

Endpoint Prevention and Response

Test period:
June – August 2026

Last revision:
9th September 2026

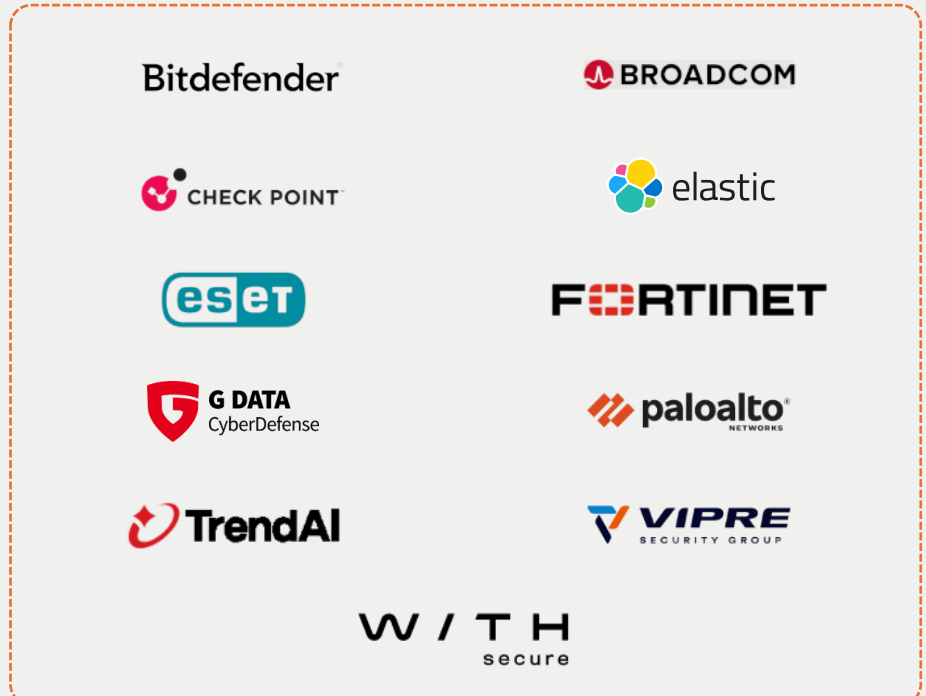
EPR Comparative Report 2026

AV-Comparatives' EPR Certification

In the 2026 Endpoint Prevention and Response (EPR) Test, certification is awarded to products that demonstrate a high level of prevention, detection, and response effectiveness within the Enterprise CyberRisk Quadrant™. To qualify, a product must achieve an average score of 92% or higher across both the Active and Passive Response phases while maintaining a low operational impact suitable for enterprise-scale deployments. Earning the Certified EPR label is a clear indicator of strong performance. It confirms that a solution delivers effective prevention and response capabilities while operating efficiently in real-world enterprise environments. The certification helps enterprise IT and security teams identify solutions that provide reliable protection against advanced threats while keeping operational overhead manageable. The operational impact model used in the CyberRisk Quadrant is based on standardized assumptions designed to enable consistent comparison across products. It should not be interpreted as representing real enterprise contract pricing or individual deployment costs. Certification is intentionally challenging and requires consistently strong performance across a broad range of realistic attack scenarios and enterprise-focused evaluation criteria. AV-Comparatives considers products that achieve certification in the EPR Test to have demonstrated leadership-level prevention, detection, and response capabilities. Certified Leader status therefore represents a significant achievement.

AV-Comparatives' EPR Certified Leaders

The table below shows which vendors achieved certification in this year's EPR Test. These products met the requirements of the Enterprise CyberRisk Quadrant, earning Certified Leader status.



Products that did not reach the certification threshold are not listed among the certified solutions. Vendor A, Vendor B and Vendor C, which did not meet the requirements, chose to remain anonymous.

Not Certified Products



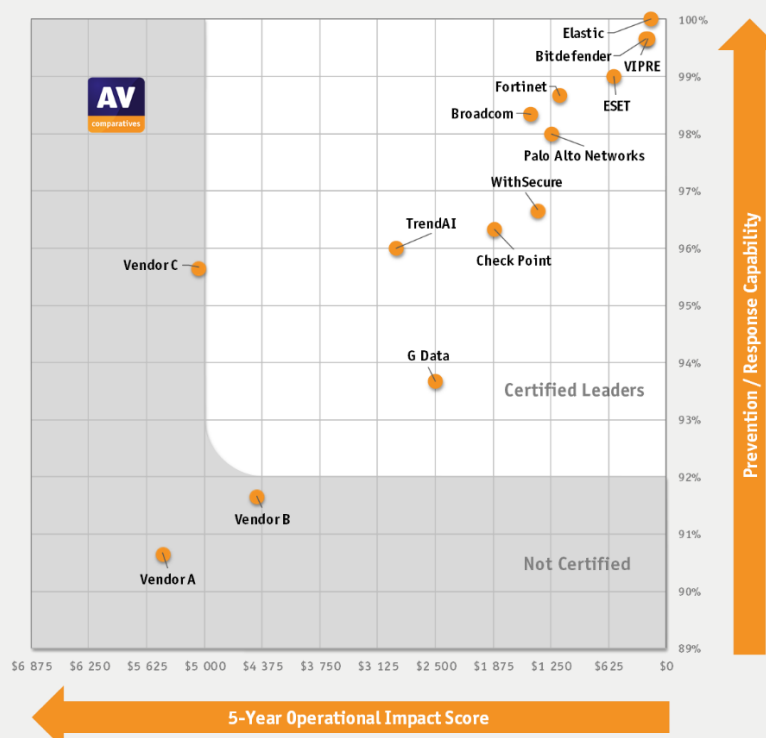
EPR Executive Summary

AV-Comparatives conducted the 2026 Endpoint Prevention and Response (EPR) Test between June and August 2026, with the report published in September 2026. The evaluation covered **50 targeted attack scenarios, each divided into three phases**, across fourteen enterprise security solutions. In addition to technical performance, an operational impact model estimated the long-term deployment impact of each product based on a five-year scenario for 5,000 endpoints. Eleven vendors met the certification criteria, demonstrating strong performance across active and passive response phases while maintaining a low overall operational impact.

The 2026 scenarios reflected **realistic attack chains**, incorporating techniques such as phishing, lateral movement, data exfiltration, and abuse of legitimate system tools. AV-Comparatives also used **AI-assisted development techniques to create testing tools and scenario variations**, helping to reflect emerging attacker capabilities and attack patterns.

The following vendors earned Certified Leader status: **Bitdefender, Broadcom, Check Point, Elastic, ESET, Fortinet, G Data, Palo Alto Networks, TrendAI, VIPRE** and **WithSecure**. Their products demonstrated strong detection and response capabilities across the evaluated attack scenarios.

The Enterprise CyberRisk Quadrant™ visualizes how tested products compare in terms of prevention and response effectiveness and their modelled operational impact over a five-year deployment period. The operational impact model combines factors including prevention accuracy, response effectiveness, workflow overhead, and standardized cost-related assumptions. **The quadrant provides a high-level overview of relative product positioning rather than a precise ranking. Small differences in graphical position should not be interpreted as meaningful differences between products.** Organizations should therefore consider the underlying test results and individual metrics alongside the overall quadrant position.



Contents

AV-Comparatives' EPR Certification	2
EPR Executive Summary.....	3
Contents.....	4
Introduction	5
About this test	6
Understanding the Enterprise CyberRisk Quadrant	7
Which product is right for my enterprise?	8
EPR CyberRisk Quadrant Overview	9
Tested Products.....	11
Product Configurations and Settings	13
EPR and MITRE ATT&CK	15
MITRE ATT&CK Matrix for Enterprise	15
Test Results.....	16
Detailed Test Results	17
Phase 1 Metrics: Endpoint Compromise and Foothold.....	17
Phase 2 Metrics: Internal Propagation.....	20
Phase 3 Metrics: Asset Breach	22
Standardized Pricing Inputs.....	25
Operational-Accuracy and Workflow-Delay Costs.....	26
Products functionality	28
Product features	28
Feature List.....	30
Overview of EDR Technologies	31
EPR Test Methodology.....	34
EPR Testing Workflow.....	35
EPR Validation Overview.....	37
Copyright and Disclaimer.....	39

Introduction

Endpoint Protection Products (EPP), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) solutions are vital components of enterprise security, providing protection against targeted threats such as advanced persistent threats (APTs). AV-Comparatives' Endpoint Prevention and Response (EPR) Test is designed to evaluate the effectiveness of these solutions in countering complex, multi-stage attacks that can affect an organization's entire infrastructure. In this report, we refer to all EPP, EDR, XDR, and similar products collectively as "**EPR**" solutions for simplicity.

Beyond securing individual endpoints, these systems are expected to analyse attack origins, tactics, and objectives, enabling security teams to contain threats, remediate affected systems, and prevent future incidents. AV-Comparatives' Endpoint Prevention and Response Test remains one of the industry's most comprehensive evaluations of such solutions. This year's test covered 14 products, each subjected to 50 targeted attack scenarios simulating real-world threats across three critical phases: Endpoint Compromise and Foothold, Internal Propagation, and Asset Breach.

Each product was evaluated on whether it automatically blocked the attack (active response) or provided actionable intelligence for manual intervention (passive response). If an attack was not blocked in one phase, the scenario continued to the next. The test also examined each product's ability to take remedial action and collect indicators of compromise in an accessible and actionable way.

To provide a meaningful comparison, we developed the Enterprise EPR CyberRisk Quadrant™, which considers not only breach prevention effectiveness but also operational accuracy and workflow efficiency. The model applies a standardized operational impact framework based on a hypothetical enterprise with 5,000 client PCs over a five-year period. As part of our ongoing efforts to enhance the quadrant, several refinements were introduced in 2026 to reflect evolving enterprise needs and threat realities.

About this test

AV-Comparatives' Endpoint Prevention and Response (EPR) Test AV-Comparatives' Endpoint Prevention and Response (EPR) Test represents one of the most comprehensive and demanding independent evaluations in the field of enterprise security. Achieving certification in this test requires consistently strong performance across a broad range of realistic attack scenarios and enterprise-focused evaluation criteria. Products were tested using configurations recommended by the respective vendors. These configurations were reviewed and confirmed by each vendor prior to the start of testing, ensuring that all products were evaluated under fair and representative conditions.



Our Expertise

We've honed our expertise over two decades to deliver precise assessments of security solutions. Unlike some imitations attempted by other testing labs, our experience uniquely positions our test to provide an accurate portrayal of capabilities.



Real-World Conditions

To maintain the integrity of the assessment, vendors were not informed in advance of the exact test timing or attack specifics, simulating real-world conditions where attackers strike without warning. Consequently, products must ensure continuous protection rather than optimizing solely for evaluation purposes.



Comprehensive Insight

To obtain an overall picture of the protection and response capabilities of any of the tested EPR products, readers should also consider the results of the other tests in AV-Comparatives' Enterprise Main-Test Series¹.



Complexity and Realism

This challenging test mirrors realistic scenarios but is inherently manual due to its complexity, making it cost-intensive to run. The methodology focuses on prevention and response capabilities. Vendors are advised to enable prevention and protection features and configure detection effectively, all while avoiding high costs due to poor operational accuracy or workflow delays. Costs arising from imperfect operational accuracy and workflow delays are considered. Additionally, telemetry-based threat-hunting is not within the scope of this test.



Comprehensive Assessment

The test phases consist of attack tactics commonly encountered by enterprises. Our EPR test spans the entire attack chain, encompassing real-world attack tactics and techniques, from initial intrusion and internal propagation to data exfiltration and actual harm to the target system or network.



Test Scenarios

We create test scenarios by utilizing publicly available cyber threat intelligence to reflect the current threat landscape. These scenarios are then mapped to a spectrum of ATT&CK techniques, simulating diverse actions and providing valuable insights into the product's effectiveness against modern intrusions. As part of the development process, AI-assisted techniques were used in the creation of testing tools and scenario variations, enabling broader coverage of realistic attack techniques and emerging threat patterns. We used 50 test scenarios primarily inspired by tactics and techniques employed by distinct APT groups and financially motivated threat actors attributed to China (e.g., APT15, APT41, BackdoorDiplomacy, Mustang Panda, Earth Lusca), Russia (e.g., APT28, APT29, Turla, Gamaredon, Wizard Spider), Iran (e.g., OilRig, APT39, MuddyWater), North Korea (e.g., Lazarus, Kimsuky), and financially motivated groups (e.g., FIN6, FIN7, Black Basta, LockBit, Royal/Conti). Please note that our test scenarios draw inspiration from these threat actors without replicating their actions, nor are they limited to them, although there may be overlap in the techniques, sub-techniques, and tools used.

¹ <https://www.av-comparatives.org/enterprise/>

Understanding the Enterprise CyberRisk Quadrant

The quadrant distinguishes between two levels: Certified Leaders and Not Certified. Achieving Certified Leader status reflects a high level of performance across the key areas evaluated in this test and confirms that the product meets the rigorous standards of our methodology. Certified Leader status is not easily achieved and remains a strong indicator of enterprise-grade prevention, detection, and response capabilities. This streamlined presentation provides clarity while preserving the significance and prestige of being Certified.



Certified Leaders

Certified solutions also provide well-integrated workflow capabilities that help security teams efficiently investigate incidents, collect relevant indicators, and respond to threats. Products that achieve certification are designated as Certified Leaders within the Enterprise CyberRisk Quadrant. The official certification awarded by AV-Comparatives remains the Certified EPR certification and associated badge.



Not Certified

Products that achieve a combined Active and Passive Response score of less than 92% are not certified. A product may also fall outside the Certified category if its overall operational impact is significantly higher than that of comparable solutions. In addition, if a product reaches five full breaches during testing, it is automatically disqualified (not certified), and testing is stopped at that point as the product would fall outside the quadrant.

Which product is right for my enterprise?

The fact that a product appears in the upper area of the quadrant does not necessarily mean it is the best choice for every enterprise environment. Solutions placed in lower areas of the quadrant may include specific features or operational characteristics that make them better suited to particular infrastructure, workflows, or security requirements. However, AV-Comparatives does not recommend the use of products that did not achieve certification in this test.

Placement of the dots

The position of each vendor's dot on the Y-axis of the quadrant reflects the effectiveness of the solution's active and passive response capabilities. This score also influences the X-axis, as solutions that respond effectively or stop attacks at earlier stages reduce the operational impact of incidents over time.

The X-axis represents a modelled five-year operational impact, which considers several factors including prevention effectiveness, operational accuracy, workflow delays (for example those caused by sandbox analysis), and estimated breach-related costs. Product list price is included as one standardized modelling input among these factors.

EPR CyberRisk Quadrant Overview

The CyberRisk Quadrant considers multiple factors that influence the overall operational impact of a security solution. These include the effectiveness of each product in preventing breaches, the reduction in incident-related impact resulting from this protection, the product's operational accuracy, and the efficiency of security workflows during investigation and response.

One of the most significant consequences of a security breach is the disruption and financial impact it can cause for the affected organisation. According to IBM, the average cost of a breach in 2026 was USD 4.99 million. Deploying an effective EPR solution that can detect and stop attacks early therefore plays an important role in reducing the potential impact of security incidents on enterprise operations.

In this section, we analyse the operational impact associated with deploying the tested security products alongside their effectiveness in preventing security breaches. Based on IBM's estimate of USD 4.99 million as the average cost of a data breach, we model the potential impact reduction that an organisation could achieve by deploying each of the tested EPR solutions. The results show that all tested products provide meaningful protection, with their combined active and passive response capabilities preventing most attacks. However, some solutions demonstrate stronger overall performance than others. The more effective a solution is at preventing breaches, the lower the expected operational and incident-response impact for the organisation.

The graphic below outlines the model used to estimate the overall operational impact of each product. Several factors are considered. These include the product's list price and associated service and support components, which are included as standardized modelling inputs. In addition, the model incorporates costs related to operational accuracy. Over-blocking or excessive alerting can create investigation overhead for security teams and therefore increase operational workload. In 2015, the Ponemon Institute estimated that organisations waste roughly USD 1.3 million per year due to inaccurate or erroneous intelligence. Adjusted for inflation, and combined with similar research from IBM in 2026, the figure would be approximately USD 1.47 million. This value is used in the model as a reference point for estimating the potential operational impact associated with products that do not meet the operational-accuracy validation criteria. Costs related to workflow delays are also considered. If a product introduces additional investigation steps or operational friction due to its features, policies, or behaviour, this will be reflected in the CyberRisk Quadrant.

The model also considers the impact of successful breaches. A product that theoretically blocks all attacks would result in no breach-related impact within this model, whereas a solution that fails to stop attacks would incur the full estimated breach impact.

The operational impact model uses standardized assumptions to ensure comparability between products and should not be interpreted as a reflection of real enterprise contract pricing or individual deployment costs.



For each scenario, a breach-impact value was calculated based on the EPR product's ability to actively or passively respond during the execution of the attack. The model reflects the principle that earlier detection and response reduce the overall impact of a security incident. Passive response still incurs partial impact because the attack is not automatically stopped and requires manual investigation and remediation by the security team. The breach-impact percentages used in the 2026 evaluation are outlined below.

Active Response in Phase 1

If the attack was automatically stopped and reported in Phase 1, the breach impact for the scenario was 0%. If the attack was silently blocked without reporting, 12.5% of the total breach impact was applied.

Only Passive Response in Phase 1

If no active response occurred but the product provided passive response capabilities in Phase 1, 12.5% of the total breach impact was applied.

Active Response in Phase 2

If the attack was stopped automatically in Phase 2, 25% of the total breach impact was applied. If the attack was silently blocked without reporting, 35% was applied.

Only Passive Response in Phase 2

If no active response occurred but passive response capabilities were present in Phase 2, 50% of the total breach impact was applied.

Active Response in Phase 3

If the attack was stopped automatically in Phase 3, 75% of the total breach impact was applied. If the attack was silently blocked without reporting, 85% was applied.

Only Passive Response in Phase 3

If no active response occurred but passive response capabilities were present in Phase 3, 95% of the total breach impact was applied.

No Active or Passive Response in any of the three Phases / Full Breach

If neither active nor passive response occurred in any phase, the scenario was classified as a full breach, and 100% of the breach impact was applied. If a product reaches five full breaches, it is automatically disqualified (not certified), and testing is stopped at that point.

To calculate the X-axis in the EPR CyberRisk Quadrant, we apply an operational impact model that incorporates several factors, including product list price, operational accuracy (such as false positives, over-blocking, or excessive reporting), workflow delays, and the estimated reduction in breach impact achieved by prevention and response capabilities. The response component is calculated by averaging the cumulative active response scores for phases 1–3 and the cumulative passive response scores for phases 1–3. The overall response score is then derived as the average of these two results. This model reflects the role of EPR solutions in enterprise environments: preventing threats where possible and providing effective detection and response when prevention is not feasible. Higher prevention rates reduce the operational impact associated with incident response and remediation, while strong detection capabilities (such as clear visibility and detailed forensic information) enable security teams to investigate and respond more efficiently. As part of our ongoing methodology development, we regularly review feedback from enterprises and industry experts to ensure that the evaluation metrics remain aligned with evolving enterprise security needs.



Active Response (Prevention)

An active response stops the attack automatically and normally reports it. A silent block prevents the attack without generating a corresponding report and is therefore treated separately in the operational impact model.



Passive Response (Detection)

A passive response does not stop the attack but reports suspicious activity.

Tested Products

We congratulate the following vendors for taking part in this EPR Test. All tested vendors were provided with detailed information on their respective missed scenarios, so that they can further improve their products. Please note that vendors which do not reach the certification have the option to remain anonymous - we have referred to them as "Vendor A", "Vendor B" and "Vendor C".













Vendor A

Vendor B

Vendor C

Vendor	Product	Version
Bitdefender	GravityZone Business Security Enterprise	8.26
Broadcom	Symantec Endpoint Security Complete	16.0
Check Point	Endpoint Security Advanced	89.10
Elastic	Security	9.4
ESET	PROTECT Enterprise Cloud	7.1
Fortinet	FortiEndpoint with EDR Essentials	6.2
G Data	XDR	1.0
Palo Alto Networks	Cortex XDR Prevent	9.1
TrendAI	Vision One Endpoint Security Essentials	14.0
VIPRE	Endpoint Detection & Response	13.4
WithSecure	Elements XDR	26.2
Vendor A – B – C	Product A – B – C	n/a

Individual Product Reports

This comparative report provides an overview of the results for all tested products. There are also individual reports for each product, which are available at the links provided below:

Vendor	Link
Bitdefender	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_Bitdefender_2026.pdf
Broadcom	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_Broadcom_2026.pdf
Check Point	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_CheckPoint_2026.pdf
Elastic	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_Elastic_2026.pdf
ESET	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_ESET_2026.pdf
Fortinet	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_Fortinet_2026.pdf
G Data	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_GDATA_2026.pdf
Palo Alto Networks	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_PaloAlto_2026.pdf
TrendAI	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_TrendAI_2026.pdf
VIPRE	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_VIPRE_2026.pdf
WithSecure	https://www.av-comparatives.org/wp-content/uploads/2026/09/EPR_WithSecure_2026.pdf

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).

BROADCOM

In "Antimalware Policy", the "Blocking Intensity Level" was increased from "HID level 200" to "HID level 300". "Microsoft Outlook Auto-Protect", "Firewall" and "Intrusion Prevention" were enabled. In the "Adaptive Protection Policy", all settings were kept in "Monitor mode".

CHECK POINT

In Threat Prevention policy rules (default "Connected" mode), policy profile was switched to predefined "Optimized".

G DATA CyberDefense

Default settings were used.

elastic

("windows.advanced.malware.threshold") set to "aggressive" (verified)

MalwareScore

set to

FORTINET

"Execution Prevention", "Exfiltration Prevention", "Ransomware Prevention" were enabled and everything set to "Block", with exception of "Sandbox Analysis", "Unconfirmed File Detected", "Debugged Process", "Network Scanning Attempt Detected", "Partially Mapped", "Protected System Configuration", and "Stack Tampering", which were set to "Log". "Default Playbook" was enabled.

Bitdefender

"Advanced Threat Control", "Advanced Anti-Exploit", "Firewall", "Network Content Control", "Network Attack Defense", "Kernel-API Monitoring" and "EDR Sensor" were enabled. "Scan mode" was set to "Local Scan". "Relay Servers" and "Default Update Servers" were deleted. "Update Ring" was set to "Fast Ring". "On-access Scanning" for archives bigger than 100MB was enabled with depth 16. "AMSI" setting and "Report analysis results to AMSI" were enabled. "Ransomware Mitigation" and "Email Traffic Scan" were activated. "HyperDetect" was enabled and set to "Block" (for network) and to "Disinfect" (for files). "Protection Level" was set to "Normal" for all settings on "HyperDetect". "Scan SSL" and "Sandbox Analyzer" were enabled and set to "Monitoring". In "Advanced Anti-Exploit", the "LSASS Protection" was disabled. In "Anti-Tampering", the remediation action was set to "Isolate Endpoint". For "Antimalware" the actions were set to "Disinfect". "Scan Process Memory" was enabled, as well as "Sensitive Registry Protection", "Kernel Api Monitoring" and "Ransomware Mitigation". In the "Network Protection" section, "Scan HTTPS" was enabled and additional process were added for the "Intercept Encrypted Traffic", namely "powershell.exe", "wscript.exe", "cscript.exe" and "pwsh.exe". For "Web Traffic Scan" the action was set to "Block". For "Email Traffic Scan", all available e-mail protocols (POP3, IMAP, SMTP, MAPI) were selected. For "Network Attacks", "inspect Traffic Scan" and "Server Traffic Scan" were enabled, as well as "Inspect encrypted domain controller traffic".



All "Real-Time & Machine Learning Protection", "Potentially Unwanted Applications", "Potentially Unsafe Applications" and "Suspicious Applications" settings were set to "Aggressive". "Runtime packers" and "Advanced heuristics" enabled for "ThreatSense". In "Cloud-based Protection", "LiveGuard", "LiveGrid Feedback System" and "LiveGrid Reputation System" were set to "On". The "Detection threshold" for "LiveGuard" was set to "Suspicious", the "Proactive protection" was set to "Block execution until receiving the analysis result" and the "Maximum wait time for the analysis result" was set to "5 min". "Automatic submission of suspicious samples" enabled for all file types. In "ESET Inspect", all detection rules and exclusions were enabled, except the "optional" ones.



"XDR Prevent Endpoints", "Dynamic Driver Protection", "Unpatched Vulnerabilities Protection" and "On-Write File Examination" were fully enabled. Under "Malware Profile", "Portable Executable and DLL examination", "JScript File Examination", "ASP & ASPX Files", "PowerShell Script Files", VB Scripts Examination" and "Ransomware Protection" were set to "Quarantine".



"Incompatible Software Handling" disabled. In "Active Protection", "Disinfect on ATC code buffer detections of intra-process injections" was enabled. "Network Attack Protection" was enabled and set to "Block" for all categories. "Enhanced Detections" and "Inspect Encrypted Domain Controller Traffic" were also enabled. "Firewall" enabled.

Vendor A B C Non-default settings were used.



The "endpoint sensor" was enabled and the "Monitoring Level" was set to "hypersensitive mode" / "3-Aggressive". The "Identity Security Sensor and the "Browser Extension" were also enabled. In "General Settings", the "Dynamic Intelligence Mode" was disabled. The "Do not scan files which exceeds MB" was set to "100 MB". The "Monitoring Level" was set to "Protection 2 / Detection 3". In "Real-time Scan", "All scannable files" was selected, and "Scan all files in removable storage devices after plugging in" was enabled. The "Maximum Layers" was set to "6". "CVE exploit scanning for files downloaded through web and email channels" was enabled. "Event Monitoring" was enabled, and the Action was set to "Ask when necessary", except for "AI App Guard". For "Predictive Machine Learning", the "Monitoring Level" was set to "Protection 2 / Detection 3". The "Security Level" for "Web Reputation" was set to "High". For "Suspicious Connection" the "Monitoring Level" was set to "Protection 2 / Detection 3". For "Sandbox Submission", "Send suspicious files to a virtual sandbox for analysis" was enabled. On the Server, "Dynamic Intelligence Mode" was disabled. For "Anti-Malware", "Predictive Machine Learning", "Behavior" and "AMSI", the "Monitoring Level" were set to "Protection 2 / Detection 3". The "Remediation action" was set to "Quarantine". "Network directory scan" was enabled. "Web Reputation" was enabled and the security level was set to "High".



"Advanced response" enabled, "Action when USB device is plugged in" set to "Silently scan USB", For "Browsing Protection", enabled "Include the blocked URLs in all security events". Twenty-four client policies were enabled and set to "Audit".

EPR and MITRE ATT&CK

MITRE ATT&CK Matrix for Enterprise

The diagram below shows the MITRE ATT&CK Matrix for Enterprise. The column headings represent the ATT&CK tactics (objectives), while the boxes beneath them represent the ATT&CK techniques used to achieve those objectives. Our EPR test exercises techniques across the full attack lifecycle, using realistic attack scenarios that reflect modern adversary tradecraft. Across the 50 attack scenarios used in this EPR test, we exercised a broad range of the techniques highlighted in the matrix below. The highlighted ATT&CK techniques represent those exercised by the test scenarios and are not intended to provide comprehensive coverage of the entire ATT&CK framework.

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

Initial Access	Execution	Persistence	Privilege Escalation	Stealth	Defense Impairment	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Content Injection	BITS Jobs	Account Manipulation	Abuse Elevation Control Mechanism	Access Token Manipulation	Disable or Modify System Firewall	Adversary in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Drive-by Compromise	Download and Sorting of Remote File	BITS Jobs	Access Token Manipulation	BITS Jobs	Disable or Modify Tools	Brute Force	Application Window Discovery	Internal Reconnaissance	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploit Public-Facing Application	Exploitation for Client Execution	Boot or Login Automated Execution	Account Manipulation	Debugger Evasion	Domain or Tenant Policy Modification	Credential Stuffing	Browser Information Discovery	Local Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
External Remote Services	HTTP Session Fixation	Boot or Login Initialization Scripts	Boot or Login Automated Execution	Delay Execution	Downgrade Attack	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Hardware Additions	Input Injection	Compromise Host Software Binary	Boot or Login Initialization Scripts	Disfigure/Disable File or Information	Exploitation for Defense Impairment	Format Authentication	Device Driver Discovery	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Phishing	Inter-Process Communication	Create Account	Create or Modify System Process	Direct Volume Access	File and Directory Permissions Modification	Forge Web Credentials	Domain Trust Discovery	Registration Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Registration Through Removable Media	Native API	Create or Modify System Process	Domain or Tenant Policy Modification	Execution Guardrails	Modify Authentication Process	Input Capture	File and Directory Discovery	Software Deployment Tools	Data from Information Resources	Emergent Channel	Exfiltration Over Web Service	Email Bouncing
Supply Chain Compromise	Scheduled Task/Job	Event Triggered Execution	Escape to Host	Exploitation for Stealth	Modify Registry	Modify Authentication Process	Group Policy Discovery	Target Shared Content	Data from Local System	Feedback Channels	Scheduled Transfer	Endpoint Denial of Service
Trusted Relationship	Shared Modules	Exclusive Control	Event Triggered Execution	Hide Artifacts	Prevent Command History Logging	Multi-Factor Authentication Interception	Local Storage Discovery	Use Alternate Authentication Material	Data from Network Shared Drive	Hide Infrastructure		Financial Theft
Valid Accounts	Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	HTTP Session Fixation	Rogue Domain Controller	Multi-Factor Authentication Request Generation	Log Enumeration		Data from Removable Media	Ingress Tool Transfer		Firmware Corruption
WAF Networks	System Services	Modify Authentication Process	Process Injection	Indicator Injection	Safe Mode Boot	Network Sniffing	Network Service Discovery		Data Staged	Multi-Stage Channels		Inhibit System Recovery
	Trusted Developer Utilities Proxy Execution	Modify Registry	Scheduled Task/Job	Indirect Command Execution	Subvert Tool Controls	OS Credential Dumping	Network Share Discovery		Email Collection	Non-Application Layer Protocol		Network Denial of Service
	User Execution	Office Application Startup	Valid Accounts	Manipulating		Steal or Forge Authentication Certificates	Network Sniffing		Input Capture	Non-Standard Port		Resource Hijacking
	Windows Management Instrumentation	Power Settings		Obfuscated Request Information		Steal or Forge Network Tokens	Password Policy Discovery		Screen Capture	Protocol Tunneling		Service Stop
		Pre-OS Boot		Pre-OS Boot		Steal Web Session Cookies	Peripheral Device Discovery		Video Capture	Proxy		System Shutdown/Reboot
		Scheduled Task/Job		Process Injection		Unaccounted Credentials	Permission Groups Discovery					
		Server Software Component		Reflective Code Loading			Process Discovery					
		Software Extensions		Rootkit			Query Registry					
		Traffic Signaling		Selective Exclusion			Remote System Discovery					
		Valid Accounts		Social Engineering			Software Discovery					
				System Binary Proxy Execution			System Information Discovery					
				System Script Proxy Execution			System Location Discovery					
				Template Injection			System Network Configuration Discovery					
				Traffic Signaling			System Network Connections Discovery					
				Trusted Developer Utilities Proxy Execution			System Operational Discovery					
				Valid Accounts			System Service Discovery					
				Virtualization/ Sandbox Evasion			System Time Discovery					
				XSL Script Processing			Virtual Machine Discovery					
							Virtualization/ Sandbox Evasion					

For a magnified view of the above table click on this link²:

Link

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.

² <https://www.av-comparatives.org/wp-content/uploads/2026/08/EPR2026.svg>

Test Results

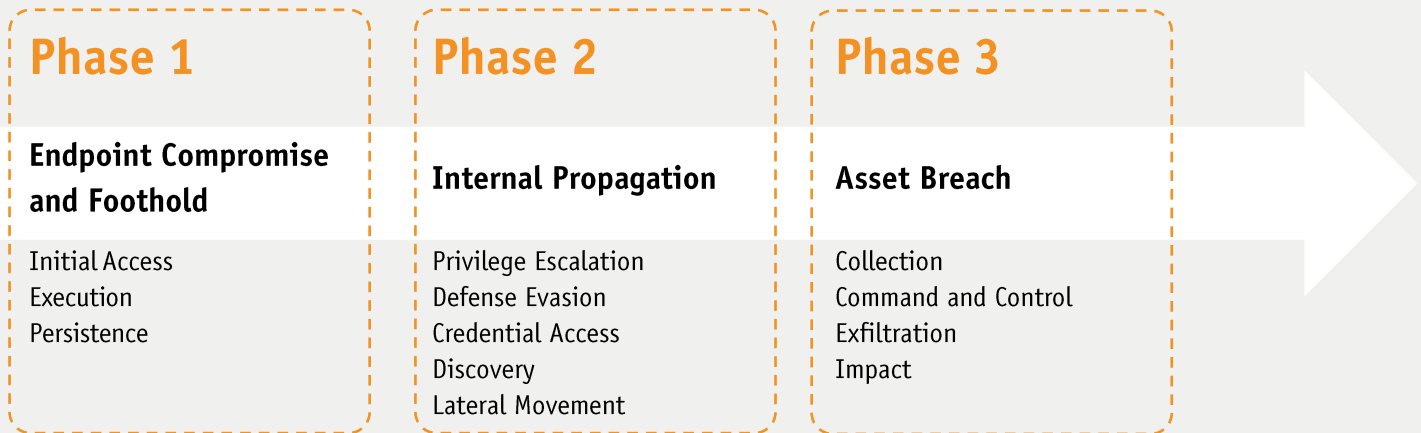
For an active response (preventative action) to be credited, we verified whether the product made an active response during the respective phase. Similarly, for a passive response (detection event) to be credited, we verified that the product gave an active alert tied to the attack during the respective phase, allowing the system administrator to take appropriate actions.

Product	Active Response	Passive Response	Combined Prevention/Response Capabilities Y-Axis	Operational Accuracy Costs	Workflow Delay Costs	5-Year Operational Impact Score (Per Agent) X-Axis
Bitdefender	100%	99.3%	99.7%	None	None	\$225
Broadcom	98.0%	98.7%	98.3%	Low	None	\$1 469
Check Point	96.0%	96.7%	96.3%	Low	None	\$1 856
Elastic	100%	100%	100%	None	None	\$162
ESET	98.7%	99.3%	99.0%	None	None	\$569
Fortinet	97.3%	100%	98.7%	Low	None	\$1 158
G Data	94.0%	93.3%	93.7%	None	None	\$2 499
Palo Alto Networks	98.0%	98.0%	98.0%	Low	None	\$1 243
TrendAI	94.0%	98.0%	96.0%	Moderate	None	\$2 925
VIPRE	100%	99.3%	99.7%	None	None	\$200
WithSecure	96.0%	98.7%	97.3%	None	None	\$1 143
Vendor A	88.7%	92.7%	90.7%	Moderate	None	\$5 453
Vendor B	91.3%	92.0%	91.7%	Low	None	\$4 432
Vendor C	96.0%	95.3%	95.7%	High	Moderate	\$5 062

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

Detailed Test Results

The three attack phases may consist of the Tactics outlined below:



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 can be 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.

[More Details](#)



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.

[More Details](#)



Persistence

Once the attacker gets inside the target environment, they might 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.

[More Details](#)

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

Active and Passive Response for Phase 1

● Active response / prevention

○ No active response / prevention

▲ Passive response / detection

△ No passive response / detection

Scenario	Framework	File Type	Description	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIIPRE	WithSecure	Vendor A	Vendor B	Vendor C
1	Metasploit / Meterpreter	EXE	Obfuscated EXE loader with EDR unhooking and shellcode injection	●▲	●▲	○▲	●▲	●▲	●▲	○▲	●▲	○▲	●▲	●▲	○▲	○▲	●▲
2		ISO	ISO-delivered dropper bypassing MOTW restrictions	●▲	●▲	○▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲	○▲	●▲	●▲
3		CPL	Obfuscated CPL with spoofed certificate and EDR bypass	●▲	●▲	○▲	●▲	●▲	●▲	○▲	●▲	○▲	●▲	○▲	●▲	○▲	●▲
4		XLL	USB-delivered Excel add-in with in-process shellcode injection	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
5		CHM	Compiled help file executing in-memory shellcode	●▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	○▲	●▲	●▲	○▲	●▲	●▲
6		VBS	USB VBScript decoding and executing embedded payload	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
7		PS1	PowerShell launcher with AMSI bypass and obfuscation	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
8		HTA	HTA payload abusing MSHTA for stealthy execution	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
9		MSI	Signed installer leveraging MSIExec for trusted execution	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
10		HTA	HTA launcher abusing MSHTA for proxy execution	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
11	Commercial #1	EXE	Obfuscated EXE loader with DNS-based shellcode staging	●▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲	●▲	●▲	●▲	○▲	○▲	●▲
12		EXE	Decoy installer delivering stageless shellcode	●▲	○▲	●▲	●▲	●▲	○▲	●▲	●▲	●▲	●▲	○▲	○▲	○▲	○▲
13		CPL	USB CPL abusing trusted Control Panel execution	●▲	●▲	●▲	●▲	●▲	○▲	○▲	●▲	●▲	●▲	○▲	○▲	●▲	●▲
14		HTA	HTA stager executing without dropping a PE file	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
15		EXE	Installer dropper with DNS-based stageless payload	●▲	●▲	○▲	●▲	●▲	○▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
16	PowerShell Empire	EXE	Obfuscated EXE loader with EDR bypass and shellcode injection	●▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲	○▲	●▲	○▲	○▲	●▲
17		CPL	Obfuscated CPL executing payload under trusted host	●▲	●▲	●▲	●▲	○▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲	●▲
18		EXE	Memory-evasive loader with stealthy shellcode execution	●▲	○▲	●▲	●▲	●▲	●▲	○▲	●▲	○▲	●▲	○▲	○▲	○▲	●▲
19		SCR	Obfuscated screen saver with ETW bypass	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	○▲	○▲
20		EXE	Backdoored installer executing embedded shellcode	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	○▲	○▲	●▲
21		VBS	VBScript launcher executing under valid user context	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
22		VBS	Obfuscated VBScript launching encoded PowerShell	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
23		BAT	Batch script executing encoded PowerShell payload	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
24		EXE	Masqueraded dropper delivering embedded shellcode	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
25		HTA	HTA script staging payload through MSHTA	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲

Scenario	Framework	File Type	Description	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIIPRE	WithSecure	Vendor A	Vendor B	Vendor C
26	Commercial #2	EXE	Spoofed installer with weak certificate and in-memory implant	●▲	●▲	○▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲	●▲	○▲	○▲	○▲
27		SCR	Obfuscated screen saver with EDR bypass	●▲	●▲	●▲	●▲	●▲	●▲	○▲	○▲	○▲	●▲	●▲	●▲	○▲	○▲
28		CPL	USB CPL disabling logging before payload execution	●▲	○▲	●▲	●▲	○▲	●▲	○▲	●▲	●▲	●▲	○▲	○▲	●▲	○▲
29		PIF	Stealthy PIF loader bypassing endpoint defences	●▲	●▲	○▲	●▲	○▲	●▲	○▲	○▲	○▲	●▲	●▲	○▲	○▲	○▲
30		EXE	Obfuscated EXE loader launching in-memory implant	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	○▲
31	Metasploit / Meterpreter	ISO	ISO-delivered dropper bypassing MOTW protections	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
32		HTA	HTA payload abusing MSHTA without dropping binaries	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
33		PIF	Obfuscated PIF loader with defence evasion	●▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	○▲	●▲	●▲	●▲	●▲	●▲
34		LNK	USB shortcut launching hidden payload	●▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	○▲	●▲	●▲	●▲	●▲	●▲
35		DLL	DLL sideloading via Rundll32	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
36		SCR	Obfuscated screen saver with shellcode injection	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
37		HTA	Trusted HTA launcher executing under insider context	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
38		MSI	Trusted MSI installer deploying payload silently	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
39		VBS	Trusted VBScript staging payload under user context	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
40		EXE	Trusted utility clone loading in-memory shellcode	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲
41	PowerShell Empire	EXE	Spoofed utility loader with EDR unhooking	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	○▲	●▲	●▲
42		CHM	Compiled help file launching obfuscated PowerShell	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
43		CPL	Obfuscated CPL hosted under spoofed process	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	○▲	○▲	●▲	●▲
44		SCR	Screen saver abusing SCT-based execution	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
45		BAT	Batch script launching encoded PowerShell stager	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
46		XLL	USB Excel add-in executing in-memory payload	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
47		HTA	Trusted HTA staging payload via PowerShell	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
48		SCR	Spoofed screen saver with process masquerading	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
49		VBS	Trusted VBScript launching encoded PowerShell	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲
50		DLL	Trusted DLL launcher executing in-memory shellcode	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲	●▲

Bitdefender, ESET, G DATA, VIPRE, WithSecure and Vendor C had some silent blocks in Phase 1, meaning the attack was blocked but not reported.

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.

[More Details](#)

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 to hide the attack.

[More Details](#)

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.

[More Details](#)

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.

[More Details](#)

Lateral Movement

The attacker will move laterally within the environment, 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.

[More Details](#)

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

Active and Passive Response for Phase 2

- Active response / prevention
- ▲ Passive response / detection
- ✓ Already prevented before
- No active response / prevention
- △ No passive response / detection

Scenario	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIIPRE	WithSecure	Vendor A	Vendor B	Vendor C
1	✓	✓	●▲	✓	✓	✓	●▲	✓	●▲	✓	✓	●▲	●▲	✓
2	✓	✓	●▲	✓	✓	✓	✓	✓	●▲	✓	✓	●▲	✓	✓
3	✓	✓	●▲	✓	✓	✓	●▲	✓	●▲	✓	●▲	●▲	●▲	✓
5	✓	✓	✓	✓	✓	✓	●▲	✓	●▲	✓	✓	●▲	✓	✓
11	✓	✓	✓	✓	✓	●▲	✓	✓	✓	✓	✓	●▲	●▲	✓
12	✓	●▲	✓	✓	✓	●▲	✓	✓	✓	✓	✓	●▲	○△	●▲
13	✓	✓	✓	✓	✓	●▲	●▲	✓	✓	✓	●▲	●▲	✓	✓
15	✓	✓	●▲	✓	✓	●▲	✓	✓	✓	✓	✓	✓	✓	✓
16	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲	✓
17	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓	✓	✓
18	✓	●▲	✓	✓	✓	✓	✓	✓	●▲	✓	●▲	●▲	●▲	✓
19	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲
20	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲	✓
26	✓	✓	●▲	✓	✓	✓	✓	●▲	✓	✓	✓	●▲	●▲	●▲
27	✓	✓	✓	✓	✓	✓	●▲	●▲	●▲	✓	✓	✓	●▲	●▲
28	✓	●▲	✓	✓	●▲	✓	●▲	✓	✓	✓	●▲	○△	✓	●▲
29	✓	✓	●▲	✓	●▲	✓	●▲	●▲	●▲	✓	✓	●▲	○△	●▲
33	✓	✓	✓	✓	✓	✓	●▲	✓	●▲	✓	✓	✓	✓	✓
34	✓	✓	✓	✓	✓	✓	●▲	✓	●▲	✓	✓	✓	✓	✓
40	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓	✓
41	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓	✓
43	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲	✓	✓

Phase 3 Metrics: Asset Breach

The final phase of the workflow, asset breach, is where attackers execute their ultimate objective. Below, we outline relevant tactics from the MITRE ATT&CK Framework:



Collection

Gathering target information, often involving the theft of documents, emails, or databases.

[More Details](#)

Command and Control

Enabling communication between the attacker's system and the targeted network, allowing for command execution and data exchange, often camouflaged as regular network traffic.

[More Details](#)

Impact

Refers to direct harm inflicted on the targeted organization's network, which can include manipulation, disruption, or destruction of operational systems and data. It may serve as an end goal (sabotage) or a means to obfuscate data theft by complicating breach investigations.

[More Details](#)

Exfiltration

Covertly copying the collected data from the targeted network to the attacker's server, typically utilizing a command-and-control infrastructure.

[More Details](#)

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

Active and Passive Response for Phase 3

- Active response / prevention
- ▲ Passive response / detection
- ✓ Already prevented before
- No active response / prevention
- △ No passive response / detection

Scenario	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIIPRE	WithSecure	Vendor A	Vendor B	Vendor C
12	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓
28	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓	✓
29	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓

Although for **Vendor A**, **Vendor B** and **Vendor C** a few scenarios were only blocked during Phase 3, no full unknown breaches were observed with any of the tested products this year.

The following table shows the cumulative active response by phase(s) for each product.

Active Response	Phase 1 Only	Phase 1 & 2	Overall (Phase 1, 2 & 3)
Bitdefender	100%	100%	100%
Broadcom	94%	100%	100%
Check Point	88%	100%	100%
Elastic	100%	100%	100%
ESET	96%	100%	100%
Fortinet	92%	100%	100%
G Data	82%	100%	100%
Palo Alto Networks	94%	100%	100%
TrendAI	82%	100%	100%
VIPRE	100%	100%	100%
WithSecure	88%	100%	100%
Vendor A	68%	98%	100%
Vendor B	78%	96%	100%
Vendor C	88%	100%	100%

The following table shows the cumulative passive response by phase(s) for each product.

Passive Response	Phase 1 Only	Phase 1 & 2	Overall (Phase 1, 2 & 3)
Bitdefender	98%	100%	100%
Broadcom	96%	100%	100%
Check Point	90%	100%	100%
Elastic	100%	100%	100%
ESET	98%	100%	100%
Fortinet	100%	100%	100%
G Data	80%	100%	100%
Palo Alto Networks	94%	100%	100%
TrendAI	94%	100%	100%
VIPRE	98%	100%	100%
WithSecure	96%	100%	100%
Vendor A	80%	98%	100%
Vendor B	80%	96%	100%
Vendor C	86%	100%	100%

Standardized Pricing Inputs

Product cost estimates are based on vendor-provided **list prices** in USD at the time of testing (summer 2026). For the purpose of this evaluation, list price refers to the vendor's **standard MSRP or end-customer list price before discounts**. Distributor, reseller, partner, volume-discounted, or individually negotiated prices are not used as standardized pricing inputs. Actual costs for enterprise customers may vary significantly depending on factors such as negotiated agreements, volume discounts, geographic region, distribution channels, or bundled services.

For the evaluation model, product costs are calculated for an environment of 5,000 endpoints over a five-year deployment period.

It is important to note that product pricing represents only one input within the operational impact model and has a relatively small influence on the overall results compared with factors such as breach prevention effectiveness, response capabilities, operational accuracy, and workflow efficiency.

Product	EPR Cost 5,000 / 5 Years
Bitdefender	\$ 500,777
Broadcom	\$ 3,125,000
Check Point	\$ 950,000
Elastic	\$ 808,500
ESET	\$ 972,500
Fortinet	\$ 1,825,000
G Data	\$ 642,390
Palo Alto Networks	\$ 1,000,000
TrendAI	\$ 1,625,000
VIPRE	\$ 375,000
WithSecure	\$ 726,750
Vendor A	\$ 1,200,000
Vendor B	\$ 1,500,000
Vendor C	\$ 2,500,000

These figures represent **standardized list-price inputs** used in the operational impact model and should not be interpreted as representative of actual enterprise purchase or contract pricing.

Each product offers different capabilities, architectures, and service components. Organizations should therefore consider the full functionality, operational requirements, and security performance of each solution rather than focusing solely on these list-price inputs.

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	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

The costs arising from imperfect Operational Accuracy are worked out using Cost Units of USD 1.47 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 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 cannot, 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	< 2	x0
Low	2-5	x0.5
Moderate	6-10	x2.5
High	11-20	x5
Very High	> 20	x10

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 operational impact.

Results

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

	Operational Accuracy		Workflow Delays
	Active Response	Passive Response	
Bitdefender	None	None	None
Broadcom	None	Low	None
Check Point	Low	None	None
Elastic	None	None	None
ESET	None	None	None
Fortinet	Low	None	None
G Data	None	None	None
Palo Alto Networks	Low	None	None
TrendAI	None	Moderate	None
VIPRE	None	None	None
WithSecure	None	None	None
Vendor A	Moderate	None	None
Vendor B	Low	Low	None
Vendor C	None	High	Moderate

Combined results table for Operational Accuracy and Workflow Delays

Products functionality

Product features

In this section, we provide an overview of the products' features and some of 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.



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.

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.



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, 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 Endpoint Prevention and Response (EPR) - as of Summer 2026											
	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIPRE	WithSecure
Product Name	GravityZone Business Security Enterprise	Symantec Endpoint Security Complete	Endpoint Security Advanced	Security	ESET PROTECT Enterprise Cloud	FortiEndpoint with EDR Essentials	XDR	Cortex XDR Prevent	Vision One Endpoint Security Essentials	Endpoint Detection & Response	Elements XDR
Version Number	8.26	16.0	89.10	9.4.1	6.3	6.2	1.0	9.1	14.0	13.4	26.2
Supported languages - endpoint client	English, Spanish, German, Romanian, French	English, French, Japanese, Portuguese, Spanish	English, German, Polish, Czech, Greek, Italian, Russian, French, Japanese, Spanish, Portuguese, Ukrainian	English	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese	English	German, English	English, German, Japanese, Spanish, French, Chinese	English, Japanese	English	English, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Chinese
Supported languages - management console	English, Spanish, German, Romanian, French, Japanese, Vietnamese	English, French, Japanese, Portuguese, Spanish	English, Japanese, Chinese	English	English, Spanish, German, Romanian, French, Japanese, Vietnamese	English, Japanese, Chinese, French	German, English, Polish, Dutch, French, Spanish, Italian, Portuguese	English	English, Japanese	English, Spanish, German, Romanian, French, Japanese, Vietnamese	English, Finnish, French, German, Italian, Japanese, Polish, Portuguese, Spanish, Swedish
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	proprietary	Sophos	proprietary	proprietary	proprietary	Bitdefender	proprietary	proprietary	Bitdefender	Avira
2-factor authentication	obligatory	optional	obligatory	obligatory	obligatory	optional	optional	optional	optional	optional	obligatory
Phishing protection for web browsers	•	•	•		•	•			•	•	•
Web access control	•	•			•	•		•	•	•	•
External device control	•	•	•	•	•	•	•	•	•	•	•
Sandbox feature	•	•	•		•	•		•	•	•	•
Right-click on-demand scan	•	•	•		•		•	•	•	•	•
Lock settings	•	•	•	•	•	•	•	•	•	•	•
Lock uninstalling	•	•	•	•	•	•	•	•	•	•	•
Optional / Supported Operating Systems											
Microsoft Windows											
↳ 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 analyze volatile data?		•	•				•		•		•
Additional Security Features											
Does it analyze user behavior 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?	•		•	•	•	•		•	•		•
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, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian, Czech, Chinese, Korean	English, French, Japanese, Spanish, Portuguese, German, Italian, Chinese	All	English	English, Arabic, Bulgarian, Chinese, Croatian, Czech, Dutch, Estonian, Finnish, French, German, Greek, Hebrew, Hungarian, Indonesian, Italian, Japanese, Kazakh, Korean, Latvian, Lithuanian, Norwegian, Polish, Portuguese, Romanian, Russian, Spanish, Swedish, Slovak, Slovenian, Thai, Turkish, Ukrainian, Vietnamese, Malay, Indonesian, Kazakh	English	German, English, Polish, Dutch, French, Spanish, Italian, Portuguese	English	English, Japanese, French, German, Spanish, Italian	English, Swedish, Danish	English, German, French, Swedish, Finnish, Japanese.

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. The following information offers a high-level overview of these technologies, highlighting their importance in the ever-changing cybersecurity landscape. These technologies encompass the Anti-Malware Scan Interface (AMSI), User-Mode Hooking, Callbacks, and Kernel Drivers.

1. Anti-Malware 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 is 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.

EDR Technology	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIIPRE	WithSecure
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 Anti-Malware (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.	●	●	○	○	○	○	○	○	○	●	○

EDR Technology	Bitdefender	Broadcom	Check Point	Elastic	ESET	Fortinet	G Data	Palo Alto Networks	TrendAI	VIIPRE	WithSecure
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.	●	●	○	●	●	●	○	●	●	●	●
● EDR technology implemented ○ EDR technology not implemented											

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.

EPR Test Methodology

Endpoint Prevention Response vs MITRE ATT&CK Framework

This EPR product report is a comprehensive validation of features, product efficacy and other relevant metrics to guide your risk assessment. A total of 50 scenarios were executed against real-world enterprise use-cases. These scenarios comprised several prevention and detection workflows operating under normal operational environments by different user personas. The results for the validation can be efficiently and effectively mapped to the MITRE ATT&CK® Platform³ 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 LifeCycle⁴

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.

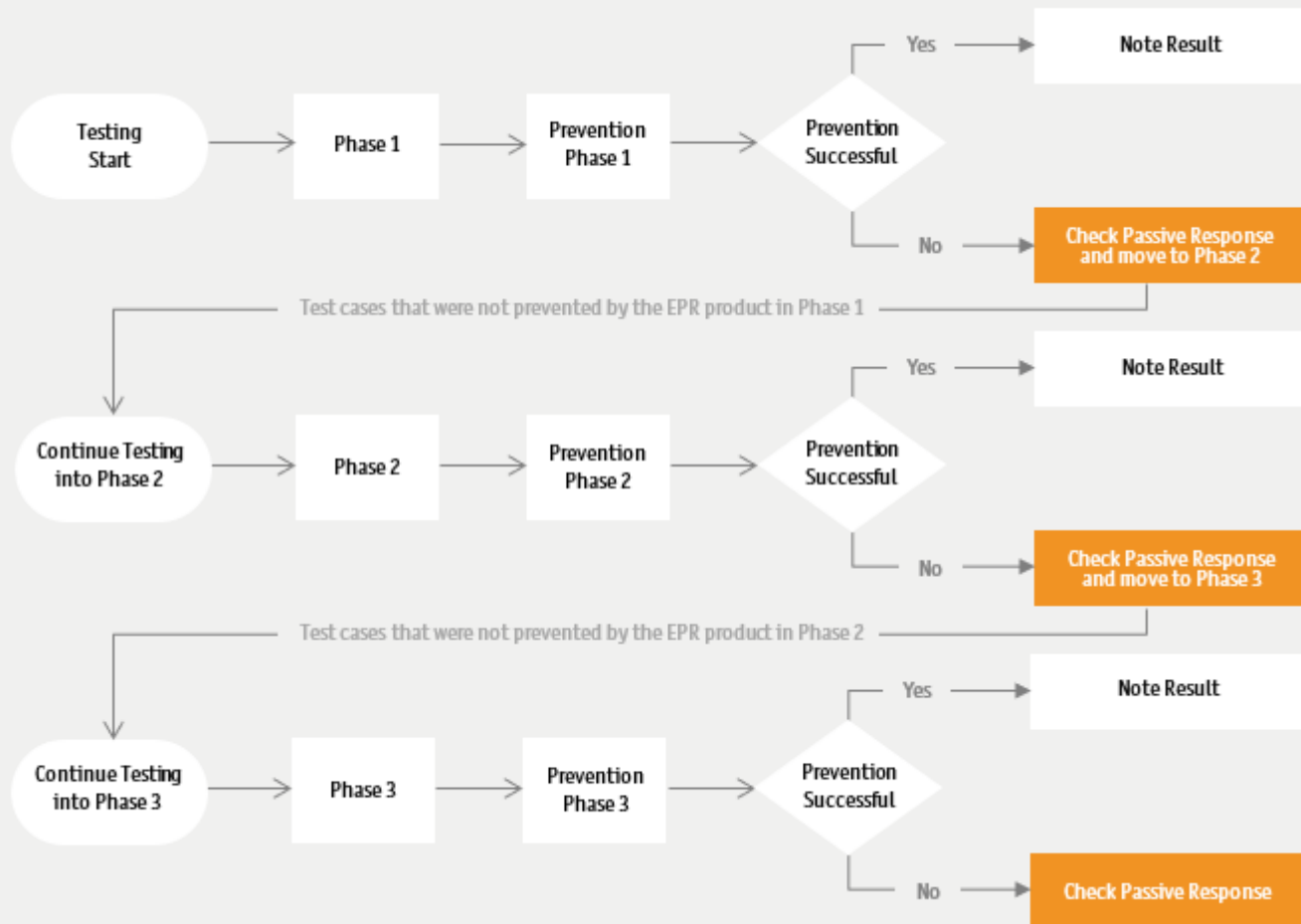
As part of the development process, AI-assisted techniques were used in the creation of testing tools and scenario variations, helping to reflect emerging attacker capabilities and evolving attack patterns. This approach helps ensure that test scenarios reflect the evolving methods available to both attackers and defenders.

³ © 2015-2026, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.

⁴ <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 to 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)

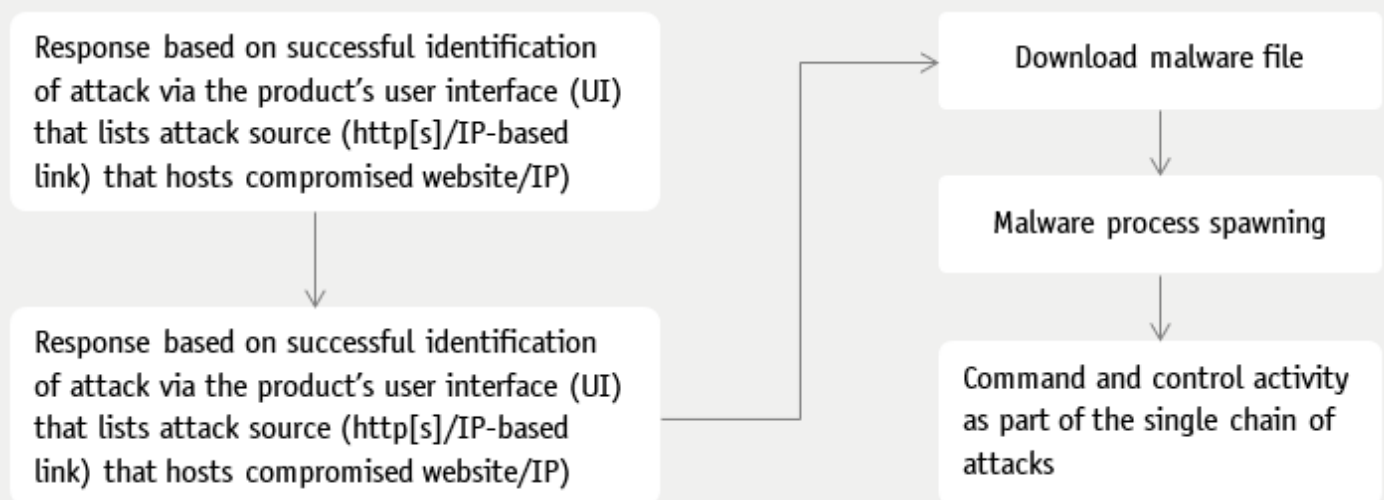
Passive response, as defined in this test, is a set of response mechanisms offered by the product with cohesive detection, correlation, reporting and actionable capabilities. Once an attacker is already inside the enterprise environment, traditional response mechanisms kick in, for example IOC and IOA 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.

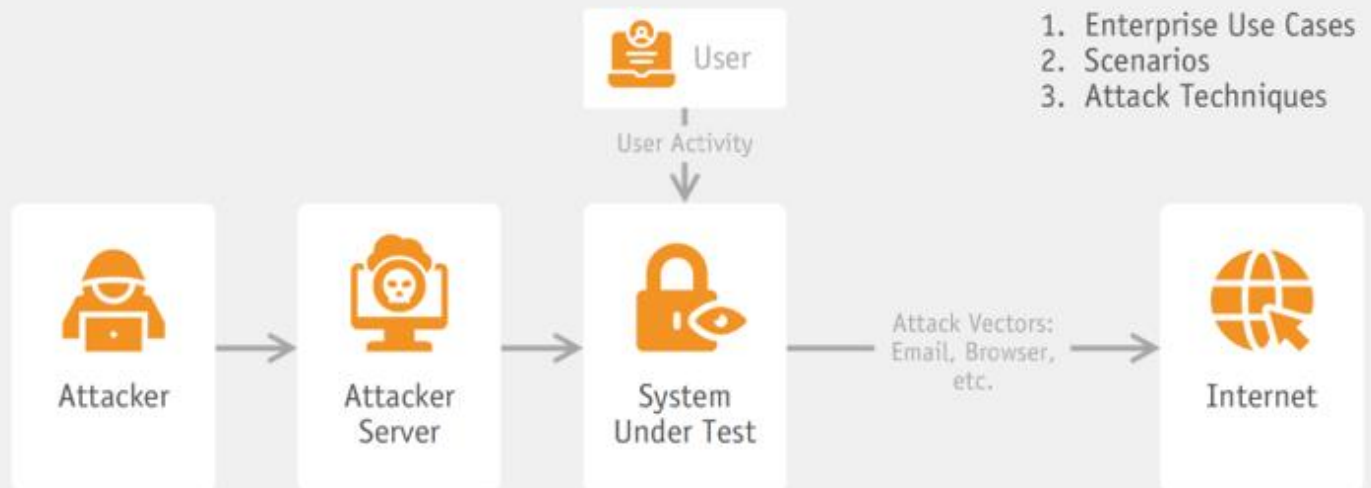
Correlation of Process, Endpoint and Network

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



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.



Enterprise EPR Workflow 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 can 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.

1.	2.	3.
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.

The increasing availability of generative AI technologies is lowering the barrier to creating sophisticated and stealthy malware, and attack-chain variations. To reflect this evolution of the threat landscape, selected test scenarios were developed and refined using AI-assisted techniques.

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 was 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 2026 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.



All the attacks were crafted using open-source and commercial tools⁵/frameworks and were developed using in-house expertise. The reason why we include commercial C2 frameworks⁶ is that these are frequently abused by attackers in real-life APTs; not using them would cause a „blind spot“ and lead to a false sense of security.

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 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 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 can identify credit-card data on Server 1, which they extract via an open C2 channel.

⁵ <https://attack.mitre.org/software/>

⁶ <https://redfoxsec.com/blog/introduction-to-c2-frameworks/>



AV-Comparatives
(September 2026)



Copyright and Disclaimer

This publication is Copyright © 2026 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.

<https://www.av-comparatives.org>