Independent Tests of
Anti-Virus Software

Endpoint Prevention and Response (EPR) Product Validation Report

Cisco Secure Endpoint Essentials

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

WWW.AV-COMPARATIVES.ORG

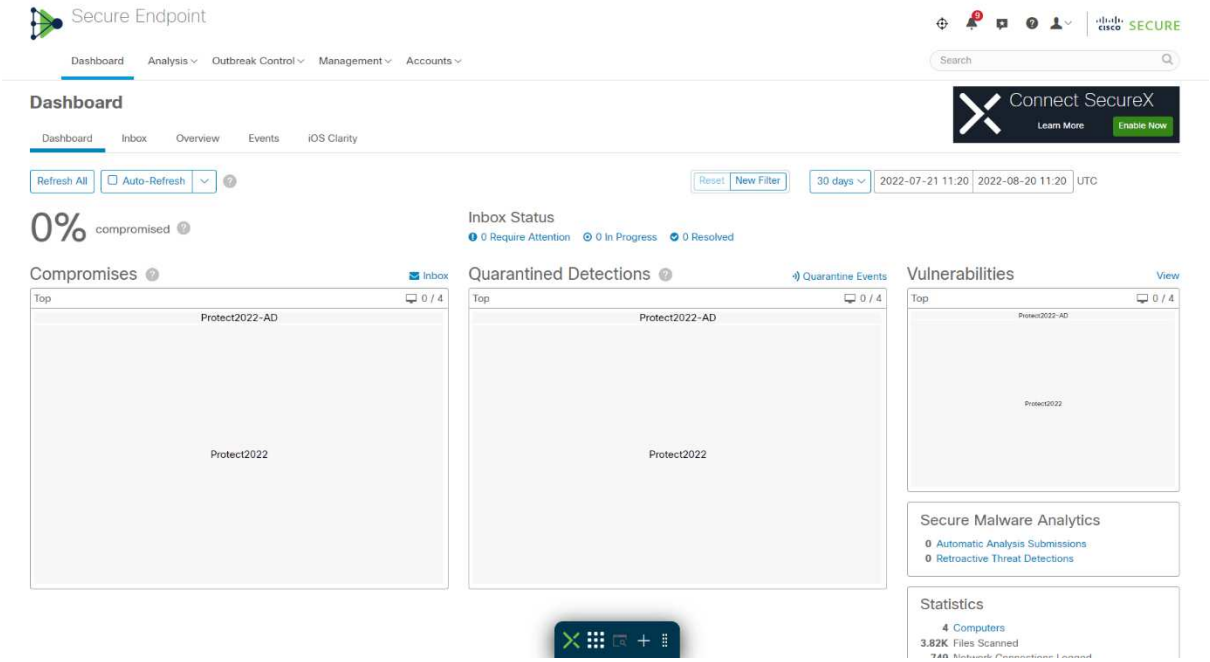
Content

TESTED PRODUCT	3
PRODUCT THUMBNAIL	3
HARDWARE AND SOFTWARE REQUIREMENTS	3
CISCO EPR PRODUCT: EXECUTIVE SUMMARY	4
MITRE ATT&CK MATRIX FOR ENTERPRISE	7
PHASE 1 METRICS: ENDPOINT COMPROMISE AND FOOTHOLD	8
PHASE 2 METRICS: INTERNAL PROPAGATION	10
PHASE 3 METRICS: ASSET BREACH	11
OPERATIONAL-ACCURACY AND WORKFLOW-DELAY COSTS	12
EPR COMPETITIVE PRODUCT DIFFERENTIATOR (PROVIDED BY CISCO)	14
PRODUCT FEATURES	15
CISCO PRODUCT RESPONSE MECHANISM	17
CENTRAL MANAGEMENT AND REPORTING	18
CISCO PRODUCT CONFIGURATIONS AND SETTINGS	20
APPENDIX	21
ABOUT THIS TEST	26
COPYRIGHT AND DISCLAIMER	27

Tested Product

Cisco Secure Endpoint Essentials was tested by AV-Comparatives in summer 2022. The product version number was 7.5.

Product Thumbnail



Cisco Secure Endpoint Essentials management console

Hardware and Software Requirements

To help system administrators assess the compatibility of the security product with their existing IT infrastructure, we have listed below its hardware and software requirements for endpoints (as provided by the respective vendor). For hardware, we consider CPU, RAM and system-disk space required, with figures for both minimum (acceptable) and recommended (optimal) configurations. For software, we include any additional software needed (e.g. a specific .NET Framework version), and configuration (e.g. enabling file sharing).

***Minimum* hardware requirements for Windows 10/11 client PCs:**
CPU: 1 GHz processor
RAM: 2 GB
Disk space: 650 MB (Cloud-Only Mode); 1 GB (TETRA)

***Recommended* hardware requirements for Windows 10/11 client PCs:**
CPU: 2.6 GHz processor
RAM: 16 GB
Disk space: 256 GB *total* disk space

Software and configuration requirements for Windows 10/11 client PCs:
None

Cisco EPR Product: Executive Summary

Cisco Secure Endpoint Essentials was tested by AV-Comparatives to validate if the product could provide effective enterprise prevention and response capabilities.

Cisco Secure Endpoint Essentials did exceptionally well at handling threats targeted towards enterprise users, in particular before the threat could progress inside and infiltrate the organisation's network. The product demonstrated several safeguards that helped in protecting the enterprise systems and network against the scenarios we tested.

The product's management console was easy to use, intuitive, and provided contextual data useful to SOC analysts in determining which threats to prioritize. The product had different response options for mitigated threats, and information for the SOC analyst to further investigate/inspect.

The product had good mapping to MITRE's TTPs, thus providing low-level SOC analysts with the data needed to investigate further and escalate when necessary. Alerts were prioritized and aggregated, so as to minimize noise from all the alerts generated. The product can be easily configured and deployed in a domain or workgroup environment.

Active Response (Prevention): This occurs when the product stops the attack automatically, and reports it. Cisco had an Active Response to **50/50** scenarios across all the phases tested. This resulted in a cumulative Active Response rate of **100**%.

Passive Response (Detection): This occurs when the product does not stop the specific attack phase, but reports suspicious activity. Cisco had a Passive Response to **50/50** scenarios across all the phases tested. This resulted in a cumulative Passive Response rate of **100**%.

Operational Accuracy Costs: These occur when legitimate programs/actions are blocked/detected. Cisco had **few costs** arising from imperfect Operational Accuracy.

Workflow Delay Costs: These arise e.g. when the user has to wait while a file is being analysed by the product. Cisco had **no costs** relating to workflow delays.

Description	Details
EPR Certification Level Reached:	**Strategic Leader**
Overall **Active Response** Rate (Prevention Rate):	**100%**
Overall **Passive Response** Rate (Response Rate):	**100%**
Operational Accuracy Costs:	**Low**
Workflow Delay Costs:	**None**

Executive Summary

The table below depicts Cisco's EPR prevention & detection rates across the different phases and categories of attack. For more details on the workflows and phases, please see the appendix.

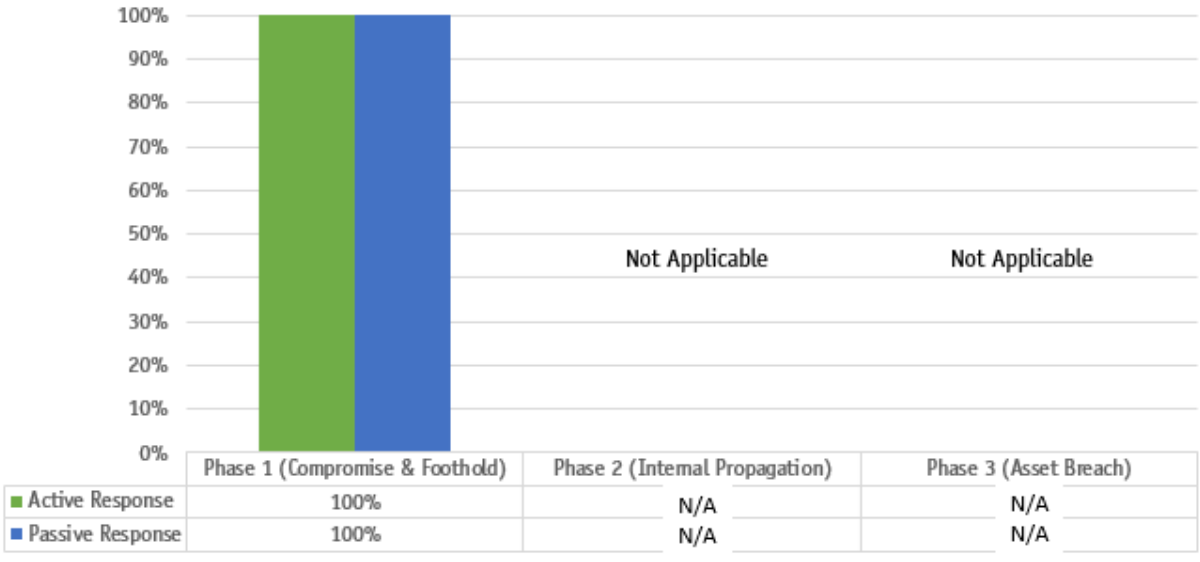
Description	Number Tested
Scenarios	50
Phases	**Combined Prevention & Detection**
Phase 1 (Compromise & Foothold)	
Active Response (Prevention)	100%
Passive Response (Detection)	100%
Phase 2 (Internal Propagation)	
Active Response (Prevention)	N/A
Passive Response (Detection)	N/A
Phase 3 (Asset Breach)	
Active Response (Prevention)	N/A
Passive Response (Detection)	N/A
Operational Accuracy Costs	Few
Workflow Delay Costs	None

Combined Prevention & Detection Rates

Cisco prevented 100% of the scenarios already in Phase 1 (Compromise and foothold). Hence, none of the scenarios progressed to next phases.

The graphic below breaks down Cisco's Active versus Passive Response capabilities for the duration of the test.

"**Not Applicable**" below thus indicates that no test scenario was able to progress to Phases 2 or 3.



Active vs Passive Response of Cisco Secure Endpoint Essentials

Modern threats usually come with layers of techniques to evade prevention and response, such as encryption, obfuscation, anti-analysis, packing, file-less malware, exploit, and privilege escalation.

AV-Comparatives' Enterprise EPR methodology covers some of the most prevalent enterprise scenarios and system-administrator EPR workflows, specifically requested by enterprises based on inquiries and primary research.

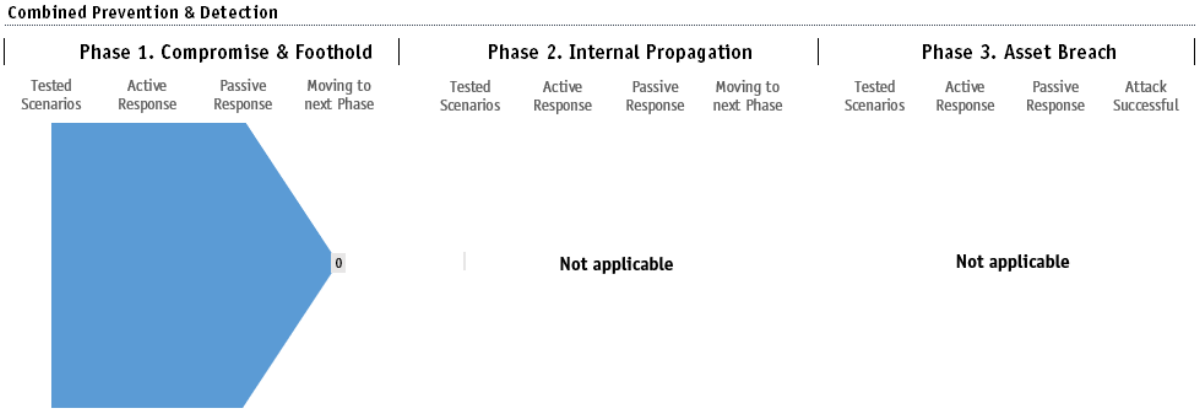
Cumulative Prevention and Response by phases

Response Type	Phase 1 Only	Phase 1 & 2	Overall (Phase 1, 2 & 3)
Active Response	100% (50/50)	100% (50/50)	100% (50/50)
Passive Response	100% (50/50)	100% (50/50)	100% (50/50)

Cumulative Prevention and Response by Phase

The graphic below depicts Cisco's Active and Passive Response capabilities in the three attack phases tested.

"**Not Applicable**" indicates that no test scenario was able to progress to Phase 3.



EPR Efficacy per Phase of Cisco Secure Endpoint Essentials

Phase 1:

- 50 out of 50 scenarios prevented
- 50 out of 50 scenarios detected
- No scenario was able to progress to Phase 2.

Phase 2:

- Not applicable, because no scenario was able to progress to Phase 2.

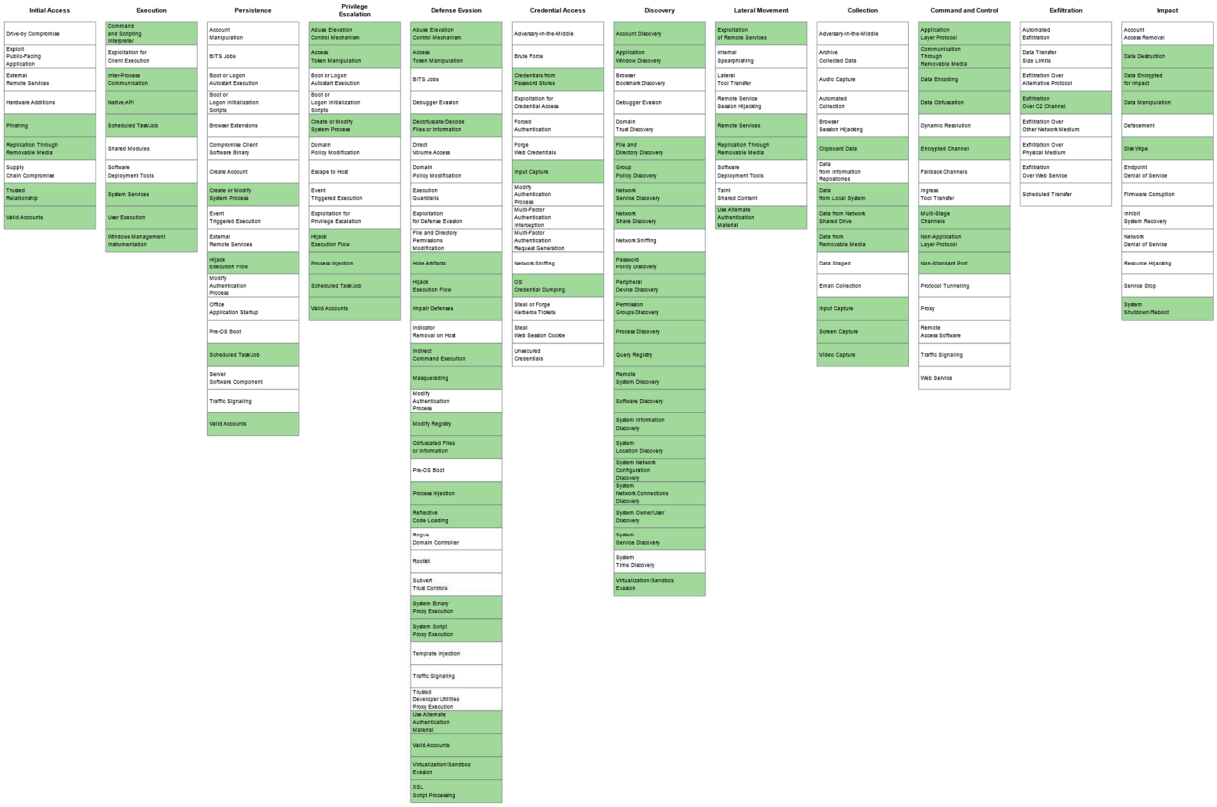
Phase 3:

- Not applicable, because no scenario was able to progress to Phase 3.

MITRE ATT&CK Matrix for Enterprise

The diagram below[1] shows the entire MITRE ATT&CK Matrix for Enterprise[2]. The column headings represent the ATT&CK Tactics[3] (aims), while the boxes below them represent the ATT&CK Techniques[4] used to achieve those goals. Our EPR test covers the entire attack chain shown here, using the most realistic possible scenarios. Across the 50 attack scenarios used in this EPR test, we tried to employ all of the Techniques shown in the green boxes below.

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



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

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

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

[1] Generated with https://mitre-attack.github.io/attack-navigator/
[2] https://attack.mitre.org/matrices/enterprise/
[3] https://attack.mitre.org/tactics/enterprise/
[4] https://attack.mitre.org/techniques/enterprise/

Phase 1 Metrics: Endpoint Compromise and Foothold

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

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

Cisco Secure Endpoint Essentials was subjected to the various attack steps as highlighted above and described in detail in AV-Comparatives' EPR CyberRisk Test Methodology. The resulting table below showcases the product's Active Response and Passive Response capabilities for the attack scenarios in Phase 1.

Tested Scenario	Description	Active Response	Passive Response
1	PowerShell Empire - Obfuscated PowerShell in-memory	✓	✓
2	PowerShell Empire - AMSI bypass with in-memory payload	✓	✓
3	PowerShell Empire - MS Word Macro	✓	✓
4	PowerShell Empire - WMIC/XSL Oneliner	✓	✓
5	PowerShell Empire - Rundll32 Encrypted DLL	✓	✓
6	PowerShell Empire - Masqueraded PowerShell binary	✓	✓
7	PowerShell Empire - VBScript	✓	✓
8	PowerShell Empire - Shortcut Payload	✓	✓
9	PowerShell Empire - MS Excel Macro	✓	✓
10	PowerShell Empire - JavaScript	✓	✓
11	PowerShell Empire - MS Word Macro	✓	✓
12	PowerShell Empire - JavaScript MSIexec	✓	✓
13	PowerShell Empire - JavaScript Excel	✓	✓
14	PowerShell Empire - Batch File	✓	✓
15	PowerShell Empire - Obfuscated VBScript	✓	✓
16	Covenant - Obfuscated PowerShell from file	✓	✓
17	Covenant - AMSI bypass with a PowerShell payload from file	✓	✓
18	Covenant – Obfuscated Binary	✓	✓
19	Covenant - WMIC/XSL Oneliner	✓	✓

20	Covenant - PowerShell Oneliner	✓	✓
21	Covenant - Rundll32	✓	✓
22	Covenant - Masqueraded Binary	✓	✓
23	Covenant – Encrypted Binary	✓	✓
24	Covenant - JavaScript MSIexec	✓	✓
25	Covenant - MS Office Macro: Excel	✓	✓
26	Covenant – Staged JavaScript	✓	✓
27	Covenant - Batch File Stager	✓	✓
28	Covenant - HTML Help File	✓	✓
29	Covenant – Staged Binary	✓	✓
30	Covenant - JavaScript	✓	✓
31	Metasploit Framework - Obfuscated PowerShell in-memory	✓	✓
32	Metasploit Framework - AMSI bypass with PowerShell payload in-memory	✓	✓
33	Metasploit Framework - MS Word Macro	✓	✓
34	Metasploit Framework – Encrypted HTA	✓	✓
35	Metasploit Framework - VBScript	✓	✓
36	Metasploit Framework - VBA-EXE	✓	✓
37	Metasploit Framework - HTA	✓	✓
38	Metasploit Framework – Default Binary	✓	✓
39	Metasploit Framework - Batch File Stageless	✓	✓
40	Metasploit Framework - Batch File Stager	✓	✓
41	BRc4 - AMSI bypass & ETW patching combined with a PS payload in-memory	✓	✓
42	BRc4 - Rundll32	✓	✓
43	BRc4 – Stageless Binary	✓	✓
44	BRc4 - MS Excel Macro	✓	✓
45	BRc4 - Batch File Stager	✓	✓
46	Metasploit Framework - Staged PowerShell	✓	✓
47	Metasploit Framework – Encrypted MS Word Macro	✓	✓
48	Metasploit Framework - Obfuscated HTA	✓	✓
49	Metasploit Framework - MSI	✓	✓
50	Metasploit Framework - Stageless HTA	✓	✓

Phase 1: Active versus Passive Response of Cisco Secure Endpoint Essentials

✗ - Indicates the product **failed** to prevent/detect the attack in the tested scenario during this phase.
✓ - Indicates the product **successfully** prevented/detected the attack in the tested scenario during this phase.

In all 50 test scenarios in Phase 1, Cisco provided both a Passive Response (detection) and an Active Response (prevention).

Phase 2 Metrics: Internal Propagation

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

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

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

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

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

Lateral Movement: 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.

Tested Scenario	Description	Active Response	Passive Response
N/A	N/A	N/A	N/A

Phase 2: Active versus Passive Response of Cisco Secure Endpoint Essentials

Phase 2 scenarios were N/A (not applicable) to Cisco, as the threats had already been prevented in Phase 1.

Phase 3 Metrics: Asset Breach

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

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

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

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

Tested Scenario	Description	Active Response	Passive Response
N/A	N/A	N/A	N/A

Phase 3: Active versus Passive Response of Cisco Secure Endpoint Essentials

Phase 3 scenarios were N/A (not applicable) to Cisco, as the threats had already been prevented in Phase 1.

Operational-Accuracy and Workflow-Delay Costs

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

Costs arising from imperfect operational accuracy

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

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

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

		Operational Accuracy	
Group	Number of affected scenarios	*Active Response Multiplying Factor*	*Passive Response Multiplying Factor*
None	0	x0	x0
Low	1	x1	x0.75
Moderate	2-3	x5	X3.75
High	4-5	x10	x7.5
Very High	6+	x20	x15

Multiplying factors for Operational Accuracy costs

The costs arising from imperfect Operational Accuracy are worked out using Cost Units of USD 1.43 million. The number of Cost Units a product is deemed to have caused is calculated using a Multiplying Factor. This varies according to the Group, and also whether the scenario was affected by an Active Response (action blocked), or by a Passive Response (action not blocked, but detection alert shown in the console). The Multiplying Factor for an erroneous Passive Response is always three-quarters of that of an erroneous Active Response, because less time and effort is required to resolve the problem.

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

Costs arising from workflow delays

Some EPR products will cause delays in the user's workflow because they e.g. stop the execution of a previously unknown file and send it to the vendor's online sandbox for further analysis. Due to this behaviour, execution is stalled, and the user is not able to proceed till the analysis comes back from the sandbox. We noted the delay caused by such analysis, for both scenarios we knew to be clean and scenarios we knew to be malicious.

Where a product caused significant delays when analysing a scenario, this was penalised. The analysis time for each product was calculated as follows. For *clean* scenarios, we took the longest observed delay for any one scenario. So, for example, a product with two delays - of 2 minutes and 10 minutes respectively - for *clean* scenarios would have a recorded time of 10 minutes. For *malicious* scenarios, we took the average of all the delays. So, a product with two delays - of 2 minutes and 10 minutes respectively - for *malicious* scenarios, would have a recorded time of 6 minutes. Products are then assigned to one of five Workflow Delay Groups (None, Low, Moderate, High and Very High), depending on how long the respective delay is. These are shown in the table below.

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

Multiplying factors for Workflow Delay costs

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

Results

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

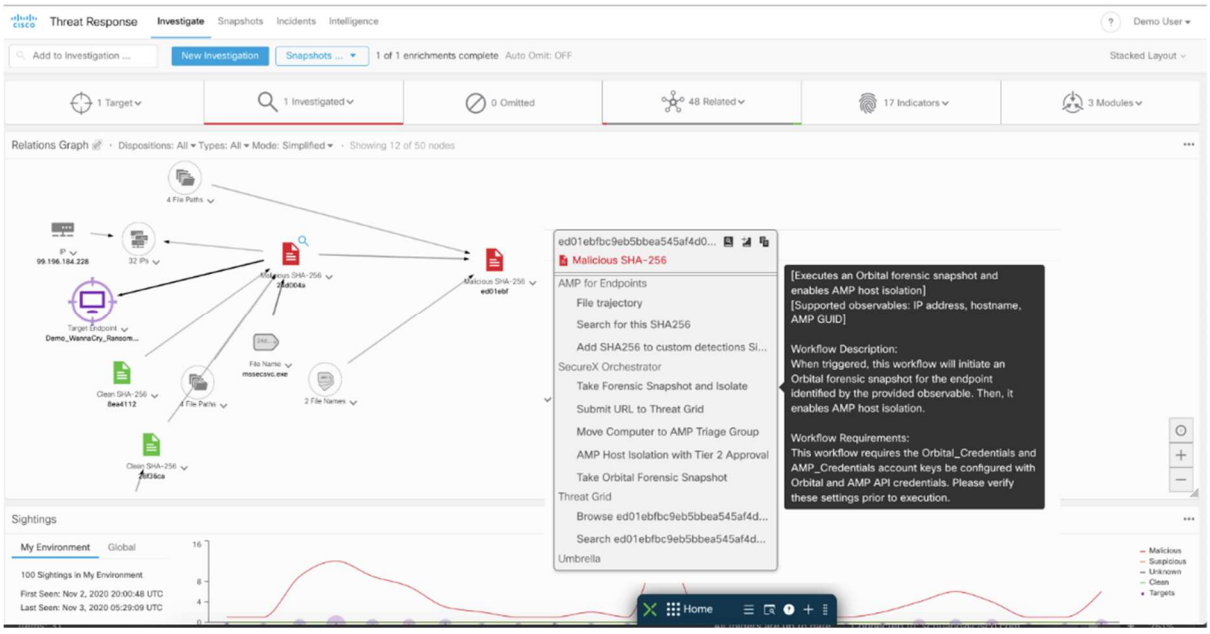
	Operational Accuracy		Workflow Delays
	Active Response	*Passive Response*	
Cisco	None	Few	Low

Combined results table for Operational Accuracy and Workflow Delays

Cisco incurred some (minor) Operational Accuracy costs for Passive Responses.

EPR Competitive Product Differentiator (provided by Cisco)

- Cisco Secure Endpoint helps simplify security with a cloud-native, built-in platform experience that connects our Cisco Secure portfolio and existing customer infrastructure. It is integrated and open for simplicity, unified in one location for visibility, and maximizes operational efficiency with automated workflows. Radically reduce threat dwell time and human-powered tasks to stay compliant and counter attacks.
- Cisco Secure Endpoint is industry-recognized (AV-Comparatives Enterprise Main-Test Series and Techvalidate) to be simple to deploy and use and provides EPP and EDR capabilities within a single agent.
- Cisco Secure Endpoint is amongst the few leading solutions that offer an on-premises offering that can be supported in air-gapped environments.
- Cisco Secure Endpoint is recognized to be natively integrated with a broad range of Cisco security products in the portfolio; providing a "see it once, block it everywhere" capability to customer security infrastructure investments.
- Cisco Secure Endpoint is powered by Cisco Talos Intelligence Group which is one of the largest commercial threat intelligence teams in the world, comprised of over 350 world-class researchers, analysts, and engineers. Talos is supported by unrivaled telemetry from the Cisco product portfolio covering IPS, identity, firewalls, endpoint, email, web, DNS, and more; and sophisticated systems to create accurate, rapid, and actionable threat intelligence for Cisco customers.
- Cisco Secure Endpoint leverages multiple layers of integrated detection techniques and does not rely on a specific detection technology that may be subject to adversary training.
- Cisco Secure Endpoint comes with cloud-based sandboxing for built-in dynamic file analysis.
- Cisco Secure Endpoint provides endpoint protection, detection, and response in a single agent with the broadest platform support: Windows, macOS, Linux, Android, and Apple iOS.
- Cisco Secure Endpoint is redefining endpoint security by bringing together user and device protection. The DUO + Cisco Secure Endpoint integration allows customers to realize risk-based access control, preventing compromised devices from being used for multi-factor authentication.



Cisco Secure Endpoint's SecureX Threat Response

Product features

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

Support features

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

Support features

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

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

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

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

General features

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

Product Name	Cisco Secure Endpoint Essentials
Third-party scan engine used (in addition to its own)	Bitdefender
Phishing protection for web browsers (blocking of phishing URLs)	✓
Web access control (custom blacklisting of specific site categories such as adult content)	☐
Device control (manage/block external drives)	✓
Sandbox feature	✓
2-factor authentication: obligatory/optional/not included	Obligatory
Remote shell capability: GUI/command line/not included	Not included
Right-click on-demand scan of files/folders	✓
Can the endpoint client be password protected from the console to prevent users changing settings?	✓
Can the endpoint client be password protected from the console to prevent users uninstalling it?	✓
Which interface languages is the endpoint client available in?	English, Japanese, Korean, Chinese
Which interface languages is the management console available in?	

General features

Cisco Product Response Mechanism

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

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

Response Actions	Cisco
Quarantine	✓
Delete Files and Directories	✓
Process Termination	✓
Shutdown or Reboot of Endpoint	✓
Edit Registry Keys and Values	✓
Network Isolation	✓
User Isolation	✓
Execution Prevention	✓
Block Processes from Communication	✓
Uninstall Services	✓
System Restoration	✓
System Imaging	✓
Patching	✓
Guided Response Available	✓

EPR Response actions

Central Management and Reporting

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

Management: Threat Visibility, System Visibility, and Data Sharing

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

Reporting Features	Cisco
Threat Visibility	
Attack Visualization, Context, Timeline	✓
System Visibility	
Continuous Monitoring	✓
Running applications & process	✓
Behaviour Monitoring (File/registry/etc..)	✓
Whitelisting capability	✓

Threat & System Visibility

Data Sharing Features	Cisco
Customizable default security policies	✓
Customized reporting and management	✓
Custom reporting and filtering	✓
Report automation	✓
Standard output format (JSON, Syslog, CEF, etc..)	✓
Splunk & Syslog integration	✓
Automated data export	✓
Policy and/or signature rollback	✓
System scanning capability	✓
Integration with security products	✓
Standards-based application programming interface (API) for access	✓
Disaster Recovery	✓
Audit trail support in the management console	✓
Management to agent encryption	✓
Encryption of data at rest	▢
Multiple EPR system-administrator/user-focused workflow support	✓
Enterprise recording and data storage – forensic analysis	✓
Built-in-reporting capabilities for different user categories	✓
Cloud marketplace support	✓
Compliance reports (GDPR, PCI-DSS, etc.)	▢

Management: Threat Visibility, System Visibility, and Data Sharing

EPR Product Reporting Capabilities

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

IOC Integration

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

External Data Correlation	Cisco
Threat Intelligence data assimilation	✓
SIEM	✓
Proprietary product integration (NGFW, IPS, ...)	✓
YARA Signatures	✓
Support of IoC upload	✓
Sandboxing logs	✓
Scan results	✓
Retrospective analysis and logs	✓
Endpoint prevention product logs	✓
Multi-factor authentication logs	✓
Network traffic flow logs	✓
DNS Logs	✓
DHCP Logs	✓

External data correlation

Cisco Product Configurations and Settings

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

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

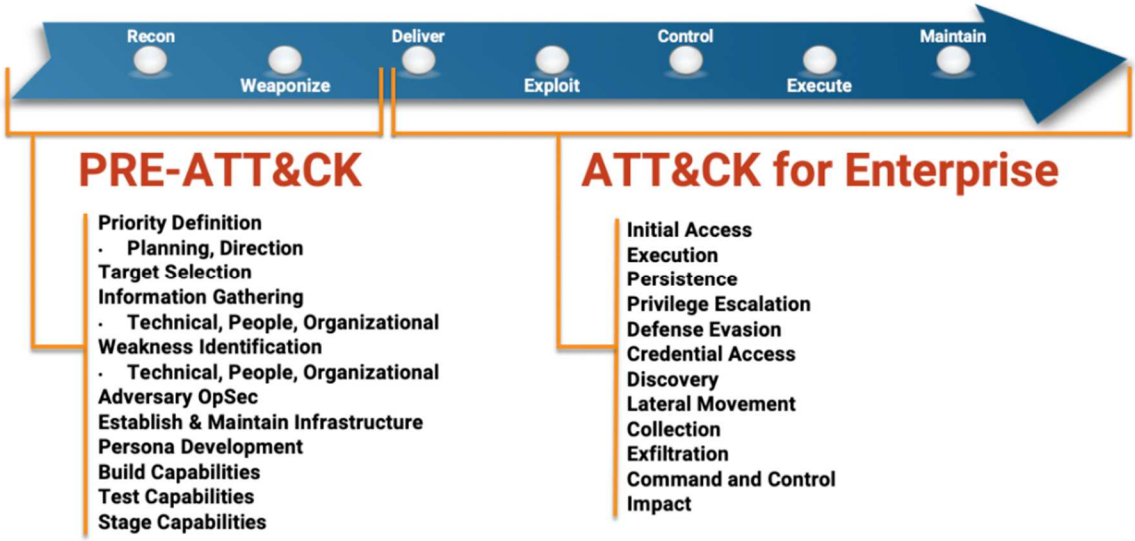
Below we have listed relevant non-default settings (i.e. settings used by the vendor for this test).

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

Appendix

Endpoint Prevention Response vs MITRE ATT&CK Framework

This EPR product report is a comprehensive validation of features, product efficacy and other relevant metrics to guide your risk assessment. A total of 50 scenarios were executed against real-world enterprise use-cases. These scenarios comprised several prevention and detection workflows operating under normal operational environments by different user personas. The results for the validation can be efficiently and effectively mapped to the MITRE ATT&CK® Platform[5] and NIST platform, so that it becomes easier to operationalize the risk regarding a specific endpoint.



MITRE ATT&CK for Enterprise vs Seven Stage Cyber Attack LifeCycle[6]

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

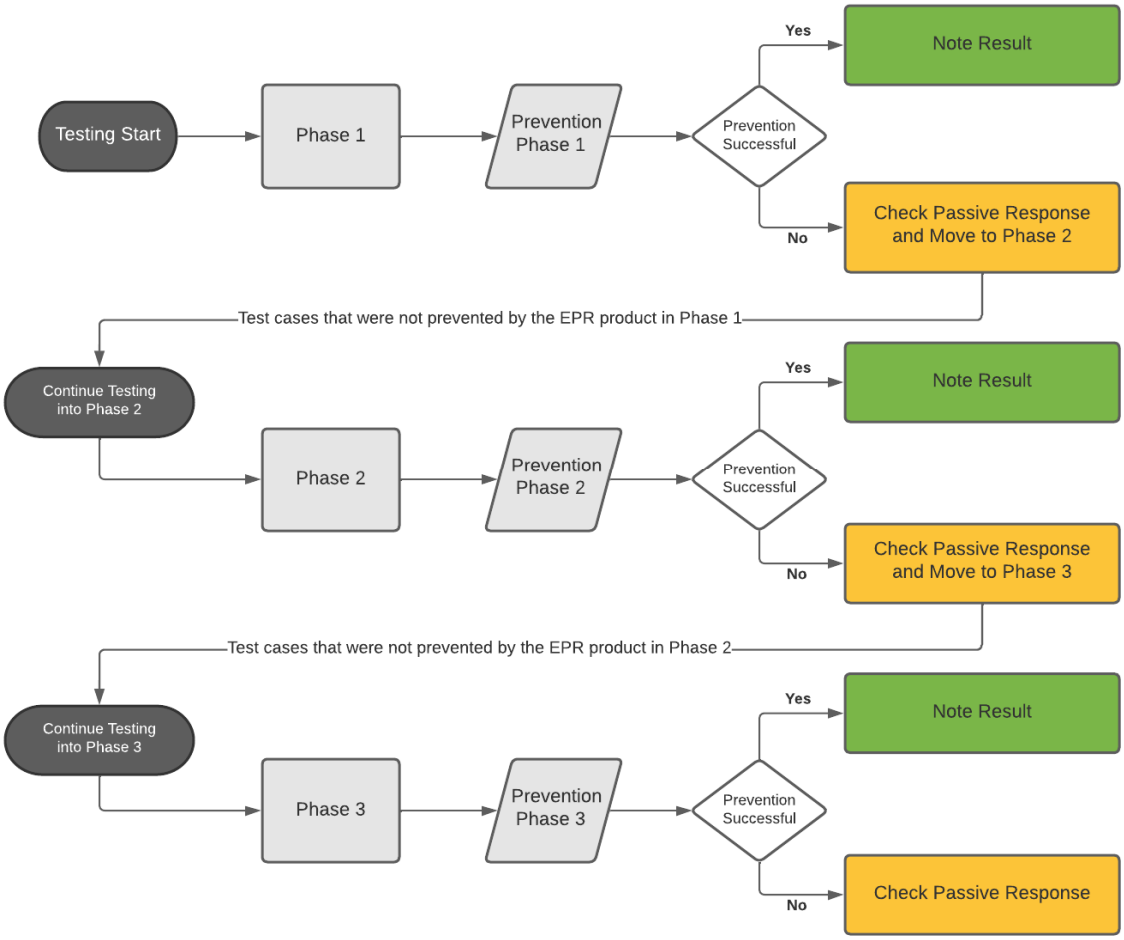
As illustrated in the graphic on the next page, we moved away from "atomic" testing, i.e. tests that only look at a particular component of the ATT&CK framework, and instead evaluated the EPR products from the context of the entire attack kill-chain, with workflows interconnecting at every stage from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

[5] © 2015-2022, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

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

EPR Testing Workflow

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



Enterprise EPR Workflow Overview

Prevention (Active Response)

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

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

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

Detection (Passive Response)

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

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

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

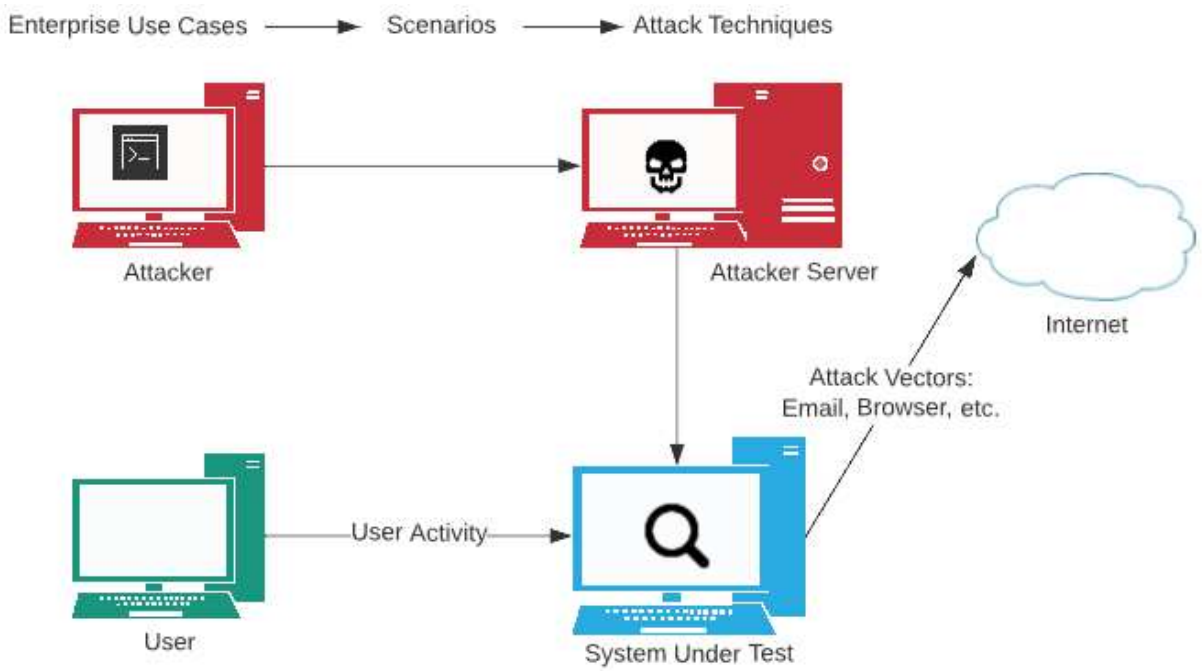
Correlation of Process, Endpoint and Network

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

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

EPR Validation Overview

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



EPR Test Topology Overview

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

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

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

Test Objective

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

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

Targeted Use-Cases

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

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

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

The test was conducted in summer 2022, and used an attacker-driven mindset as the attack progressed through the attack nodes to finally meet its objective. User activities were simulated throughout the test such that they were as close to a real-life environment as possible. Once the attacker got initial access to the environment, they tried to be as stealthy as possible so that defence mechanisms would not be triggered.

All the attacks were crafted using open-source and commercial tools[7]/frameworks, and were developed using in-house expertise. The reason why we included commercial C2 frameworks is that these are frequently misused[8] by attackers in real-life APTs; not using them would cause a „blind spot" and lead to a false sense of security. Due to license agreement restrictions, we took measures to prevent samples created by commercial C2 frameworks from being distributed to the EPR vendors. These restrictions are made to prevent vendors from focussing on the tools instead of the techniques.

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

[7] https://attack.mitre.org/software/

[8] https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/

About this test

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

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

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

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

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

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

To get an overall picture of the protection and response capabilities of any of the tested EPR products, readers should look at the results of the other tests in AV-Comparatives' Enterprise Main-Test Series[9] too.

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

Copyright and Disclaimer

This publication is Copyright © 2022 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(October 2022)

Credits: Icons made by icon_king1 from freeicons.io