Independent Tests of
Anti-Virus Software

Endpoint Prevention and Response
EPR Comparative Report

TEST PERIOD: JUNE - AUGUST 2022
LAST REVISION: 24TH OCTOBER 2022

WWW.AV-COMPARATIVES.ORG

Content

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 10 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, such as isolating an endpoint from the network, restoring it from a system image, or editing the Windows Registry, was noted. Likewise, each product's ability to investigate the nature of an attack was examined. 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. On the basis of this, we have certified products on three levels. These are, from highest to lowest: Strategic Leaders, CyberRisk Visionaries, and Strong Challengers.

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 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.

Bitdefender	cisco	eset	kaspersky	paloalto NETWORKS
Vendor A	Vendor B	Vendor C	Vendor D	Vendor E

The following products were tested by AV-Comparatives:

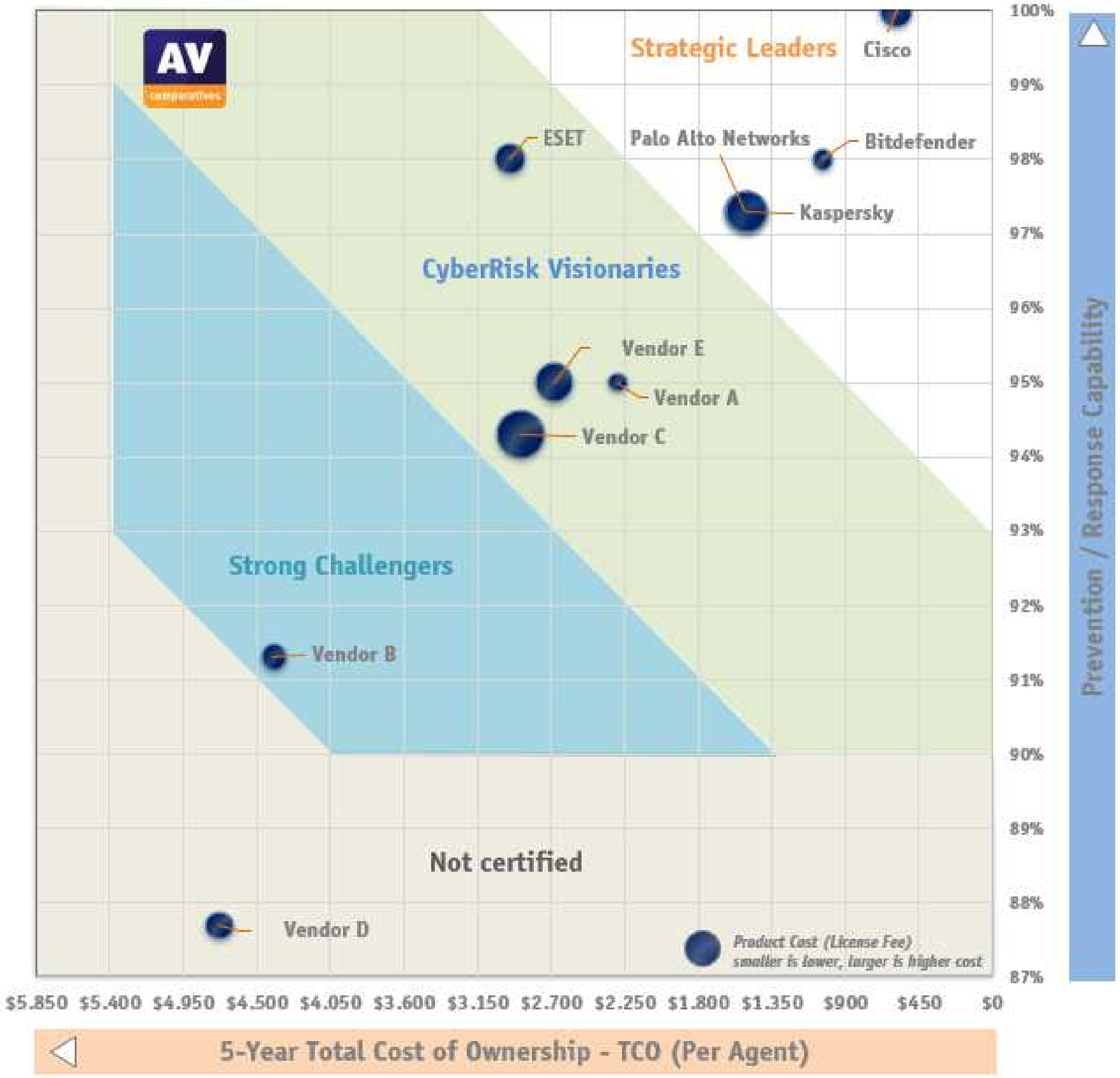
Vendor	Product	Version
Bitdefender	GravityZone Business Security Enterprise	7.5
Cisco	Secure Endpoint Essentials	7.5
ESET	PROTECT Enterprise Cloud	9.0
Kaspersky	Endpoint Detection and Response Expert (on-premises)	4.0
Palo Alto Networks	Cortex XDR Pro	7.7
Vendor A	Product A	n/a
Vendor B	Product B	n/a
Vendor C	Product C	n/a
Vendor D	Product D	n/a
Vendor E	Product E	n/a

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:

Bitdefender:	https://www.av-comparatives.org/wp-content/uploads/2022/10/EPR_Bitdefender_2022.pdf
Cisco:	https://www.av-comparatives.org/wp-content/uploads/2022/10/EPR_Cisco_2022.pdf
ESET:	https://www.av-comparatives.org/wp-content/uploads/2022/10/EPR_ESET_2022.pdf
Kaspersky:	https://www.av-comparatives.org/wp-content/uploads/2022/10/EPR_Kaspersky_2022.pdf
Palo Alto Networks:	https://www.av-comparatives.org/wp-content/uploads/2022/10/EPR_PaloAlto_2022.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
Bitdefender	$100	98.0%	98.0%	**98.0%**	None	Low	**$1,013**
Cisco	$158	100%	100%	**100%**	Low	None	**$587**
ESET	$149	96.7%	99.3%	**98.0%**	Moderate	None	**$2,946**
Kaspersky	$206	97.3%	97.3%	**97.3%**	Low	None	**$1,505**
Palo Alto Networks	$210	96.7%	98.0%	**97.3%**	Low	None	**$1,509**
Vendor A	$90	94.0%	96.0%	**95.0%**	Low	None	**$2,293**
Vendor B	$130	91.3%	91.3%	**91.3%**	Low	None	**$4,394**
Vendor C	$249	92.7%	96.0%	**94.3%**	Low	None	**$2,888**
Vendor D	$134	84.7%	90.7%	**87.7%**	Low	None	**$4,730**
Vendor E	$190	94.7%	95.3%	**95.0%**	Low	Low	**$2,601**

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

Explanation of the EPR CyberRisk Quadrant

Strategic Leaders

These are EPR products that have a very high return on investment, and thus provide very low total cost of ownership (TCO). This is due to exceptional technical capabilities, combined with reasonable costs. These products generally demonstrated outstanding prevention, detection, response and reporting capabilities, combined with optimal operational and system-administrator workflow features.

CyberRisk Visionaries

These EPR products offer a high return on investment, providing low TCO by offering excellent 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 that 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.

EPR CyberRisk Quadrant Overview

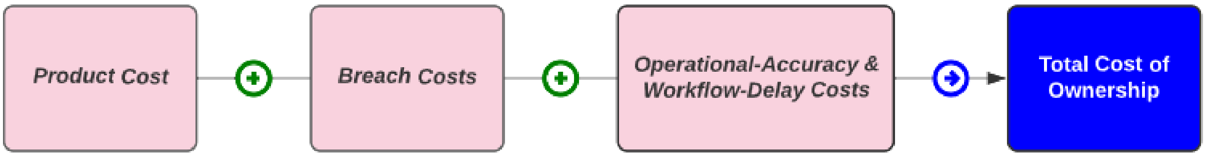
We have developed an Enterprise EPR CyberRisk Quadrant that factors in the effectiveness of each product at preventing breaches, the calculated savings resulting from this, the purchase costs of the product, and the product's accuracy costs (incurred due to false positives).

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 4.35 million[1]. 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 4.35 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 Institute[2] estimated that companies waste roughly USD 1.3 million per year due to inaccurate or erroneous intelligence. To allow for inflation over the last seven years, a reasonable estimate for 2022 would be USD 1.43 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.



Total Cost of Ownership Formula

[1] https://www.ibm.com/security/data-breach

[2] 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 2022 is given below:

1. If there was active response 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.

In the 2020 and 2021 EPR Tests, as well as this year, we observed the “Time to Prevent” and “Time to Respond” over a period of 24 hours. However, in none of the cases with any of the products did the initial values change over the 24 hours period. We note that data breaches in large organisations are typically discovered weeks or even months later, so including the extra day to our study had virtually no effect. Consequently, we have decided not to consider this metric anymore.

We continually strive to make the metrics used in this test relevant to the current situation. We listened to feedback from enterprises, and took this into account where appropriate (such as taking Operational Accuracy and Workflow Delay costs into account and removing unneeded metrics).

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

For this test, we are giving three different levels of certification to qualifying products, based on their respective positions in the Enterprise CyberRisk Quadrant™. To be certified, a product must achieve an average of at least 90% for combined Active and Passive Response, and not cause high costs. Certification levels are (from high to low): Strategic Leader, CyberRisk Visionary, Strong Challenger.

The table below shows the levels reached by the tested products in AV-Comparatives’ 2022 EPR Test:

AV comparatives Certified EPR 2022 Strategic Leader	Bitdefender kaspersky	CISCO paloalto NETWORKS
AV comparatives Certified EPR 2022 CyberRisk Visionary	eset Vendor C	Vendor A Vendor E
AV comparatives Certified EPR 2022 Strong Challenger	Vendor B	
NOT CERTIFIED	Vendor D	

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 Access[3]: 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.

Execution[4]: 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.

Persistence[5]: 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.

[3] https://attack.mitre.org/tactics/TA0001/
[4] https://attack.mitre.org/tactics/TA0002/
[5] https://attack.mitre.org/tactics/TA0003/

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

Scenario	Description	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
1	PowerShell Empire - Obfuscated PowerShell in-memory	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓
2	PowerShell Empire - AMSI bypass with in-memory payload	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✗ ✓
3	PowerShell Empire - MS Word Macro	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
4	PowerShell Empire - WMIC/XSL Oneliner	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✗ ✗	✓ ✓
5	PowerShell Empire - Rundll32 Encrypted DLL	✗ ✗	✓ ✓	✓ ✓	✗ ✗	✗ ✗	✗ ✗	✓ ✓	✓ ✓	✓ ✓	✗ ✗
6	PowerShell Empire - Masqueraded PowerShell binary	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✗ ✗	✗ ✗	✓ ✓	✓ ✓	✗ ✗	✗ ✗
7	PowerShell Empire - VBScript	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓
8	PowerShell Empire - Shortcut Payload	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓
9	PowerShell Empire - MS Excel Macro	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✗ ✗
10	PowerShell Empire - JavaScript	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
11	PowerShell Empire - MS Word Macro	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✓ ✓	✗ ✗
12	PowerShell Empire - JavaScript MSIexec	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
13	PowerShell Empire - JavaScript Excel	✓ ✓	✓ ✓	✗ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✓ ✓	✗ ✗
14	PowerShell Empire - Batch File	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✗ ✗	✓ ✓
15	PowerShell Empire - Obfuscated VBScript	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓
16	Covenant - Obfuscated PowerShell from file	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓	✓ ✓
17	Covenant - AMSI bypass with a PowerShell payload from file	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
18	Covenant - Obfuscated Binary	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
19	Covenant - WMIC/XSL Oneliner	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✗ ✗	✗ ✗	✗ ✓	✗ ✗	✓ ✓
20	Covenant - PowerShell Oneliner	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
21	Covenant - Rundll32	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
22	Covenant - Masqueraded Binary	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
23	Covenant - Encrypted Binary	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✓	✓ ✓
24	Covenant - JavaScript MSIexec	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
25	Covenant - MS Office Macro: Excel	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✗ ✗	✓ ✓	✓ ✓
26	Covenant - Staged JavaScript	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
27	Covenant - Batch File Stager	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓
28	Covenant - HTML Help File	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓	✓ ✓

29	Covenant - Staged Binary	🛡✎	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎
30	Covenant - JavaScript	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
31	Metasploit Framework - Obfuscated PowerShell in-memory	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
32	Metasploit Framework - AMSI bypass with PowerShell payload in-memory	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
33	Metasploit Framework - MS Word Macro	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
34	Metasploit Framework - Encrypted HTA	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
35	Metasploit Framework - VBScript	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
36	Metasploit Framework - VBA-EXE	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
37	Metasploit Framework - HTA	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎
38	Metasploit Framework - Default Binary	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎
39	Metasploit Framework - Batch File Stageless	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎
40	Metasploit Framework - Batch File Stager	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
41	BRc4 - AMSI bypass and ETW patching combined with a PowerShell payload in-memory	⊘☒	🛡✎	⊘✎	🛡✎	🛡✎	⊘✎	⊘☒	⊘☒	⊘☒	⊘☒
42	BRc4 - Rundll32	🛡✎	🛡✎	⊘☒	🛡✎	🛡✎	🛡✎	⊘☒	⊘✎	⊘☒	🛡✎
43	BRc4 – Stageless Binary	⊘☒	🛡✎	⊘✎	🛡✎	🛡✎	⊘☒	🛡✎	⊘☒	⊘✎	🛡✎
44	BRc4 - MS Excel Macro	🛡✎	🛡✎	⊘✎	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎	🛡✎	🛡✎
45	BRc4 - Batch File Stager	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	⊘☒	🛡✎	🛡✎	⊘☒
46	Metasploit Framework - Staged PowerShell	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
47	Metasploit Framework - Encrypted MS Word Macro	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
48	Metasploit Framework - Obfuscated HTA	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
49	Metasploit Framework - MSI	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎
50	Metasploit Framework - Stageless HTA	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎

Active and Passive Response for Phase 1

🛡 Active response / prevention ✎ Passive response / detection
⊘ No active response / no prevention ☒ 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 Escalation[6]: 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 Evasion[7]: 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 Access[8]: 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.

Discovery[9]: 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 Movement[10]: 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.

[6] https://attack.mitre.org/tactics/TA0004/
[7] https://attack.mitre.org/tactics/TA0005/
[8] https://attack.mitre.org/tactics/TA0006/
[9] https://attack.mitre.org/tactics/TA0007/
[10] https://attack.mitre.org/tactics/TA0008/

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

Scenario	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
1	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
2	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	🛡✎
4	✓	✓	✓	✓	✓	✓	🛡✎	✓	🛡✎	✓
5	🛡✎	✓	✓	🛡✎	🛡✎	🛡✎	✓	✓	✓	🛡✎
6	✓	✓	✓	🛡✎	🛡✎	🛡✎	✓	✓	🛡✎	🛡✎
7	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
8	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
9	✓	✓	✓	🛡✎	✓	✓	✓	🛡✎	✓	🛡✎
11	✓	✓	✓	🛡✎	✓	✓	🛡✎	✓	✓	🛡✎
13	✓	✓	🛡✎	✓	✓	✓	🛡✎	✓	✓	🛡✎
14	✓	✓	✓	✓	✓	✓	🛡✎	✓	🛡✎	✓
15	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
16	✓	✓	✓	✓	🛡✎	✓	✓	🛡✎	✓	✓
19	✓	✓	✓	✓	🛡✎	🛡✎	🛡✎	🛡✎	🛡✎	✓
23	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
25	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓	✓
29	✓	✓	✓	✓	🛡✎	✓	✓	✓	🛡✎	✓
37	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
38	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
39	✓	✓	✓	✓	✓	✓	✓	✓	🛡✎	✓
41	🛡✎	✓	🛡✎	✓	✓	⊘☒	⊘☒	🛡✎	⊘✎	🛡✎
42	✓	✓	🛡✎	✓	✓	✓	⊘☒	⊘☒	⊘✎	✓
43	🛡✎	✓	🛡✎	✓	✓	⊘☒	✓	⊘☒	⊘✎	✓
44	✓	✓	🛡✎	✓	✓	✓	🛡✎	✓	✓	✓
45	✓	✓	✓	✓	✓	✓	🛡✎	✓	✓	🛡✎

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 is asset breach. This is the stage where an attacker starts carrying out their ultimate objective. We have explained below the relevant Tactics from the MITRE ATT&CK Framework.

Collection[11]: This involves gathering the target information – assuming of course that information theft, rather than sabotage, is the object of the exercise. The data concerned could be in the form of documents, emails or databases.

Command and Control[12]: A Command-and-Control mechanism allows communication between the attacker's system and the targeted network. This means that the attacker can send commands to, or receive data from, the compromised system. Typically, the attacker will try to mask such communications by disguising them as normal network traffic.

Exfiltration[13]: Once the attacker has reached the objective of collecting the target information, they will want to copy it covertly from the targeted network to their own server. In almost all cases, exfiltration involves the use of a command-and-control infrastructure.

Impact[14]: This can be defined as the direct damage done to the targeted organisation's network. It includes the manipulation, disruption or destruction of operational systems and/or data. This might be an end in itself (sabotage), or a means of covering up data theft, by making it more difficult to investigate the breach.

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

Scenario	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
41	✓	✓	✓	✓	✓	⊘☒	⊘☒	✓	⊘☒	✓
42	✓	✓	✓	✓	✓	✓	⊘☒	⊘☒	⊘☒	✓
43	✓	✓	✓	✓	✓	⊘☒	✓	⊘☒	⊘☒	✓

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 B has 2 full unknown breaches (scenario 41 and 42). **Vendor A** and **Vendor C** each had 1 full unknown breach (scenario 43), i.e. the attack was neither prevented nor detected in any of the three phases.

[11] https://attack.mitre.org/tactics/TA0009/
[12] https://attack.mitre.org/tactics/TA0011/
[13] https://attack.mitre.org/tactics/TA0010/
[14] 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)
Bitdefender	94%	100%	100%
Cisco	100%	100%	100%
ESET	90%	100%	100%
Kaspersky	92%	100%	100%
Palo Alto Networks	90%	100%	100%
Vendor A	90%	96%	96%
Vendor B	82%	96%	96%
Vendor C	86%	96%	96%
Vendor D	66%	94%	94%
Vendor E	84%	100%	100%

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)
Bitdefender	94%	100%	100%
Cisco	100%	100%	100%
ESET	98%	100%	100%
Kaspersky	92%	100%	100%
Palo Alto Networks	94%	100%	100%
Vendor A	92%	98%	98%
Vendor B	82%	96%	96%
Vendor C	92%	98%	98%
Vendor D	72%	100%	100%
Vendor E	86%	100%	100%

Cumulative Passive Response by phases

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

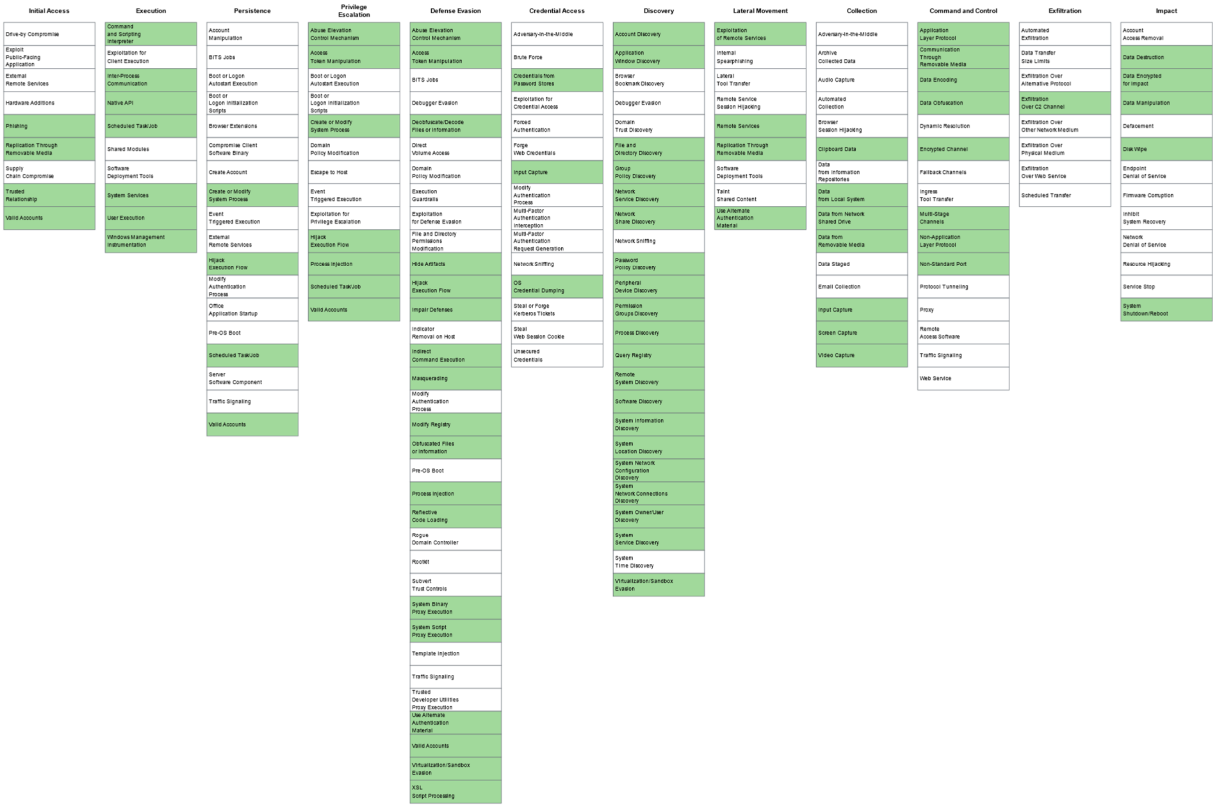
Product	Scenarios	Overall Active Prevention	Overall Passive Response	No Prevention/Response
Bitdefender	50	50	50	0
Cisco	50	50	50	0
ESET	50	50	50	0
Kaspersky	50	50	50	0
Palo Alto Networks	50	50	50	0
Vendor A	50	48	49	1
Vendor B	50	48	48	2
Vendor C	50	48	49	1
Vendor D	50	47	50	0
Vendor E	50	50	50	0

Responses per scenario

MITRE ATT&CK Matrix for Enterprise

The diagram below[15] shows the entire MITRE ATT&CK Matrix for Enterprise[16]. The column headings represent the ATT&CK Tactics[17] (aims), while the boxes below them represent the ATT&CK Techniques[18] 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.

The Tactics relate to our 3 attack Phases as follows:
Phase 1 = Initial Access, Execution, Persistence
Phase 2 = Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement
Phase 3 = Collection, Command and Control, Exfiltration, Impact



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	🟩 Command and Scripting Interpreter	Account Manipulation	🟩 Abuse Elevation Control Mechanism	🟩 Abuse Elevation Control Mechanism	Adversary-in-the-Middle	🟩 Account Discovery	🟩 Exploitation of Remote Services	Adversary-in-the-Middle	🟩 Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	🟩 Access Token Manipulation	🟩 Access Token Manipulation	Brute Force	🟩 Application Window Discovery	Internal Spearphishing	Archive Collected Data	🟩 Communication Through Removable Media	Data Transfer Size Limits	🟩 Data Destruction
External Remote Services	🟩 Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	🟩 Credentials from Password Stores	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	🟩 Data Encoding	Exfiltration Over Alternative Protocol	🟩 Data Encrypted for Impact
Hardware Additions	🟩 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Debugger Evasion	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking	Automated Collection	🟩 Data Obfuscation	🟩 Exfiltration Over C2 Channel	🟩 Data Manipulation
🟩 Phishing	🟩 Scheduled Task/Job	Browser Extensions	🟩 Create or Modify System Process	🟩 Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	🟩 Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
🟩 Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification	Direct Volume Access	Forge Web Credentials	🟩 File and Directory Discovery	🟩 Replication Through Removable Media	🟩 Clipboard Data	🟩 Encrypted Channel	Exfiltration Over Physical Medium	🟩 Disk Wipe
Supply Chain Compromise	Software Deployment Tools	Create Account	Escape to Host	Domain Policy Modification	🟩 Input Capture	🟩 Group Policy Discovery	Software Deployment Tools	Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
🟩 Trusted Relationship	🟩 System Services	🟩 Create or Modify System Process	Event Triggered Execution	Execution Guardrails	Modify Authentication Process	🟩 Network Service Discovery	Taint Shared Content	🟩 Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
🟩 Valid Accounts	🟩 User Execution	Event Triggered Execution	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	🟩 Network Share Discovery	🟩 Use Alternate Authentication Material	🟩 Data from Network Shared Drive	🟩 Multi-Stage Channels		Inhibit System Recovery
	🟩 Windows Management Instrumentation	External Remote Services	🟩 Hijack Execution Flow	File and Directory Permissions Modification	Multi-Factor Authentication Request Generation	Network Sniffing		🟩 Data from Removable Media	🟩 Non-Application Layer Protocol		Network Denial of Service
		🟩 Hijack Execution Flow	🟩 Process Injection	🟩 Hide Artifacts	Network Sniffing	🟩 Password Policy Discovery		Data Staged	🟩 Non-Standard Port		Resource Hijacking
		Modify Authentication Process	🟩 Scheduled Task/Job	🟩 Hijack Execution Flow	🟩 OS Credential Dumping	🟩 Peripheral Device Discovery		Email Collection	Protocol Tunneling		Service Stop
		Office Application Startup	🟩 Valid Accounts	🟩 Impair Defenses	Steal or Forge Kerberos Tickets	🟩 Permission Groups Discovery		🟩 Input Capture	Proxy		🟩 System Shutdown/Reboot
		Pre-OS Boot		Indicator Removal on Host	Steal Web Session Cookie	🟩 Process Discovery		🟩 Screen Capture	Remote Access Software		
		🟩 Scheduled Task/Job		🟩 Indirect Command Execution	Unsecured Credentials	🟩 Query Registry		🟩 Video Capture	Traffic Signaling		
		Server Software Component		🟩 Masquerading		🟩 Remote System Discovery			Web Service		
		Traffic Signaling		Modify Authentication Process		🟩 Software Discovery					
		🟩 Valid Accounts		🟩 Modify Registry		🟩 System Information Discovery					
				🟩 Obfuscated Files or Information		🟩 System Location Discovery					
				Pre-OS Boot		🟩 System Network Configuration Discovery					
				🟩 Process Injection		🟩 System Network Connections Discovery					
				🟩 Reflective Code Loading		🟩 System Owner/User Discovery					
				Rogue Domain Controller		🟩 System Service Discovery					
				Rootkit		System Time Discovery					
				Subvert Trust Controls		🟩 Virtualization/Sandbox Evasion					
				🟩 System Binary Proxy Execution							
				🟩 System Script Proxy Execution							
				Template Injection							
				Traffic Signaling							
				Trusted Developer Utilities Proxy Execution							
				🟩 Use Alternate Authentication Material							
				🟩 Valid Accounts							
				🟩 Virtualization/Sandbox Evasion							
				🟩 XSL Script Processing							

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

For a magnified view of the above table, please click here: https://www.av-comparatives.org/wp-content/uploads/2022/09/EPR2022.svg

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.

[15] Generated with https://mitre-attack.github.io/attack-navigator/
[16] https://attack.mitre.org/matrices/enterprise/
[17] https://attack.mitre.org/tactics/enterprise/
[18] https://attack.mitre.org/techniques/enterprise/

EPR Cost Structure

Product costs are based on list prices in USD provided by vendors at the time of the test (summer 2022). The actual cost to end users might be lower depending on e.g. negotiated discounts. In general, pricing may vary based on e.g. volume discounts, negotiated discounts, geo-location, channel, and partner margins.

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
Bitdefender GravityZone Business Security Enterprise	$500,777
Cisco Secure Endpoint Essentials	$792,000
ESET PROTECT Enterprise Cloud	$742,500
Kaspersky Endpoint Detection and Response Expert (on-premises)	$1,032,000
Palo Alto Networks Cortex XDR Pro	$1,050,000
Product A	$450,000
Product B	$650,850
Product C	$1,247,190
Product D	$669,300
Product E	$950,000

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 about a dozen 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.

		Operational Accuracy	
Group	Number of affected scenarios	*Active Response Multiplying Factor*	*Passive Response Multiplying Factor*
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 1.43 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 we knew to be clean and scenarios we knew to be 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 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*	
Bitdefender	None	None	Low
Cisco	None	Low	None
ESET	None	Moderate	None
Kaspersky	None	Low	None
Palo Alto Networks	None	Low	None
Vendor A	Low	None	None
Vendor B	Low	Low	None
Vendor C	Low	None	None
Vendor D	Low	None	None
Vendor E	Low	None	Low

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 are showing for each product the Support features, General features, Product Response, Management and Reporting, as well as IOC Integration features.

Support features

Product Name	Bitdefender GravityZone Business Security Enterprise	Cisco Secure Endpoint Essentials	ESET PROTECT Enterprise Cloud	Kaspersky Endpoint Detection and Response Expert (on-premises)	Palo Alto Cortex XDR Pro
Required installation time for 5,000 endpoints (according to the vendors)	< 12 hours	< 1 hour	< 1 hour	< 24 hours	< 2 hours
Is free, basic, human support for the deployment process included in the licence for 5,000 endpoints?	Yes	No	Yes	No	Yes
How many security staff members does the vendor recommend for day-to-day management of the product for a network of 5,000 endpoints? (according to the vendors)	at least 2	at least 1	at least 2	at least 2	at least 1
Is professionally assisted training provided for the customer's IT staff (as part of 5,000 endpoints license)?	at additional costs	at additional costs	at additional costs	at additional costs	at additional costs
Do you offer Incident Response?	No	at additional costs	at additional costs	at additional costs	at additional costs
Do you also offer a managed version (MDR) of the tested product in your portfolio?	Yes	Yes	Yes	Yes	Yes
Do you offer cybersecurity insurance, or do you partner with an insurance company?	No	via Partner	No	No	No
Which languages can be used to contact support?	English, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian, Czech, Chinese, Korean	English, Japanese, Korean, Chinese, Russian, Arabic, Spanish, Portuguese, Ukrainian, Turkish, Hebrew, German, Swedish, French, Romanian, Polish, Dutch, Italian, Hungarian, Greek, Czech, Hindi, Vietnamese, Thai, Korean, Malay, Indonesian, Kazakh	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	English, French, German, Italian, Russian, Spanish, Japanese, Chinese, Turkish, Portuguese, Arabic	English

Support features for products 1-5

Product Name	Product A	Product B	Product C	Product D	Product E
Required installation time for 5,000 endpoints (according to the vendor)	< 48 hours	< 48 hours	< 2 hours	< 24 hours	< 1 hour
Is free, basic, human support for the deployment process included in the licence for 5,000 endpoints?	No	No	Yes	No	Yes
How many security staff members does the vendor recommend for day-to-day management of the product for a network of 5,000 endpoints? (according to the vendors)	at least 2	at least 3	at least 6	at least 1	at least 1
Is professionally assisted training provided for the customer's IT staff (as part of 5,000 endpoints license)?	No	at additional costs	Yes, for 10 users	No	at additional costs
Do you offer Incident Response?	at additional costs	at additional costs	at additional costs	at additional costs	at additional costs
Do you also a managed version (MDR) of the tested product in your portfolio?	No	Yes	Yes	No	Yes
Do you offer cybersecurity insurance, or do you partner with an insurance company?	No	No	via Partner	No	No
Which languages can be used to contact support?	German, English, French, Italian, Spanish, Portuguese, Polish, Turkish, Russian	English, Russian, Portuguese, French, Italian, German, Spanish, Chinese, Japanese, Korean, Portuguese, Czech, Polish	English	English	All

Support features for products 6-10

Required installation time: this information was provided by the respective vendor. It assumes a network of 5,000 endpoints, and that optimal conditions (network connectivity, hardware, Active Directory etc.) already exist. We suggest that the times stated here should be regarded as a theoretical minimum, and that more time may well be required in practice.

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.

Security staff numbers needed: this information was provided by the respective vendor, and assumes a network of 5,000 endpoints. We suggest that staff numbers provided by vendors here might need to be (at least) doubled to allow for 24/7 operations and vacations.

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.

General features

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

Product Name	Bitdefender GravityZone Business Security Enterprise	Cisco Secure Endpoint Essentials	ESET PROTECT Enterprise Cloud	Kaspersky Endpoint Detection and Response Expert (on-premises)	Palo Alto Cortex XDR Pro
Third-party scan engine used (in addition to its own)	proprietary	Bitdefender	proprietary	proprietary	proprietary
Phishing protection for web browsers (blocking of phishing URLs)	✓	✓	✓	✓	□
Web access control (custom blacklisting of specific site categories such as adult content)	✓	□	✓	✓	✓
Device control (manage/block external drives)	□	✓	✓	✓	✓
Sandbox feature	✓	✓	✓	✓	✓
2-factor authentication: obligatory/optional/not included	Obligatory	Obligatory	Obligatory	Optional	Optional
Remote shell capability: GUI/command line/not included	command line	Not included	command line	Not included	command line
Right-click on-demand scan of files/folders	✓	✓	✓	✓	✓
Can the endpoint client be password protected from the console to prevent users changing settings?	✓	✓	✓	✓	✓
Can the endpoint client be password protected from the console to prevent users uninstalling it?	✓	✓	✓	✓	✓
Which interface languages is the endpoint client available in?	English, Spanish, German, Romanian, French	English, Japanese, Korean, Chinese	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	Russian, English, German, French, Spanish, Portuguese, Italian, Japanese, Polish, Dutch, Turkish, Arabic, Chinese, Vietnamese, Korean, Kazakh, Czech, Romanian, Hungarian	English, German, Japanese, Spanish, French, Chinese
Which interface languages is the management console available in?	English, Spanish, German, Romanian, French, Japanese, Vietnamese				English

General features for products 1-5

Product Name	Product A	Product B	Product C	Product D	Product E
Third-party scan engine used (in addition to its own)	Yes	proprietary	proprietary	proprietary	Yes
Phishing protection for web browsers (blocking of phishing URLs)	✓	✓	□	✓	✓
Web access control (custom blacklisting of specific site categories such as adult content)	✓	✓	□	✓	✓
Device control (manage/block external drives)	✓	✓	✓	✓	✓
Sandbox feature	□	□	□	□	✓
2-factor authentication: obligatory/optional/not included	Not included	Optional	Obligatory	Obligatory	Optional
Remote shell capability: GUI/command line/not included	Not included	Not included	command line	Not included	command line
Right-click on-demand scan of files/folders	✓	✓	□	✓	✓
Can the endpoint client be password protected from the console to prevent users changing settings?	✓	✓	✓	✓	✓
Can the endpoint client be password protected from the console to prevent users uninstalling it?	□	✓	✓	✓	✓
Which interface languages is the endpoint client available in?	German, English, French, Italian, Spanish, Portuguese, Polish	English, Russian, Portuguese, French, Italian, German, Spanish, Chinese, Japanese, Korean, Portuguese, Czech, Polish	English	English, German, Italian, Spanish, French	English, German, Polish, Czech, Greek, Italian, Russian, French, Japanese, Spanish, Portuguese, Ukrainian
Which interface languages is the management console available in?					English, Japanese, Chinese

General features for products 6-10

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.

Response Actions	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
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	✓	✓	□	✓	✓	□	✓	□	□	□

EPR Response actions

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.

Reporting Features	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
Threat Visibility										
Attack Visualization	✓	✓	✓	✓	✓	□	✓	✓	✓	✓
Attack Timeline	✓	✓	✓	□	✓	✓	✓	✓	□	✓
Attack Context	✓	✓	✓	✓	✓	□	✓	✓	✓	✓
System Visibility										
Continuous Monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Running applications & process	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Behaviour Monitoring (File/registry/etc..)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Whitelisting capability	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Threat & System Visibility

Data Sharing Features	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
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.)	□	□	✓	□	✓	□	✓	✓	□	✓

Data Sharing, Encryption, Discovery, Reporting, Workflow, Disaster Recovery and Third-party integration

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.

External Data Correlation	Bitdefender	Cisco	ESET	Kaspersky	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D	Vendor E
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	□	✓	□	□	✓	□	✓	□	□	□

External Data Correlation

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).

Bitdefender: "Advanced Threat Control", "Advanced Anti-Exploit", "Firewall", "Network Content Control", "Network Attack Defense" and "EDR Sensor" were enabled. "Scan mode" was set to "Local Scan". "Relay Servers" and "Default Update Servers" were deleted. "Update Ring" was set to "Fast Ring". "On-access Scanning" for archives bigger than 100MB was enabled with depth 16. "AMSI" setting and "Report analysis results to AMSI" were enabled. "Ransomware Mitigation" and "Email Traffic Scan" were activated. "HyperDetect" was enabled and set to "Block" (for network) and to "Disinfect" (for files). "Protection Level" was set to "Aggressive" for all settings on "HyperDetect". "Scan SSL" and "Sandbox Analyzer" were enabled and set to "Block".

Cisco: "Malicious Activity Prevention" and "Exploit Prevention – Script Control" were set to "Block". "Event Tracing for Windows" was enabled. "Custom Detections" for "Outbreak Control" were set to "Standard". "Connector Protection" and "Command Line logging" was enabled. "Connector Log Level" and "Tray Log Level" was set to "Debug". For "File and Process Scan", the "Verbose History" was enabled, "On Execute" was set to "Active" and the "Max Archive Scan File Size" was increased to 100MB. "Endpoint Isolation" was enabled. "Deep Scan Files" for "TETRA" was enabled and the "Content Update Interval" was set to 30 minutes. The "Detection Action" for "Network" was set to "Block" and "Terminate and Quarantine".

ESET: All "Real-Time & Machine Learning Protection", "Potentially Unwanted Applications", "Potentially Unsafe Applications" and "Suspicious Applications" settings were set to "Aggressive". 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". In "ESET Inspect", all detection rules and exclusions were enabled. "Also evaluate rules from Windows Firewall" was enabled.

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: Non-default settings were used.

Vendor B: Non-default settings were used.

Vendor C: Non-default settings were used.

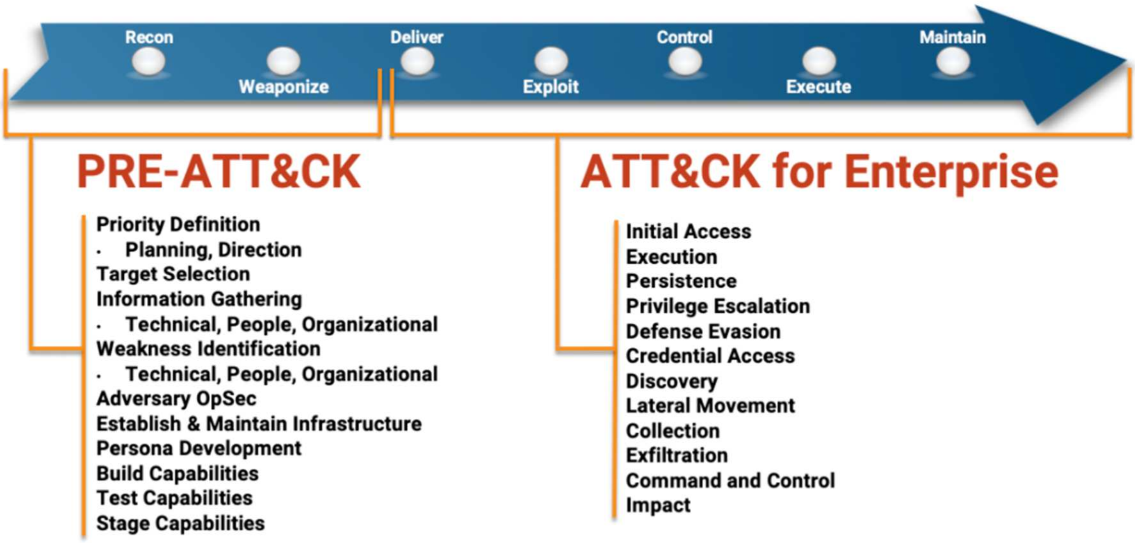
Vendor D: Non-default settings were used.

Vendor E: 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® Platform[19] 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 LifeCycle[20]

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.

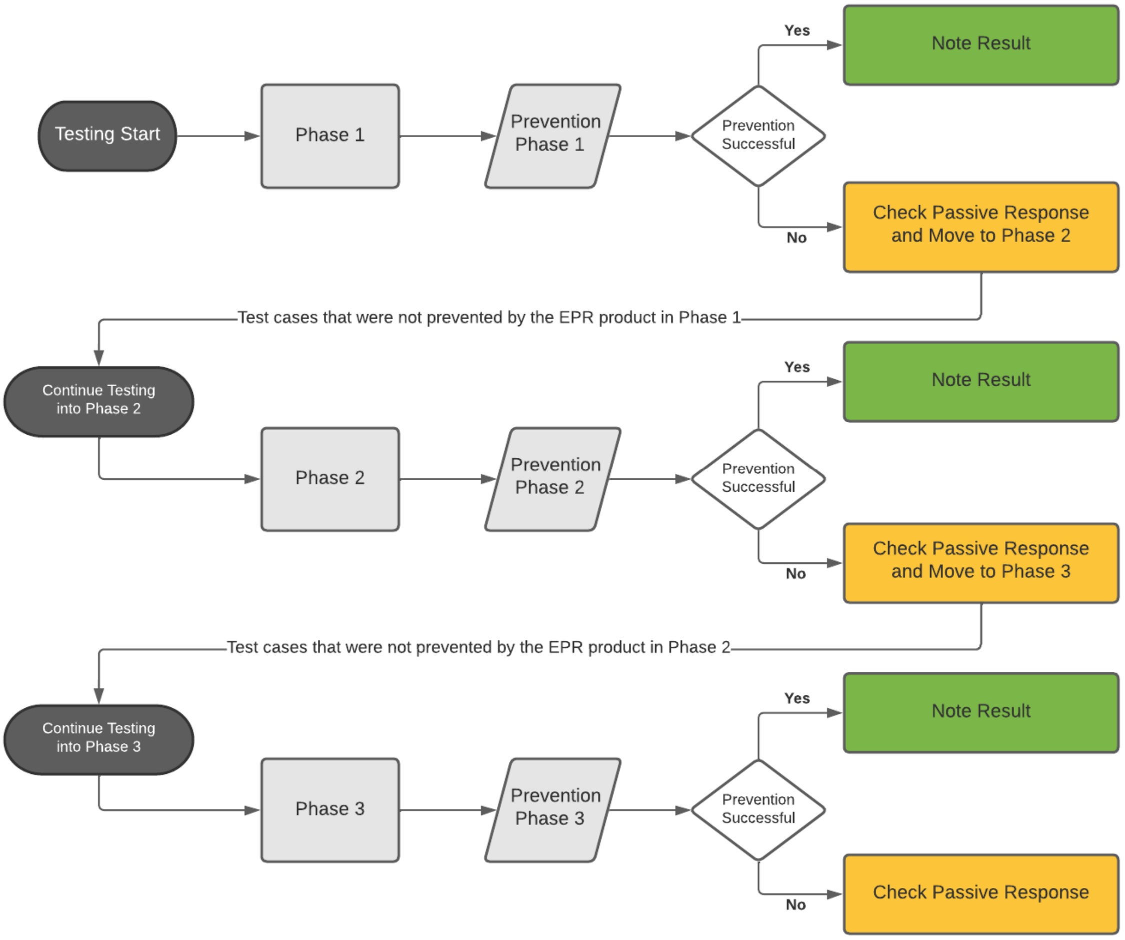
As illustrated in the graphic on the next page, we moved away from “atomic” testing, i.e. tests that only look at a particular component of the ATT&CK framework, and instead evaluated the EPR products from the context of the entire attack kill-chain, with workflows interconnecting at every stage from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

[19] © 2015-2022, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

[20] Source: https://attack.mitre.org/resources/enterprise-introduction/

EPR Testing Workflow

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


Testing Start
Phase 1
Prevention Phase 1
Prevention Successful
Yes
Note Result
No
Check Passive Response and Move to Phase 2
Test cases that were not prevented by the EPR product in Phase 1
Continue Testing into Phase 2
Phase 2
Prevention Phase 2
Prevention Successful
Yes
Note Result
No
Check Passive Response and Move to Phase 3
Test cases that were not prevented by the EPR product in Phase 2
Continue Testing into Phase 3
Phase 3
Prevention Phase 3
Prevention Successful
Yes
Note Result
No
Check Passive Response

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 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.

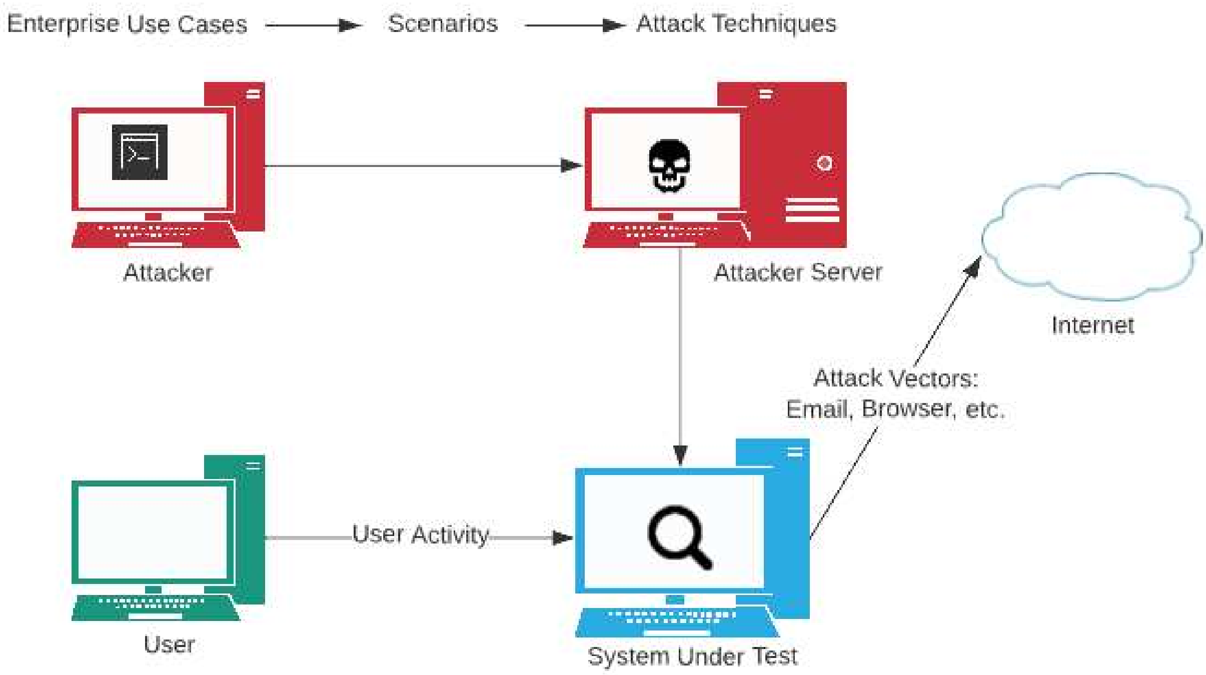
Correlation of Process, Endpoint and Network

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.



EPR Test Topology Overview

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 2022, 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. Once the attacker got initial access to the environment, they tried to be as stealthy as possible so that defence mechanisms would not be triggered.

All the attacks were crafted using open-source and commercial tools[21]/frameworks, and were developed using in-house expertise. The reason why we included commercial C2 frameworks is that these are frequently misused[22] by attackers 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.

[21] https://attack.mitre.org/software/
[22] https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/

About this test

AV-Comparatives' 2022 Endpoint Prevention and Response (EPR) Test for enterprise products is in its third iteration this year. Having the product named in the main comparative EPR report is at the vendor's discretion. We tested the products with configurations as suggested by the vendors and verified them together with the vendors before the test started.

The test is very challenging but reflects realistic scenarios. Feedback from many vendors' technical departments, analysts, and enterprises has been overwhelmingly positive. However, we have also had a few suggestions for perfecting the test methodology, and we have implemented some of these, where we felt that they were in the genuine interests of users, and helped to promote the most realistic testing of the EPR products.

The complex nature of the test means that automation is not possible, and so it has to be performed entirely manually, making it cost-intensive to run. This methodology is tailored towards the prevention and response capabilities. Therefore, vendors were advised to turn on the prevention and protection capabilities (ability to block), and configure detection features so that they work effectively, but without causing high costs due to poor operational accuracy or workflow delays.

The test phases consist of the attack tactics which most enterprises today are exposed to, and the security team has to counter. Some vendors claim that certain tactics (e.g. Discovery) might be hard to detect, but a good EPR product needs to deal with them as they are frequently used in targeted attacks. The different phases of the EPR test cover the full attack chain, including all the common real-world attack tactics and techniques, from the first foothold and internal propagation to the exfiltration of target information and actual damage done to the target system or network.

Because the aim of the test is to measure prevention and response capabilities, we did not tell any vendors when exactly the test would be performed, nor provide any details of the attacks beforehand. This avoids giving vendors the opportunity to monitor the attacks in real time and interact with their products when they think it beneficial. In real life, attackers do not tell their victims when or how they are going to attack, so products must aim to provide full protection all the time, rather than being optimized for evaluation.

Providing the customer with as much telemetry and sensor data as possible, and producing excessive numbers of alerts, can be counter-productive. Not all companies have the resources to investigate every single alert. Rather than overwhelming security experts with a load of raw data, which IT staff have to filter, analyse, and correlate manually, products should support the investigation process in a more reasonable and efficient way. Costs arising from imperfect operational-accuracy as well as costs due to workflow delays are taken into account. Additionally, telemetry-based threat-hunting is not within the scope of the test.

To get an overall picture of the protection and response capabilities of any of the tested EPR products, readers should look at the results of the other tests in AV-Comparatives' Enterprise Main-Test Series[23] too.

[23] https://www.av-comparatives.org/enterprise/

Copyright and Disclaimer

This publication is Copyright © 2022 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 2022)

Icons: feathericons.com