinct**, **Kaspersky**, **McAfee**, **Microsoft**, **Sophos**, **VIPRE**, **FireEye** and **ESET** 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 7th April to 10th June 2021.
- 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). We allow other browser extensions when a tested product requests a user install one or more.

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)
Broadcom	Endpoint Security Enterprise Edition	14.3.3384.1000	14.3.3580.1100
Crowdstrike	Falcon	6.20.13408.0	6.24.13806.0
Deep Instinct	D-Client	2.5.0.5	2.5.1.4
ESET	Endpoint Security	8.0.2028.0	8.0.2028.0
FireEye	Endpoint Security	32.30.13	33.46.0
Kaspersky	Endpoint Security	11.5.0.590 AES256	11.6.0.394 AES256
McAfee	Endpoint Security	10.7.0.2421	10.7.0.2687
Microsoft	Defender Antivirus (enterprise)	1.335.850.0	1.341.377.0
Sophos	Intercept X	2.0.20	2.18.2
VIPRE	Endpoint Security	12.0.7874	12.0.7874

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
Broadcom Endpoint Security Enterprise Edition	75	25	100
Crowdstrike Falcon	75	25	100
Deep Instinct D-Client	75	25	100
Kaspersky Endpoint Security	75	25	100
McAfee Endpoint Security	75	25	100
Microsoft Defender Antivirus (enterprise)	75	25	100
Sophos Intercept X	75	25	100
VIPRE Endpoint Security	75	25	100
FireEye Endpoint Security	74	25	99
ESET Endpoint Security	73	25	98

SE Labs Report Disclaimer