Independent Tests of
Anti-Virus Software

Endpoint Prevention and Response EPR Comparative Report

TEST PERIOD: OCTOBER 2020
LAST REVISION: 17th DECEMBER 2020

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 (ATPs). Whilst endpoint security products are expected to detect and block malware and network attacks on individual workstations, EPR products 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 9 products in the test were subjected to 49 separate targeted attacks, 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 test determined whether the product detected the attack, 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. Firstly, the time to respond is noted. Clearly, the sooner an attack is stopped or detected, the better. The tested products were given a window of 24 hours after the start of each attack in which to take action. 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, including a timeline and breakdown of phases, was investigated. 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, and the product's accuracy costs, (incurred due to false positives). 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.

The following products were tested by AV-Comparatives:

Vendor	Product	Version
Bitdefender	GravityZone Ultra	6.6
Cisco	Secure Endpoint (AMP for Endpoints) Cloud[1]	7.3.1
CrowdStrike	Falcon Enterprise	5.40 & 5.41
ESET	PROTECT Enterprise	7.2
Palo Alto Networks	Cortex XDR Pro	7.2
Vendor A	Product A	n/a
Vendor B	Product B	n/a
Vendor C	Product C	n/a
Vendor D	Product D	n/a

The settings which were applied to each respective product can be found in the Appendix 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/2020/12/EPR_Bitdefender_2020.pdf
Cisco:	https://www.av-comparatives.org/wp-content/uploads/2020/12/EPR_Cisco_2020.pdf
CrowdStrike:	https://www.av-comparatives.org/wp-content/uploads/2020/12/EPR_CrowdStrike_2020.pdf
ESET:	https://www.av-comparatives.org/wp-content/uploads/2020/12/EPR_ESET_2020.pdf
Palo Alto Networks:	https://www.av-comparatives.org/wp-content/uploads/2020/12/EPR_PaloAlto_2020.pdf

[1] Previously known as “Essentials” tier.

EPR CyberRisk Quadrant™

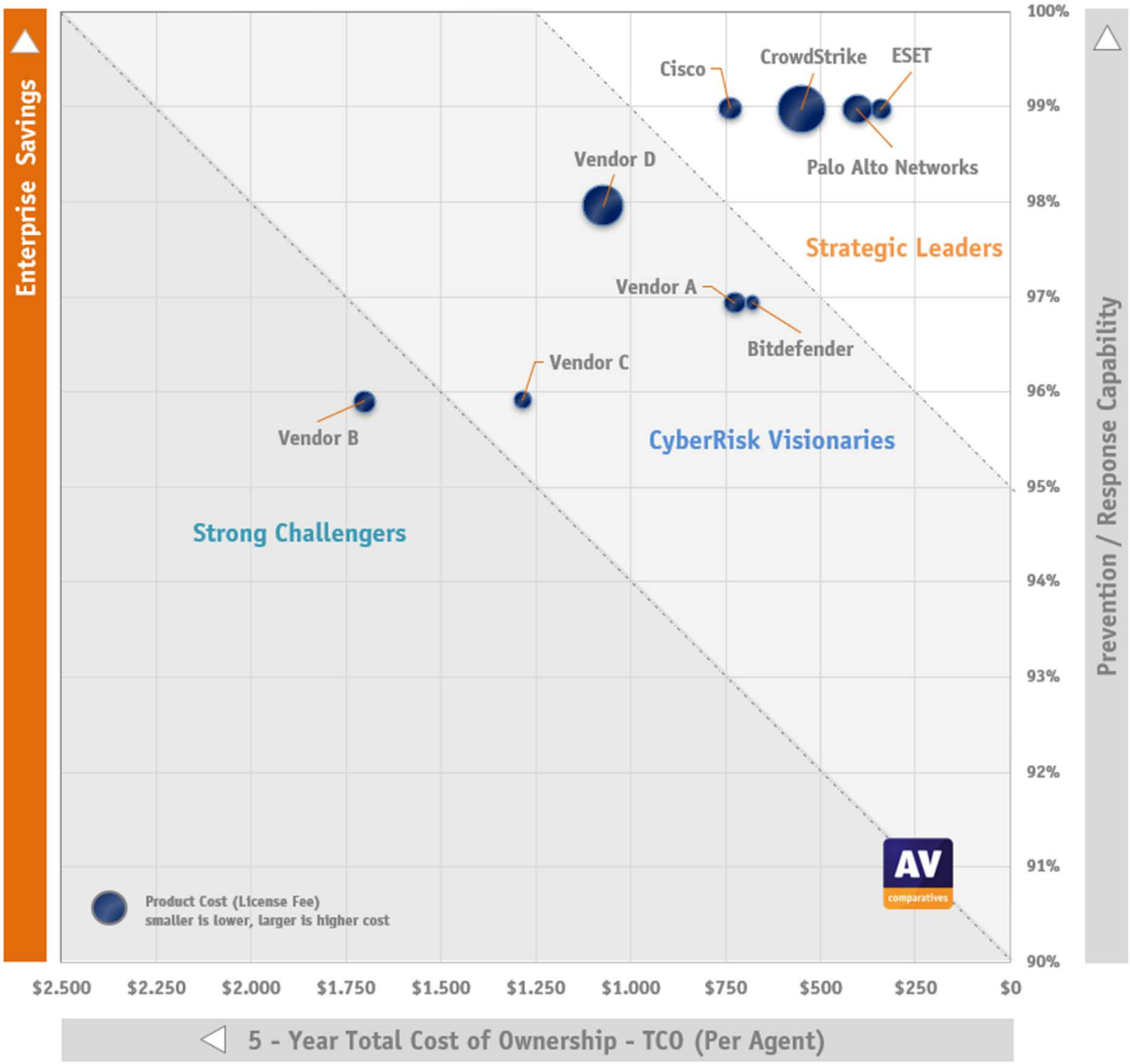


Figure 1 – Endpoint Prevention and Response (EPR) – ECRQ - Enterprise CyberRisk Quadrant™

Product	5-Year Product Cost (Per Agent)	Active Response	Passive Response	Combined Prevention/Response Capabilities Y-Axis	5-Year TCO (Per Agent) X-Axis
Bitdefender	$100	93.9%	100%	**96.9%**	**$679**
Cisco	$158	98.0%	100%	**99.0%**	**$737**
CrowdStrike	$357	98.0%	100%	**99.0%**	**$550**
ESET	$149	98.0%	100%	**99.0%**	**$342**
Palo Alto Networks	$210	98.0%	100%	**99.0%**	**$403**
Vendor A	$146	93.9%	100%	**96.9%**	**$725**
Vendor B	$158	93.9%	98.0%	**95.9%**	**$1,702**
Vendor C	$125	93.9%	98.0%	**95.9%**	**$1,283**
Vendor D	$300	98.0%	98.0%	**98.0%**	**$1,072**

Figure 2 – CyberRisk Quadrant Key Metrics- based on 5000 clients

Strategic Leaders

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

Strategic Leaders show others the way forward by setting ambitious targets and meeting them. They develop ground-breaking ideas and implement these impressively in their products.

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 analyst workflow capabilities. These products demonstrated good enterprise-class prevention, detection, response and reporting capabilities, along with above-average operational and analyst workflow capabilities.

CyberRisk Visionaries can see what will be required in the future, and strive to make it happen today. They constantly develop their products in an attempt to improve them.

Strong Challengers

EPR products that have an acceptable return on investment, offering effective technical capabilities while providing reasonable enterprise TCO.

Strong Challengers have set themselves the goal of being the best, and work hard at trying to achieve that aim.

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 according to the active and passive response rate

Although the vendors missed the same overall scenarios and had the same overall active/passive response rates, the vendor ‘dot’ placement in the quadrant was driven by how good the active response or passive response capabilities were. Vendors who demonstrated high active response in all the phases of prevention stands to have lesser TCO as the response cost is lower.

Vendors who had reasonable active response capabilities but once had passive response capabilities stands to have a higher TCO as the response cost is higher. Refer to the report explanation on how active and passive response credit was given to vendors. So essentially, even with a same overall % the Dot placement will move left or right depending on how well each vendor did in active response in each of the individual phases.

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 3.86 million[2]. 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 3.86 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 figure 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 false positives caused by the product, which is defined as operational accuracy costs below, which have to be investigated and remediated. 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.

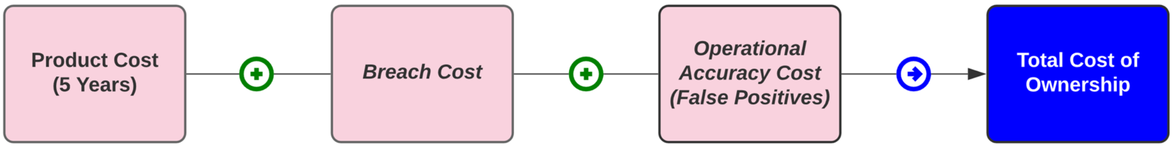


Figure 3 –Total Cost of Ownership Formula

The breach-cost of each product per scenario was calculated based on the ability of the EPR product to actively and passive respond at the time of execution (T0), and between the time of execution and the end of the test window (T0-T24 Hrs).

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

Based on the approach above, each EPR product incurred an additional breach cost based on how it handled each of the tested scenarios.

1. If there was NO active or passive response for the scenario within the tested time window of 24 hrs, then 100% of the total breach cost was added for the scenario.
2. If there was NO active response between T0-T24, but the product showcased passive response capabilities between T0-T24, then 75% of the total breach cost was added for the scenario.
3. If there was NO active response at time T0, but there was one before time T24, 50% of the total breach cost was added for the scenario.
4. If there was NO active response at time T0, but the product showcased passive response capabilities at time T0, then 25% of the total breach cost was added for the scenario.
5. If there was active response at time T0, then 0% of the total breach cost was added for the scenario.

To calculate the X-axis in the EPR CyberRisk Quadrant, the list price of the product, operational accuracy (false positive) savings, and the breach-cost savings were used. As previously mentioned, actively responding to a threat yields a higher cost saving than discovering a threat later, or worse still not being able to respond to it within the 24-hour test window. The following two figures depict how the calculations were applied.

Product	Scenarios	Overall Active Prevention	Overall Passive Response	No Prevention/Response	Operational Accuracy Savings
Bitdefender	49	46	49	0	✓
Cisco	49	48	49	0	✓
CrowdStrike	49	48	49	0	✓
ESET	49	48	49	0	✓
Palo Alto Networks	49	48	49	0	✓
Vendor A	49	46	49	0	✓
Vendor B	49	46	48	1	✓
Vendor C	49	46	48	1	✓
Vendor D	49	48	48	1	✓

Figure 4 - Product Cost and Breach Savings

As can be seen in Figure 4, all the vendors were able to achieve operational accuracy (false positives) savings. Most vendors also saw substantial breach savings. **Vendor B**, **Vendor C** and **Vendor D** were not able to either prevent or respond to one threat.

Active Response / Prevention: An active response is an effective response strategy that provides detection with effective prevention and reporting capabilities.

Passive Response: Passive response is set of response mechanisms offered by the product with cohesive detection, correlation, reporting and actionable capabilities.

EPR Test Metrics and Scoring

The goal of every EPR system is to prevent threats, or at least provide effective response capabilities as soon as possible. Endpoint products that offer a high active *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 also provide a high *detection* rate (visibility and forensic detail) will realize savings because compromises do not have to be investigated manually.

EPR Product Evaluation	Enterprise Savings
Prevents most attacks and offers effective passive response	High
Prevents most attacks, but offers weaker passive response	Medium
Weak prevention and weak passive response	Low

Figure 5 — Use-Case Scenarios Scoring

High Enterprise Savings: If most threats are detected and prevented by the EPR product at or soon after execution, and if the product provides the necessary detection information to help with an effective passive response (partially/fully automated), it will result in the high enterprise savings. The averages of both active and passive response needs to be equal to or greater than 95%.

Medium Enterprise Savings: If most threats are detected and prevented by the EPR product at or soon after execution, but with limited details surrounding the detection, it will result in a weaker passive response strategy. This is because of the operational overhead that is required to respond to and remediate the effects of a compromised system, resulting in an increase in enterprise costs. The averages of both active and passive response required for medium enterprise savings needs to be equal to or greater than 90%.

Low Enterprise Savings: Lastly, if most threats are not prevented by the EPR product, and the product provides no details surrounding the detection, this will result in both a weaker active and a weaker passive response strategy, with only low enterprise savings. The averages of both active and passive response in this case is less than 90%.

EPR Test Results

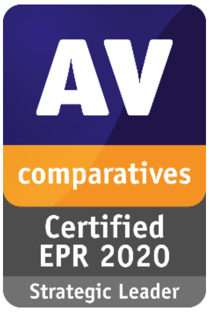
	Combined Prevention/Response Capabilities	Enterprise Savings	EPR CyberRisk Enterprise Quadrant
Cisco	99.0%	High	Strategic Leader
CrowdStrike	99.0%	High	Strategic Leader
ESET	99.0%	High	Strategic Leader
Palo Alto Networks	99.0%	High	Strategic Leader
Bitdefender	96.9%	High	CyberRisk Visionary
Vendor D	98.0%	High	CyberRisk Visionary
Vendor A	96.9%	High	CyberRisk Visionary
Vendor C	95.9%	High	CyberRisk Visionary
Vendor B	95.9%	High	Strong Challenger

Figure 6 – Enterprise Savings

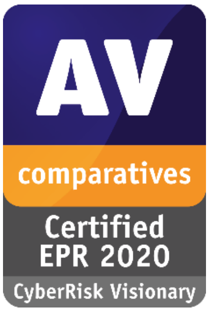
AV-Comparatives' EPR Certification

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 averages of at least 90% for combined active and passive response, thus reaching Medium Enterprise Savings as defined above. Certification levels are: Strategic Leader, CyberRisk Visionary, Strong Challenger.

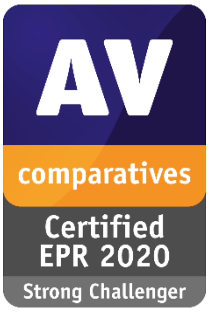
We congratulate the vendors shown below, whose products met the certification criteria, and are thus given AV-Comparatives' EPR Product Certifications for 2020:



ESET
paloalto NETWORKS
CISCO
CROWDSTRIKE



Bitdefender
Vendor A
Vendor C
Vendor D



Vendor B

Detailed Test Results

Phase-1 Metrics: Endpoint Compromise and Foothold

Phase-1 can be triggered by an attack based on the MITRE ATT&CK and other methods, and can be effectively mapped to Lockheed's Cyber Kill Chain. This workflow can be operationalized by going through the various attack phases described below.

Initial Access: 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: 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: 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 to gain a foothold inside the environment. These include registry manipulation, specifying dynamic-link-library values in the registry, shell scripts that can contain shell commands, application shimming, and account manipulation.

For an active response (preventative action) to be credited, we verified whether the product made an active response during any of the three phases. Similarly, for a detection event to be credited, we verified that the product saw various indicators that tied the actions to the attack.

And finally, for the passive response to be credited, we verified whether or not it was possible for the SOC analyst to respond to that threat using the product.

Figure 7 depicts the results for each of the products tested for Phase 1.

Scenario	Description	Bitdefender	Cisco	CrowdStrike	ESET	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D
1	Customized File generated from Koadic	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓	✓✓
2	Custom Office Macro Document	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
3	Custom Office Macro Document	✓✓	✓✓	✓✓	✗✓	✓✓	✓✓	✓✓	✓✓	✓✓
4	Custom Signed reverse Shell payload	✗✓	✗✓	✗✓	✓✓	✗✓	✓✓	✗✗	✗✗	✓✓
5	Custom PowerShell File	✗✓	✗✓	✓✓	✓✓	✓✓	✓✓	✗✓	✗✓	✗✗
6	Custom PowerShell File	✗✓	✓✓	✓✓	✓✓	✗✓	✗✓	✗✗	✗✗	✓✓
7	Custom Office Macro Document	✗✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓	✓✓
8	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
9	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
10	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
11	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
12	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
13	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
14	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
15	Custom Payload Generated from MSF Template	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
16	Macro enabled SYLK file	✓✓	✓✓	✗✓	✓✓	✓✓	✗✓	✓✓	✓✓	✓✓
17	Internet Explorer Vulnerability	✓✓	✓✓	✓✓	✓✓	✓✓	✗✗	✓✓	✓✓	✓✓
18	Custom Backdoored Obfuscated bat File	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
19	Custom Backdoored HTA File	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✗	✓✓
20	Custom Backdoored Executable	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
21	Custom Backdoored Executable	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
22	Custom Backdoored Executable	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
23	Custom Remote Access Trojan	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
24	Custom Remote Access Trojan	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓	✓✓	✓✓
25	Custom Payload Generated using windows shellcode injection	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
26	Custom Payload Generated using windows shellcode injection	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
27	Custom Payload Generated using windows shellcode injection	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
28	Custom Payload Generated using windows shellcode injection	✓✓	✗✗	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓

29	Custom Payload Generated using windows shellcode injection	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
30	Custom Payload Generated using windows shellcode injection	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
31	Custom Payload Generated using windows shellcode injection	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
32	Custom Payload Generated using windows shellcode injection	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
33	Custom Payload Generated using windows shellcode injection	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
34	Fileless Attack	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
35	File and embedded command obfuscated using Content obfuscation	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
36	File obfuscated using Content obfuscation with variable naming	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
37	Custom Excel Macro	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
38	Customized File generated from Koadic	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
39	Customized File generated from Koadic	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
40	Customized File generated from Koadic	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
41	Customized File generated from Koadic	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
42	C# stager using DotNetToJScript using VBScript	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
43	C# stager using DotNetToJScript using JScript	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
44	Remote Service Vulnerability	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
45	Custom Payload Generated from MSF Template	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
46	Malicious Office Document 1	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
47	Malicious Office Document 2	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
48	Malicious Office Document 3	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎
49	Malicious Office Document 4	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎	🛡 ✎

Figure 7 – Prevent and Passive Response for Phase 1

🛡 Active response / prevention	✎ Passive response
🚫 No active response / no prevention	✗ No passive response

Phase-2 Metrics: Internal Propagation

In this phase, the EPR product should be able to prevent internal propagation. This phase is triggered when the prevention of the threat fails. The EPR product in this phase should enable the analyst to immediately identify and track the internal propagation of the threat in real time.

Privilege Escalation: 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.

For a detection event to be credited, we looked at various indicators that tied the action to the attack. And finally, for the passive response to be credited, we looked at whether or not it was possible for the SOC analyst to respond to that threat by using the tested product.

Discovery for Lateral Movement: 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.

Credential Access: 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.

Lateral Movement: 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.

Figure 8 depicts the results for each of the products tested for Phase 2.

Scenario	Bitdefender	Cisco	CrowdStrike	ESET	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D
1	✓	✓	✓	✓	✓	✓	🛡✎	✓	✓
3	✓	✓	✓	⊘✎	✓	✓	✓	✓	✓
4	🛡✎	🛡✎	🛡✎	✓	🛡✎	✓	🛡✎	🛡✎	✓
5	□	🛡✎	✓	✓	✓	✓	□	□	□
6	□	✓	✓	✓	□	□	□	□	□
7	⊘✎	✓	✓	✓	✓	✓	⊘✎	✓	✓
16	✓	✓	□	✓	✓	□	✓	✓	✓
17	✓	✓	✓	✓	✓	🛡✎	✓	✓	✓
19	✓	✓	✓	✓	✓	✓	✓	⊘✎	✓
24	✓	✓	✓	✓	✓	⊘✎	✓	✓	✓
28	✓	⊘✎	✓	✓	✓	✓	✓	✓	✓

Figure 8 – Prevent and Passive Response for Phase 2 showing only scenarios which passed Phase 1

🛡 Active response / prevention	✎ Passive response
⊘ No active response / no prevention	☒ No passive response

✓ Already prevented before

□ The scenario did not have a standalone Phase-2 or Phase-3 attack associated with it and the vendor had successfully responded to it in an earlier phase.

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.

Collection: 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.

Exfiltration: 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: Having found and extracted the target information, the attacker will try to delete or destroy all the evidence of the attack that remains within the target network. An ideal scenario for the attacker may well be one in which the victim does not even realize that the attack has taken place. Whether or not this is possible, the attacker will try to manipulate data inside the target environment to ensure that their tracks are covered as far as possible. This will ensure that the victim does not have the forensic information needed to understand the attack or trace the attacker. Data manipulation, deletion and encryption (as used in ransomware) are the typical techniques that are used to do this.

Figure 9 depicts the results for each of the products tested for Phase 3.

Scenario	Bitdefender	Cisco	CrowdStrike	ESET	Palo Alto Networks	Vendor A	Vendor B	Vendor C	Vendor D
3	✓	✓	✓	□	✓	✓	✓	✓	✓
7	⊘✎	✓	✓	✓	✓	✓	⊘☒	✓	✓
19	✓	✓	✓	✓	✓	✓	✓	⊘✎	✓
24	✓	✓	✓	✓	✓	⊘✎	✓	✓	✓
28	✓	⊘☒	✓	✓	✓	✓	✓	✓	✓

Figure 9 – Prevention and Passive Response for Phase 3 showing only scenarios which passed Phase 2

🛡 Active response / prevention	✎ Passive response
⊘ No active response / no prevention	☒ No passive response

✓ Already prevented before
□ The scenario did not have a standalone Phase-2 or Phase-3 attack associated with it and the vendor had successfully responded to it in an earlier phase.

Reduction in TTP (Time to Prevent)

As seen in the CyberRisk Quadrant calculations, time to prevent threats matters. Therefore, the speed with which a product can prevent the threat is an important feature to consider. This could also be referred to as the effective reduction in active time to respond. We recorded the time the threat was introduced into the test cycle and how long it took the product to prevent it. Within the 24-hour window, cumulative protection and detection rates are calculated each hour until attacks are prevented and responded to by the product.

<table>
<tr><th rowspan="2"></th><th colspan="9">Time to Prevent (in hours)</th></tr>
<tr><th>0
(T0)</th><th>&lt;1</th><th>&lt;2</th><th>&lt;5</th><th>&lt;10</th><th>&lt;15</th><th>&lt;20</th><th>&lt;24</th><th>24
(T1)</th></tr>
<tr><td>Bitdefender</td><td colspan="9" rowspan="9"><i>All the active-response values shown in the table below were achieved at T0, and did not change over the 24-hour period (T1)</i></td></tr>
<tr><td>Cisco</td></tr>
<tr><td>CrowdStrike</td></tr>
<tr><td>ESET</td></tr>
<tr><td>Palo Alto Networks</td></tr>
<tr><td>Vendor A</td></tr>
<tr><td>Vendor B</td></tr>
<tr><td>Vendor C</td></tr>
<tr><td>Vendor D</td></tr>
</table>

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	91.8%	93.9%	93.9%
Cisco	93.9%	98.0%	98.0%
CrowdStrike	95.9%	98.0%	98.0%
ESET	98.0%	98.0%	98.0%
Palo Alto Networks	95.9%	98.0%	98.0%
Vendor A	91.8%	93.9%	93.9%
Vendor B	89.8%	93.9%	93.9%
Vendor C	91.8%	93.9%	93.9%
Vendor D	98.0%	98.0%	98.0%

Cumulative Active Response (Prevention) by phases

Reduction in TTR (Time to Respond)

Time is critical when an incident that is not prevented has the potential to cause a breach.

<table>
<tr><th rowspan="2"></th><th colspan="9">Time to Respond (in hours)</th></tr>
<tr><th>0
(T0)</th><th>&lt;1</th><th>&lt;2</th><th>&lt;5</th><th>&lt;10</th><th>&lt;15</th><th>&lt;20</th><th>&lt;24</th><th>24
(T1)</th></tr>
<tr><td>Bitdefender</td><td colspan="9" rowspan="9"><i>All the passive-response values shown in the table below were achieved at T0, and did not change over the 24-hour period (T1)</i></td></tr>
<tr><td>Cisco</td></tr>
<tr><td>CrowdStrike</td></tr>
<tr><td>ESET</td></tr>
<tr><td>Palo Alto Networks</td></tr>
<tr><td>Vendor A</td></tr>
<tr><td>Vendor B</td></tr>
<tr><td>Vendor C</td></tr>
<tr><td>Vendor D</td></tr>
</table>

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	100%	100%	100%
Cisco	93.9%	100%	100%
CrowdStrike	95.9%	98.0%	98.0%
ESET	100%	100%	100%
Palo Alto Networks	100%	100%	100%
Vendor A	98.0%	100%	100%
Vendor B	95.9%	98.0%	98.0%
Vendor C	95.9%	98.0%	98.0%
Vendor D	98.0%	98.0%	98.0%

Cumulative Passive Response by phases

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 if any form of intended remediation mechanisms mentioned below could be completed by the SOC analyst (Response Enablement) - based on what is supported by the product - this was evaluated and verified by AV-Comparatives. Results are shown in the table below.

	System Imaging	Patching	System Restore	Quarantine	Network Isolation	Process Termination
Bitdefender	✓	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	□	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	✓
Palo Alto Networks	□	□	✓	✓	✓	✓
Vendor A	✓	□	✓	✓	✓	✓
Vendor B	□	□	□	✓	✓	✓
Vendor C	✓	✓	□	✓	✓	✓
Vendor D	✓	✓	□	✓	✓	✓

Figure 10 — EPR Response actions available for SOC Analyst (part 1)

	Execution Prevention	Uninstall Services	Shutdown or Reboot of Endpoint	Edit Registry Keys & Values	Block Processes from Communication	Delete Files & Directories
Bitdefender	✓	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓	✓	✓
Vendor B	□	✓	✓	✓	✓	✓
Vendor C	✓	✓	✓	✓	✓	✓
Vendor D	✓	✓	✓	✓	✓	✓

Figure 11 — EPR Response actions available for SOC Analyst (part 2)

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-deployed appliance. A full trail of audit logs is available in the management console. Communication between the agent and management console is done via SSL. Figure 12 till Figure 17 provide information on the applicable capabilities of each of the tested products.

	Attack Visualization	Attack Timeline	Attack Phases	Attack Context
Bitdefender	✓	✓	✓	✓
Cisco	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓
ESET	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓
Vendor B	✓	✓	✓	✓
Vendor C	✓	✓	✓	✓
Vendor D	✓	✓	✓	✓

Figure 12 – Threat Visibility

	Continuous Monitoring	Running applications and processes	Behaviour Monitoring (File/registry/etc..)	Whitelisting capability
Bitdefender	✓	✓	✓	✓
Cisco	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓
ESET	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓
Vendor B	✓	✓	✓	✓
Vendor C	✓	✓	✓	✓
Vendor D	✓	✓	✓	✓

Figure 13 – System Visibility

	Standards-based API for access	Standard output format (JSON, Syslog, etc.)	Automated Data Export	Syslog Integration	Splunk Integration	Additional Reporting Features
Bitdefender	✓	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	□	✓	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓	✓	✓
Vendor B	✓	✓	✓	✓	✓	✓
Vendor C	✓	✓	✓	✓	✓	✓
Vendor D	✓	✓	✓	✓	✓	✓

Figure 14 Data Sharing

	Encryption of data at rest	Targeted capture / e-discovery	Customizable default security policies	Policy and/or signature rollback	Management to agent encryption	Built-in-reporting for different user categories
Bitdefender	✓	✓	✓	✓	✓	□
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	□
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓	✓	□
Vendor B	✓	✓	✓	✓	✓	□
Vendor C	✓	✓	✓	✓	✓	□
Vendor D	✓	✓	✓	✓	✓	✓

Figure 15 – Encryption, Discovery and Reporting

	Multiple EPR Analyst/User-focused workflow	Report Automation	Compliance reports (GDPR, PCI-DSS, etc.)	Audit Trail support management console	System scanning capability	Disaster Recovery
Bitdefender	✓	✓	□	✓	✓	✓
Cisco	✓	✓	□	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓	✓	✓
Vendor B	✓	✓	✓	✓	✓	✓
Vendor C	✓	✓	✓	✓	✓	✓
Vendor D	✓	✓	✓	✓	✓	✓

Figure 16 – Workflow, Reporting and Disaster Recovery

	Cloud Marketplace Support	Integration with security products	Enterprise recording and data storage – Forensic analysis	Customized Reporting and Management	Custom Reporting and Filtering
Bitdefender	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓	✓
Vendor B	✓	✓	✓	✓	✓
Vendor C	✓	✓	✓	✓	✓
Vendor D	✓	✓	✓	✓	✓

Figure 17 – Third-party integration and Reporting

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. While providing maximum flexibility to senior analysts, the EPR should support predefined (but configurable) workflows for less-experienced personnel, who will be assigned specific tasks during an investigation.

IOC Integration

This is to identify the digital footprint by means of which the malicious activity in 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, snort signatures or threat intelligence feeds etc. as shown in the below figure.

	SIEM	DNS Logs	Network traffic flow logs	DHCP Logs	Scan Results	YARA Signatures
Bitdefender	✓	□	□	□	□	□
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	□	□	□	□	□
ESET	✓	□	□	□	□	□
Palo Alto Networks	✓	✓	✓	✓	✓[3]	✓
Vendor A	✓	□	□	□	□	□
Vendor B	✓	□	□	□	□	□
Vendor C	✓	□	□	□	✓	□
Vendor D	✓	✓	✓	□	✓	□

Figure 18 – External Data Correlation

	Multi-factor Authentication logs	Sandboxing logs	Retrospective Analysis and Logs	Endpoint Prevention Product logs	Proprietary product integration	Threat intelligence data assimilation
Bitdefender	□	✓	□	□	□	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	□	□	□	□	□	✓
ESET	□	□	□	□	□	✓
Palo Alto Networks	✓	✓	✓	✓[4]	✓	✓
Vendor A	□	□	□	□	□	✓
Vendor B	□	□	□	□	□	✓
Vendor C	✓	✓	□	□	✓	✓
Vendor D	✓	✓	✓	✓	✓	✓

Figure 19 – External Data Correlation

[3] Capability is provided also by Palo Alto Networks' endpoint product.

EPR Cost Structure

Product costs are based on list prices in USD provided by vendors at the time of the test (October 2020). 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 5000 clients, based on a 5-year contract:

Product	EPR Cost (5000 Clients) 5 Years
Bitdefender GravityZone Ultra	$500,777
Cisco Secure Endpoint Cloud	$792,000
CrowdStrike Falcon Enterprise	$1,784,450
ESET PROTECT Enterprise	$742,500
Palo Alto Networks Cortex XDR Pro	$1,050,000
Product A	$732,375
Product B	$787,500
Product C	$625,000
Product D	$1,500,000

Figure 20 — 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 may make them particularly suitable for some organisations.

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. The in-depth testing ran for a four-week period. A total of 49 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[4] and NIST platform, such that it becomes easier to operationalize the risk regarding a specific endpoint.

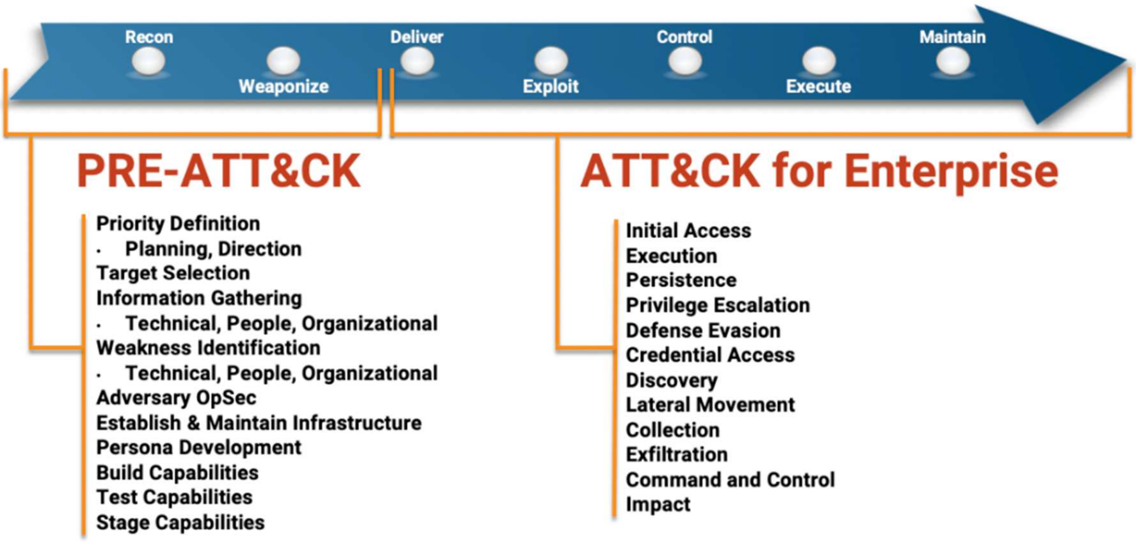


Figure 21: MITRE ATT&CK for Enterprise vs Seven Stage Cyber Attack LifeCycle[5]

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 towards mapping the kill-chain visibility with the MITRE ATT&CK framework.

As illustrated in Figure 22 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.

[4] © 2015-2020, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
[5] Source: https://attack.mitre.org/resources/enterprise-introduction/

Active Response vs Passive Response Workflow

This EPR report includes security efficacy metrics around different test scenarios and product differentiating factors. This will enable enterprises to make informed decisions on the suitability of each tested product for their requirements.

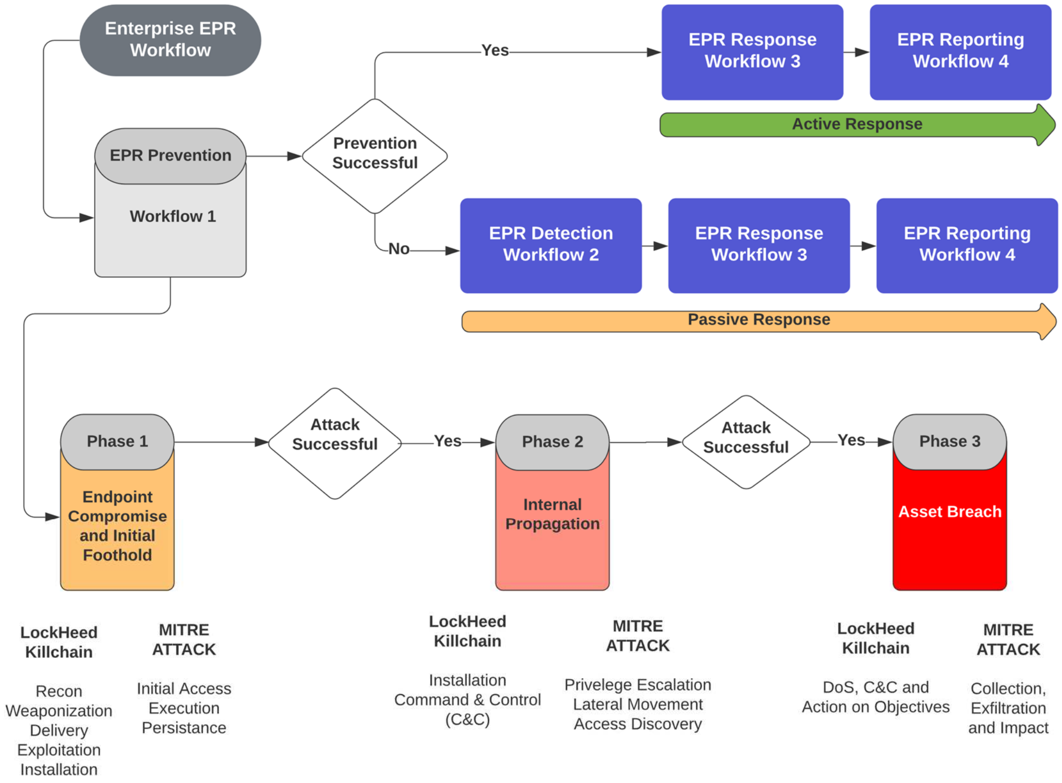


Figure 22 — Enterprise EPR Workflow Overview

Whether attacks are defined as malicious operations, campaigns, detections, kill chains or anything else, it is these human pathways that should be highlighted, which we are referencing as four distinct workflows in this report.

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 security analyst 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 analyst workflows and scenarios, and not on the technology used to prevent, detect or respond to it.

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.

A passive response as defined in this test, is an effective response strategy that provides detection with effective response and reporting capabilities all done in a manual/semi-automated way thus involving valuable time and resources warranting further investigation.

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 analyst. Once they have been identified, the analyst 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.

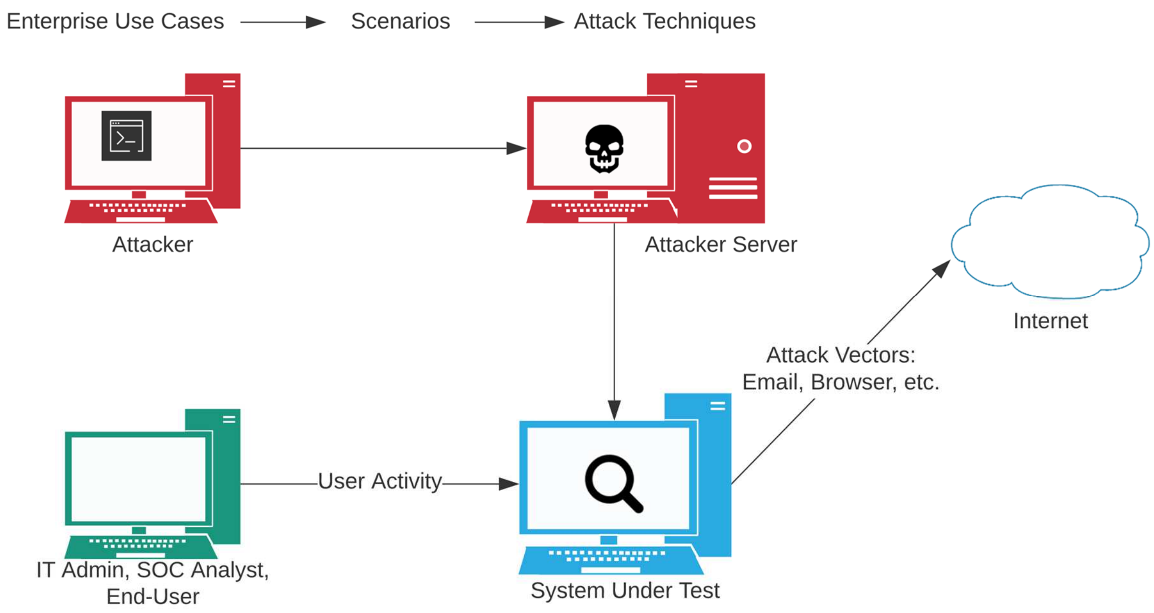


Figure 23 — EPR Test Topology Overview

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 49 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 in 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 Iteration Objective

The objective of the testing was to assess the prevention-centric workflow with specific use-cases targeted for EPR prevention Workflow-1 (referenced in the methodology) with threats that typically target enterprise users in a normal operational environment. This iteration helped us to assess the default prevention capability of the product along with the detection mechanism. If a threat was not prevented, we evaluated if the EPR product was able to take appropriate detection and response measures in a timely manner.

The following assessment was made to validate if the EPR endpoint security product was able to prevent and detect all the attacks on the EPR Prevention Workflow-1 and Detection workflow.

- Did the prevention occur during Phase 1 (Endpoint Compromise and Foothold) of the prevention workflow?
- Did the EPR product provide us with the appropriate threat classification, threat triage and demonstrated accurate threat timeline of the attacks with relevant Endpoint and User Data?
- Did the EPR product demonstrate any negative issues on the operational accuracy test which was executed in conjunction with the attack scenarios?

Targeted Use-Cases

The use cases that we went after during the test iterations were “IT Administrator”, “Regular Enterprise user”, “SOC team Professional”, and “Analyst”. 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, when executed, successfully allowed an attacker to get a foothold inside the environment and take additional steps to act upon its objectives.

During the time duration of testing, our analyst acted as an SOC analyst, administrator and an SOC professional by logging 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 analyst in a timely and clear way. We tested the responses as available by products under the test.

EPR Test Iteration Timeframe

The evaluation was conducted in four phases, each phase lasting a week. As weeks progressed, AV-Comparatives was able to have a detailed understanding of the product under test and attacks were crafted in such a way that they stressed the product’s true capabilities. Furthermore, Workflow-1 was conducted with attacker driven mindset as the attack progressed through the attack nodes to finally meet its objective. The evaluation was conducted between September and October 2020. User persona and user activities were simulated throughout the test such that they were as close to the real environment as possible.

All the attacks were crafted using open-source tools and samples were developed using in-house expertise. Once the attacker got initial access to the environment, the attacker tried to be as stealthy as possible such that defender and defences are not triggered.

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 configure their products to achieve the best protection available. Results presented in this test were only accomplished by applying the respective product configurations as described here.

The configurations were applied by the engineers of the respective vendors during setup. This configuration is typical in enterprises, which have their own teams of SOC analysts looking after their defences. The personas and the threat emulation that were run in this evaluation represent such scenarios. It is common for products of these kinds that vendor experts assist companies on the deployment and configuration best suited for the type of enterprise. Below we have listed relevant deviations from default settings.

Bitdefender: "Risk Management", "Sandbox Analyzer" and "Scan SSL" were enabled. "HyperDetect" was enabled and set to "Block" (for network) and to "Disinfect" (for files). "On-Access scan" for archives bigger than 100MB was enabled with depth 16.

Cisco: First time Set up Wizard Workstation Recommended Settings were applied, i.e.:
"Files", "Malicious Activity Protection" and "Script Protection" were set to "Quarantine".
"Network" and "Exploit Prevention" were set to "Block".
"System Process Protection" and "Behavioral Protection" were set to "Protect"
"Two Factor Authentication" for "Automatic Analysis" and "Command Line Capture" was enabled.
"Connector Protection" and "Orbital Advanced Search" were enabled.
"Malicious Activity Protection - Monitor Network Drives" was enabled.
"Detection Action" was set to "Block, Terminate and Quarantine".

CrowdStrike: everything enabled and set to maximum, i.e. "Extra Aggressive".

ESET: All "Real-Time & Machine Learning Protection" settings set to "Aggressive".

Palo Alto Networks: Default settings.

Vendor A: Default settings.

Vendor B: Non-default settings.

Vendor C: Non-default settings.

Vendor D: Non-default settings.

Copyright and Disclaimer

This publication is Copyright © 2020 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
(December 2020)

Icons: feathericons.com