www.av-comparatives.org

EPR Product Validation

Kaspersky EDR Expert (on-premises)

Test period:
June – August 2025

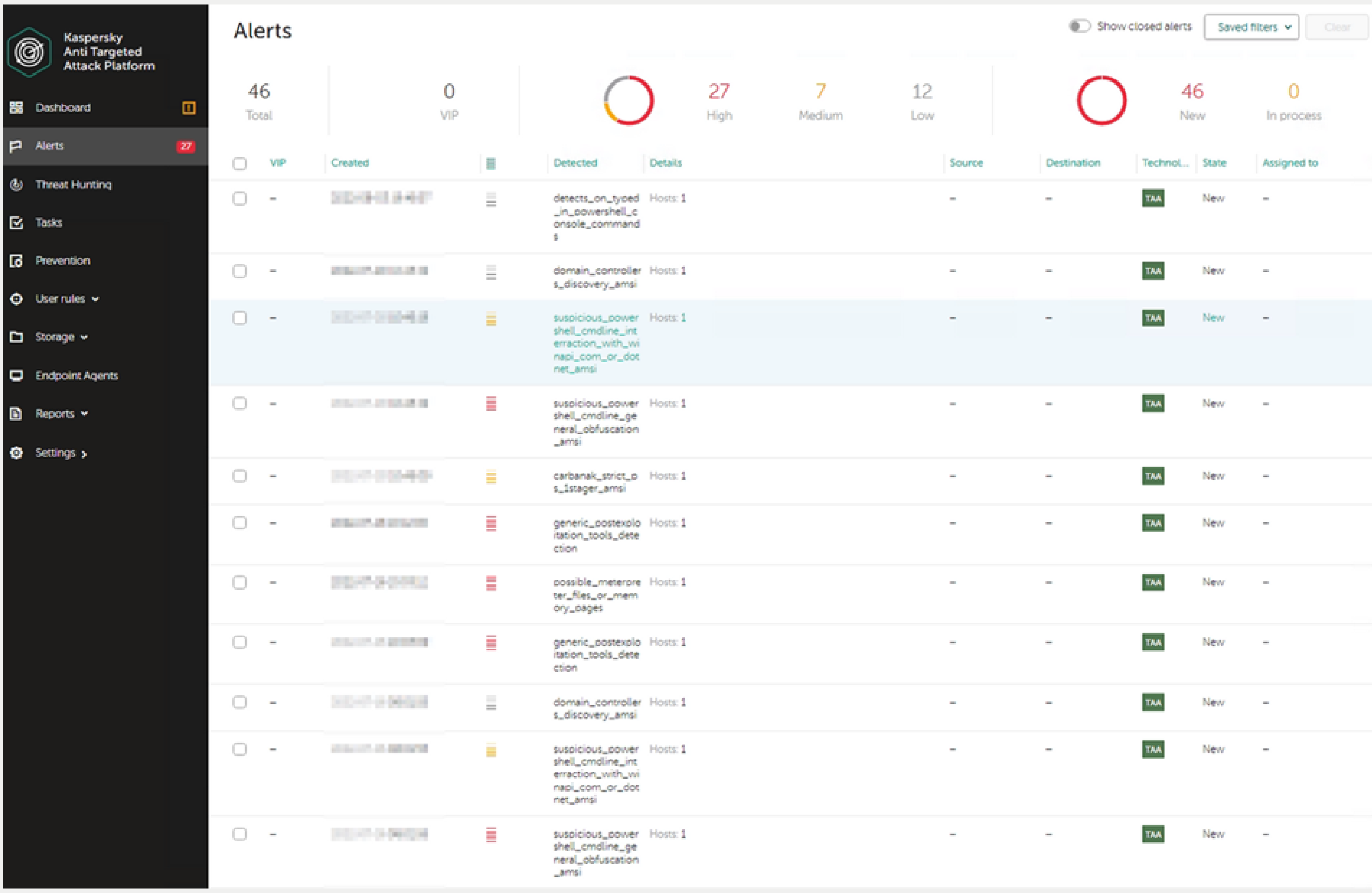
Last revision:
12th September 2025

Contents

Tested Product

Kaspersky EDR Expert (on-premises) was tested as part of AV-Comparatives' Endpoint Prevention and Response (EPR) Test in summer 2025. The product version number was 7.0.

Product Thumbnail



Kaspersky EDR Expert (on-premises) management console

Certification

In this evaluation, certification is granted based on a product's performance in the EPR-Test 2025 of AV-Comparatives, where it must achieve an average score of at least 92% for combined Active and Passive Response, without incurring excessive costs. Achieving a 'Certified' designation signifies that a product has demonstrated a high level of performance and effectiveness. The tested solution was "Certified" in the EPR-Test of 2025.

Kaspersky's EPR Product: Executive Summary

Kaspersky EDR Expert (on-premises) was tested by AV-Comparatives to validate if the product could provide effective enterprise prevention and response capabilities.

Kaspersky EDR Expert (on-premises) did well at handling threats targeted towards enterprise users, in particular before the threats 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 test included a wide mix of attack vectors - executables, scripts, installers, add-ins, and USB-propagated payloads. The product showed strong resilience, detecting these advanced attempts despite stealth and evasion layers.

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. Kaspersky 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. Kaspersky 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. Kaspersky had **Moderate 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. Kaspersky had **no costs** relating to workflow delays.

Description	Details
EPR Certification Level Reached:	**CERTIFIED**
Overall **Active Response** Rate (Prevention Rate):	**95.3%**
Overall **Passive Response** Rate (Response Rate):	**96.7%**
Operational Accuracy Costs:	**Moderate**
Workflow Delay Costs:	**None**

Executive Summary

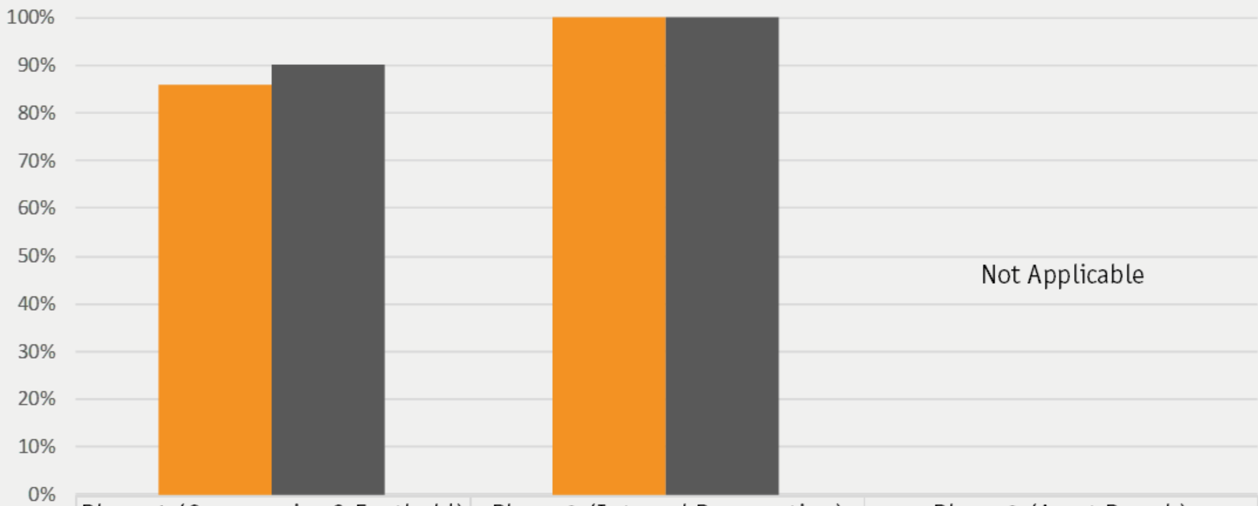
The table below depicts Kaspersky's EPR prevention & detection rates across the different phases and categories of attack. For more details on the workflows and phases, please see the appendix.

Description	Number Tested
Scenarios	50
Phases	**Combined Prevention & Detection**
Phase 1 (Compromise & Foothold)	
Active Response (Prevention)	86%
Passive Response (Detection)	90%
Phase 2 (Internal Propagation)	
Active Response (Prevention)	100%
Passive Response (Detection)	100%
Phase 3 (Asset Breach)	
Active Response (Prevention)	N/A
Passive Response (Detection)	N/A
Operational Accuracy Costs	Moderate
Workflow Delay Costs	None

Combined Prevention & Detection Rates

Kaspersky provided an Active Response (prevention) to 86% of scenarios in Phase 1 (Compromise and Foothold), and a Passive Response to a further 4% of scenarios, making a total response rate of 90% in Phase 1. For the 7 scenarios (14%) that were able to progress to Phase 2 (Internal Propagation), Kaspersky detected and acted upon all of them in this phase. Hence, none of the scenarios progressed to Phase 3.

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



	Phase 1 (Compromise & Foothold)	Phase 2 (Internal Propagation)	Phase 3 (Asset Breach)
Active Response	86%	100%	N/A
Passive Response	90%	100%	N/A

Active vs Passive Response of Kaspersky EDR Expert (on-premises)

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.

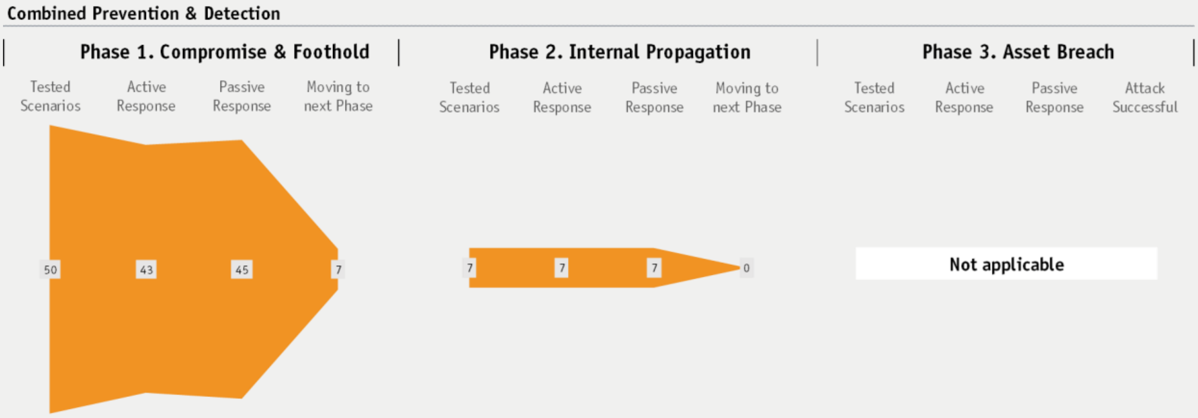
AV-Comparatives' Enterprise EPR methodology covers some of the most prevalent enterprise scenarios and system-administrator EPR workflows, specifically requested by enterprises based on inquiries and primary research.

Cumulative Prevention and Response by phases

Response Type	Phase 1 Only	Phase 1 & 2	Overall (Phase 1, 2 & 3)
Active Response	86% (43/50)	100% (50/50)	100% (50/50)
Passive Response	90% (45/50)	100% (50/50)	100% (50/50)

Combined Prevention & Detection Rates

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



EPR Efficacy per Phase of Kaspersky EDR Expert (on-premises)

Phase 1:

- 43 out of 50 scenarios prevented.
- 45 out of 50 scenarios detected.
- 7 scenarios were able to progress to Phase 2.

Phase 2:

- 7 out of 7 scenarios prevented.
- 7 out of 7 scenarios detected.
- 0 scenarios were able to progress to Phase 3.

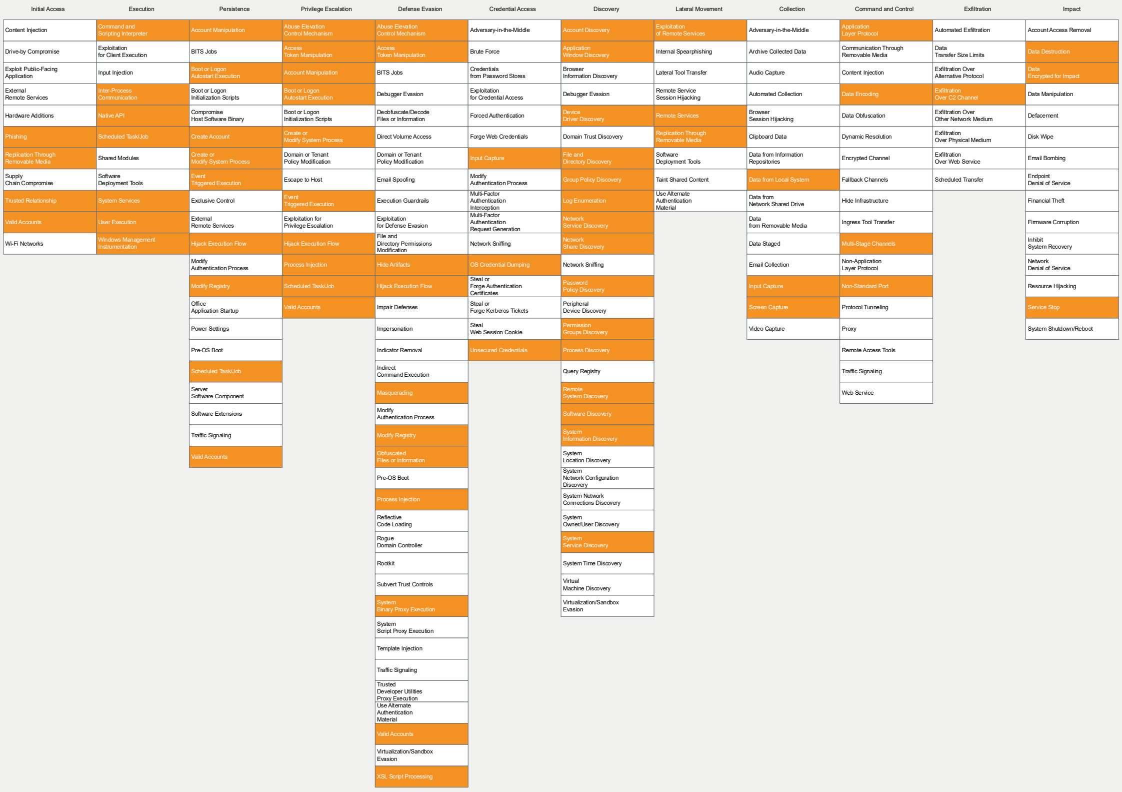
Phase 3:

- 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/2025/07/EPR2025.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.

Kaspersky EDR Expert (on-premises) 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	Framework	File Type	Description	Active Response	Passive Response
1	PowerShell Empire	EXE	Obfuscated dropper with spoofed cert and bypasses	✓	✓
2		CPL	Obfuscated CPL with ETW bypass and spoofing	✓	✓
3		EXE	Signed utility clone with stealthy memory bypass	✗	✗
4		SCR	Obfuscated screen saver with ETW bypass logic	✓	✓
5		EXE	USB-propagated dropper with stealthy memory evasion	✓	✓
6		VBS	Obfuscated VBScript with macro-style injection	✓	✓
7		VBS	VBScript payload leveraging valid user credentials	✓	✓
8		BAT	Obfuscated batch script abusing valid account access	✓	✓
9		EXE	Signed loader with logging bypass and obfuscation	✓	✓
10		HTA	HTA payload abusing MSHTA for proxy execution	✓	✓
11	Metasploit / Meterpreter	EXE	Signed stageless loader with full telemetry evasion	✓	✓
12		PIF	Stealthy PIF loader bypassing MOTW and logs	✗	✗
13		CPL	Obfuscated CPL dropper spoofing update installer dialog	✗	✓
14		XLL	Obfuscated Excel add-in with logging evasion logic	✓	✓
15		CHM	Compiled help file triggering stealthy shellcode injection	✓	✓
16		VBS	VBScript payload executing from removable media device	✓	✓
17		PS1	PowerShell reverse shell with manual AMSI bypass	✓	✓
18		HTA	HTA dropper abusing MSHTA for remote shell	✓	✓
19		MSI	Signed installer leveraging MSIexec for stealthy access	✓	✓
20		HTA	Remote shell via MSHTA and clipboard launch	✓	✓

21	Commercial #1	EXE	Spoofed binary with obfuscated stageless shellcode loader	✗	✗
22		EXE	Installer decoy delivering obfuscated stageless shellcode payload	✗	✗
23		CPL	Obfuscated CPL loader spoofing trusted installer metadata	✓	✓
24		HTA	HTA script from USB abusing MSHTA execution	✓	✓
25		EXE	Spoofed remote tool executing obfuscated DNS shellcode	✓	✓
26	PowerShell Empire	EXE	Legitimate binary backdoored with obfuscated shellcode	✓	✓
27		CHM	Compiled help file executing obfuscated PowerShell loader	✓	✓
28		CPL	Obfuscated CPL loader abusing control panel execution	✓	✓
29		SCT	SCT file leveraging regsvr32 for stealth execution	✓	✓
30		BAT	Obfuscated batch script launching shellcode from USB	✓	✓
31		XLL	Malicious Excel add-in with stealth update lure	✓	✓
32		HTA	HTA script leveraging trusted access and MSHTA	✓	✓
33		SCR	Spoofed screensaver dropper with stealthy execution flow	✓	✓
34		VBS	VBScript payload leveraging trusted lateral access path	✓	✓
35		DLL	Malicious DLL executed via trusted rundll32 proxy	✓	✓
36	Metasploit / Meterpreter	EXE	Spoofed scanner binary with MOTW and log evasion	✗	✗
37		HTA	Malicious support tool leveraging MSHTA execution proxy	✓	✓
38		PIF	Spoofed installer dropper disabling logs and defences	✓	✓
39		LNK	LNK shortcut dropper with icon-based obfuscation	✓	✓
40		DLL	Obfuscated DLL dropper executed via rundll32 export	✓	✓
41		SCR	Masqueraded screensaver loader with logging evasion logic	✓	✓
42		HTA	HTA payload abusing trust and MSHTA execution	✓	✓
43		MSI	Malicious installer leveraging MSIexec in trusted context	✓	✓
44		VBS	VBScript payload launched via trusted internal access	✓	✓
45		EXE	Obfuscated executable mimicking tool in trusted environment	✓	✓
46	Commercial #2	EXE	Spoofed installer evading kernel-based detection mechanisms	✓	✓
47		SCR	Spoofed screensaver evading logging and userland hooks	✓	✓
48		CPL	Spoofed control panel applet bypassing logging controls	✓	✓
49		PIF	Obfuscated PIF masquerading as installer with evasion	✗	✓
50		XLL	Stealthy Excel add-in faking log export operation	✓	✓

Phase 1: Active versus Passive Response of Kaspersky EDR Expert (on-premises)

✗ - 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.

Kaspersky provided an Active Response (prevention) to 86% of scenarios in Phase 1 (Compromise and Foothold), and a Passive Response to a further 4% of scenarios, making a total response rate of 90% in Phase 1. For the 7 scenarios (14%) that were able to progress to Phase 2 (Internal Propagation), Kaspersky detected and acted upon all of them in this phase. Hence, none of the scenarios progressed to Phase 3.

Phase 2 Metrics: Internal Propagation

In this phase, the EPR product must prevent internal propagation if Phase 1 doesn't stop the attack. It should empower the system admin to immediately detect and track the threat's internal spread in real-time. Relevant tactics from the MITRE ATT&CK Framework include:

Privilege Escalation: In enterprise networks, users typically use standard accounts without admin privileges. If an enterprise endpoint is attacked, the attacker won't have the needed permissions. Privilege escalation methods involve user-access token manipulation, exploitation, application shimming, hooking, or permission weaknesses. Active response assessment considered preventive actions within each method.

Defense Evasion: Attackers aim to go undetected while achieving their objectives. Defense evasion involves actions like tampering with security software, process obfuscation, and abusing system tools to hide the attack.

Credential Access: Attackers secure legitimate network user account access for their activities, avoiding detection. Methods vary depending on the network's nature, from on-site input capture (e.g., keyloggers) to offline copying of the password database for later cracking.

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
3	PowerShell Empire Framework - Signed utility clone with stealthy memory bypass	✓	✓
12	Metasploit / Meterpreter Framework - Stealthy PIF loader bypassing MOTW and logs	✓	✓
13	Metasploit / Meterpreter Framework - Obfuscated CPL dropper spoofing update installer dialog	✓	✓
21	Commercial Framework - Spoofed binary with obfuscated stageless shellcode loader	✓	✓
22	Commercial Framework - Installer decoy delivering obfuscated stageless shellcode payload	✓	✓
36	Metasploit / Meterpreter Framework - Spoofed scanner binary with MOTW and log evasion	✓	✓
49	Commercial Framework - Obfuscated PIF masquerading as installer with evasion	✓	✓

Phase 2: Active versus Passive Response of Kaspersky EDR Expert (on-premises)

× - 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 scenarios in Phase 2, Kaspersky provided both a Passive Response (detection) and an Active Response (prevention).

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.

Phase 3 scenarios were **N/A** (**not applicable**) to Kaspersky, as the threats had already been prevented in a previous phase.

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 or malfunctions

Operational accuracy testing was performed by simulating a typical user activity in the enterprise environment. This included opening clean files of different types (such as executables, scripts, documents with macros) and browsing to different clean websites. Furthermore, different administrator-friendly tools and scripts were also executed in the test environment to ensure that productivity was not affected by the respective product configuration used for the test. To assess operational accuracy, each product is tested with a battery of clean scenarios. Over-blocking or over-reporting of such scenarios means that a product reaches high prevention and detection rates, but also causes increased costs. Where legitimate programs/actions are blocked, the system administrator will have to investigate, restore/reactivate any blocked programs etc, and take steps to prevent it happening again. The principle of "The boy who cried wolf" may also apply; the greater the number of false alerts, the more difficult it becomes to recognise a genuine alert.

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

Group	Number of affected scenarios	Operational Accuracy *Active Response Multiplying Factor*	Operational Accuracy *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	5+	x20	x15

Multiplying factors for Operational Accuracy costs

The costs arising from imperfect Operational Accuracy are worked out using Cost Units of USD 1.76 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).

Products that exhibit significant bugs or malfunctions during testing incur an additional penalty factor of 12. We are pleased to report that no such issues were observed in this year's test.

Costs arising from workflow delays

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

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

Multiplying factors for Workflow Delay costs

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

Results

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

	Operational Accuracy		Workflow Delays
	Active Response	*Passive Response*	
Kaspersky	None	Moderate	None

Combined results table for Operational Accuracy and Workflow Delays

Kaspersky had moderate Operational Accuracy costs for Passive Responses, but no additional costs in either of the other two categories.

EPR Competitive Product Differentiator (provided by Kaspersky)

Kaspersky Endpoint Detection and Response (EDR) Expert delivers comprehensive visibility and superior defenses across all endpoints, providing a painless upgrade to full XDR functionality. It offers deployment options for every organization: cloud-based, on-premises or in air-gapped networks. Enhanced threat hunting and discovery leverages Kaspersky's unique threat intelligence, while automated routine tasks, guided investigation processes and customizable detections all promote speedy and efficient incident resolution. Kaspersky EDR Expert enables organizations to:

Effectively control and monitor all endpoints: By being able to see the full picture - where the threat originated, how it spread, which hosts it affected, and what exactly can and should be done to prevent the consequences.

Streamline the IT security team's work: Fast, accurate threat containment and incident resolution across distributed infrastructure is supported through centralized and automated actions, helping to streamline the IT security team's work. No more costly additional resources are needed, and there is no more expensive downtime or lost productivity.

Successfully hunt and mitigate threats – fast: Raw data and analyses are centrally aggregated, and investigation capabilities boosted through Kaspersky's unique IoAs, MITRE ATT&CK enrichment, a flexible query builder, and access to the Kaspersky Threat Intelligence Portal. All this significantly facilitates effective threat hunting and fast incident response, for damage limitation and prevention.

Respond faster – and more effectively: Guided investigation and a faster, more accurate response are crucial in dealing with APTs. Kaspersky EDR Expert provides a seamless workflow with centralized incident management and guided investigation across all endpoints on the corporate network.

Get maximum value from the product – and existing experts: Kaspersky EDR Expert is based on the most tested, most awarded EPP solution, which automatically handles the vast majority of alerts. This frees up analysts to focus on those ones that really require their attention and expertise. Kaspersky's EPP and EDR products work together as a single solution, through the same endpoint agent.

Product Features

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

General features

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

Product Response Mechanism

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

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

Central Management and Reporting

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

Management: Threat Visibility, System Visibility, and Data Sharing

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

EPR Product Reporting Capabilities

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

IOC Integration

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

Support features

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

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

Feature List

Below you can find the list of features. Please note that this only applies to the test product and version (7.0).

Feature List	
Product Name	Kaspersky EDR Expert (on-premises)
Version Number	7.0
Supported languages - endpoint client	Arabic, Czech, Chinese, Dutch, English, French, Japanese, Hungarian, Italian, German, Kazakh, Korean, Polish, Portuguese, Portuguese, Romanian, Russian, Spanish, Turkish, Vietnamese
Supported languages - management console	Arabic, German, English, Spanish, French, Italian, Japanese, Kazakh, Korean, Polish, Portuguese, Russian, Turkish. Chinese
Product Features for 5,000 endpoints (included in the given list price)	
Do you also offer a managed version (MDR) of the tested product in your portfolio?	✓
Is Incident Response service included?	☐
Are Incident Response services available in general (which can be purchased separately)	✓
General Features	
Third-party scan engine used (in addition to its own)	proprietary
2-factor authentication	optional
Phishing protection for web browsers	✓
Web access control	✓
External device control	✓
Sandbox feature	✓
Right-click on-demand scan	✓
Lock settings	✓
Lock uninstalling	✓
Supported Operating Systems	
Microsoft Windows	
↳Windows 7	✓
↳Windows 8.1	✓
↳Windows 10	✓
↳Windows 11	✓
Virtual environments (such as VMware, HyperV)	✓
Apple macOS	✓
Linux	✓
Google Android	✓
Apple iOS	✓
Response Actions	
Guided Response Available	✓
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	✓
Start Services	✓
Stop Services	✓
Pause Services	✓
Resume Services	✓
Delete Services	✓
Modify startup type of Service	✓
Patching	✓
System Restoration	✓
System Imaging	✓
Reporting Features	
Attack Visualization	✓
Attack Context	✓
Attack Timeline	☐
Continuous Monitoring	✓
Behaviour Monitoring (File/registry/etc..)	✓
Whitelisting capability	✓
Running applications & process	✓
Endpoint Forensics	
Get process list	✓
Get file list	✓
Get file	✓
Get autorun points	✓
Get registry key	✓
Get process memory dump	✓
Get full memory dump	✓
Get NTFS service files	✓
Data Sharing Features	
Customizable default security policies	✓
Customized reporting and management	✓
Custom reporting and filtering	✓
Report automation	✓
Standard output format (JSON, Syslog, CEF, etc..)	✓
Are SIEM / 3rd party Log Managers supported	✓
Automated data export	✓
Policy and/or signature rollback	✓
System scanning capability	✓
Standards-based application programming interface (API) for access	✓
Disaster Recovery	✓
Audit trail support in the management console	✓
Multiple EPR system-administrator/user-focused workflow support	✓
Built-in-reporting capabilities for different user categories	✓
Can users create customizable dashboards for monitoring?	✓
Enterprise recording and data storage –forensic analysis	✓
Management to agent encryption	✓
Encryption of data at rest	✓
Cloud marketplace support	☐

Compliance reports (GDPR, PCI-DSS, etc.)	☐
External Data Correlation	
Threat Intelligence data assimilation	✓
Are there APIs available for integration with other systems?	✓
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	☐
EDR Features	
Does the solution offer remote control capabilities for endpoints?	✓
Are there built-in tools for incident response?	✓
Are memory forensics included to analyse volatile data?	✓
Additional Security Features	
Does it analyse user behaviour to identify potential security incidents (adaptive anomaly detection)?	✓
Are there DLP features to prevent unauthorized data exfiltration?	☐
Does it leverage AI for threat detection and response, via open chat-like prompts?	☐
Does the product include remote browser isolation (RBI) to prevent web-based threats?	☐
Support	
Is free, basic, human support for the deployment process included in the licence for 5,000 endpoints?	✓
Assisted training for the IT staff in portfolio	✓
Supported languages of support	English, French, German, Italian, Russian, Spanish, Japanese, Chinese, Turkish, Portuguese, Arabic

Overview of EDR technologies

In the dynamic field of cybersecurity, IT security professionals need a deep understanding of antivirus (AV/EPP) and endpoint detection and response (EDR) systems, which are crucial for comprehensive defence strategies. One key aspect is understanding how different AV and EDR systems implement essential technologies[5]. The following information offers a high-level overview of these technologies, highlighting their importance in the ever-changing cybersecurity landscape. These technologies encompass the Antimalware Scan Interface (AMSI), User-Mode Hooking, Callbacks, and Kernel Drivers.

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

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

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

[5] https://kwcsec.gitbook.io/the-red-team-handbook/techniques/defense-evasion/basics/iocs/high-level-overview-of-edr-technologies

EDR Technology	Kaspersky
Antimalware Scan Interface (AMSI) - This is a standard interface that allows applications and services to integrate with any antimalware product present on a machine.	●
Event Tracing for Windows (ETW) - This is a mechanism for tracing and logging events that are raised by both user-mode applications and kernel-mode drivers.	●
Microsoft Threat Intelligence (EtwTi) - This is a mechanism for tracing and logging events using Microsoft Threat Intelligence.	●
User Space API-Hooking - This is a technique used to intercept API function calls in user space. This can be used by EPP/EDR solutions to monitor and potentially block suspicious behaviour.	●
Kernel Space API-Hooking - Similar to user space API hooking, but this intercepts API function calls in the kernel space.	●
Kernel Callback Routines - These are functions that the kernel calls when certain events or conditions occur. EPP/EDR solutions can use these to monitor system events.	●
Filter Driver - This is a type of driver used to monitor and potentially modify the behaviour of device drivers. EPP/EDR solutions may use this to monitor for suspicious device behaviour.	●
Minifilter Driver - This is a specific type of filter driver that can be used to monitor and potentially modify the behaviour of file system operations.	●
Early Launch Antimalware (ELAM) Driver - This is a driver that starts early in the boot process to scan drivers for malware before they're loaded.	●
Firmware Protection Driver - This is a driver that protects the system's firmware from modification. EPP/EDR solutions may use this to prevent malware from modifying the firmware.	●
Hardware Breakpoints - These are CPU functions that pause program execution when specific memory locations are accessed or modified. Used, for example, to trigger a registered VEH.	○
PEB Manipulation - This involves modifying the Process Environment Block (PEB), more specifically double linked lists within the PEB, e.g. InLoadOrderModuleList, to manipulate the order in which DLLs are loaded, for example.	●
Vectored Exception Handling - The product registers its own Vectored Exception Handler (VEH) to handle specific exceptions and take control (avoiding handling by the SEH), such as when a specific guard page flag or hardware breakpoint is triggered.	○
Call Stack Analysis User Mode - This involves examining the call stack of a running application to trace function calls and debug execution flow.	●

Kaspersky 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).

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

AV-Comparatives
(September 2025)

Copyright and Disclaimer

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

https://www.av-comparatives.org