# SE Labs
INTELLIGENCE-LED TESTING

BREACH RESPONSE TEST:
Kaspersky Anti Targeted
Attack Platform

SE Labs tested **Kaspersky Anti Targeted Attack Platform** against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

Full chains of attack were used, meaning that testers behaved as real attackers, probing targets using a variety of tools, techniques and vectors before attempting to gain lower-level and more powerful access. Finally, the testers/ attackers attempted to complete their missions, which might include stealing information, damaging systems and connecting to other systems on the network.

CONTENTS

INTRODUCTION

Breach Security Testing
Testing anti-breach products needs the full chain of attack

This Breach Response Test is a new kind of test. We believe that the testing behind this report used the largest range of relevant threats in any publicly available test and that the analysis of how the products tested work is the most in-depth.

We go into some detail on **page 9** about how threats work in a chain of stages because this is a really important and possibly unique feature of the Breach Response Test. It's crucial to copy attackers' techniques in full when assessing security products.

A computer breach causes some kind of damage, whether that involves deleting or encrypting files on a computer system; stealing data that damages a company's ability to compete; or stealing personal data for use in fraud. The possibilities and combinations are endless, but ultimately damage has to be done. Cyber criminals don't usually hack systems out of simple idle curiosity.

This is an important detail frequently overlooked in security testing, which often examines a product or service's ability to stop certain stages of attack, but not the full chain of events

that run from the initiation of an attack through to a successful completion of the attacker's prime goal.

Testers should not assume that certain approaches to protection are better than others. If a security company makes the world's best behavioural detection system but a test pays attention only to URL blocking technologies then the product will fail the test, while in reality customers who use it would be protected.

It is common for us to see a product appear to fail, and allow malware to run, even to the point where we obtain a remote connection to the target. However, when we try to take control of that system we may be blocked from doing so. A tester that sees the connection open might wrongly conclude that the product has failed. It is only by running through the entire attack process that it is possible to assess a product's full abilities.

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.

Executive Summary

Kaspersky Anti Targeted Attack Platform v.2.0 (KATA) was tested against a range of hacking attacks designed to compromise systems and penetrate target networks in the same way as criminals and other attackers breach systems and networks.

We examined its abilities to:
- Detect highly targeted attacks
- Protect against the actions of highly targeted attacks
- Provide remediation to damage and other risks posed by the threats
- Handle legitimate applications and other objects

Legitimate files were used alongside the threats to measure any false positive detections or other sub-optimum interactions.

Kaspersky Anti Targeted Attack Platform v.2.0 (KATA) detected all of the targeted attacks and protected the targets from 82 of the 85 attacks, preventing them from effectively providing remote access, causing damage or stealing data.

■ **Kaspersky Anti Targeted Attack Platform was effective against a diverse set of exploits, file-less attacks and malware attachments, comprising the widest range of threats in any currently available public test.**
All of these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over. The threats used in this are similar or identical to those used by the threat groups listed in **3. Threat Details** on page 8.

■ **Sometimes what seems like a bad result is a good one.**
In some test cases the product, on the face of it, failed to protect the system but in-depth testing showed that an attacker would not have been able to achieve any useful goals, despite what appeared to be a failure in protection. Testing using the full attack chain is crucial for accurate results.

■ **There were no issues with false positives.**
The product was completely accurate when handling legitimate objects, which shows that its settings were not too aggressively deployed. **Kaspersky Anti Targeted Attack Platform** performed very well in this test and achieved a **AAA** award.

EXECUTIVE SUMMARY			
Product Tested	Protection Accuracy (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Kaspersky Anti Targeted Attack Platform	92%	100%	95%

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.

1. Total Accuracy Rating

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.

Scoring a products response to a potential breach requires a granular method, which we outline in **4. Threat Responses** on page 9.

Enterprise Endpoint Protection Awards

The following product win SE Labs awards:

■ **Kaspersky** Anti Targeted Attack Platform

TOTAL ACCURACY RATING			
Product	Total Accuracy Rating	Total Accuracy Rating(%)	Award
Kaspersky Anti Targeted Attack Platform	563	95%	AAA

Total Accuracy Ratings combine protection and false positives.

2. Threat Types

This test includes a diverse set of exploits, file-less attacks and malware attachments, comprising the widest range of threats in any currently available public test. The threats were directed at Windows 7 and Windows 10 targets running a number of different web browsers, email clients and other relevant applications.

Not every specific attack used in the test was compatible with both target platforms (Windows 7/ 10), so some attacks would only work with Windows 7, for example, while others would work only against Windows 10.

Many attacks were tried with both unencrypted and encrypted connections between the target and the attacker to identify potential weaknesses in a product's detection and protection systems.

Categorisations

The threats used in this test can be categorised in a number of ways including by vector and by the type of the threat's initial stages and payload.

The vector categorisation is useful if you want to know how many threats were sent in as email attachments (23), for example, and how many were introduced via a collaboration tool like Slack (10).

There were six main types of threat used, regardless of vector. These are described in the table below.

For a detailed breakdown of the types of threats used with different vectors see **Appendix C: Threat Types and Vectors** on page 19.

THREAT TYPES	
Threat Type	**Description**
Exploit (File Format)	File format-based exploits are threats that come in the form of a file such as a PDF, Word, Excel or PowerPoint document. Their success relies on targets opening such files in applications that are vulnerable to the malicious construction of the document.
Exploit (File-less)	File-less threats exist in memory rather than writing data to the hard disk. In practice files are involved in a 'file-less' attack but they are not written to long-term storage devices.
Injection	The 'Injection' attacks in this test involve injecting malicious code into otherwise legitimate applications in an effort to disguise the threats.
Injection (Evasion)	The 'Injection (Evasion)' attacks in this test involve generating malicious executable files that inject themselves straight into memory in an effort to evade detection.
Script (File-less)	Threats using script-based technologies such as Powershell, Visual Basic and HTML Application can run on the system without writing their own code to the hard disk.
Script (Evasion)	Evasive script attacks use script-based technologies delivered in ways that make it harder for some security products to detect.

3. Threat Details

All of these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over. The threats used in this test are similar or identical to those used by the following threat groups. Attributions are taken from public sources:

■ **APT19** A Chinese group believed to have targeted defence, energy, telecommunications and other industries.

■ **APT28** Thought to be connected with Russian military cyber operations, APT28 targets government, military and security organisations.

■ **APT29** Thought to be connected with Russian military cyber operations, APT29 targets government, military and telecommunications sectors.

■ **APT32** This supposedly Vietnam-based group predominantly focusses on private businesses and foreign governments as targets.

■ **APT33** Focussing on aviation and energy industries, this group is believed to be based in Iran.

■ **Sandworm** A Russian-based group that appears to target Ukrainian industry, government and media organisations.

Other threats include well-known and prevalent banking malware used in widely-spread campaigns; threats used to serve malware through online advertisements; and threats aimed directly at financial institutions.

When the US non-profit company The MITRE Corporation released details of its ATT&ACK framework we rejoiced. MITRE effectively educated the market about targeted attack testing using the full attack chain, just as we perform it. In fact, we take things further than ATT&ACK does, by rolling out attacks with different options, but it's fair to say that the way we test is an extension of MITRE ATT&ACK.

MITRE's ATT&CK techniques include the following, all of which are included in our testing:

THREAT DETAILS	
Attack Technique	**Examples**
Initial Access	Spear Phishing Link (a link to a malicious file on a website sent in an email to a specific user on the target network).
Execution	Malware, script or exploit is run on the targeted endpoint.
Persistence	Add a new service that starts automatically on reboot.
Privilege Escalation	Exploitation of Windows to gain more powerful access to the system.
Defence Evasion	File-less attacks using scripts that do not write their own code to the hard disk.
Credential Access	Credential dumping of encrypted passwords.
Discovery	Listing user accounts.
Lateral Movement	Logging into other systems on the same network from the compromised target.
Collection	Logging keystrokes from the user's keyboard.
Command and Control	Remote access though encrypted connections.
Exfiltration	Uploading stolen data to systems controlled by the attacker.
Impact	Deletion or encryption of important files on the target systems.

4. 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 contains 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 (steps 5-7).

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.

ATTACK CHAIN STAGES

Figure 1. A typical attack starts with an initial contact and progresses through various stages, including reconnaissance, stealing data and causing damage.
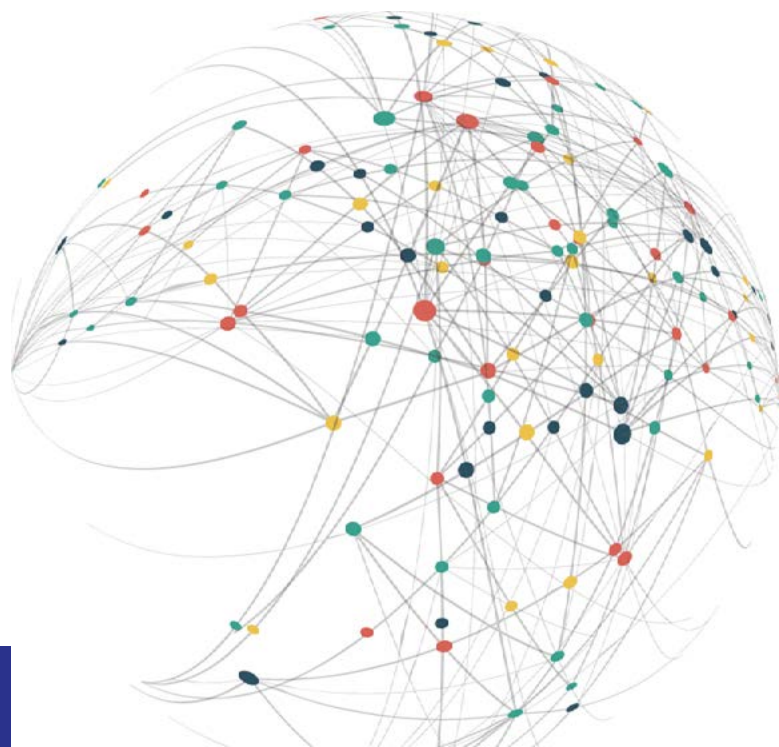
In figure 2. a product or service has interfered with the attack, allowing it to succeed only as far as stage 3, after which it was detected and neutralised. The attacker was unable to progress through stages 4 and onwards.

It is possible for an attack to run in a different order with, for example, the attacker attempting to connect to other systems without needing to escalate privileges. However, it is common for password theft (see step 5) to occur before using stolen credentials to move further through the network.

It is also 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 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.
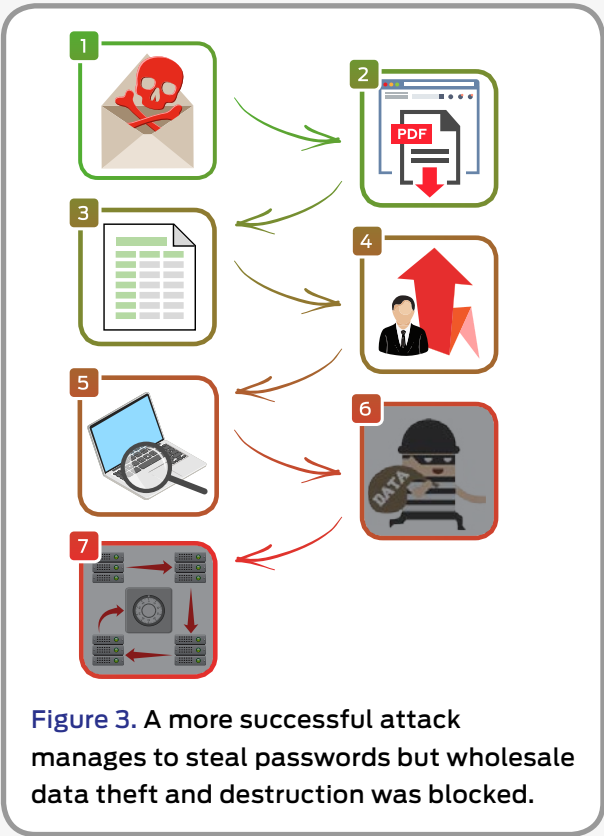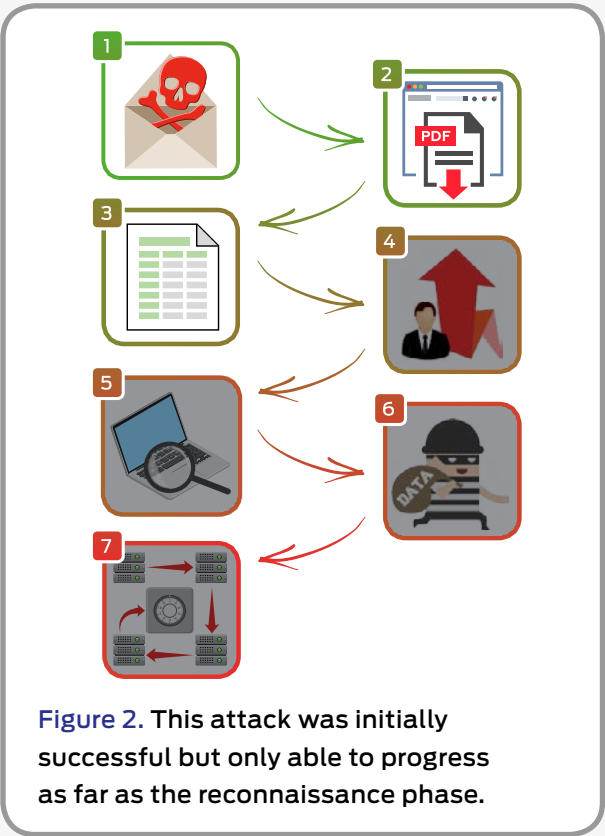
5. Protection Ratings

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

■ **Detected (+1)**

If the product detects the threat with any degree of useful information, we award it one point.

■ **Blocked (+2)**

Threats that are disallowed from even starting their malicious activities are blocked. Blocking products score two points.

■ **Neutralised (+1)**

Products that kill all running malicious processes 'neutralise' the threat and win one point.

■ **Complete Remediation (+1)**

If, in addition to neutralising a threat, the product removes all significant traces of the attack, it gains an additional one point.

■ **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 **7. 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 ACCURACY RATINGS		
Product	Protection Accuracy Rating	Protection Accuracy Rating (%)
Kaspersky Anti Targeted Attack Platform	313	92%

Kaspersky Anti Targeted Attack Platform	
0 170 340	Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

6. Protection Score

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 Anti Targeted Attack Platform	82

Kaspersky Anti Targeted Attack Platform	
0 17 34 51 68 85	Protection Scores are a simple count of how many times a product protected the system.
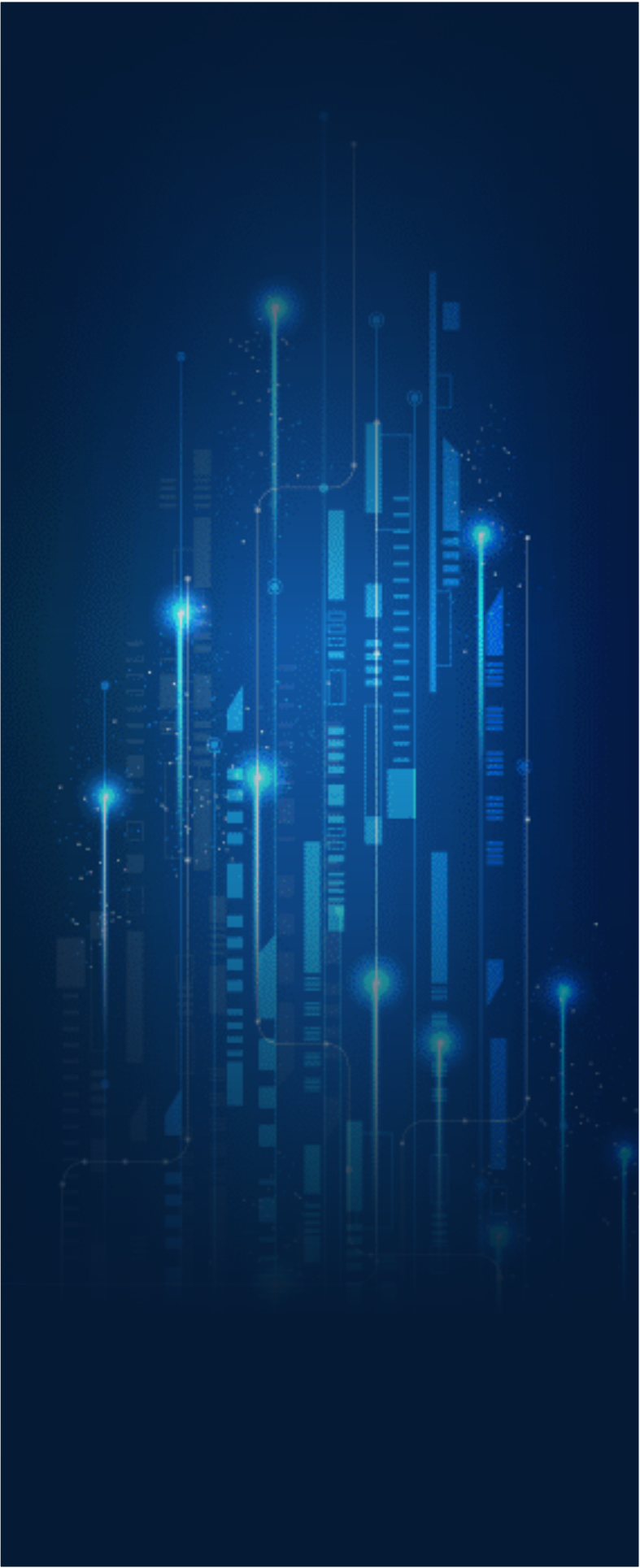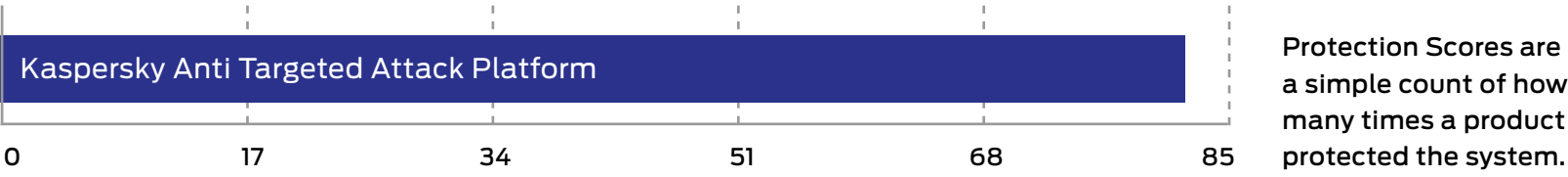
7. Protection Details

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	Complete Remediation	Neutralised	Compromised	Protected
Kaspersky Anti Targeted Attack Platform	85	82	70	0	3	82

Kaspersky Anti Targeted Attack Platform

0   17   34   51   68   85

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

- Defended
- Complete Remediation
- Neutralised
- Compromised
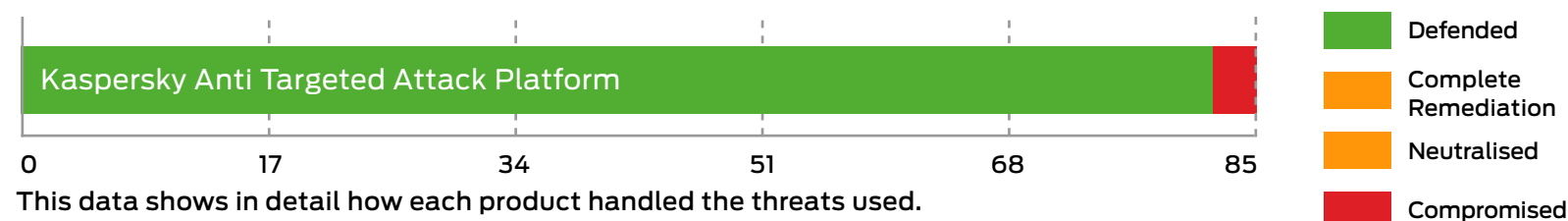
The following table lists the cases in which the product protected against specific types of threat.

THREAT PROTECTION DETAILS							
Product	Exploit (File Format)	Exploit (File-less)	Injection	Injection (Evasion)	Script (Evasion)	Script (File-less)	Protected
Kaspersky Anti Targeted Attack Platform	12	21	10	18	2	19	82

These results summarise the number of times the product protected against different threat types.

8. 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 **8.3 Accuracy Ratings** on page **16**.

LEGITIMATE SOFTWARE RATINGS		
Product	Legitimate Accuracy Rating	Legitimate Accuracy Rating(%)
Kaspersky Anti Targeted Attack Platform	250	100%

Kaspersky Anti Targeted Attack Platform					
0	50	100	150	200	250

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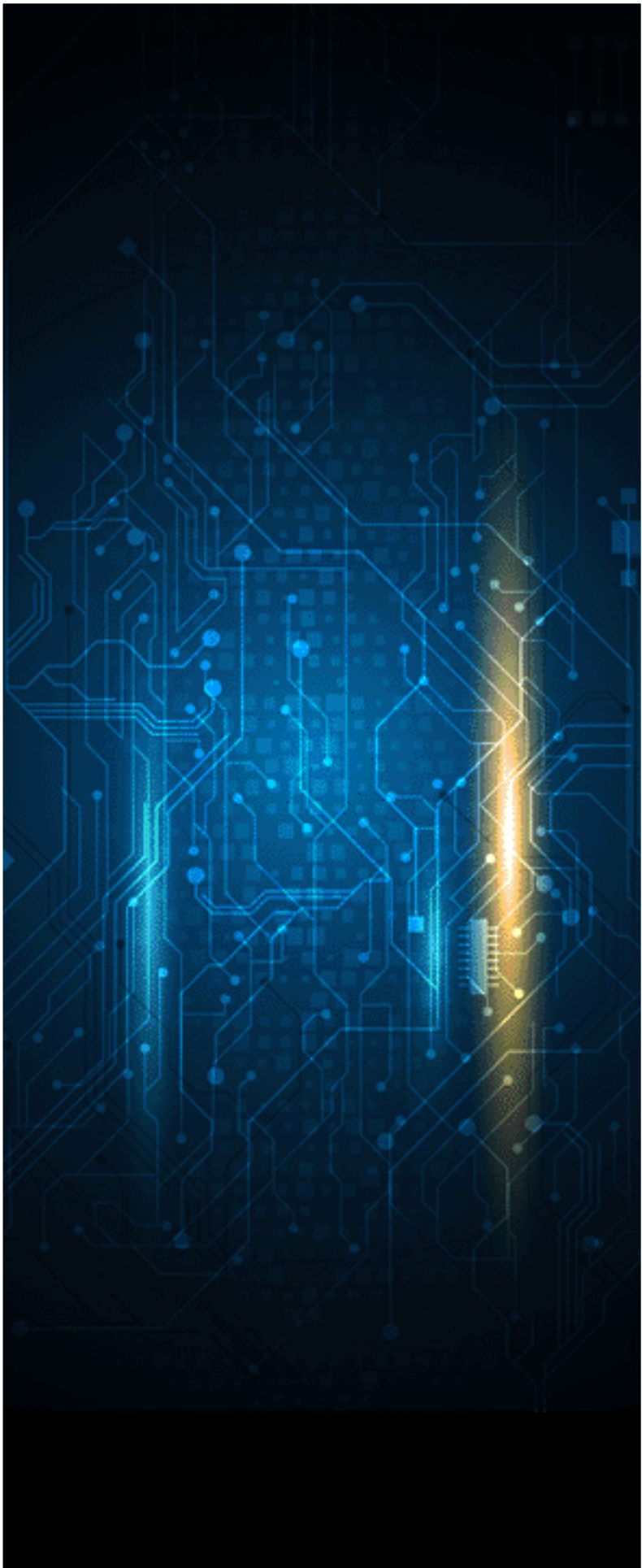
8.1 Interaction Ratings

It's crucial that endpoint security 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)	None (Blocked)
Kaspersky Anti Targeted Attack Platform	100	0

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

8.2 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.

8.3 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 **8. Legitimate Software Ratings** on page **14**.

8.4 Distribution of Impact Categories

Endpoint products that were most accurate in handling legitimate objects achieved the highest ratings. If all objects were of the highest prevalence, the maximum possible rating would be 1,000 (100 incidents x (2 interaction rating x 5 prevalence rating)).

In this test there was a range of applications with different levels of prevalence. The table below shows the frequency:

LEGITIMATE SOFTWARE CATEGORY FREQUENCY	
Prevalence Rating	Frequency
Very High Impact	25

9. Conclusions

This test exposed **Kaspersky Anti Targeted Attack Platform (KATA)** to a diverse set of exploits, file-less attacks and malware attachments, comprising the widest range of threats in any currently available public test. All of these attack types have been witnessed in real-world attacks over the previous few years. They are representative of a real and present threat to business networks the world over. The threats used in this are similar or identical to those used by the threat groups listed in **3. Threat Details** on page 8.

It is important to note that while the test used the same types of attacks, new files were used. This exercised the tested product's abilities to detect and protect against certain approaches to attacking systems rather than simply detecting malicious files that have become well-known over the previous few years. The results are an indicator of potential future performance rather than just a compliance check that the product can detect old attacks.

The product detected all of the threats and protected fully against most. In 82 cases the threats were unable to move beyond the earliest stages of the attack chain, meaning that as soon as the target systems were exposed to the threats, the attacks were detected immediately and were either blocked from running or, in 12 cases, were allowed to run only briefly before being neutralised.

This prevented them from causing any damage, including data theft.

In some cases of neutralisation the attacks created a connection to the attacker, who was then unable to progress further. In three cases the injection with evasion attacks worked, but only to a point. The tester was able to gain access to the target and steal some information about the system and from its filesystem. However, it was not possible to escalate privileges and steal passwords, install keyloggers and modify the filesystem. This illustrates the need for full attack chain testing: if a tester sees the connection being made and assumes that the attack has succeeded then the results for that test would not be accurate. Furthermore, an apparently successful compromise might be more limited than it first appears.

The results are strong and most attacks could not progress far enough to the point at which the testers would start hacking through the targets. Sometimes products are overly aggressive and detect everything, including threats and legitimate objects. In this test **Kaspersky Anti Targeted Attack Platform (KATA)** generated no such false positive results, which is as expected.

Kaspersky Anti Targeted Attack Platform (KATA) wins a AAA award for its excellent performance.

Appendices

APPENDIX A: Terms Used

TERM	MEANING
Compromised	The attack succeeded, resulting in malware running unhindered on the target. In the case of a targeted attack, the attacker was able to take remote control of the system and carry out a variety of tasks without hindrance.
Blocked	The attack was prevented from making any changes to the target.
False positive	When a security product misclassifies a legitimate application or website as being malicious, it generates a 'false positive'.
Neutralised	The exploit or malware payload ran on the target but was subsequently removed.
Complete Remediation	If a security product removes all significant traces of an attack, it has achieved complete remediation.
Target	The test system that is protected by a security product.
Threat	A program or sequence of interactions with the target that is designed to take some level of unauthorised control of that target.
Update	Security vendors provide information to their products in an effort to keep abreast of the latest threats. These updates may be downloaded in bulk as one or more files, or requested individually and live over the internet.

APPENDIX B: FAQs

A **full methodology** for this test is available from our website.
- This test contains results for Kaspersky Anti Targeted Attack Platform v.2.0. At the time of publication a later version was available.
- The test was unsponsored.
- The test was conducted between October 2018 to February 2019.
- 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.

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: Threat Types and Vectors

The following table categorises the attacks used in the test according to vector and type. It also breaks these details down into techniques used by specific historical campaigns. For example, it is possible to see not only how many threats were sent via email attachments but also how many were file format-based exploits; how many used executables that inject into memory; and how many included (file-less) scripts that do not touch the filesystem.

THREAT TYPES AND VECTORS						
Threat Campaign Details	Exploit (File Format)	Exploit (File-less)	Injection	Injection (Evasion)	Script (File-less)	Script (Evasion)
Web Browser						
Drive-by Compromise - APT 38	0	7	0	0	0	0
Hanjuan Exploit kit - Malvertising campaign	0	3	0	0	0	0
Web Browser Total	**0**	**10**	**0**	**0**	**0**	**0**
Email Attachment						
APT19 - Malicious RTF - Spearphishing Attachment	3	0	0	0	0	0
Cactustorch, APT29, APT 33	0	0	0	0	6	0
Dridex - banking malware	0	0	0	0	3	0
Exploitation for Client Execution - APT32	1	3	0	0	0	0
Sandworm - Quadagh (Mitre says it might be the same so stick with Sandworm)	6	0	0	0	0	0
Carbanak - Process Injection for evasion	0	0	0	1	0	0
Email Attachment Total	**10**	**3**	**0**	**1**	**9**	**0**

THREAT TYPES AND VECTORS						
Threat Campaign Details	Exploit (File Format)	Exploit (File-less)	Injection	Injection (Evasion)	Script (File-less)	Script (Evasion)
Web Browser (IE) Direct						
Drive-by Compromise - APT 38	0	8	0	0	0	0
Web Browser (IE) Direct Total	**0**	**8**	**0**	**0**	**0**	**0**
Web Browser (IE) Email Link						
APT28 downloads and executes powershell scripts	0	0	0	0	0	2
Exploitation for Client Execution - APT32	2	0	0	0	0	0
Carbanak - Process Injection for evasion	0	0	0	11	0	0
Web Browser (IE) Email Link Total	**2**	**0**	**0**	**11**	**0**	**2**
Web Browser (Chrome) Email Link						
APT32- has used Powershell-based tools, Powershell one-liners, and shellcode loaders for execution.	0	0	0	0	10	0
Web Browser (Chrome) Email Link Total	**0**	**0**	**0**	**0**	**10**	**0**
Internal Web Server						
Carbanak - Process Injection for evasion	0	0	0	9	0	0
Internal Web Server	**0**	**0**	**0**	**9**	**0**	**0**
Web browser (Chrome) Slack						
Dragonfly - Found samples in the wild with Shellter signatures	0	0	10	0	0	0
Web browser (Chrome) Slack Total	**0**	**0**	**10**	**0**	**0**	**0**

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.