

Independent Tests of Anti-Virus Software



Endpoint Prevention and Response EPR Comparative Report 2023

TEST PERIOD: JUNE - SEPTEMBER 2023
LAST REVISION: 16TH OCTOBER 2023

WWW.AV-COMPARATIVES.ORG

Contents

EPR MANAGEMENT SUMMARY	3
TESTED PRODUCTS	4
EPR CYBERRISK QUADRANT OVERVIEW	7
AV-COMPARATIVES' EPR CERTIFICATION	9
DETAILED TEST RESULTS	10
PHASE 1 METRICS: ENDPOINT COMPROMISE AND FOOTHOLD	10
PHASE 2 METRICS: INTERNAL PROPAGATION	13
PHASE 3 METRICS: ASSET BREACH	15
MITRE ATT&CK MATRIX FOR ENTERPRISE	17
EPR COST STRUCTURE	19
OPERATIONAL-ACCURACY AND WORKFLOW-DELAY COSTS	20
PRODUCT FEATURES	22
EDR TELEMETRY	25
OVERVIEW OF EDR TECHNOLOGIES	27
PRODUCT CONFIGURATIONS AND SETTINGS	29
EPR TEST METHODOLOGY	30
ABOUT THIS TEST	35
COPYRIGHT AND DISCLAIMER	36

EPR Management Summary

Endpoint prevention and response (EPR) products are used in enterprises to detect, prevent, analyse and respond to targeted attacks such as advanced persistent threats (APTs). Whilst endpoint security products are expected to detect and block malware and network attacks on individual workstations, EPR solutions have to deal with multi-stage attacks that aim to infiltrate an organisation's entire network. In addition to protecting individual devices, endpoint prevention and response systems are expected to provide detailed analysis of an attack's origin, methods and aims. This allows security staff to understand the nature of the threat, prevent it from spreading, remediate any damage done, and take precautions to prevent similar attacks in the future.

AV-Comparatives' Endpoint Prevention and Response Test is the most comprehensive test of EPR products ever performed. The 12 products in the test were subjected to 50 separate targeted attack scenarios, which used a variety of different techniques. If left unchecked, the attacks would progress through three separate phases: Endpoint Compromise and Foothold; Internal Propagation; Asset Breach. At each stage, the full attack-chain test determined whether the product took automated action to block the threat (active response), or provided information about the attack which the administrator could use to take action themselves (passive response). If an EPR product did not block an attack at one stage, the attack would continue to the next phase, and the product's response here would be noted.

This report includes the results of the tests, showing at which stage (if any) each product provided active or passive response to each threat. However, a number of other factors are also considered. The ability of each product to take remedial action was noted. Also considered was the ability of each product to collect and present information on indicators of compromise in an easily accessible form.

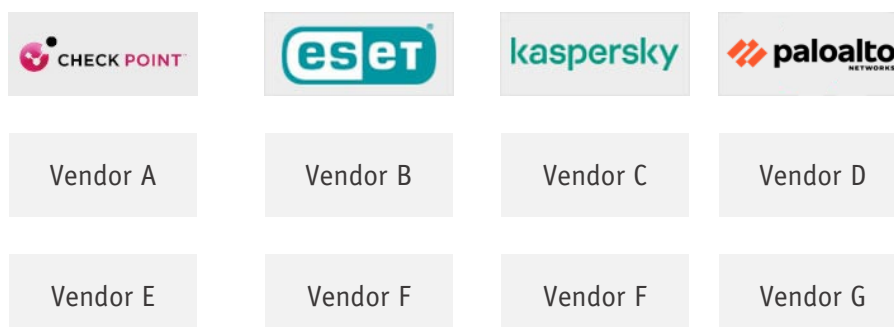
We have developed an Enterprise EPR CyberRisk Quadrant that factors in the effectiveness of each product at preventing breaches, the calculated savings resulting from this, the purchase costs of the product, the product's operational accuracy costs, and workflow-delay costs. For this calculation, we have assumed an enterprise with 5,000 client PCs over a period of 5 years.

In our continuous effort to enhance our Enterprise EPR CyberRisk Quadrant, we have made some refinements this year. Our assessment factors still include breach prevention effectiveness, cost-effectiveness, operational accuracy, and workflow efficiency. However, our presentation has evolved to provide more clarity and simplicity. Now, products are categorized based on their performance levels within the quadrant, while our award badge has been streamlined to display either 'Certified' or 'Not Certified'. This adjustment allows us to deliver insightful categorization while offering a more straightforward recognition system.

Tested Products

We congratulate the following vendors for taking part in this EPR Test and having their results published. All tested vendors were provided with detailed information on their respective missed scenarios, so that they can further improve their products.

Please note that some of the vendors in this test chose to remain anonymous, so we have referred to them as “Vendor A”, “Vendor B”, etc. We have included their results in the report in order to provide an overview of the performance levels currently available on the market.



The following products were tested by AV-Comparatives:

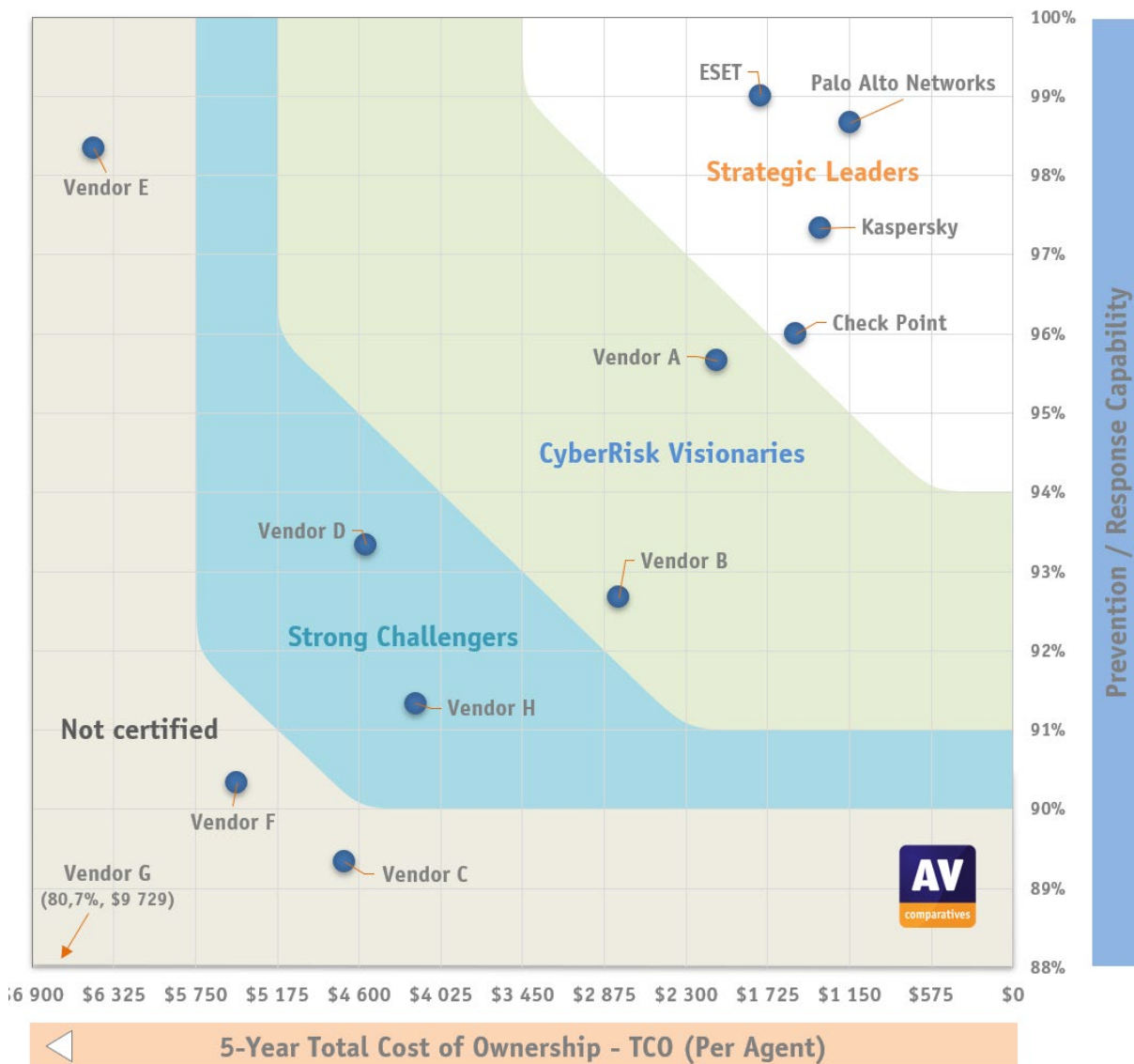
Vendor	Product	Version
Check Point	Harmony Endpoint Advanced	87.30
ESET	PROTECT Enterprise Cloud	10.1
Kaspersky	Endpoint Detection and Response Expert (on-premises)	5.0
Palo Alto Networks	Cortex XDR Pro	8.0
Vendor A	Product A	n/a
Vendor B	Product B	n/a
Vendor C	Product C	n/a
Vendor D	Product D	n/a
Vendor E	Product E	n/a
Vendor F	Product F	n/a
Vendor G	Product G	n/a
Vendor H	Product H	n/a

The settings which were applied to each respective product can be found on page 29 of this report.

This comparative report provides an overview of the results for all tested products. There are also individual reports for each product, which are available at www.av-comparatives.org at the links provided below:

Check Point: https://www.av-comparatives.org/wp-content/uploads/2023/10/EPR_CheckPoint_2023.pdf
 ESET: https://www.av-comparatives.org/wp-content/uploads/2023/10/EPR_ESET_2023.pdf
 Kaspersky: https://www.av-comparatives.org/wp-content/uploads/2023/10/EPR_Kaspersky_2023.pdf
 Palo Alto Networks: https://www.av-comparatives.org/wp-content/uploads/2023/10/EPR_PaloAlto_2023.pdf

EPR CyberRisk Quadrant™



Endpoint Prevention and Response (EPR) – ECRQ - Enterprise CyberRisk Quadrant™

Product	5-Year Product Cost (Per Agent)	Active Response	Passive Response	Combined Prevention/Response Capabilities Y-Axis	Operational Accuracy Costs	Workflow Delay Costs	5-Year TCO (Per Agent) X-Axis
Check Point	\$190	96.0%	96.0%	96.0%	None	None	\$1 525
ESET	\$152	98.7%	99.3%	99.0%	Moderate	None	\$1 776
Kaspersky	\$206	97.3%	97.3%	97.3%	Few	None	\$1 354
Palo Alto Networks	\$350	98.7%	98.7%	98.7%	Few	None	\$1 139
Vendor A	\$190	95.3%	96.0%	95.7%	None	None	\$2 081
Vendor B	\$100	92.7%	92.7%	92.7%	None	None	\$2 770
Vendor C	\$190	89.3%	89.3%	89.3%	None	None	\$4 700
Vendor D	\$160	93.3%	93.3%	93.3%	Moderate	None	\$4 550
Vendor E	\$318	98.0%	98.7%	98.3%	High	Moderate	\$6 464
Vendor F	\$135	90.0%	90.7%	90.3%	Low	Moderate	\$5 455
Vendor G	\$85	74.0%	76.7%	75.3%	Moderate	None	\$9 729
Vendor H	\$420	91.3%	91.3%	91.3%	None	None	\$4 203

EPR CyberRisk Quadrant Key Metrics - based on 5,000 agents

Explanation of the EPR CyberRisk Quadrant

The quadrant shows these levels from high to low: Strategic Leader, CyberRisk Visionary, Strong Challenger, Not Certified. These levels offer a comprehensive overview of a product's overall performance. They provide vendors with valuable insights into specific aspects of their offerings that may benefit from further development. In essence, while 'Certified' signifies excellence, the subcategories serve as a roadmap for vendors, guiding them towards continuous innovation and refinement. Our goal is to not only recognize outstanding products but also encourage the ongoing pursuit of excellence within the cybersecurity landscape.

Strategic Leaders

EPR products classified as Strategic Leaders offer an exceptional return on investment, resulting in a significantly reduced total cost of ownership (TCO). Their remarkable technical capabilities, coupled with bug-free performance¹, keep costs in check. These products consistently excel in prevention, detection, response, and reporting, while also delivering optimal workflow features for system administrators and operations.

CyberRisk Visionaries

EPR products classified as CyberRisk Visionaries offer a high return on investment, providing low TCO by offering impressive technical capabilities combined with very good operational and system-administrator workflow capabilities. These products generally demonstrated very good prevention, detection, response and reporting capabilities, along with above-average operational and system-administrator workflow capabilities.

Strong Challengers

EPR products classified as Strong Challengers provide a satisfactory return on investment, thus providing an acceptable TCO. They generally offer effective prevention, detection, response and reporting capabilities, and competent operational and system-administrator workflow capabilities.

Not Certified

Products with a combined Active and Passive Response of less than 90%, and/or other costs that made the TCO too high, are not certified.

Which product is right for my enterprise?

The fact that a product is shown here in the highest area of the quadrant does not necessarily mean that it is the best product for your enterprise needs. Products in lower areas of the quadrant could have features that make them well suited to your particular environment.

Placement of the dots

The vendor 'dot' placement on the Y axis of the quadrant was driven by how good the active response or passive response capabilities were. This score will also have an influence on the X axis; a product with a high active response rate will have a lower TCO, as the response costs are smaller. Furthermore, products that stop an attack in an earlier phase will also incur fewer costs. Other factors in the TCO calculation include purchase price, operational accuracy, and workflow delays caused by e.g. sandbox analysis. Please see the full explanation on page 8 as to how active and passive response credits were given to vendors.

¹ In the future, we may downgrade a product if it does not function properly.

EPR CyberRisk Quadrant Overview

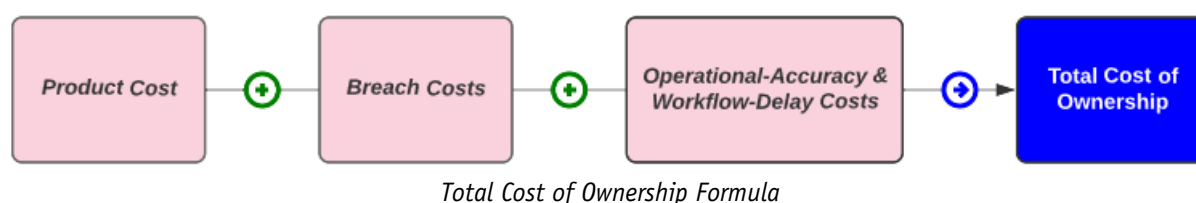
We have developed an Enterprise EPR CyberRisk Quadrant that factors in the effectiveness of each product at preventing breaches, the calculated savings resulting from this, the purchase costs of the product, and the product's accuracy costs (incurred due to false positives).

One of the significant problems caused by a security breach is the financial cost incurred by the targeted organisation. According to IBM, the average cost of a breach is USD 4.45 million². Therefore, purchasing an effective EPR product that minimises the negative impact of an attack can be a good investment. If a company stands to lose USD 2 million if an attack is successful, then spending even USD 1.5 million on security measures makes good financial sense, aside from any other considerations.

In this section, we consider the overall costs involved in deploying the tested security products, and their effectiveness in preventing security breaches. This enables us to calculate how good a financial investment each of the products represents. Using IBM's estimate of USD 4.45 million as the loss to the enterprise if an attack is successful, we calculate how much the organisation could save by purchasing each of the tested EPR products. The figures show that all the tested products are effective, and that their combined active and passive response scores cover the great majority of attacks. However, some products are clearly better than others in this respect. The more effective a product is at preventing security breaches, the less the expected costs for dealing with breaches will be.

The graphic below outlines the formula used to arrive at the total cost of ownership for a product, which includes the following factors. Firstly, there is the price paid to the product's vendor for the product and associated service and support charges. Next come any costs associated with over-blocking/over-reporting caused by the product, which are defined as Operational Accuracy costs below. These cases have to be investigated and remediated. In 2015, the Ponemon's Institute³ estimated that companies waste roughly USD 1.3 million per year due to inaccurate or erroneous intelligence. To allow for inflation over the last eight years, a reasonable estimate for 2023 would be USD 1.72 million. This has been factored in as the added yearly cost that you can expect to pay for a product failing our operational-accuracy validation this year. Costs arising from imperfect Operational Accuracy are penalised, and costs due to workflow delays are also taken into account. Hence, if a user is operationally impacted by e.g. a product's features, policies or behaviour, this will be reflected in the EPR CyberRisk quadrant rating as well.

Next come the costs associated with breaches, whereby a product that could theoretically block 100% of attacks would have zero breach costs here, whilst a product that did not block any attacks would incur the full cost of a breach.



² <https://www.ibm.com/security/data-breach>

³ <https://www.ponemon.org/research/ponemon-library/security/the-cost-of-malware-containment.html>

The breach cost of each product per scenario was calculated, based on the ability of the EPR product to actively and passively respond at the time of execution. The procedure we used for calculating breach costs in 2023 is given below:

1. If there was active response (i.e. the attack was successfully stopped automatically *and* reported) in Phase 1, then 0% of the total breach cost was added for the scenario.
2. If there was NO active response in Phase 1, but the product showcased passive response capabilities in Phase 1, then only 12.5% of the total breach cost was added for the scenario.
3. If there was active response in Phase 2, then 25% of the total breach cost was added for the scenario.
4. If there was NO active response in Phase 2, but the product showcased passive response capabilities in Phase 2, then 50% of the total breach cost was added for the scenario.
5. If there was active response in Phase 3, then 75% of the total breach cost was added for the scenario.
6. If there was NO active response in Phase 3, but the product showcased passive response capabilities in Phase 3, then 95% of the total breach cost was added for the scenario.
7. If there was NO active or passive response for the scenario, then 100% of the total breach cost was added for the scenario.

To calculate the X-axis in the EPR CyberRisk Quadrant, we used the list price of the product, operational accuracy (such as false positives/over-blocking/over-reporting) costs, workflow-delay costs, and the breach-cost savings.

Scores shown on the X axis of the Quadrant are calculated as follows. For active response, we take the cumulative response scores for phases 1, 2 and 3, and find the average of these. We then do the same with the cumulative passive response scores for phases 1, 2 and 3. Finally, we take the average of these two scores to provide the overall response score.

We have made slight enhancements to our quadrant calculations. These changes primarily resulted from inflation-driven cost increases and rising product expenses. We have also made very minor refinements to the TCO calculation.

We are steadfast in our commitment to ensuring the utmost relevance of the metrics used in this evaluation. We considered feedback from enterprises, and took this into account where appropriate. This iterative approach ensures that our assessment process continually adapts to the ever-changing enterprise landscape.

EPR systems aim to prevent threats where this is possible, or provide effective detection/response capabilities where it isn't. Endpoint products that offer a high *prevention* rate incur fewer costs, since there is no operational overhead required to respond to and remediate the effects of an attack. Furthermore, EPR products that provide a high *detection* rate (visibility and forensic detail) will realize savings, because the product provides the information needed to investigate the attack.

Active Response (Prevention): An active response stops the attack automatically, and reports it.

Passive Response (Detection): A passive response does not stop the attack, but reports suspicious activity.

AV-Comparatives' EPR Certification





In this evaluation, certification is granted based on a product's performance in the EPR CyberRisk Quadrant™, where it must achieve an average score of at least 90% for combined Active and Passive Response, without incurring excessive costs. Achieving certification signifies a product's excellence, regardless of the specific quadrant level attained within the EPR Quadrant.

Receiving a 'Certified' designation in our Enterprise EPR CyberRisk Quadrant signifies that a product has demonstrated a high level of performance and effectiveness. It reflects our endorsement of its quality and suitability for enterprise use.

The table below show which of the tested vendors in AV-Comparatives' 2023 EPR Test got certified:



NOT CERTIFIED

	
	
Vendor A	Vendor B
Vendor D	Vendor H
Vendor C	Vendor E
Vendor F	Vendor G

Detailed Test Results

For an active response (preventative action) to be credited, we verified whether the product made an active response during the respective phase. Similarly, for a passive response (detection event) to be credited, we verified that the product gave an active alert tied to the attack during the respective phase, allowing the system administrator to take appropriate actions.

Phase 1 Metrics: Endpoint Compromise and Foothold

The Phase 1 content of the executed attacks can be described by means of MITRE ATT&CK and other frameworks. The following Tactics are part of this phase.

Initial Access⁴: Initial access is the method used by the attacker to get a foothold inside the environment that is being targeted. Attackers may use a single method, or a combination of different techniques. Threats may come from compromised websites, email attachments or removable media. Methods of infection can include exploits, drive-by downloads, spear phishing, macros, trusted relationships, valid accounts, and supply-chain compromises.

Execution⁵: The next goal of the attacker is to execute their own code inside the target environment. Depending upon the circumstances, this could be done locally or via remote code execution. Some of the methods used include client-side execution, third-party software, operating-system features like PowerShell, MSHTA, and the command line.

Persistence⁶: Once the attacker gets inside the target environment, they will try to gain a persistent presence there. Depending upon the target operating system, an attacker may use operating-system tools and features. These include registry manipulation, specifying dynamic-link-library values in the registry, shell scripts that can contain shell commands, application shimming, and account manipulation.

⁴ <https://attack.mitre.org/tactics/TA0001/>

⁵ <https://attack.mitre.org/tactics/TA0002/>

⁶ <https://attack.mitre.org/tactics/TA0003/>

The table below depicts the results for each of the products tested for Phase 1.

Scenario	Description	Check Point	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E	Vendor F	Vendor G	Vendor H
1	Metasploit Framework - Binary Direct SysCalls												
2	Metasploit Framework - Binary Asynchronous Procedure Call Injection												
3	Metasploit Framework - Binary Indirect SysCalls												
4	Metasploit Framework - Visual Basic Script												
5	Metasploit Framework - Staged MSlexec												
6	Metasploit Framework - JavaScript DLL Sideload												
7	Metasploit Framework - Staged DLL via Rundll32												
8	Metasploit Framework - PowerShell Script with AMSI and ETW Patch												
9	Metasploit Framework - Staged HTA												
10	Metasploit Framework - Visual Basic Script and AMSI Patch												
11	PowerShell Empire - Masqueraded Binary Indirect SysCalls												
12	PowerShell Empire - Binary UUID Exec												
13	PowerShell Empire - Visual Basic Script with obfuscated strings												
14	PowerShell Empire - Stageless MSlexec												
15	PowerShell Empire - Stageless Visual Basic Script												
16	PowerShell Empire - Excel Shellcode Injection via VBS												
17	PowerShell Empire - Stageless DLL via Rundll32												
18	PowerShell Empire - PowerShell Script with AMSI Patch												
19	PowerShell Empire - Stageless HTA												
20	PowerShell Empire - Visual Basic Script												
21	Commercial Framework - Masqueraded Binary Indirect SysCalls Shellcode												
22	Commercial Framework - Masqueraded Binary NTAPI and ETW Bypass												
23	Commercial Framework - Process Injection into Excel via PPT Macro												
24	Metasploit Framework - Binary with Invalid Code Signature and UUID Exec												

25	Metasploit Framework - Masqueraded Binary and ETW-Patch												
26	Metasploit Framework - Obfuscated JavaScript DLL Sideload												
27	Metasploit Framework - Obfuscated Visual Basic Script non-standard port												
28	Metasploit Framework - Packed MSlexec non-standard port												
29	Metasploit Framework - Binary Process Hollowing and ETW-Patch												
30	Metasploit Framework - Encrypted DLL via Rundll32												
31	Metasploit Framework - Stageless obfuscated PowerShell Script												
32	Metasploit Framework - Obfuscated HTA												
33	Metasploit Framework - Obfuscated Visual Basic Script shellcode fetch												
34	Metasploit Framework - Binary NTAPI												
35	Metasploit Framework - JavaScript DLL Sideload NTAPIs												
36	PowerShell Empire – Obfuscated .PIF file and ETW-Patch												
37	PowerShell Empire - Masqueraded obfuscated .SCR file SysCalls												
38	PowerShell Empire - HTML file (.chm) process injection into Office process												
39	PowerShell Empire - Visual Basic Script shellcode fetch												
40	PowerShell Empire - Packed MSI												
41	PowerShell Empire - Binary DLL Sideload (Process Hollowing)												
42	PowerShell Empire - DLL shellcode fetch via rundll32												
43	PowerShell Empire - Heavily Obfuscated PowerShell Script												
44	PowerShell Empire - Stageless obfuscated HTA												
45	PowerShell Empire - Visual Basic Script Win32 APIs												
46	PowerShell Empire - Packed MSI												
47	PowerShell Empire - JavaScript DLL Sideload via MSlexec												
48	Commercial Framework - Encrypted JavaScript DLL Sideload												
49	Commercial Framework - Masqueraded Binary with obfuscated shellcode												
50	Commercial Framework - Encrypted Control Panel Applet Application												

Active and Passive Response for Phase 1

Active response / prevention
 No active response / no prevention

Passive response / detection
 No passive response / no detection

Phase 2 Metrics: Internal Propagation

In this phase, the EPR product should be able to prevent internal propagation. This phase is triggered if the attack is not stopped in Phase 1. The EPR product in this phase should enable the system administrator to immediately identify and track the internal propagation of the threat in real time. We have explained below the relevant Tactics from the MITRE ATT&CK Framework.

Privilege Escalation⁷: In enterprise networks, it is standard practice for users (including system admins on their own personal computers) to use standard user accounts without administrator privileges. If an enterprise endpoint is attacked, the logged-on account will not have the permissions the attacker requires to launch the next phase of the attack. In these cases, privilege escalation must be obtained, using techniques such as user-access token manipulation, exploitation, application shimming, hooking, or permission weakness. Once the adversary has got a foothold inside the environment, they will try to escalate the privileges. For an active response to be credited, we looked at various phases inside each method to see if there was a preventative action by the product.

Defense Evasion⁸: The attacker's aim is to carry out their objectives without being detected or blocked. Defense Evasion consists of measures used to ensure that the attack remains undiscovered. This could include tampering with security software, obfuscating processes, and abusing e.g. system tools so as to hide the attack.

Credential Access⁹: This is a method used by the attacker to ensure their further activities are carried out using a legitimate network user account. This means that they can access the resources they want, and will not be flagged as an intruder by the system's defences. Different credential-access methods can be used, depending on the nature of the targeted network. Credentials can be obtained on-site, using a method such as input capture (e.g., keyloggers). Alternatively, it might be done using the offline method, where the attacker copies the entire password database off-site, and can then use any method to crack it without fear of discovery.

Discovery¹⁰: Once the attacker has gained access to the target network, they will explore the environment, with the aim of finding those assets that are the ultimate target of the attack. This is typically done by scanning the network.

Lateral Movement¹¹: The attacker will move laterally within the environment, so as to access those assets that are of interest. Techniques used include pass the hash, pass the ticket, and exploitation of remote services and protocols like RDP.

⁷ <https://attack.mitre.org/tactics/TA0004/>

⁸ <https://attack.mitre.org/tactics/TA0005/>

⁹ <https://attack.mitre.org/tactics/TA0006/>

¹⁰ <https://attack.mitre.org/tactics/TA0007/>

¹¹ <https://attack.mitre.org/tactics/TA0008/>

The table below depicts the results for each of the products tested for Phase 2.

Scenario	Check Point	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E	Vendor F	Vendor G	Vendor H
1	✓	✓	✓	✓	✓	✓	✓	○	✓	✓	○	✓
2	✓	✓	✓	✓	✓	✓	✓	○	✓	✓	○	✓
3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
6	○	✓	✓	✓	✓	✓	✓	✓	✓	✓	○	✓
11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
21	○	○	○	✓	○	○	✗	✗	○	✗	✗	✓
22	✓	✓	✓	✓	○	✓	✗	○	✓	✗	✗	✓
23	✓	✓	✓	✓	✓	✓	✗	✓	○	✗	✗	✗
25	○	✓	○	✓	✓	○	○	✓	✓	✓	○	✓
26	✓	○	✓	✓	✓	○	✓	✓	✓	○	✗	✓
35	○	✓	✓	✓	✓	○	○	✓	✓	✓	○	○
36	○	✓	○	✓	✓	○	○	✓	✓	✓	✗	✗
37	○	✓	○	○	✓	○	○	✓	✓	○	✗	✗
47	✓	✓	✓	✓	○	✓	✓	○	✓	✗	✗	✓
48	✓	✓	✓	✓	○	○	○	○	✓	○	✗	✗
49	✓	✓	✓	○	✗	✗	✗	✗	○	✗	✗	✓
50	✓	✓	✓	✓	✓	○	○	✓	✓	○	○	○

Active and Passive Response for Phase 2 showing only scenarios which passed Phase 1

○ Active response / prevention

○ Passive response / detection

✗ No active response / no prevention

✗ No passive response / no detection

✓ Already prevented before

Phase 3 Metrics: Asset Breach

The final phase of the workflow, asset breach, is where attackers execute their ultimate objective. Below, we outline relevant tactics from the MITRE ATT&CK Framework:

Collection¹²: Gathering target information, often involving the theft of documents, emails, or databases.

Command and Control¹³: Enabling communication between the attacker's system and the targeted network, allowing for command execution and data exchange, often camouflaged as regular network traffic.

Exfiltration¹⁴: Covertly copying the collected data from the targeted network to the attacker's server, typically utilizing a command-and-control infrastructure.

Impact¹⁵: Refers to direct harm inflicted on the targeted organization's network, which can include manipulation, disruption, or destruction of operational systems and data. It may serve as an end goal (sabotage) or a means to obfuscate data theft by complicating breach investigations.

The table below depicts the results for each of the products tested for Phase 3.

Scenario	Check Point	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E	Vendor F	Vendor G	Vendor H
3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
11	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
21	✓	✓	✓	✓	✓	✓	○	○	✓	○	✗	✓
22	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✗	✓
23	✓	✓	✓	✓	✓	✓	○	✓	✓	○	✗	○
26	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
36	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
37	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
47	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓
48	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗
49	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✗	✓

Active and Passive Response for Phase 3 showing only scenarios which passed Phase 2

○ Active response / prevention

○ Passive response / detection

✗ No active response / no prevention

✗ No passive response / no detection

✓ Already prevented before

Vendor A, **Vendor B**, and **Vendor D** experienced 1 complete unknown breach (Scenario 49). **Vendor C** and **Vendor F** each encountered 2 full unknown breaches (Scenarios 22 and 49). **Vendor H** suffered 3 complete unknown breaches (Scenarios 36, 37, and 48), while **Vendor G** was impacted by 7 full unknown breaches (Scenarios 21, 22, 23, 36, 37, 48, and 49). In other words, none of these attacks were either prevented or detected in any of the three phases.

¹² <https://attack.mitre.org/tactics/TA0009/>

¹³ <https://attack.mitre.org/tactics/TA0011/>

¹⁴ <https://attack.mitre.org/tactics/TA0010/>

¹⁵ <https://attack.mitre.org/tactics/TA0040/>

The following table shows the cumulative active response by phase(s) for each product.

Active Response	Phase 1 Only	Phase 1 & 2	Overall (Phase 1, 2 & 3)
Check Point	88%	100%	100%
ESET	96%	100%	100%
Kaspersky	92%	100%	100%
Palo Alto Networks	96%	100%	100%
Vendor A	90%	98%	98%
Vendor B	82%	98%	98%
Vendor C	80%	92%	96%
Vendor D	86%	96%	98%
Vendor E	94%	100%	100%
Vendor F	82%	92%	96%
Vendor G	66%	86%	86%
Vendor H	88%	92%	94%

Cumulative Active Response by phases

The following table shows the cumulative passive response by phase(s) for each product.

Passive Response	Phase 1 Only	Phase 1 & 2	Overall (Phase 1, 2 & 3)
Check Point	88%	100%	100%
ESET	98%	100%	100%
Kaspersky	92%	100%	100%
Palo Alto Networks	96%	100%	100%
Vendor A	92%	98%	98%
Vendor B	82%	98%	98%
Vendor C	80%	92%	96%
Vendor D	86%	96%	98%
Vendor E	96%	100%	100%
Vendor F	84%	92%	96%
Vendor G	74%	86%	86%
Vendor H	88%	92%	94%

Cumulative Passive Response by phases

The following table shows the raw data, i.e. numbers of scenarios prevented/reported.

Product	Scenarios	Overall Active Prevention	Overall Passive Response	No Prevention/Response
Check Point	50	50	50	0
ESET	50	50	50	0
Kaspersky	50	50	50	0
Palo Alto Networks	50	50	50	0
Vendor A	50	49	49	1
Vendor B	50	49	49	1
Vendor C	50	48	48	2
Vendor D	50	49	49	1
Vendor E	50	50	50	0
Vendor F	50	48	48	2
Vendor G	50	43	43	7
Vendor H	50	47	47	3

Responses per scenario

The diagram below¹⁶ shows the entire MITRE ATT&CK Matrix for Enterprise¹⁷. The column headings represent the ATT&CK Tactics¹⁸ (aims), while the boxes below them represent the ATT&CK Techniques¹⁹ used to achieve those goals. Our EPR test covers the entire attack chain shown here, using the most realistic possible scenarios. Across the 50 attack scenarios used in this EPR test, we tried to employ all of the Techniques shown in the green boxes below.

Phase 1 = Initial Access, Execution, Persistence

Phase 3 = Collection, Command and Control, Exfiltration, Impact

MITRE ATT&CK Tactics and Techniques covered by this EPR Test

An example scenario might look like this: phishing mail with script payload is sent to user on Workstation A – internal discovery is performed – access to C\$ share on Workstation B is found – lateral movement to Workstation B – network admin session on Workstation B is found – LSASS dumped to obtain admin credentials – lateral movement to Server 1 – defence evasion used to bypass security product on Server 1 – credit-card data found – data is extracted via open C2 channel.

¹⁹ <https://attack.mitre.org/techniques/enterprise/>

The difference between MITRE ATT&CK Engenuity and the AV-Comparatives EPR Test

Both tests have their merits, but while MITRE Engenuity evaluates techniques from a single attack chain, carried out by a preselected and announced APT, AV-Comparatives' EPR Test involves 50 separate attack scenarios from undisclosed APTs. AV-Comparatives refrains from disclosing the attack methods and techniques in advance, mirroring real-world scenarios. This approach aims to showcase a solution's ability to prevent, detect, and remediate attacks while providing passive response to users.

Historically, MITRE assessed solutions in Detect-Only mode, examining product responses to individual techniques within attack chains. However, MITRE only began testing Protection scenarios, meaning the attack was blocked or disrupted, in Round 3 (2020-2021). On the other hand, AV-Comparatives has been dedicated to validating Protection capabilities since the test's inception in 2020.

MITRE Engenuity permits the use of customized product settings and allows vendors to list these configurations on dedicated product pages. While vendors might use highly specific settings to enhance test results, these settings may not be practical for real-world use due to potential false positives, performance issues, and alert fatigue for real-world EDR/XDR operators. AV-Comparatives maintains control over setting changes, reporting them in the test results, so as to better inform users.

Traditionally, MITRE Engenuity participants are aware of the adversary groups chosen for upcoming evaluations through Calls for Participation. However, the Call for Participation in Managed Services Round 2023-2024 represents a departure from this practice. This latest Call for Contribution also allows participants to potentially impact test complexity by submitting data about APT tactics, techniques, and procedures known only to them.

MITRE Engenuity lacks a straightforward scoring system to compare products' effectiveness against threats and lacks comprehensive incident telemetry. AV-Comparatives addresses this gap by introducing a simple comparison scoring system, aiding customers in evaluating product efficiencies. Additionally, AV-Comparatives introduced a Total Cost of Ownership metric for product comparison, providing better insight into the numbers. MITRE Engenuity participants all claim to be the winner at the end. In contrast, AV-Comparatives testing poses greater challenges, allowing participants to remain anonymous. Achieving certification signifies exceptional proficiency, even for Strong Challengers.

Unlike AV-Comparatives' EPR-Test, the MITRE Engenuity assessment does not consider False Positive scenarios (operational accuracy). This approach, combined with the flexibility to modify product configurations, introduces a risk of misinterpreting final results. In contrast, AV-Comparatives' EPR-Test assesses operational accuracy and emphasizes the importance of balancing false negatives and operational accuracy.

MITRE Engenuity testing occurs over varying timeframes, with several months potentially separating evaluations. Those who join early have the option to be tested later.

In devising its Engenuity tests, MITRE employs telemetry, heavily relying on data interpretation skills to uncover insights. Manufacturers with knowledge of what to search for are better equipped to uncover valuable findings in the data. Alternatively, AV-Comparatives devises its EPR tests based on its research of attack scenarios its specialists are aware of and have analysed in depth themselves.

EPR Cost Structure

Product costs are based on list prices in USD provided by vendors at the time of testing (summer 2023). The actual cost to end users might be lower, depending on different factors. In general, pricing may vary based on factors like volume discounts, negotiated discounts, geographic location, distribution channel, and partner margins. Compared to previous years, some products have notably increased their list prices, with increases ranging up to 25%, while others have remained unchanged in price for years.

The EPR Cost incorporates the product costs for 5,000 clients, based on a 5-year contract:

Product	EPR Cost 5,000 Clients / 5 Years
Check Point	\$ 950,000
ESET	\$ 760,833
Kaspersky	\$ 1,032,000
Palo Alto Networks	\$ 1,750,000
Vendor A	\$ 950,500
Vendor B	\$ 500,777
Vendor C	\$ 1,250,000
Vendor D	\$ 800,000
Vendor E	\$ 1,590,000
Vendor F	\$ 675,000
Vendor G	\$ 425,000
Vendor H	\$ 2,100,000

Total EPR Cost Structure

Please note that each product has its own particular features and advantages. We suggest that readers consider each product in detail, rather than looking at these list prices alone. Some products might have additional / different features and services that make them particularly suitable for some organisations.

Operational-Accuracy and Workflow-Delay Costs

Costs arising from imperfect operational accuracy and workflow delays are calculated as follows.

Costs arising from imperfect operational accuracy

Operational accuracy testing was performed by simulating a typical user activity in the enterprise environment. This included opening clean files of different types (such as executables, scripts, documents with macros) and browsing to different clean websites. Furthermore, different administrator-friendly tools and scripts were also executed in the test environment to ensure that productivity was not affected by the respective product configuration used for the test.

To assess operational accuracy, each product is tested with a battery of clean scenarios. Over-blocking or over-reporting of such scenarios means that a product reaches high prevention and detection rates, but also causes increased costs. Where legitimate programs/actions are blocked, the system administrator will have to investigate, restore/reactivate any blocked programs etc, and take steps to prevent it happening again. The principle of “The boy who cried wolf” may also apply; the greater the number of false alerts, the more difficult it becomes to recognise a genuine alert.

Products are then assigned to one of five Groups (None, Low, Moderate, High, and Very High, whereby lower is better), according to the number of affected scenarios. These are shown in the table below.

Group	Number of affected scenarios	Operational Accuracy	
		Active Response <i>Multiplying Factor</i>	Passive Response <i>Multiplying Factor</i>
None	0	x0	x0
Low	1	x1	x0.75
Moderate	2-3	x5	x3.75
High	4-5	x10	x7.5
Very High	6+	x20	x15

Multiplying factors for Operational Accuracy costs

The costs arising from imperfect Operational Accuracy are worked out using Cost Units of USD 1.72 million. The number of Cost Units a product is deemed to have caused is calculated using a Multiplying Factor. This varies according to the Group, and also whether the scenario was affected by an Active Response (action blocked), or by a Passive Response (action not blocked, but detection alert shown in the console). The Multiplying Factor for an erroneous Passive Response is always three-quarters of that of an erroneous Active Response, because less time and effort is required to resolve the problem.

How this works in practice is best explained by looking at the table above. Products in the “None” Group have a Multiplying Factor of 0 for both Active and Passive Responses, therefore Operational Accuracy costs are zero. Products in the “Low” Group (1 affected scenario) have a Multiplying Factor of 1 for erroneous Active Responses, but only 0.75 for an erroneous Passive Response. Hence, a product with one erroneous Active Response incurs one Cost Unit, while a product with one erroneous Passive Responses only incurs 0.75 Cost Units. If a product had 2 affected scenarios, one being an Active Response, the other a Passive Response, it would incur 8.75 Cost Units (5 for the Active Response, and 3.75 for the Passive Response).

Costs arising from workflow delays

Some EPR products will cause delays in the user's workflow because they e.g. stop the execution of a previously unknown file and send it to the vendor's online sandbox for further analysis. Due to this behaviour, execution is stalled, and the user is not able to proceed till the analysis comes back from the sandbox. We noted the delay caused by such analysis, for both scenarios (clean and malicious). Where a product caused significant delays when analysing a scenario, this was penalised. The analysis time for each product was calculated as follows. For *clean* scenarios, we took the longest observed delay for any one scenario. So, for example, a product with two delays - of 2 minutes and 10 minutes respectively - for *clean* scenarios would have a recorded time of 10 minutes. For *malicious* scenarios, we took the average of all the delays. So, a product with two delays - of 2 minutes and 10 minutes respectively - for *malicious* scenarios, would have a recorded time of 6 minutes. Products are then assigned to one of five Workflow Delay Groups (None, Low, Moderate, High and Very High), depending on how long the respective delay is. These are shown in the table below.

Group	Delay Caused (in minutes)	Workflow Delay Multiplying Factor
None	under 2	x0
Low	2-5	x0.5
Moderate	6-10	x2.5
High	11-20	x5
Very High	over 20	x10

Multiplying factors for Workflow Delay costs

The costs of these delays are calculated using the same Cost Units as for operational accuracy. Again, there is a multiplying factor, which varies according to the Workflow Delay Group. Products in the Low Workflow Delay Group have a Multiplying Factor of 0.5, hence incurring costs of 1 Cost Unit; products in the Very High Workflow Delay Group have a Multiplying Factor of 10, thus incurring costs of 10 Cost Units. Products in the latter category would be disqualified from certification, due to the excessive costs incurred.

Results

The costs arising from imperfect Operational Accuracy and Workflow Delays are shown below:

	Operational Accuracy		Workflow Delays
	Active Response	Passive Response	
Check Point	None	None	None
ESET	None	Moderate	None
Kaspersky	None	Low	None
Palo Alto Networks	Low	None	None
Vendor A	None	None	None
Vendor B	None	None	None
Vendor C	None	None	None
Vendor D	Moderate	None	None
Vendor E	High	Moderate	Moderate
Vendor F	Low	None	Moderate
Vendor G	Low	Moderate	None
Vendor H	None	None	None

Combined results table for Operational Accuracy and Workflow Delays

Product features

In this section, we provide an overview of the products' features and the associated services provided by their respective vendors. Please note that in each case, these refer only to the specific product, tier and configuration used in our test. A different product/tier from the same vendor may have a different feature set. On the following pages we describe the General features, Product Response, Management and Reporting, IOC Integration features, Support features, Support features and then provide a feature list showing which products support these features.

General features

This section looks at general features such as phishing protection, web access control, device control, interface languages, and supported operating systems.

Product Response Mechanism

EPR products will use their response mechanisms to deal with the intrusions that have occurred inside the protected environment. At a minimum, an EPR product is expected to allow the correlation of endpoints, processes and network communications, as well as the correlation of external IOCs with the internal environment. EDR capabilities were tested and examined by using the detection and response capabilities of the product. We were able to examine the events that correlated with the various steps that attacker took while attempting to breach the environment.

The EPR product should enable complete visibility of the malicious artifacts/operations that make up the attack chain, making any response-based activities easy to complete. This means that where any form of intended remediation mechanism is available in the product (Response Enablement), this mechanism is shown below. Please note that the capabilities shown below only apply to the specific product/version used in this test. A vendor might offer additional features as an add-on or in another product.

Central Management and Reporting

Management workflow is a top differentiator for enterprise security products. If a product is difficult to manage, it will not be used efficiently. The intuitiveness of a product's management interface is a good determiner of how useful the product will be. Minutes saved per activity can translate into days and even weeks over the course of a year.

Management: Threat Visibility, System Visibility, and Data Sharing

The ability to provide threat context is a key component of an EPR product. This visibility can be critical when organizations are deciding whether to either supplement an existing technology or replace it. The management console can be deployed as physical appliance, virtual appliance, or cloud-based appliance. A full trail of audit logs is available in the management console. Communication between the agent and management console is done via SSL. The following tables provide information on the applicable capabilities of each of the tested products.

EPR Product Reporting Capabilities

An EPR platform should have the ability to unify data, that is to say, bring together information from disparate sources, and present it all within its own UI as a coherent picture of the situation. Technical integration with the operating system and third-party applications (Syslog, Splunk, SIEM or via API) is an important part of this. An EPR system should be able to offer response options appropriate to the organization.

IOC Integration

This is to identify the digital footprint by means of which the malicious activity on an endpoint/network can be identified. We will examine this use case by looking at the EPR product's ability to use external IOCs including Yara signatures or threat intelligence feeds etc. as shown in the table below.

Support features

Free, basic human support for deployment: this means real-time communication with a member of the support staff, who will talk you through the deployment process and can provide immediate answers to any basic questions you have. Of course, many vendors will provide user manuals, videos and premium (paid-for) deployment support services instead/in addition.

Professionally assisted training: this includes any form of interactive training with an instructor. A few vendors include professional training as part of the license fee paid for 5,000 clients, while others charge additionally for it. Some other vendors might only offer videos and other online material for self-training.

Feature List Endpoint Prevention and Response (EPR) - as of Summer 2023				
Vendor	Check Point	ESET	Kaspersky	Palo Alto Networks
Product Name	Harmony Endpoint Advanced	PROTECT Enterprise Cloud	Endpoint Detection and Response Expert (on-premises)	Cortex XDR Pro
Version Number	87.30	10.1	5.0	8.0.2
Supported languages - endpoint client	English, German, Polish, Czech, Greek, Italian, Russian, French, Japanese, Spanish, Portuguese, Ukrainian	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese	Arabic, Czech, German, English, Spanish, French, Hungarian, Italian, Kazakh, Korean, Dutch, Polish, Portuguese, Portuguese (Brazil), Romanian, Russian, Turkish, Vietnamese, Chinese	English, German, Japanese, Spanish, French, Chinese
Supported languages - management console	English, Japanese, Chinese		Arabic, German, English, Spanish, French, Italian, Japanese, Kazakh, Korean, Polish, Portuguese, Russian, Turkish, Chinese	English
Product Features for 5,000 endpoints				
Do you also offer a managed version (MDR) of the tested product in your portfolio?	•	•	•	•
General Features				
Third-party scan engine used (in addition to its own)	Kaspersky, Sophos	proprietary	proprietary	proprietary
Phishing protection for web browsers	•	•	•	
Web access control	•	•	•	•
External device control	•	•	•	•
Sandbox feature	•	•	•	•
2-factor authentication	optional	obligatory	optional	optional
Right-click on-demand scan	•	•	•	•
Lock settings	•	•	•	•
Lock uninstalling	•	•	•	•
Supported Operating Systems				
Microsoft Windows	•	•	•	•
↳ Windows 7	•	•	•	
↳ Windows 8	•	•	•	
↳ Windows 10	•	•	•	•
↳ Windows 11	•	•	•	•
Virtual environments (such as VMware, HyperV)	•	•	•	•
Apple macOS	•	•	•	•
Linux	•	•	•	•
Google Android	•	•	•	•
Apple iOS	•	•	•	•
Response Actions				
Quarantine	•	•	•	•
Delete Files and Directories	•	•	•	•
Process Termination	•	•	•	•
Shutdown or Reboot of Endpoint	•	•	•	•
Edit Registry Keys and Values	•	•	•	•
Network Isolation	•	•	•	•
User Isolation	•			
Execution Prevention	•	•	•	•
Block Processes from Communication	•	•	•	•
Uninstall Services		•	•	•
System Restoration	•	•	•	•
System Imaging		•	•	•
Patching	•	•	•	
Guided Response Available	•	•	•	•
Reporting Features				
Attack Visualization	•	•	•	•
Attack Timeline	•	•		•
Attack Context	•	•	•	•
Continuous Monitoring	•	•	•	•
Running applications & process	•	•	•	•
Behaviour Monitoring (File/registry/etc..)	•	•	•	•
Whitelisting capability	•	•	•	•
Data Sharing Features				
Customizable default security policies	•	•	•	•
Customized reporting and management	•	•	•	•
Custom reporting and filtering	•	•	•	•
Report automation	•	•	•	•
Standard output format (JSON, Syslog, CEF, etc..)	•	•	•	•
Splunk & Syslog integration	•	•	•	•
Automated data export	•	•	•	•
Policy and/or signature rollback	•	•	•	•
System scanning capability	•	•	•	•
Integration with security products	•	•	•	•
Standards-based application programming interface (API) for access		•	•	•
Disaster Recovery	•	•	•	•
Audit trail support in the management console	•	•	•	•
Management to agent encryption	•	•	•	•
Encryption of data at rest	•	•	•	•
Multiple EPR system-administrator/user-focused workflow support	•	•	•	•
Enterprise recording and data storage –forensic analysis	•	•	•	•
Built-in-reporting capabilities for different user categories	•	•	•	•
Cloud marketplace support	•	•		•
Compliance reports (GDPR, PCI-DSS, etc.)	•			•
External Data Correlation				
Threat Intelligence data assimilation	•	•	•	•
SIEM		•		•
Proprietary product integration (NGFW, IPS, ...)	•		•	•
YARA Signatures	•		•	•
Support of IoC upload	•	•	•	•
Sandboxing logs	•		•	•
Scan results	•		•	•
Retrospective analysis and logs	•		•	•
Endpoint prevention product logs	•		•	•
Multi-factor authentication logs				•
Network traffic flow logs	•			•
DNS Logs	•			•
DHCP Logs				•
Support				
Is free, basic, human support for the deployment process included in the licence for 5,000 endpoint	•	•		•
Assisted training for the IT staff in portfolio	•	•	•	•
Supported languages of support	All	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese, Malay, Indonesian, Kazakh	English, French, German, Italian, Russian, Spanish	English
Total EPR Cost Structure (may vary)				
5 Years TCO - 5000 Clients (USD)	950 000	760 833	1 032 000	1 750 000

EDR Telemetry

For IT security professionals, especially those on the blue team, understanding the telemetry²⁰ capabilities of antivirus (AV) and endpoint detection and response (EDR) solutions²¹ is paramount. Telemetry offers a comprehensive view of endpoint activity, enabling a deeper grasp of security alerts. This knowledge is crucial for swift threat response and invaluable for forensic investigations, allowing teams to trace and analyse attack evolution. Telemetry also serves a proactive role, helping identify new attack vectors and the tactics, techniques, and procedures used by adversaries.

However, it goes beyond defence. Telemetry comprehension allows teams to refine configurations, reduce false positives, and optimize operations. In an era prioritizing data privacy, it's essential to ensure telemetry remains compliant with stringent regulations. Detecting potential security gaps becomes easier with telemetry insights, aiding in pinpointing areas requiring additional protection or tools. Additionally, assessing data collection's impact on system performance ensures a seamless user experience.

Armed with this data, integrating AV and EDR insights into security information and event management (SIEM) solutions becomes more seamless. Furthermore, this foundational knowledge fosters enhanced collaboration, enabling blue teams to work cohesively with other departments, such as red teams or IT operations, to bolster the organization's security posture.

This data should be readily accessible and investigated by customers when using the respective products. Some vendors transparently provide this information in their documentation²², empowering users to maximize the data/product for their defence strategies. Please note that this data pertains solely to the product/tier assessed in this report; the vendor may offer other products/tiers with additional telemetry features and support. The listed data was verified and provided by the vendors.

LEGEND	
✓	Implemented
✗	Not Implemented
~	Partially Implemented
Logs	Via Windows EventLogs (EDR is inspecting Windows event logs to collect the telemetry)
Telemetry	Via EnablingTelemetry (Additional telemetry that can be enabled easily as part of the EDR product but is not ON by default.)

²⁰ <https://kostas-ts.medium.com/edr-telemetry-project-a-comprehensive-comparison-d5ed1745384b>

²¹ https://docs.google.com/spreadsheets/d/1ZMFrD6F6tvPtF_8McC-kWrNBBec_6Si3NW6AoWf3Kbg/htmlview

²² <https://github.com/tsale/EDR-Telemetry/wiki#product-documentation-references>

Telemetry Feature Category	Sub-Category	Check Point	ESET	Kaspersky	Palo Alto Networks
Process Activity	Process Creation	✓	✓	✓	✓
	Process Termination	✓	✓	✓	✓
	Process Access	✓	~	✗	✓
	Image/Library Loaded	✓	✓	✓	✓
	Remote Thread Creation	✓	✓	✗	✓
	Process Tampering Activity	✓	✗	✗	✓
File Manipulation	File Creation	✓	~	✓	✓
	File Opened	✓	✗	✓	✓
	File Deletion	✓	✓	Telemetry	✓
	File Modification	✓	✓	Telemetry	✓
	File Renaming	✓	✓	✓	✓
User Account Activity	Local Account Creation	✓	✓	Logs	✓
	Local Account Modification	✓	✓	Logs	✓
	Local Account Deletion	✓	✓	Logs	✓
	Account Login	✓	✓	Logs	✓
	Account Logoff	✓	✓	Logs	✓
Network Activity	TCP Connection	✓	✓	✓	✓
	UDP Connection	✓	✗	✓	✓
	URL	✓	✓	✓	✓
	DNS Query	✓	✓	Telemetry	✓
	File Downloaded	✓	~	~	✓
Hash Algorithms	MD5	✓	✓	✓	✓
	SHA256	✓	✓	✓	✓
	IMPHASH	✗	✗	✗	✗
Registry Activity	Key/Value Creation	✓	✓	✓	✓
	Key/Value Modification	✓	✓	✓	✓
	Key/Value Deletion	✓	✓	✓	✓
Schedule Task Activity	Scheduled Task Creation	✓	✗	~	✓
	Scheduled Task Modification	✓	✗	~	✓
	Scheduled Task Deletion	✓	✗	~	✓
Service Activity	Service Creation	✓	✗	~	✓
	Service Modification	✓	✗	~	✓
	Service Deletion	✗	✗	~	✓
Driver/Module Activity	Driver Loaded	✗	✓	✓	✓
	Driver Modification	✗	✗	✗	✓
	Driver Unloaded	✗	✗	✗	✗
Device Operations	Virtual Disk Mount	✓	✗	✗	✓
	USB Device Unmount	✗	✗	✗	✓
	USB Device Mount	✗	✗	✗	✓
Other Relevant Events	Group Policy Modification	✗	✗	Logs	✓
Named Pipe Activity	Pipe Creation	✓	✓	✗	✓
	Pipe Connection	✓	✗	✗	✓
EDR SysOps	Agent Start	✓	✗	✗	✓
	Agent Stop	✓	✗	✗	✓
	Agent Install	✓	✓	✗	✓
	Agent Uninstall	✓	✓	✗	✓
	Agent Keep-Alive	✓	✓	✗	✓
	Agent Errors	✓	✓	✗	✓
WMI Activity	WmiEventConsumerToFilter	✓	✓	✗	✓
	WmiEventConsumer	✓	✓	✗	✓
	WmiEventFilter	✓	✓	✗	✓
BIT JOBS Activity	BIT JOBS Activity	~	✗	✗	✗
PowerShell Activity	Script-Block Activity	✓	✓	✓	✓

Overview of EDR technologies

In the dynamic field of cybersecurity, IT security professionals need a deep understanding of antivirus (AV/EPP) and endpoint detection and response (EDR) systems, which are crucial for comprehensive defence strategies. One key aspect is understanding how different AV and EDR systems implement essential technologies²³. The following information offers a high-level overview of these technologies, highlighting their importance in the ever-changing cybersecurity landscape. These technologies encompass the Antimalware Scan Interface (AMSI), User-Mode Hooking, Callbacks, and Kernel Drivers.

1. **Antimalware Scan Interface (AMSI):** AMSI in Windows is an API set designed for enhanced malware detection. Integrated into components such as PowerShell, Windows Script Host, and .NET, it intercepts scripts post-deobfuscation at runtime. AMSI communicates directly with the system's antimalware solution, forwarding content for analysis. As an interface, it's agnostic to the specific antimalware vendor. Its integration ensures real-time threat detection, even for dynamically executed content.
2. **User-Mode Hooking:** User-mode hooking intercepts function calls in application-level processes in Windows. By overwriting a function's start, calls are redirected to a custom function. For instance, an EDR might hook `CreateFileW` in `kernel32.dll`, redirecting it to its own DLL. When an application uses `CreateFileW`, it's first processed by the EDR's function, allowing real-time monitoring or restrictions before proceeding with the original call.
3. **Callbacks:** EPP/EDR solutions leverage kernel callback routines for deep system monitoring. These routines notify registered callbacks when specific OS events occur. By tapping into these events, EPPs/EDRs observe real-time system behaviour. For instance, an EPP/EDR might monitor process creation events. When a new process starts, the callback inspects its details and origin. This allows the EPP/EDR to quickly detect, assess, and respond to potential threats.
4. **Kernel Drivers:** EPP/EDR solutions employ kernel drivers to deeply integrate with the operating system for advanced threat mitigation. Minifilter drivers, part of the Windows Filter Manager, allow EPP/EDR tools to monitor, modify, or block operations on files and data streams. This is crucial for real-time scanning and access restrictions. ELAM (Early Launch Anti-Malware) drivers, on the other hand, start early during the boot process, ensuring that only legitimate, signed drivers are loaded, thereby preventing rootkits or bootkits from compromising the system. Collectively, these drivers ensure comprehensive protection from boot-up to system operation.

This information equips IT security professionals with valuable insights for making informed decisions about cybersecurity solutions. Whether you need a comprehensive understanding or a quick reference, these insights empower you to navigate the complex world of IT security effectively.

It's important to note that these are just some of the technologies employed in modern cybersecurity, and others may also be included in the arsenal of IT security professionals. The absence or presence of a certain technology does not necessarily mean that a product is worse or better. The effectiveness of a cybersecurity strategy depends on its holistic approach and adaptability to evolving threats. The listed data was verified and provided by the vendors.

²³ <https://kwcsec.gitbook.io/the-red-team-handbook/techniques/defense-evasion/basics/iocs/high-level-overview-of-edr-technologies>

EDR Technology	Description	Check Point	ESET	Kaspersky	Palo Alto Networks
Antimalware Scan Interface (AMSI)	This is a standard interface that allows applications and services to integrate with any antimalware product present on a machine.	✓	✓	✓	✓
Event Tracing for Windows (ETW)	This is a mechanism for tracing and logging events that are raised by both user-mode applications and kernel-mode drivers.	✓	✓	✓	✓
Microsoft Threat Intelligence (EtwTi)	This is a mechanism for tracing and logging events using Microsoft Threat Intelligence.	✗	✓	✓	✓
User Space API-Hooking	This is a technique used to intercept API function calls in user space. This can be used by EPP/EDR solutions to monitor and potentially block suspicious behaviour.	✓	✓	✓	✓
Kernel Space API-Hooking	Similar to user space API hooking, but this intercepts API function calls in the kernel space.	✗	✗	✓	✓
Kernel Callback Routines	These are functions that the kernel calls when certain events or conditions occur. EPP/EDR solutions can use these to monitor system events.	✗	✓	✓	✓
Filter Driver	This is a type of driver used to monitor and potentially modify the behaviour of device drivers. EPP/EDR solutions may use this to monitor for suspicious device behaviour.	✗	✓	✓	✓
Minifilter Driver	This is a specific type of filter driver that can be used to monitor and potentially modify the behaviour of file system operations.	✓	✓	✓	✓
Early Launch Antimalware (ELAM) Driver	This is a driver that starts early in the boot process to scan drivers for malware before they're loaded.	✓	✓	✓	✓

Product Configurations and Settings

In business environments, and with business products in general, it is usual for products to be configured by the system administrator, in accordance with vendor's guidelines. Therefore, we asked vendors to request us to implement any changes they wanted to the default configuration of their respective products. Results presented in this test were only accomplished by applying the respective product configurations as described here.

The configurations were applied together with the engineers of the respective vendors during setup. This configuration is typical in enterprises, which have their own teams of security staff looking after their defences. It is common for products of this kind that vendor experts assist companies on the deployment and configuration best suited for the type of enterprise.

Below we have listed relevant non-default settings (i.e. settings used by the vendor for this test).

Check Point: In "Web & Files Protection" and "Behavioral Protection" everything was set on "Prevent". "Anti-Exploit Mode" was set to "Prevent". In "Analysis & Remediation", the "Protection mode" was set to "Always", "Enable Threat Hunting" was set to "On", and "Attack Remediation" was set to "Medium & High". In the "Advanced Settings", "File remediation" was set to "Quarantine" and "Terminate". All settings were set to "Connected Mode".

ESET: All "Real-Time & Machine Learning Protection", "Potentially Unwanted Applications", "Potentially Unsafe Applications" and "Suspicious Applications" settings were set to "Aggressive". "Runtime packers" and "Advanced heuristics" enabled for "ThreatSense". In "Cloud-based Protection", "LiveGuard", "LiveGrid Feedback System" and "LiveGrid Reputation System" were set to "On". The "Detection threshold" for "LiveGuard" was set to "Suspicious", the "Proactive protection" was set to "Block execution until receiving the analysis result" and the "Maximum wait time for the analysis result" was set to "5 min". "Automatic submission of suspicious samples" enabled for all file types. "Password protect settings" enabled. In "ESET Inspect", all detection rules and exclusions were enabled, except the "optional" and "[Y*]" ones.

Kaspersky: "Kaspersky Security Network (KSN)" was enabled. "Adaptive Anomaly Control" was disabled. The sandbox feature was not enabled.

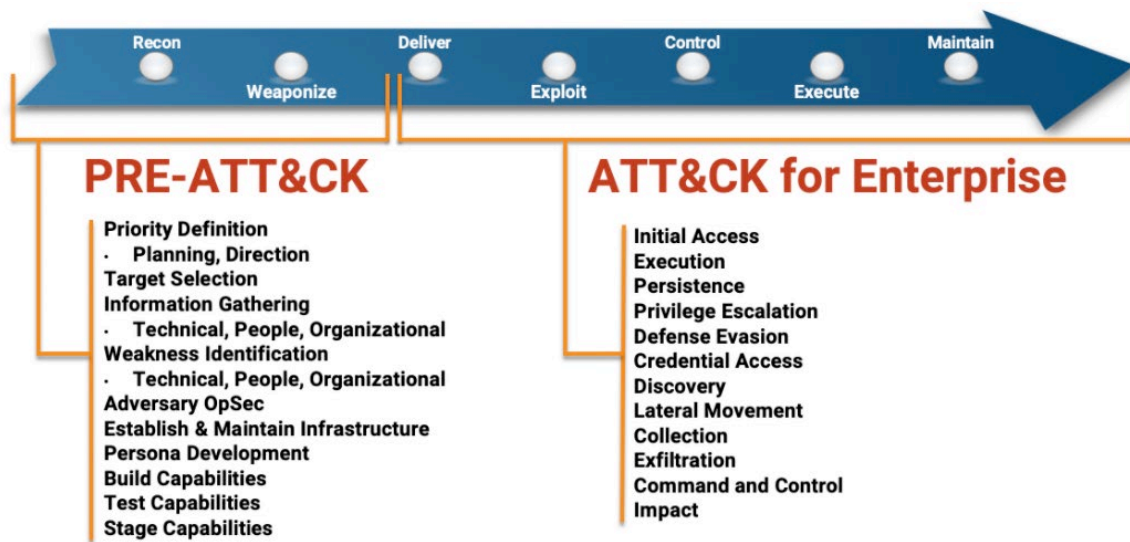
Palo Alto Networks: Under "Agent settings", in "XDR Pro Endpoints", "XDR Pro Endpoint Capabilities" were enabled. Under "Malware Profile", "Portable Executable and DLL examination", "Behavioral Threat Protection" and "Ransomware Protection" were set to "Quarantine". "Treat Grayware as Malware" was enabled.

Vendor A - H: Non-default settings were used.

EPR Test Methodology

Endpoint Prevention Response vs MITRE ATT&CK Framework

This EPR product report is a comprehensive validation of features, product efficacy and other relevant metrics to guide your risk assessment. A total of 50 scenarios were executed against real-world enterprise use-cases. These scenarios comprised several prevention and detection workflows operating under normal operational environments by different user personas. The results for the validation can be efficiently and effectively mapped to the MITRE ATT&CK® Platform²⁴ and NIST platform, so that it becomes easier to operationalize the risk regarding a specific endpoint.



MITRE ATT&CK for Enterprise vs Seven Stage Cyber Attack LifeCycle²⁵

AV-Comparatives has developed an industry-changing paradigm shift by defining a real-world EPR methodology reflecting the everyday reality of enterprise use cases and workflows to be used for mapping the kill-chain visibility to the MITRE ATT&CK framework.

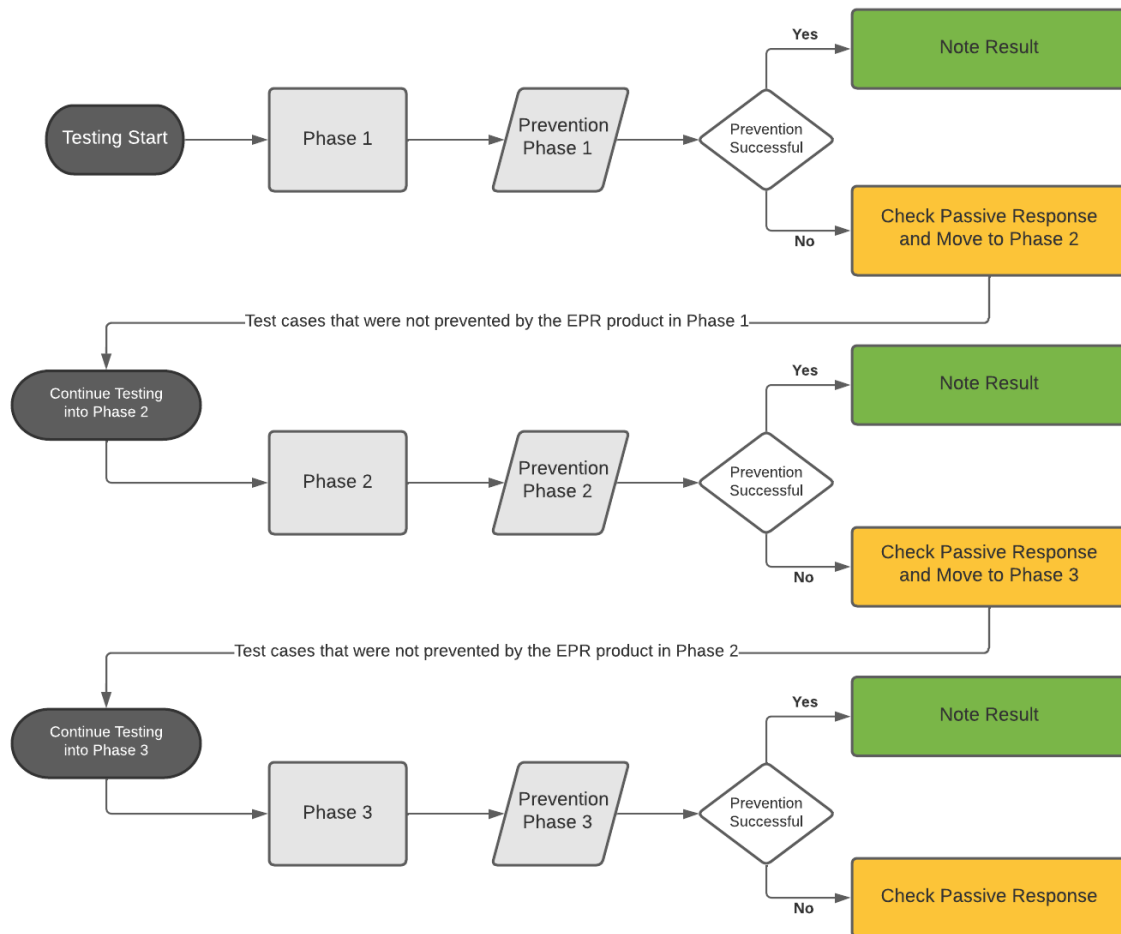
As illustrated in the graphic on the next page, we moved away from “atomic” testing, i.e. tests that only look at a particular component of the ATT&CK framework, and instead evaluated the EPR products from the context of the entire attack kill-chain, with workflows interconnecting at every stage from the initial execution to final data exfiltration/sabotage.

²⁴ © 2015-2023, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

²⁵ Source: <https://attack.mitre.org/resources/enterprise-introduction/>

EPR Testing Workflow

The graphic below provides a simplified overview of the test procedure used:



Enterprise EPR Workflow Overview

Prevention (Active Response)

The best way to respond to any threat is by preventing and effectively reporting on it as soon as possible. AV-Comparatives defines prevention as an automated, active response that kicks in 24/7, 365 days a year, without the need for human intervention, but with quantifiable metrics and reporting data points that can be leveraged for effective analysis.

An EPR product should be able to initially identify and prevent a threat on a compromised machine. The incident should be detected, identified, correlated, and remediated from a single pane of glass (centralized management system) through an effective passive response strategy (partially/fully automated) ideally in real time. Furthermore, the system administrator should be able to classify and triage a threat based on the data collection and analysis, and be able to close out a response using the EPR product with a specific workflow.

An active response, as defined in this test, is an effective response strategy that provides detection with effective prevention and reporting capabilities. This should all be done in an automated way with no manual intervention. This can be done through a multitude of technologies and mechanisms, for example: signature-based models, behaviour-based models, ML-based models, transaction rollbacks, isolation-based mechanisms, and so forth. This definition is technology-agnostic because it focuses on the outcomes of the various system-administrator workflows and scenarios, and not on the technology used to prevent, detect or respond to it.

Detection (Passive Response)

Passive response, as defined in this test, is a set of response mechanisms offered by the product with cohesive detection, correlation, reporting and actionable capabilities. Once an attacker is already inside the enterprise environment, traditional response mechanisms kick in, for example IOC and IOA correlation, external threat intel and hunting. AV-Comparatives defines these response mechanisms as Passive Response. The precondition for passive response is the detection of a potential threat by EPR products.

EPR products are typically expected to prevent initial and ongoing attacks without having to triage, while offering active response and reporting capabilities. If the attack is missed or not prevented, EPR products should then be able to assess and respond to attacks, thus providing lesser burden on resources (human/automation) and providing better ROI in the long run.

The range of available response capabilities of an EPR product is extremely important for organizations that need to review threats/compromises in multiple machines across multiple locations. An EPR product should be able to query for specific threats using the intelligence data provided to the system administrator. Once they have been identified, the system administrator should be able to use the EPR product to initiate responses based on the type of infection. AV-Comparatives expects EPR products to have non-automated or semi-automated passive response mechanisms.

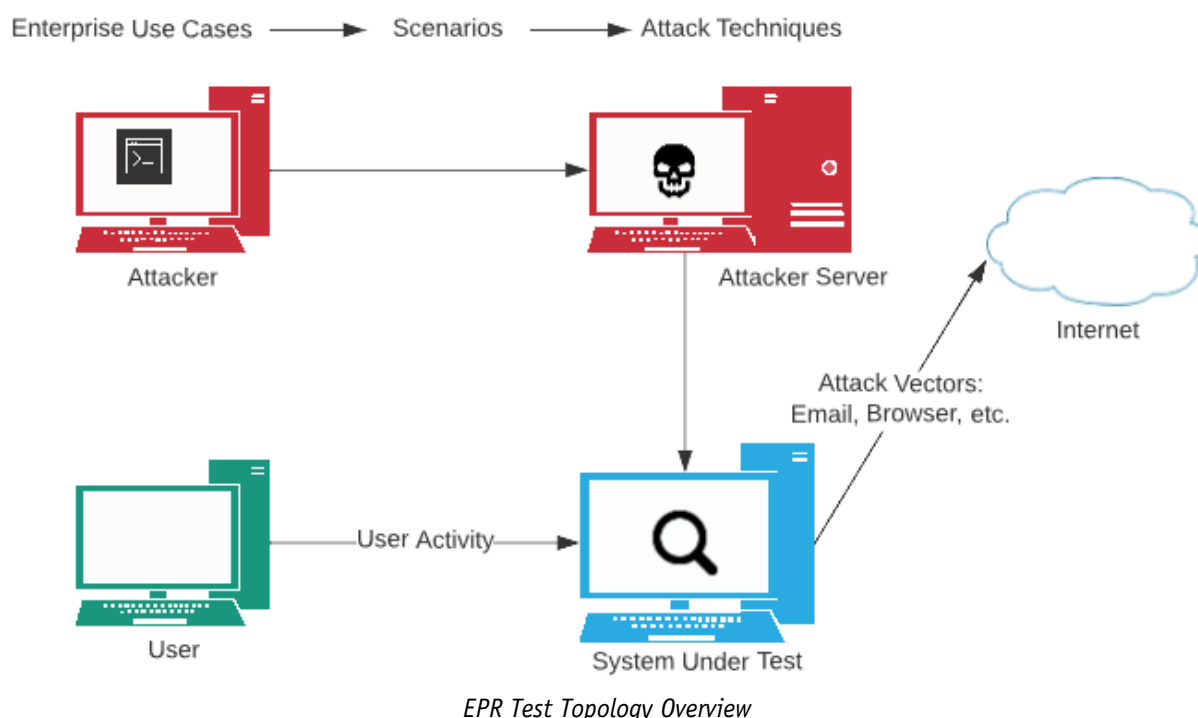
Correlation of Process, Endpoint and Network

The EPR product should be able to identify and respond to threats in one or more of the following ways:

- Response based on successful identification of attack via the product's user interface (UI) that lists attack source (http[s]/IP-based link) that hosts compromised website/IP).
- Exploit identification (based upon the CVE or generic detection of threat)
- Downloaded malware file
- Malware process spawning
- Command and control activity as part of the single chain of attacks

EPR Validation Overview

AV-Comparatives have come up with the following topology and metrics to accurately assess the capabilities of endpoint prevention and response (EPR) products.



All the tested vendors' EPR products were deployed and evaluated in a standalone mode, with each vendor actively involved in the initial setup, configuration, and baselining aspects. AV-Comparatives evaluated a list of 50 scenarios, as often requested by analysts and enterprises, highlighting several enterprise-centric use cases. Every vendor was allowed to configure their own product, to the same extent that organizations are able to do when deploying it in their infrastructure. The details of the configurations are included at the beginning of this report.

Because this methodology is tailored towards the prevention, detection and response capabilities, all vendors activated their prevention and protection capabilities (ability to block), along with detection and response, so that they emulate the real-world enterprise-class capabilities of these products.

The testing supported EPR product updates and configuration changes made by cloud management console or local area network server. We went through and executed all test scenarios from beginning to end, to the greatest extent possible.

Test Objective

The following assessment was made to validate if the EPR endpoint security product was able to react appropriately to each scenario.

- In which attack phase did the prevention/detection occur? Phase 1 (Endpoint Compromise and Foothold), Phase 2 (Internal Propagation) or Phase 3 (Asset Breach)?
- Did the EPR product provide us with the appropriate threat classification and threat triage, and demonstrate an accurate threat timeline of the attacks with relevant endpoint and user data?
- Did the EPR product incur any additional costs due to imperfect Operational Accuracy or workflow delays?

Targeted Use-Cases

The sequence of events emulated was an enterprise-based scenario where in the system-level user received a file in an email attachment and executed it. In some cases, the emails were benign, while in others they were not. The malicious email attachments, if successfully executed, allowed an attacker to get a foothold inside the environment and take additional steps to act upon their objectives.

During testing, we logged into the EPR product management and the individual test system consoles, to observe, analyse and document what kind of activity is recorded by the product. For instance, if there is an attack, are there any alerts or events, and are these true positives or true negatives?

For true positive alerts, we further investigated whether the subsequent response in terms of event correlation, triages, threat classification and threat timeline were provided to the system administrator in a timely and clear way. We tested the responses as available by products under the test.

The test was conducted in summer 2023, and used an attacker-driven mindset as the attack progressed through the attack nodes to finally meet its objective. User activities were simulated throughout the test such that they were as close to a real-life environment as possible.

All the attacks were crafted using open-source and commercial tools²⁶/frameworks, and were developed using in-house expertise. The reason why we included commercial C2 frameworks²⁷ is that these are frequently misused by attackers²⁸ in real-life APTs; not using them would cause a „blind spot“ and lead to a false sense of security. Due to license agreement restrictions, we took measures to prevent samples created by commercial C2 frameworks from being distributed to the EPR vendors. These restrictions are made to prevent vendors from focussing on the tools instead of the techniques.

To illustrate the test procedure, we provide below an example of how a typical targeted attack might work. The attacker sends a script payload (containing some defence evasion techniques such as DLL sideloading) via a phishing mail to Network User A on Workstation A. After getting a foothold in the targeted network with the User Account A, internal discovery is performed. This involves enumerating user privileges, user groups, installed security products etc. Through this process it can be seen that the compromised User Account A has access to the C\$ share on Workstation B, meaning that the account has local admin privileges on this workstation. With the knowledge gained from internal discovery, the attacker moves laterally from Workstation A to Workstation B. They then continue with internal discovery on Workstation B. This enables them to find a network administrator's open user session on Workstation B. To take advantage of this, the attacker dumps the LSASS process, and is thus able to steal the administrator's credentials. After doing this, they discover that the compromised administrator account has access to Server 1. The attacker then uses this compromised admin account to move laterally from Workstation B to Server 1, and then compromise this server. Here they perform further internal discovery, and also use some defence evasion techniques to bypass the installed security product (e.g. by patching AMSI and ETW). At the end of this procedure, they are able to identify credit-card data on Server 1, which they extract via an open C2 channel.

²⁶ <https://attack.mitre.org/software/>

²⁷ <https://redcanary.com/threat-detection-report/trends/c2-frameworks/>

²⁸ https://www.trendmicro.com/en_us/research/22/j/black-basta-infiltrates-networks-via-qakbot-brute-ratel-and-coba.html

About this test

AV-Comparatives' Endpoint Prevention and Response (EPR) Test represents the pinnacle of complexity and challenge within the realm of enterprise security product assessments. Having the product named in the main comparative EPR report is at the vendor's discretion. Some companies, especially those heavily reliant on marketing, may choose to remain anonymous if their products fail to meet the expectations they have marketed in this rigorous and realistic testing. We tested the products with configurations as suggested by the vendors and verified them together with the vendors before the test started.

Our Expertise: We've honed our expertise over two decades to deliver precise assessments of security solutions. Unlike some imitations attempted by other testing labs, our experience uniquely positions our test to provide an accurate portrayal of capabilities.

Complexity and Realism: This challenging test mirrors realistic scenarios but is inherently manual due to its complexity, making it cost-intensive to run. The methodology focuses on prevention and response capabilities. Vendors are advised to enable prevention and protection features and configure detection effectively, all while avoiding high costs due to poor operational accuracy or workflow delays. Costs arising from imperfect operational accuracy and workflow delays are taken into account. Additionally, telemetry-based threat-hunting is not within the scope of this test.

Comprehensive Assessment: The test phases consist of attack tactics commonly encountered by enterprises. Our EPR test spans the entire attack chain, encompassing real-world attack tactics and techniques, from initial intrusion and internal propagation to data exfiltration and actual harm to the target system or network.

Real-World Conditions: To maintain the integrity of the assessment, vendors were not informed in advance of the exact test timing or attack specifics, simulating real-world conditions where attackers strike without warning. Consequently, products must ensure continuous protection rather than optimizing solely for evaluation purposes.

Test Scenarios: We create test scenarios by utilizing publicly available cyber threat intelligence²⁹ to reflect the current threat landscape. These scenarios are then mapped to a spectrum of ATT&CK techniques, simulating diverse actions and providing valuable insights into the product's effectiveness against complex attacks. We've used 50 test scenarios inspired by tactics and techniques employed by distinct APT groups³⁰, used to be attributed to China (e.g., APT3, APT41, Ke3chang, Threat-Group-3390), Russia (e.g., APT28, APT29, Sandworm, Turla, WizardSpider), Iran (e.g., APT33, APT39, OilRig), North Korea (e.g., APT37, APT38, Kimsuky), and others (e.g., Carbanak, FIN6, FIN7). Please note that our test scenarios draw inspiration from these APT groups without replicating their actions (nor are they limited to them), although there may be overlap in the techniques, subtechniques, and tools used.

Comprehensive Insight: To obtain an overall picture of the protection and response capabilities of any of the tested EPR products, readers should also consider the results of the other tests in AV-Comparatives' Enterprise Main-Test Series³¹.

²⁹ <https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf>

³⁰ <https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/>

³¹ <https://www.av-comparatives.org/enterprise/>

Copyright and Disclaimer

This publication is Copyright © 2023 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(October 2023)

Icons: feathericons.com