Independent Tests of
Anti-Virus Software

Endpoint Prevention and Response
EPR Comparative Report

TEST PERIOD: OCTOBER 2021
LAST REVISION: 10TH JANUARY 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 (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 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 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	7.2
Broadcom	Symantec Endpoint Security Complete	14.3
Check Point	Harmony Endpoint Advanced	85.10
Cisco	Secure Endpoint Essentials	7.4.3
CrowdStrike	Falcon Endpoint Protection Enterprise	6.31
ESET	PROTECT Enterprise	8.1
F-Secure	F-Secure Elements EDR and EPP for Computers	21.9
Palo Alto Networks	Cortex XDR Pro	7.5
Vendor A	Product A	n/a
Vendor B	Product B	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/2022/01/EPR_Bitdefender_2021.pdf

Broadcom: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_Broadcom_2021.pdf

Check Point: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_CheckPoint_2021.pdf

Cisco: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_Cisco_2021.pdf

CrowdStrike: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_CrowdStrike_2021.pdf

ESET: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_ESET_2021.pdf

F-Secure: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_F-Secure_2021.pdf

Palo Alto Networks: https://www.av-comparatives.org/wp-content/uploads/2022/01/EPR_PaloAlto_2021.pdf

EPR CyberRisk Quadrant™

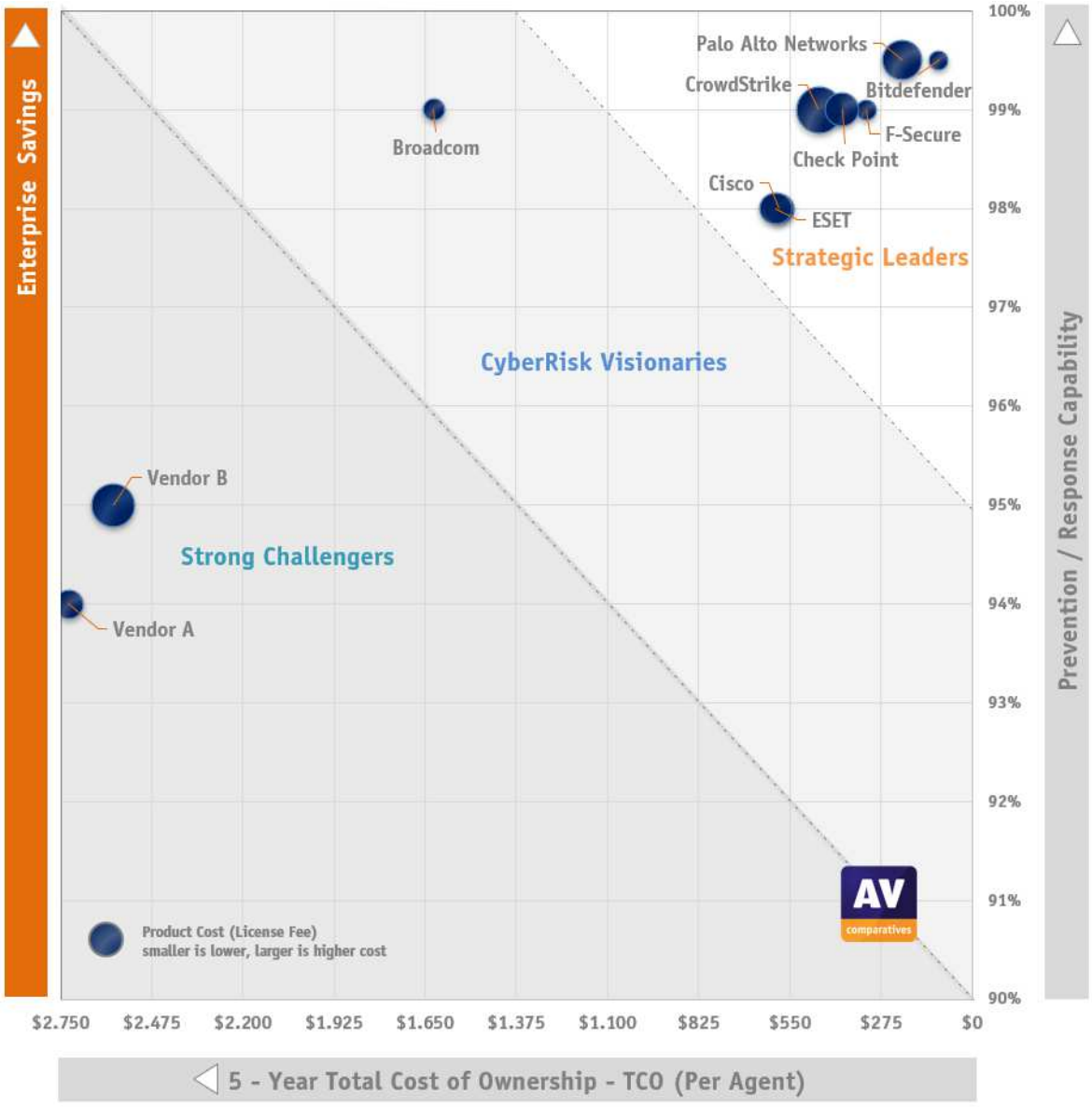

Figure 1 – Endpoint Prevention and Response (EPR) – ECRQ - Enterprise CyberRisk Quadrant™

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	99.0%	100%	**99.5%**	**$100**
Broadcom	$113	98.0%	100%	**99.0%**	**$1,734**
Check Point	$180	98.0%	100%	**99.0%**	**$392**
Cisco	$158	96.0%	100%	**98.0%**	**$582**
CrowdStrike	$249	98.0%	100%	**99.0%**	**$461**
ESET	$170	96.0%	100%	**98.0%**	**$594**
F-Secure	$106	98.0%	100%	**99.0%**	**$318**
Palo Alto Networks	$210	99.0%	100%	**99.5%**	**$210**
Vendor A	$153	88.0%	100%	**94.0%**	**$2,725**
Vendor B	$231	90.0%	100%	**95.0%**	**$2,591**

Figure 2 – CyberRisk Quadrant Key Metrics- based on 5000 agents/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 4.24 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 4.24 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. According to Ponemon's Institute[2], companies waste roughly USD 1.3 million per year due to inaccurate or erroneous Intelligence. This has been factored in as the added yearly cost that you can expect to pay for a product failing our operational-accuracy-based validation this year. In future EPR tests, costs arising from poor Operational Accuracy will be penalised more heavily, and costs due to workflow delays will also be 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.

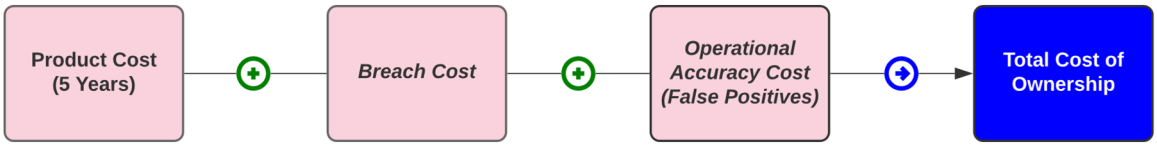

Figure 3 –Total Cost of Ownership Formula

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).

[1] https://www.ibm.com/security/data-breach
[2] https://www.ponemon.org/research/ponemon-library/security/the-cost-of-malware-containment.html

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	50	50	50	0	✓
Broadcom	50	49	50	0	✗
Check Point	50	49	50	0	✓
Cisco	50	48	50	0	✓
CrowdStrike	50	49	50	0	✓
ESET	50	48	50	0	✓
F-Secure	50	49	50	0	✓
Palo Alto Networks	50	50	50	0	✓
Vendor A	50	44	50	0	✗
Vendor B	50	45	50	0	✗

Figure 4 - Product Cost and Breach Savings

As can be seen in Figure 4, seven out of ten of the tested products were able to achieve operational accuracy (false positives) savings. Most vendors also saw substantial breach savings by either preventing or responding to all threat scenarios.

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	Operational Accuracy	Enterprise Savings	EPR CyberRisk Enterprise Quadrant
Bitdefender	99.5%	PASS	High	Strategic Leader
Palo Alto Networks	99.5%	PASS	High	Strategic Leader
Check Point	99.0%	PASS	High	Strategic Leader
CrowdStrike	99.0%	PASS	High	Strategic Leader
F-Secure	99.0%	PASS	High	Strategic Leader
Cisco	98.0%	PASS	High	Strategic Leader
ESET	98.0%	PASS	High	Strategic Leader
Broadcom	99.0%	FAIL	High	CyberRisk Visionary
Vendor B	95.0%	FAIL	High	Strong Challenger
Vendor A	94.0%	FAIL	Medium	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[3]. 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 2021:

Bitdefender, Check Point Software Technologies Ltd, Cisco, CrowdStrike, ESET, F-Secure, paloalto Networks

Symantec, A Division of Broadcom

Vendor A

Vendor B

[3] In future EPR tests, costs arising from poor Operational Accuracy will be penalised more heavily, and costs due to workflow delays will also be taken into account.

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	Broadcom	Check Point	Cisco	CrowdStrike	ESET	F-Secure	Palo Alto Networks	Vendor A	Vendor B
1	MS Word Macro with CVE-2020-0668										
2	XLM Macro AutoOpen using MSBuild for compilation										
3	MS PowerPoint Macro with CVE-2020-0796										
4	MS Word macro with CVE-2020-0796										
5	MS Excel Macro with CVE-2020-0668										
6	MS PowerPoint Macro using MSBuild for compilation										
7	SYLK Macro using MSBuild for compilation										
8	Microsoft Office Word RCE Variation 1(CVE-2021-40444)										
9	Microsoft Office Word RCE Variation 2(CVE-2021-40444)										
10	MS PowerPoint Macro										
11	MS XLM Macro with In- Memory script										
12	MS Excel Macro										
13	MS Word Macro with CVE-2021-1675										
14	MS Word DotM File										
15	MS Excel with CVE-2021-1675										
16	MS PowerPoint with CVE-2021-36934										
17	MS Excel Macro										
18	MS Word DotM with CVE-2021-36934										
19	XLSM Macro with CVE-2021-1675										
20	Koadic JSE File										
21	Koadic HTA File										
22	Koadic Bat File										
23	Koadic PowerShell										
24	Caldera PowerShell										
25	Caldera Portable Executable										
26	Covenant PowerShell File										
27	Covenant Grunt Portable Executable										
28	Encoded VBE with Wiper Payload										

29	Forged Signature added to a File	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✗✓	✓✓
30	Keylogger Writing DLL Payload to disk	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓
31	Stateless MSF Writing DLL Payload to disk	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓
32	Keylogger via HTTP Post & Writing DLL Payload to disk	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓
33	CVE-2020-0683	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓	✓✓
34	CVE-2020-0796	✓✓	✓✓	✗✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓
35	CVE-2019-1322	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
36	PowerShell ConPtyShell	✗✓	✓✓	✓✓	✗✓	✓✓	✓✓	✓✓	✓✓	✓✓	✗✓
37	PowerShell Base 64 Encoded reverse shell	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
38	PowerShell Simple Payload	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
39	PowerShell HTA Payload	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
40	PowerShell base52 stager variation 1	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
41	PowerShell base52 stager variation 2	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
42	PowerShell base52 stager variation 3	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
43	PowerShell base52 stager variation 4	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
44	PowerShell base64 stager variation 1	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
45	PowerShell base64 stager variation 2	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
46	PowerShell JOB Payload	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
47	PowerShell New Process Payload	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
48	PowerShell JOB + File Payload	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
49	PowerShell JOB + File +SCT Payload	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓
50	In-memory File execution	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓

Figure 7 – Prevent and Passive Response for Phase 1

✓ Active response / prevention
✗ No active response / no prevention
✓ Passive response
✗ 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	Broadcom	Check Point	Cisco	CrowdStrike	ESET	F-Secure	Palo Alto Networks	Vendor A	Vendor B
6	✓	✓	✓	✓	✓	🚫✎	✓	✓	✓	🚫✎
7	✓	✓	✓	✓	🚫✎	✓	✓	✓	✓	🚫✎
10	✓	✓	✓	🚫✎	✓	✓	✓	✓	✓	🚫✎
20	✓	✓	🛡✎	✓	✓	✓	✓	✓	✓	✓
24	✓	🚫✎	✓	✓	✓	🚫✎	🚫✎	✓	🚫✎	✓
29	✓	✓	✓	✓	✓	✓	✓	🛡✎	🚫✎	✓
30	✓	✓	✓	✓	✓	✓	✓	✓	🚫✎	✓
31	✓	✓	✓	✓	✓	✓	✓	✓	🚫✎	✓
32	✓	✓	✓	✓	✓	✓	✓	✓	🚫✎	✓
33	✓	✓	✓	✓	✓	✓	✓	✓	🚫✎	✓
34	✓	✓	🚫✎	✓	✓	✓	✓	✓	✓	🚫✎
36	🛡✎	✓	✓	🚫✎	✓	✓	✓	✓	✓	🚫✎

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

🛡 Active response / prevention
🚫 No active response / no prevention
✓ Already prevented before
✎ Passive response
✎ No passive response

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 make sure 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.

Phase-3 scenario-based were N/A (not applicable) for all the products, as the threats had already been either actively prevented or passively responded to in the previous phases.

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.

	Time to Prevent (in hours)								
	0 (T0)	<1	<2	<5	<10	<15	<20	<24	24 (T1)
Bitdefender Broadcom Check Point Cisco CrowdStrike ESET F-Secure Palo Alto Networks Vendor A Vendor B	*All the active-response values shown in the table below were achieved at T0, and did not change over the 24-hour period (T1)*								

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	98.0%	100%	100%
Broadcom	98.0%	98.0%	98.0%
Check Point	96.0%	98.0%	98.0%
Cisco	96.0%	96.0%	96.0%
CrowdStrike	98.0%	98.0%	98.0%
ESET	96.0%	96.0%	96.0%
F-Secure	98.0%	98.0%	98.0%
Palo Alto Networks	98.0%	100%	100%
Vendor A	88.0%	88.0%	88.0%
Vendor B	90.0%	90.0%	90.0%

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.

	Time to Respond (in hours)								
	0 (T0)	<1	<2	<5	<10	<15	<20	<24	24 (T1)
Bitdefender Broadcom Check Point Cisco CrowdStrike ESET F-Secure Palo Alto Networks Vendor A Vendor B	*All the passive-response values shown in the table below were achieved at T0, and did not change over the 24-hour period (T1)*								

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%
Broadcom	100%	100%	100%
Check Point	100%	100%	100%
Cisco	100%	100%	100%
CrowdStrike	100%	100%	100%
ESET	100%	100%	100%
F-Secure	100%	100%	100%
Palo Alto Networks	100%	100%	100%
Vendor A	100%	100%	100%
Vendor B	100%	100%	100%

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	✓	✓	✓	✓	✓	✓
Broadcom	☐	☐	☐	✓	✓	✓
Check Point	☐	☐	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	☐	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	✓
F-Secure	☐	✓	☐	✓	✓	☐
Palo Alto Networks	☐	☐	✓	✓	✓	✓
Vendor A	☐	☐	✓	☐	✓	✓
Vendor B	✓	✓	☐	✓	☐	☐

Figure 9 — 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	✓	✓	✓	✓	✓	✓
Broadcom	✓	✓	✓	✓	✓	✓
Check Point	✓	☐	✓	☐	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	✓
F-Secure	☐	☐	✓	☐	✓	☐
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	☐	✓	☐	✓	✓
Vendor B	✓	☐	✓	☐	✓	✓

Figure 10 — 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 11 till Figure 17 provide information on the applicable capabilities of each of the tested products.

	Attack Visualization	Attack Timeline	Attack Phases	Attack Context
Bitdefender	✓	✓	✓	✓
Broadcom	✓	✓	✓	✓
Check Point	✓	✓	✓	✓
Cisco	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓
ESET	✓	✓	✓	✓
F-Secure	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓
Vendor A	✓	✓	☐	✓
Vendor B	✓	✓	✓	☐

Figure 11 – Threat Visibility

	Continuous Monitoring	Running applications and processes	Behaviour Monitoring (File/registry/etc..)	Whitelisting capability
Bitdefender	✓	✓	✓	✓
Broadcom	✓	✓	✓	✓
Check Point	✓	✓	✓	✓
Cisco	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓
ESET	✓	✓	✓	✓
F-Secure	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓
Vendor B	✓	✓	✓	✓

Figure 12 – System Visibility

	Standards-based API for access	Standard output format (JSON, Syslog, etc.)	Automated Data Export	Syslog Integration	Splunk Integration	Additional Reporting Features
Bitdefender	✓	✓	✓	✓	✓	✓
Broadcom	✓	✓	✓	✓	✓	✓
Check Point	✓	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	☐[4]	✓	✓	✓	✓	✓
F-Secure	✓	✓	✓	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	☐	✓	☐	☐	✓
Vendor B	☐	☐	✓	✓	✓	✓

Figure 13 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	✓	✓	✓	✓	✓	☐
Broadcom	✓	✓	✓	✓	✓	☐
Check Point	✓	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	☐[5]
F-Secure	☐	✓	✓	✓	☐	✓
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	✓	✓	✓	✓	☐	☐
Vendor B	✓	☐	✓	☐	☐	✓

Figure 14 – 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	✓	✓	☐	✓	✓	✓
Broadcom	✓	✓	☐	✓	✓	✓
Check Point	✓	✓	✓	✓	✓	✓
Cisco	✓	✓	☐	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓	✓
F-Secure	✓	✓	☐	☐	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓	✓
Vendor A	☐	✓	☐	☐	✓	✓
Vendor B	☐	☐	☐	✓	✓	✓

[4] ESET Enterprise Inspector has its own Public REST API (https://help.eset.com/eei/1.4/en-US/api.html)
[5] Granular reporting is possible only in ESET PROTECT.

Figure 15 – 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	✓	✓	✓	✓	✓
Broadcom	✓	✓	✓	✓	✓
Check Point	✓	✓	✓	✓	✓
Cisco	✓	✓	✓	✓	✓
CrowdStrike	✓	✓	✓	✓	✓
ESET	✓	✓	✓	✓	✓
F-Secure	✓	☐	✓	✓	✓
Palo Alto Networks	✓	✓	✓	✓	✓
Vendor A	✓	✓	☐	✓	✓
Vendor B	☐	☐	✓	✓	✓

Figure 16 – 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	✓	☐	☐	☐	☐	☐
Broadcom	✓	☐	☐	☐	☐	☐
Check Point	☐	☐	☐	☐	☐	☐
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	✓	☐	☐	☐	☐	✓
ESET	✓	☐	☐	☐	☐	☐
F-Secure	✓	☐	☐	☐	☐	☐
Palo Alto Networks	✓	✓	✓	✓	✓[6]	✓
Vendor A	☐	☐	☐	☐	☐	☐
Vendor B	☐	☐	☐	☐	☐	✓

Figure 17 – 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	☐	✓	☐	☐	☐	✓
Broadcom	☐	☐	☐	☐	☐	✓
Check Point	☐	☐	✓	☐	☐	✓
Cisco	✓	✓	✓	✓	✓	✓
CrowdStrike	☐	☐	☐	☐	☐	✓
ESET	☐	☐	☐	☐	☐	✓
F-Secure	☐	☐	☐	☐	☐	☐
Palo Alto Networks	✓	✓	✓	✓[3]	✓	✓
Vendor A	☐	☐	✓	☐	☐	✓
Vendor B	☐	✓	☐	☐	☐	✓

Figure 18 – External Data Correlation

[6] 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 (autumn 2021). 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
Broadcom Symantec Endpoint Security Complete	$565,450
Check Point Harmony Endpoint Advanced	$900,000
Cisco Secure Endpoint Essentials	$792,000
CrowdStrike Falcon Enterprise	$1,247,190
ESET PROTECT Enterprise with EEI and EDTD	$848,333
F-Secure Elements EDR and EPP for Computers	$528,100
Palo Alto Networks Cortex XDR Pro	$1,050,000
Product A	$795,980
Product B	$1,156,040

Figure 19 — 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.

Operational Accuracy (False Positives)

Operational accuracy test was performed by simulating a typical user activity in the enterprise environment. This included opening different file types and browsing to different websites. Furthermore, different administrator-friendly PowerShell scripts were also executed on the test environment to ensure that productivity was not affected after product installation and configuration.

	Result
Bitdefender	PASS
Broadcom	FAIL
Check Point	PASS
Cisco	PASS
CrowdStrike	PASS
ESET	PASS
F-Secure	PASS
Palo Alto Networks	PASS
Vendor A	FAIL
Vendor B	FAIL

Seven out of ten products passed the Operation Accuracy tests.

Threat actors have been utilizing living-of-the-land binaries to attack endpoints; these binaries are juicy targets for the attackers due to the fact that these are part of the operating system, in most cases signed by operating system provider with a valid digital certificate and trusted by users. **Broadcom** applied the product configuration policy to enable the blocking mode on these binaries to mitigate potential attack vectors. However, it should also be noted that some of these binaries like MS Build have legitimate use in developer environment where it can be used to compile programs and also depending upon the nature of externally packaged program, use of such binaries are required for program's operation. Having a block policy for such programs might hamper the operational environment for users. Furthermore, system administration tools like PsExec, which can be used by system administrators for administrative tasks, were blocked by default.

It should be noted that the products of **Bitdefender** and **ESET** stop the execution of a file that hasn't been previously seen and sends it to its 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. This behaviour is observed for both malicious and clean files. In the false positive tests on legitimate applications, the sandbox verdicts came back as clean within a short time, so the Operation Accuracy tests were passed.

The products of **Vendor A** and **Vendor B** blocked different innocent file types and admin-friendly scripts/tools, thus impacting the user's operability.

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 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[7] and NIST platform, such that it becomes easier to operationalize the risk regarding a specific endpoint.

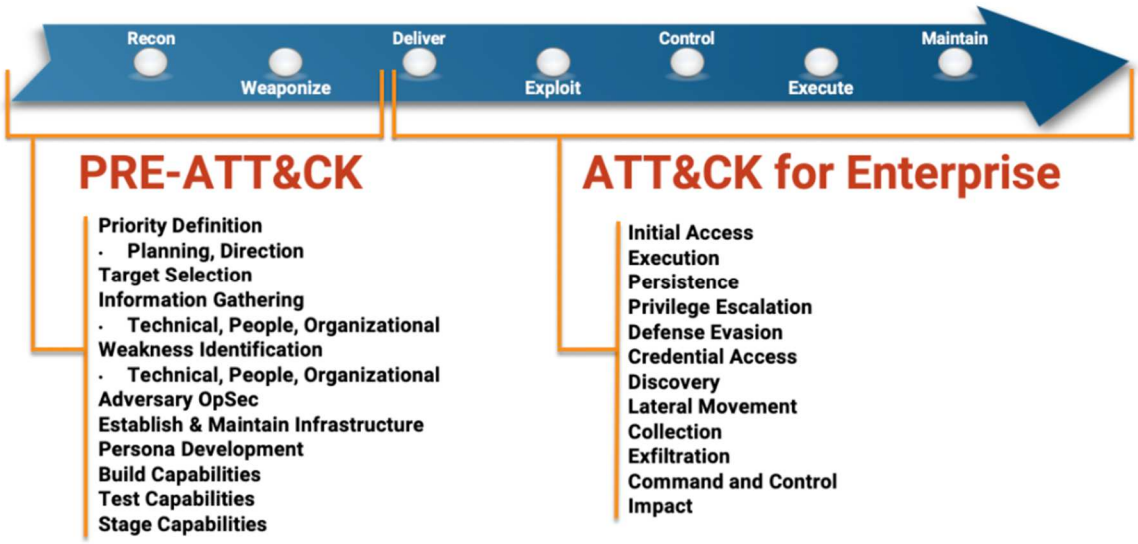

Figure 20: MITRE ATT&CK for Enterprise vs Seven Stage Cyber Attack LifeCycle[8]

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 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.

[7] © 2015-2021, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

[8] 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.

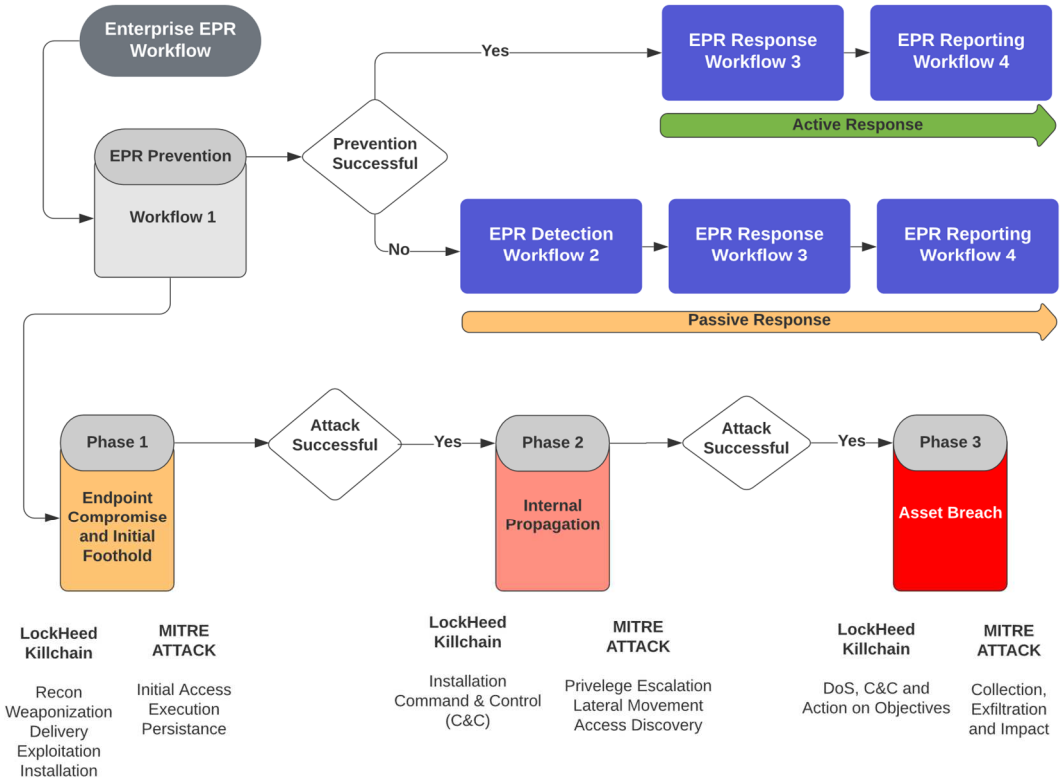

Figure 21 — Enterprise EPR Workflow Overview

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.

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.

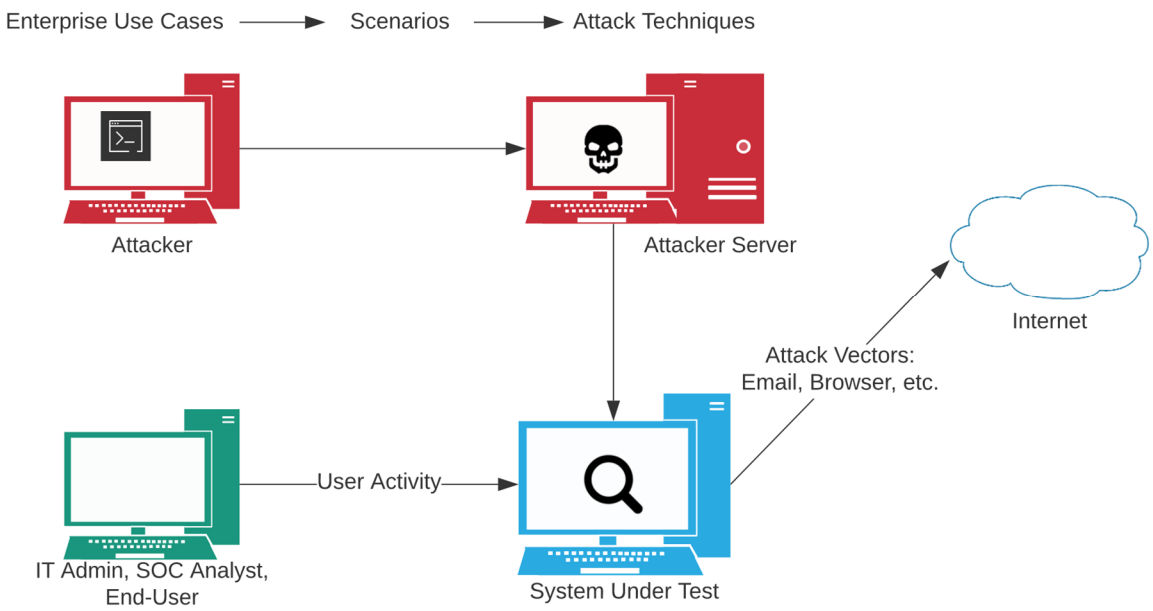

Figure 22 — EPR Test Topology Overview

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 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 an attacker-driven mindset as the attack progressed through the attack nodes to finally meet its objective. The evaluation was conducted in autumn 2021. 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 make 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 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 settings (i.e. settings used by the vendor for this test).

Bitdefender: "Risk Management", "Sandbox Analyzer" and "Scan SSL" were enabled. "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". "On-Access scan" for archives bigger than 100MB was enabled with depth 16.

Check Point: "Download (Web) Protection", "Anti-Bot", "Anti-Ransomware" and "Anti-Exploit" were set to "Prevent". "Forensic (Attack Analysis)" was set to "On". All settings were set to "Connected Mode".

Cisco: "First Time Setup 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" was enabled for "Automatic Analysis" and "Command Line Capture". "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: "Sensor Visibility" was set to "Enabled" for the following: "HTTP Detections, Engine, Redact HTTP Detection Details, Interpreter-Only, Additional User Mode Data" and "Script Based Execution Monitoring". "Cloud Machine Learning" and "Sensor Machine Learning" were set to "Extra Aggressive" for "Detection" and "Prevention". "Quarantine" was set to "Enabled". In "Malware Protection", "Execution Blocking" was set to "Enable ALL". "Exploit Mitigation", "Ransomware", "Lateral Movement and Credential Access", and "Remediation" were "Enabled"; "Exploitation Behaviour" was set to "Disabled".

ESET: All "Real-Time & Machine Learning Protection", "Potentially Unwanted Applications", "Potentially Unsafe Applications" and "Suspicious Applications" settings were set to "Aggressive" (non-default). "HIPS", "Self-Defense", "Protected Service", "Advanced Memory Scanner", "Exploit Blocker", "Deep Behavioral Inspection", "Ransomware Shield" and "HTTPS Filtering Mode" were set to "On". "Dynamic Threat Defense", "LiveGrid Feedback System" and "LiveGrid Reputation System" were set to "On". In ESET's "Dynamic Threat Defense", the "Detection Threshold" was set to "Suspicious" (non-default); the "Proactive Protection" was set to "Block Execution until Receiving Analysis Result" (non-default) and the "Max Wait Time for the Analysis Result" was set to "5 min".

F-Secure: “Real-time Scanning” and “File Scanning” were set to “On”. “Files to scan” was set to “Only files with specific extensions”; “Decide action on infection automatically” was set to “Off”; “Action on infection” was set to “Quarantine”; “Action on riskware” was set to “Block”; “Action on spyware” was set to “Quarantine”. “Protect Hosts File”, “Scan network drives”, “Scan network drives mode” and “Use F-Secure Security Cloud” were set to “On”. “DeepGuard” and “Block rare and suspicious files” were set to “On”. “AMSI”, “Web traffic scanning” and “Firewall” were set to “On”. “DataGuard” was set to “Off”. On the client, “PowerShell ScriptBlock logging” was enabled (non-default).

Palo Alto Networks: “Agent Settings”, “Agent Security”, “XDR Pro Endpoints”, “Content Auto Update” and “Direct Server Access” were enabled. “Alert Data Dump File Size” was set to “Full”. “Automatically Upload Alert Data Dump File”, “Agent Upgrade” and “Network Location Configuration” were disabled. “Browser Exploits Protection”, “Logical Exploits Protection”, “Known Vulnerable Processes Protection” and “Operating System Exploit Protection” were set to “Block”. “Exploit Protection for Additional Processes” was disabled. “Unpatched Vulnerabilities Protection” was set to “Modify Settings until the Endpoint is Patched”. “Portable Executable and DLL Examination”, “Office Files with Macros Examination”, “Behavioral Threat Protection”, “Ransomware Protection”, “Malicious Child Process Protection” and “Network Packet Inspection Engine” were set to “Block”. “Respond to Malicious Causality Chains”, “End-User Initiated Local Scan”, “Password Theft Protection” and “Monitor and Collect Forensic Data” were enabled. “Endpoint Scanning” was disabled.

Broadcom: The “Download Sensitivity” level was set to “5”; i.e. files with “5” or fewer users will have detection regardless of nature. “SONAR”, “Browser Intrusion Prevention”, “Network Intrusion Prevention”, and “Memory Exploit Mitigation” were set to “Enable”. “Tamper Protection” was set to “Block and Log”. In the “Incidents” section, all rules were enabled. In the “Intrusion Prevention Policy”, all “Audit Signatures” were enabled and set to “Log”. “Intrusion Prevention”, “Browser Protection” and “URL reputation” were enabled. “Server Performance Tuning” was disabled. All “Protection for Symantec Recommended Application Coverage” and “Java Protection” settings were enabled. All “Mitigation Techniques” were set to “Default (On)”. The “Endpoint Activity Recorder Status” was set to “On”; the following events were forwarded: “Load point Changes”, “Suspicious System activity”, “Heuristic detections”, “AMSI activity”, “ETW activity”, “Process launch activity”. “Live Shell Configuration” was “On”. In the “Antimalware Policy”, the “Intensity Level (Blocking Level)” was set to “3”. “Monitoring Level” was set to “5”. “DNS & Host File Changes” were set to “Ignore/Log-only”. For “Adaptive Protection”, the following policies were pushed to the endpoints:

Adobe Acrobat creating PE executable files	Monitor
Adobe Acrobat launching Assembly Registration Tool	Deny
Adobe Acrobat launching schtasks.exe	Deny
Adobe Acrobat launching Microsoft HTML Host	Deny
Adobe Acrobat launching Java applications	Deny
Adobe Acrobat launching InstallUtil.exe	Deny
Adobe Acrobat launching C-Sharp Compiler	Deny
Adobe Acrobat launching Windows Scripting Host (WScript)	Deny
Adobe Acrobat creating files in common persistence locations	Deny
Adobe Acrobat launching rundll32.exe	Monitor
Adobe Acrobat launching Windows Scripting Host (CScript)	Deny
Adobe Acrobat launching wmic.exe	Deny
Adobe Acrobat launching Msiexec	Deny
Adobe Acrobat launching PowerShell	Deny
Adobe Acrobat launching cmd.exe	Deny
Adobe Acrobat launching iKernel	Monitor
Adobe Acrobat launching Reg.exe	Deny
Adobe Acrobat launching RegSvr32.exe	Deny
Acrobat Reader launching cmd.exe	Deny

at.exe launching	Monitor
Bitsadmin launching	Monitor
Browser creating screensaver file	Monitor
Certutil creating PE executable	Deny
Certutil creating non-PE executable (scripts or batch jobs)	Deny
Certutil accessing network via HTTP(s)	Deny
CMSTP launching	Deny
Windows Scripting Host (CScript) creating files in common persistence locations	Monitor
Windows Scripting Host (CScript) injecting running processes	Monitor
Windows Scripting Host (CScript) modifying services registry entries	Deny
Windows Scripting Host (CScript) modifying Windows Task Scheduler settings to schedule tasks	Deny
Windows Scripting Host (CScript) launching Windows Scripting Host (CScript)	Deny
Windows Scripting Host (CScript) creating or modifying PowerShell profile script	Monitor
Windows Scripting Host (CScript) injecting into svchost.exe	Deny
Windows Scripting Host (CScript) launching Schtasks	Monitor
Windows Scripting Host (CScript) launching cmd.exe	Deny
Windows Scripting Host (CScript) launching Regsvr32	Deny
Windows Scripting Host (CScript) launching pubprn.vbs	Monitor
Windows Scripting Host (CScript) launching iKernel	Monitor
Windows Scripting Host (CScript) creating non-PE executable (scripts or batch jobs)	Monitor
Windows Scripting Host (CScript) launching Msiexec	Deny
Windows Scripting Host (CScript) launching PowerShell	Monitor
Windows Scripting Host (CScript) creating PE executable	Monitor
Windows Scripting Host (CScript) launching Microsoft HTML Host	Monitor
Windows Scripting Host (CScript) launching under a different process name	Deny
Windows Scripting Host (CScript) launching Windows Scripting Host (WScript)	Monitor
Windows Scripting Host (CScript) launching sc.exe	Monitor
Windows Scripting Host (CScript) launching winrm.vbs	Deny
Esentutl downloading a file	Deny
Microsoft Excel macros launching Msiexec	Monitor
Microsoft Excel macros launching iKernel	Monitor
Microsoft Excel macros launching Microsoft HTML Host	Deny
Microsoft Excel launching schtasks.exe	Deny
Microsoft Excel launching Reg.exe	Deny
Microsoft Excel macros launching Windows Scripting Host (WScript)	Deny
Microsoft Excel macros creating non-PE executable files	Monitor
Microsoft Excel macros launching InstallUtil.exe	Deny
Microsoft Excel macros launching Windows Scripting Host (CScript)	Monitor
Microsoft Excel macros launching cmd.exe	Monitor
Microsoft Excel launching wmic.exe	Deny
Microsoft Excel macros launching PowerShell	Deny
Excel launching Msbuild tools	Deny
Microsoft Excel launching RegSvr32.exe	Deny
Microsoft Excel launching Odbcconf.exe	Deny
Microsoft Excel launching Assembly Registration Tool	Deny
Microsoft Excel launching C-Sharp Compiler	Monitor
Microsoft Excel launching Bitsadmin.exe	Deny
Microsoft Excel macros creating files in common persistence locations	Monitor
Microsoft Excel macros creating PE executable files	Monitor
Microsoft Excel macros launching Java applications	Monitor
Expand downloading a file	Deny
Extrac32 downloading a file	Deny
Findstr downloading a file	Deny
Java applications launching Windows Scripting Host (CScript)	Monitor
Lsass loading an untrusted DLL	Deny
Makecab downloading a file	Deny
Mavinject injecting running processes	Deny
Microsoft Workflow Compiler launching	Deny
Msbuild creating PE executable	Deny
Microsoft HTML Host creating non-PE executable (scripts or batch jobs)	Monitor
Microsoft HTML Host creating PE executable	Deny
Microsoft HTML Host launching Schtasks	Deny

Microsoft HTML Host launching PowerShell	Monitor
Microsoft HTML Host accessing network via HTTP(s)	Deny
Microsoft HTML Host launching Windows Scripting Host (WScript)	Deny
Microsoft HTML Host modifying services registry entries	Deny
Microsoft HTML Host launching Windows Scripting Host (WScript)	Deny
Microsoft HTML Host launching Msiexec	Monitor
Microsoft HTML Host launching cmd.exe	Monitor
Microsoft HTML Host creating or modifying PowerShell profile script	Deny
Microsoft HTML Host launching iKernel	Monitor
Microsoft HTML Host launching Microsoft HTML Host	Monitor
Microsoft HTML Host launching under a different process name	Deny
Microsoft HTML Host launching Msbuild tools	Deny
Microsoft HTML Host launching sc.exe	Deny
Microsoft HTML Host injecting running processes	Deny
Microsoft HTML Host launching Windows Scripting Host (CScript)	Monitor
Microsoft HTML Host launching Windows Net utility (net.exe)	Monitor
Microsoft HTML Host modifying Windows Task Scheduler settings to schedule tasks	Deny
Microsoft HTML Host creating files in common persistence locations	Deny
Msiexec accessing network via HTTP(s)	Deny
Msxsl launching	Deny
Odbcconf executing a DLL file	Deny
Outlook creates a screensaver file	Deny
Microsoft Outlook executing cmd.exe	Deny
Microsoft PowerPoint launching PowerShell	Deny
Microsoft PowerPoint launching Bitsadmin.exe	Deny
Microsoft PowerPoint creating PE executable files	Deny
Microsoft PowerPoint creating PE executable files	Deny
Microsoft PowerPoint launching wmic.exe	Deny
Microsoft PowerPoint creating files in common persistence locations	Deny
Microsoft PowerPoint launching Assembly Registration Tool	Deny
Microsoft PowerPoint launching Microsoft HTML Host	Deny
Microsoft PowerPoint launching Msiexec	Deny
Microsoft PowerPoint launching Windows Scripting Host (WScript)	Deny
Microsoft PowerPoint launching C-Sharp Compiler	Deny
Microsoft PowerPoint creating non-PE executable files	Monitor
Microsoft PowerPoint launching Msbuild tools	Deny
Microsoft PowerPoint launching RegSvr32.exe	Deny
Microsoft PowerPoint launching Java applications	Deny
Microsoft PowerPoint launching schtasks.exe	Deny
Microsoft PowerPoint launching Windows Scripting Host (CScript)	Monitor
Microsoft PowerPoint launching Reg.exe	Deny
Microsoft PowerPoint launching cmd.exe	Deny
Microsoft Powerpoint launching InstallUtil.exe	Deny
Microsoft PowerPoint launching rundll32.exe	Monitor
PowerShell injecting into svchost.exe	Deny
PowerShell launching Java applications	Monitor
PowerShell launching iKernel	Monitor
PowerShell accessing network via HTTP(s)	Monitor
PowerShell creating or modifying PowerShell profile script	Monitor
PowerShell creating PE executable	Monitor
PowerShell launching with encoded command	Monitor
PowerShell launching Windows Scripting Host (WScript)	Monitor
PowerShell launching Windows Net utility (net.exe)	Monitor
PowerShell launching Microsoft HTML Host	Monitor
PowerShell injecting running processes	Monitor
PowerShell launching under a different process name	Deny
PowerShell modifying services registry entries	Monitor
PowerShell creating non-PE executable (scripts or batch jobs)	Monitor
PowerShell launching Windows Scripting Host (CScript)	Deny
PowerShell creating files in common persistence locations	Deny
PowerShell modifying Windows Task Scheduler settings to schedule tasks	Deny
PowerShell launching Msbuild tools	Monitor

PowerShell executing Windows Service Control utility (sc.exe)	Monitor
PowerShell accessing memory of Local Security Authentication Server (Lsass)	Monitor
PowerShell executing base64 encoded command	Monitor
PowerShell launching Schtasks	Monitor
Regasm launching	Monitor
Regedit dumping credentials in SAM registry key	Deny
Modifying registry run key with Windows Scripting Host (CScript) execution on system startup	Deny
Modifying registry run key with PowerShell execution on system startup	Monitor
Modifying registry run key with Wmic execution on system startup	Deny
Modifying registry run key with Windows Scripting Host (WScript) execution on system startup	Monitor
Modifying registry run key with Regsvr32 execution on system startup	Monitor
Modifying registry run key with Microsoft HTML Host execution on system startup	Monitor
Regsvc launching	Monitor
Regsvr32 injecting into svchost.exe	Deny
Regsvr32 creating PE executable	Deny
Regsvr32 launching Windows Scripting Host (CScript)	Deny
Regsvr32 creating files in common persistence locations	Monitor
Regsvr32 modifying Windows Task Scheduler settings to schedule tasks	Deny
Regsvr32 launching Schtasks	Deny
Regsvr32 accessing network via HTTP(s)	Deny
Regsvr32 creating or modifying PowerShell profile script	Deny
Regsvr32 launching PowerShell	Deny
Regsvr32 creating non-PE executable (scripts or batch jobs)	Deny
Regsvr32 modifying services registry entries	Monitor
Replace downloading a file	Deny
Rundll32 launching Schtasks	Deny
Rundll32 injecting into svchost.exe	Deny
Rundll32 creating files in common persistence locations	Monitor
Rundll32 accessing network via HTTP(s)	Deny
Rundll32 creating or modifying PowerShell profile script	Deny
Rundll32 creating non-PE executable (scripts or batch jobs)	Monitor
Rundll32 modifying Windows Task Scheduler settings to schedule tasks	Deny
Rundll32 modifying services registry entries	Monitor
Rundll32 launching Windows Scripting Host (CScript)	Monitor
Rundll32 creating PE executable	Monitor
Schtasks creating a job on PowerShell execution	Monitor
Schtasks creating a job on LNK file execution	Deny
Schtasks creating a job on HTA application execution	Deny
Schtasks creating a job on batch script execution	Monitor
Schtasks creating a job on JavaScript execution	Deny
Schtasks creating a job on VBScript execution	Monitor
Untrusted process modifying Windows Task Scheduler settings to schedule tasks	Monitor
Untrusted process launching iKernel	Monitor
Untrusted Process creating files in common persistence locations	Monitor
Wmic creating PE executable	Deny
Wmic accessing network via HTTP(s)	Deny
Wmic creating non-PE executable (scripts or batch jobs)	Deny
Wmic injecting running processes	Deny
WMI Provider Host (Wmiprvse) launching Regsvr32	Monitor
WMI Provider Host (Wmiprvse) creating files in common persistence locations	Deny
WMI Provider Host (Wmiprvse) launching Windows Scripting Host (WScript)	Monitor
WMI Provider Host (Wmiprvse) launching Rundll32	Monitor
WMI Provider Host (Wmiprvse) launching Microsoft HTML Host	Deny
Windows Management Instrumentation (WMI) launching Schtasks	Monitor
WMI Provider Host (Wmiprvse) launching Windows Scripting Host (CScript)	Monitor
WMI Provider Host (Wmiprvse) launching Windows Net utility (net.exe)	Monitor
WMI Provider Host (Wmiprvse) launching sc.exe	Monitor
WMI Provider Host (Wmiprvse) launching PowerShell	Monitor
Microsoft Word macros launching Msiexec	Deny
Microsoft Word macros launching Windows Scripting Host (WScript)	Deny
Microsoft Word macros launching cmd.exe	Monitor
Microsoft Word macros launching PowerShell	Deny

Microsoft Word macros launching Windows Scripting Host (CScript)	Deny
Microsoft Word launching Bitsadmin.exe	Deny
Microsoft Word launching wmic.exe	Deny
Microsoft Word macros creating PE executable files	Monitor
Microsoft Word launching Reg.exe	Deny
Microsoft Word macros launching Microsoft HTML Host	Deny
Microsoft Word macros creating non-PE executable files	Monitor
Microsoft Word macros launching Java applications	Deny
Microsoft Word launching C-Sharp Compiler	Monitor
Microsoft Word launching Odbcconf.exe	Deny
Microsoft Word macros launching InstallUtil.exe	Deny
Word launching Msbuild tools	Deny
Microsoft Word launching RegSvr32.exe	Deny
Microsoft Word macros creating files in common persistence locations	Deny
Microsoft Word launching schtasks.exe	Deny
Microsoft Word launching Assembly Registration Tool	Deny
Windows Scripting Host (WScript) creating non-PE executable (scripts or batch jobs)	Monitor
Windows Scripting Host (WScript) launching PowerShell	Monitor
Windows Scripting Host (WScript) injecting into svchost.exe	Deny
Windows Scripting Host (WScript) modifying Windows Task Scheduler settings to schedule tasks	Deny
Windows Scripting Host (WScript) launching iKernel	Monitor
Windows Scripting Host (WScript) creating or modifying PowerShell profile script	Deny
Windows Scripting Host (WScript) modifying services registry entries	Monitor
Windows Scripting Host (WScript) launching Windows Scripting Host (CScript)	Monitor
Windows Scripting Host (WScript) launching Windows Net utility (net.exe)	Monitor
Windows Scripting Host (WScript) launching Regsvr32	Monitor
Windows Scripting Host (WScript) launching under a different process name	Deny
Windows Scripting Host (WScript) creating files in common persistence locations	Deny
Windows Scripting Host (WScript) injecting running processes	Deny
Windows Scripting Host (WScript) launching Msiexec	Monitor
Windows Scripting Host (WScript) launching cmd.exe	Monitor
Windows Scripting Host (WScript) launching winrm.vbs	Deny
Windows Scripting Host (WScript) launching Rundll32	Monitor
Windows Scripting Host (WScript) launching pubprn.vbs	Deny
Windows Scripting Host (WScript) launching Windows Scripting Host (WScript)	Monitor
Windows Scripting Host (WScript) launching Schtasks	Monitor
Windows Scripting Host (WScript) launching sc.exe	Monitor
Windows Scripting Host (WScript) creating PE executable	Monitor
Windows Scripting Host (WScript) launching Msbuild tools	Deny
Windows Scripting Host (WScript) launching Microsoft HTML Host	Monitor

Vendor A: Non-default settings were used.

Vendor B: Non-default settings were used.

Copyright and Disclaimer

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

AV-Comparatives
(January 2022)

Icons: feathericons.com