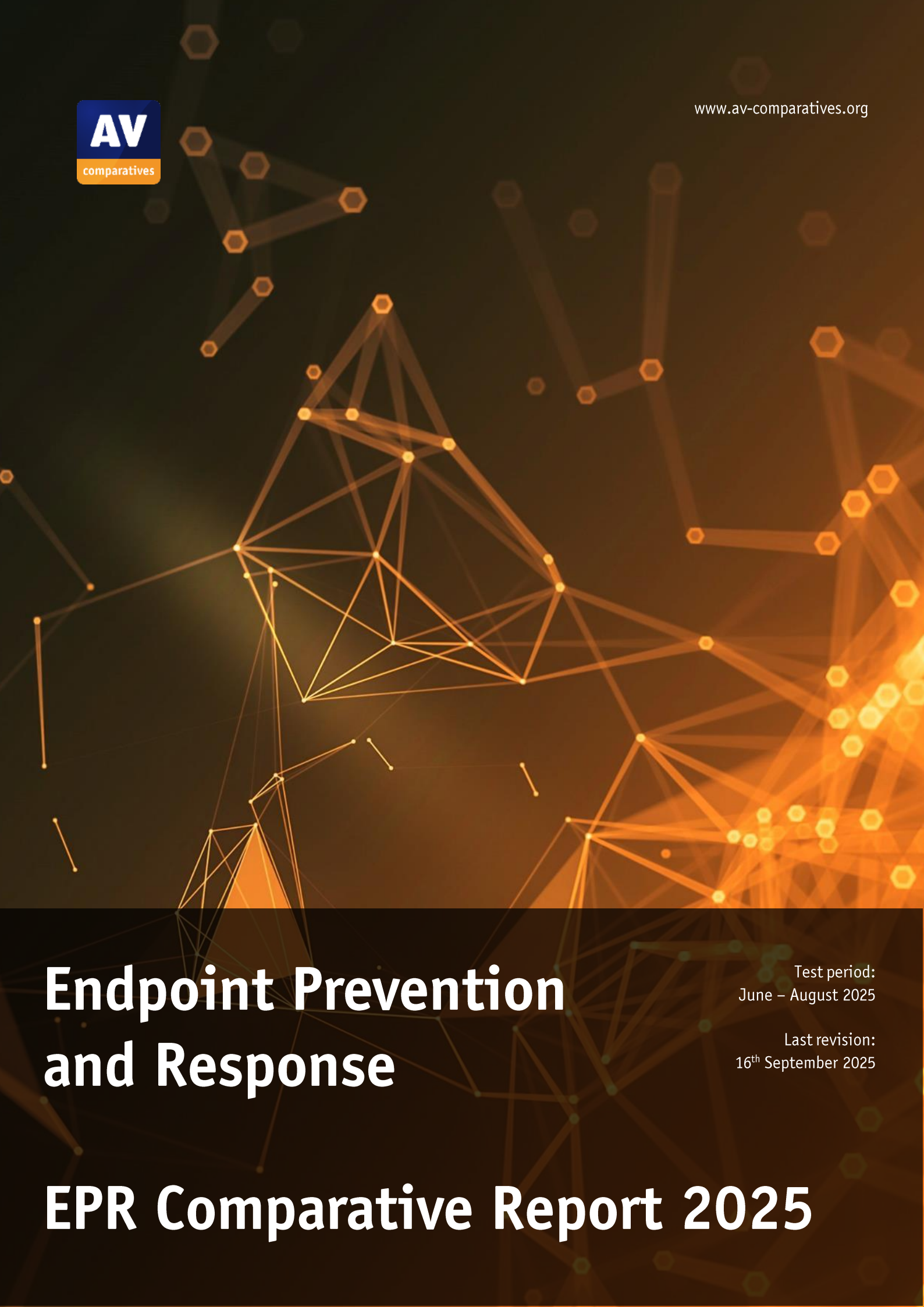


www.av-comparatives.org

Endpoint Prevention and Response

Test period:
June – August 2025

Last revision:
16th September 2025

EPR Comparative Report 2025

AV-Comparatives' EPR Certification

In the 2025 Endpoint Prevention and Response (EPR) Test, certification is awarded to products that meet a high standard of protection, detection, and response effectiveness in our Enterprise CyberRisk Quadrant™. To qualify, a product must achieve an average score of 92% or higher across both Active and Passive Response phases while maintaining cost efficiency suitable for enterprise-scale deployments.

Earning the Certified EPR label is a clear indicator of excellence. It confirms that a solution provides strong prevention, effective response capabilities, and solid overall value, making it a reliable choice for organizations facing advanced threats. Certification helps enterprise IT and security teams identify solutions that are not only technically effective but also efficient in terms of operational overhead.

AV-Comparatives' Certified EPR Products

The table below shows which of the vendors tested in AV-Comparatives' 2025 EPR Test achieved certification. These products met the defined performance and cost-effectiveness criteria, earning the Certified label in our Enterprise CyberRisk Quadrant.

Bitdefender
CHECK POINT
CROWDSTRIKE
eset
elastic
FORTINET
G DATA CyberDefense
kaspersky
paloalto NETWORKS
VIPRE SECURITY GROUP

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

Not Certified Products

Vendor A
Vendor B

EPR Executive Summary

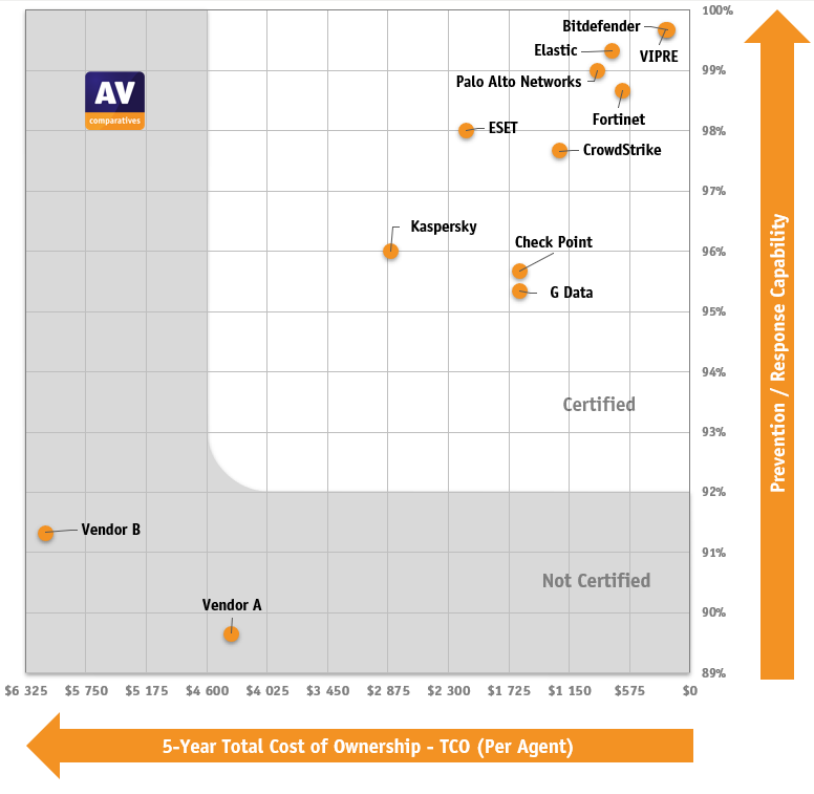
AV-Comparatives conducted the 2025 Endpoint Prevention and Response (EPR) Test between June and August 2025, with the report published in September 2025. The test comprised 50 targeted attack scenarios, each broken down into three distinct phases. Twelve enterprise security solutions were evaluated, with detailed documentation of all results. Additionally, the Total Cost of Ownership (TCO) was calculated for each product, based on a five-year deployment for 5,000 endpoints.

This year's test confirms that many leading solutions deliver both strong technical protection and solid overall value for enterprise customers. As outlined on the previous page, ten vendors met the certification criteria, demonstrating high performance across active and passive response phases while maintaining cost-effectiveness.

The 2025 test scenarios were designed to reflect real-world attack chains, including techniques such as phishing, lateral movement, data exfiltration, and abuse of legitimate tools. This approach ensures that certified products can handle complex, multi-stage threats as faced by modern enterprises.

The following vendors earned certification for their overall excellence: **Bitdefender, Check Point, CrowdStrike, ESET, Elastic, Fortinet, G Data, Kaspersky, Palo Alto Networks,** and **VIPRE**. Their certified products demonstrated strong detection and response capabilities across the evaluated attack scenarios, making them reliable choices for enterprise environments.

The Enterprise CyberRisk Quadrant™ (ECRQ) below provides a visual overview of how all tested products compare in terms of prevention/response capabilities and five-year total cost of ownership (TCO). This chart serves as complementary information to the certification results.



Contents

AV-Comparatives' EPR Certification 2
EPR Executive Summary 3
Contents 4
Introduction 5
About this test 6
Explanation of the EPR CyberRisk Quadrant 7
Which product is right for my enterprise? 7
EPR CyberRisk Quadrant Overview 8
Tested Products 10
Product Configurations and Settings 11
EPR and MITRE ATT&CK 13
MITRE ATT&CK Matrix for Enterprise 13
Test Results 14
Detailed Test Results 15
Phase 2 Metrics: Internal Propagation 18
Phase 3 Metrics: Asset Breach 20
EPR Cost Structure 23
Operational-Accuracy and Workflow-Delay Costs 24
Products functionality 26
Product features 26
Feature List 28
Overview of EDR Technologies 29
EPR Test Methodology 32
EPR Testing Workflow 33
EPR Validation Overview 35
Copyright and Disclaimer 37

Introduction

Endpoint Protection Products (EPP), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR) solutions are vital components of enterprise security, providing defences 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 impact 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 the industry's most comprehensive evaluation of such solutions. This year's test covered 12 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 noted each product's ability to take remedial action and collect indicators of compromise in an accessible way.

To provide a meaningful comparison, we developed the Enterprise EPR CyberRisk Quadrant™, which considers not only breach prevention effectiveness but also cost-effectiveness, operational accuracy, and workflow efficiency. The model is 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 2025 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 complex and demanding evaluations in the field of enterprise security. Since 2025 only vendors that do not achieve certification are given the option to remain anonymous. All certified vendors are named in the main report. 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 Series[1].

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 taken into account. 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[2] 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 complex attacks. We've used 50 test scenarios inspired by tactics and techniques employed by distinct APT groups[3], used to be attributed to China (e.g., APT3, APT41, Ke3chang, Threat-Group-3390), Russia (e.g., APT28, APT29, Sandworm, Turla, WizardSpider), Iran (e.g., APT33, APT39, OilRig), North Korea (e.g., APT37, APT38, Kimsuky), and others (e.g., Carbanak, FIN6, FIN7). Please note that our test scenarios draw inspiration from these APT groups without replicating their actions (nor are they limited to them), although there may be overlap in the techniques, subtechniques, and tools used.

[1] https://www.av-comparatives.org/enterprise/
[2] https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf
[3] https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/

Explanation of the EPR CyberRisk Quadrant

The quadrant displays two levels: **Certified** and **Not Certified**. Earning the **Certified** status reflects a high level of performance across all key areas and confirms that the product meets the rigorous standards of our evaluation. Certification is not easily achieved and remains a strong indicator of quality, reliability, and effectiveness. This streamlined presentation provides clarity while preserving the significance and prestige of being Certified.

Certified

Certified products offer an exceptional return on investment, resulting in a significantly reduced total cost of ownership (TCO). Their remarkable technical capabilities, coupled with bug-free performance, keep costs in check. These products consistently excel in prevention, detection, response, and reporting, while also delivering optimal workflow features for system administrators and operations.

Not Certified

Products with a combined Active and Passive Response of less than 92%, and/or other costs that made the TCO too high, are not certified. When a product reaches five full breaches, it is automatically disqualified (not certified) and we stop testing it further, as it would be outside of the quadrant.

Which product is right for my enterprise?

The fact that a product is shown here in the highest area of the quadrant does not necessarily mean that it is the best product for your enterprise needs. Products in lower areas of the quadrant could have features that make them well suited to your particular environment. However, we are unable to recommend the use of products that have not been certified.

Placement of the dots

The vendor 'dot' placement on the Y axis of the quadrant was driven by how good the active response or passive response capabilities were. This score will also have an influence on the X axis; a product with a high active response rate will have a lower TCO, as the response costs are smaller. Furthermore, products that stop an attack in an earlier phase will also incur fewer costs. Other factors in the TCO calculation include purchase price, operational accuracy, and workflow delays caused by e.g. sandbox analysis.

EPR CyberRisk Quadrant Overview

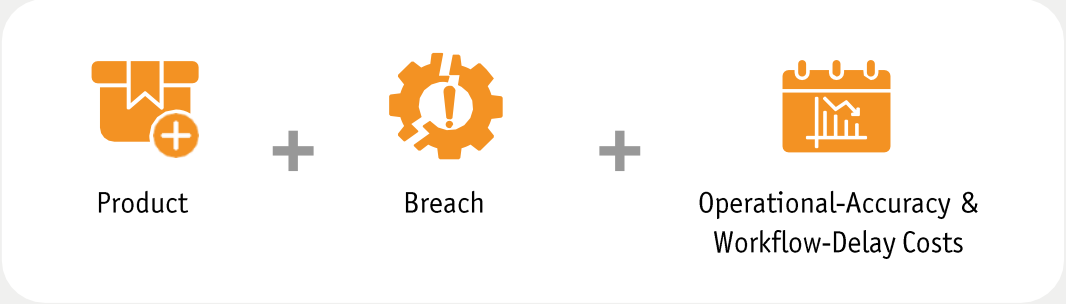
The CyberRisk Quadrant factors in the effectiveness of each product at preventing breaches, the calculated savings resulting from this, the purchase costs of the product, and the product's (in)accuracy costs.

One of the significant problems caused by a security breach is the financial cost incurred by the targeted organisation. According to IBM, the average cost of a breach in 2025 was USD 4.4 million[4]. Therefore, purchasing an effective EPR product that minimises the negative impact of an attack can be a good investment. If a company stands to lose around USD 5 million if an attack is successful, then spending even USD 2 million on security measures makes good financial sense, aside from any other considerations.

In this section, we assess the overall costs of deploying the tested security products alongside their effectiveness in preventing security breaches. This allows us to evaluate how strong a financial investment each product represents. Based on IBM's estimate of USD 4.4 million as the average cost of a data breach, we calculate the potential cost savings an organization could achieve by deploying each of the tested EPR products. The results show that all tested products provide meaningful protection, with their combined active and passive response capabilities preventing the vast majority of attacks. However, some products clearly outperform others. The more effective a solution is at preventing breaches, the lower the organization's expected costs for incident response and remediation.

The graphic below outlines the formula used to arrive at the total cost of ownership for a product, which includes the following factors. Firstly, there is the price paid to the product's vendor for the product and associated service and support charges. Next come any costs associated with over-blocking/over-reporting caused by the product, which are defined as Operational Accuracy costs below. These cases have to be investigated and remediated. In 2015, the Ponemon's Institute[5] estimated that companies waste roughly USD 1.3 million per year due to inaccurate or erroneous intelligence. To allow for inflation over the last ten years, a reasonable estimate for 2025 would be USD 1.76 million. This has been factored in as the added yearly cost that you can expect to pay for a product failing our operational-accuracy validation this year. Costs arising from imperfect Operational Accuracy are penalised, and costs due to workflow delays are also taken into account. Hence, if a user is operationally impacted by e.g. a product's features, policies or behaviour, this will be reflected in the EPR CyberRisk quadrant as well.

Next come the costs associated with breaches, whereby a product that could theoretically block 100% of attacks would have zero breach costs here, whilst a product that did not block any attacks would incur the full cost of a breach.



Total Cost of Ownership

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

The breach cost of each product per scenario was calculated, based on the ability of the EPR product to actively and passively respond at the time of execution. The procedure we used for calculating breach costs in 2025 is given below:

Active Response in Phase 1

If there was active response (i.e. the attack was successfully stopped automatically and reported) in Phase 1, then 0% of the total breach cost was added for the scenario. In case of a silent block without reporting, 12.5% of the total breach costs are added.

Only Passive Response in Phase 1

If there was NO active response in Phase 1, but the product showcased passive response capabilities in Phase 1, then only 12.5% of the total breach cost was added for the scenario.

Active Response in Phase 2

If there was active response in Phase 2, then 25% of the total breach cost was added for the scenario. In case of a silent block without reporting, 35% of the total breach costs are added.

Only Passive Response in Phase 2

If there was NO active response in Phase 2, but the product showcased passive response capabilities in Phase 2, then 50% of the total breach cost was added for the scenario.

Active Response in Phase 3

If there was active response in Phase 3, then 75% of the total breach cost was added for the scenario. In case of a silent block without reporting, 85% of the total breach costs are added.

Only Passive Response in Phase 3

If there was NO active response in Phase 3, but the product showcased passive response capabilities in Phase 3, then 95% of the total breach cost was added for the scenario.

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

If there was NO active or passive response for the scenario, then 100% of the total breach cost was added for the scenario. When a product reaches five full breaches, it is automatically disqualified (not certified) and we stop testing it further.

To calculate the X-axis in the EPR CyberRisk Quadrant, we used the list price of the product, operational accuracy (such as false positives/over-blocking/over-reporting) costs, workflow-delay costs, and the breach- cost savings. Scores shown on the X axis of the Quadrant are calculated as follows. For active response, we take the cumulative response scores for phases 1, 2 and 3, and find the average of these. We then do the same with the cumulative passive response scores for phases 1, 2 and 3. Finally, we take the average of these two scores to provide the overall response score. We are steadfast in our commitment to ensuring the utmost relevance of the metrics used in this evaluation. We considered feedback from enterprises, and took this into account where appropriate. This iterative approach ensures that our assessment process continually adapts to the ever-changing enterprise landscape. EPR systems aim to prevent threats where this is possible, or provide effective detection/response capabilities where it isn't. Endpoint products that offer a high prevention rate incur fewer costs, since there is no operational overhead required to respond to and remediate the effects of an attack. Furthermore, EPR products that provide a high detection rate (visibility and forensic detail) will realize savings, because the product provides the information needed to investigate the attack.

Active Response (Prevention)

An active response stops the attack automatically, and reports it.

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", etc.

Vendor	Product	Version
Bitdefender	GravityZone Business Security Enterprise	7.9
Check Point	Harmony Endpoint Advanced	88.70
CrowdStrike	Falcon Enterprise	7.25
Elastic	Security	9.0
ESET	PROTECT Enterprise Cloud	6.3
Fortinet	FortiEDR	5.2
G Data	Endpoint Protection Business	15.8
Kaspersky	EDR Expert (on-premises)	7.0
Palo Alto Networks	Cortex XDR Prevent	8.8
VIPRE	Endpoint Detection & Response	13.2
Vendor A - B	Product A - B	n/a

The settings which were applied to each respective product can be found on the following page.

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:

Bitdefender	Check Point	CrowdStrike	Elastic	ESET
Link	Link	Link	Link	Link

Fortinet	G Data	Kaspersky	Palo Alto Networks	VIPRE
Link	Link	Link	Link	Link

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).

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 the "Network Protection" section, additional process were added for the "Intercept Encrypted Traffic", namely "wscript.exe","cscript.exe" "powershell.exe", and "pwsh.exe".

elastic MalwareScore ("windows.advanced.malware.threshold") set to "aggressive".

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

CHECK POINT In "Web & Files Protection" and "Behavioural Protection" everything was set on "Prevent". In the "Advanced Settings", "File remediation" was set to "Quarantine" and "Terminate". "Anti-Exploit Mode" was set to "Prevent". In "Analysis & Remediation", the "Protection mode" was set to "Always", "Enable Threat Hunting" was set to "On", and "Attack Remediation" was set to "Medium & High". All settings were set to "Connected Mode".

CROWDSTRIKE Everything enabled and set to maximum, i.e. "Extra Aggressive". "On Write Script File Visibility" and "Unknown detection-related executable analysis" enabled. "On-demand Scans" and "Unknown executables analysis" enabled. "Early adopter sensor builds" enabled. "Redacted HTTP detection details" disabled. "Extended user mode data visibility" set to "Aggressive". "Identity Protection" was enabled; In "Next-Gen SIEM" a workflow was created to contain devices and add them to watchlist when the identity was compromised with the "Severity" greater than or equal to "Low". "Authentication traffic inspection" was enabled.

G DATA CyberDefense "BEAST Behavior Monitoring" set to "Halt program and move to quarantine". "G DATA WebProtection" add-on installed and activated. "Malware Information Initiative" enabled.

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

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.

Under “Agent settings”, "On-Write File Examination" was enabled. Under “Malware Profile”, “Portable Executable and DLL examination”, “Behavioural Threat Protection” and “Ransomware Protection” were set to “Quarantine”. “Treat Grayware as Malware” was enabled. "PowerShell Script Files", "VB Scripts Examination", "ASP & ASPX Files" were set to "Block".

“IDS” enabled and set to “Block With Notify”. “Firewall” enabled. “AMSI” enabled and set to "Block and disinfect". “Incompatible Software Handling” disabled.

Vendor A - B

Non-default settings were used.

EPR and MITRE ATT&CK

MITRE ATT&CK Matrix for Enterprise

The diagram below shows the entire MITRE ATT&CK Matrix for Enterprise. The column headings represent the ATT&CK Tactics (aims), while the boxes below them represent the ATT&CK Techniques 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 orange boxes below.

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Content Injection	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	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	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploit Public-Facing Application	Input Injection	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
External Remote Services	Inter-Process Communication	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Debugger Evasion	Exploitation for Credential Access	Debugger Evasion	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Hardware Additions	Native API	Compromise Host Software Binary	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication	Device Driver Discovery	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Phishing	Scheduled Task/Job	Create Account	Create or Modify System Process	Direct Volume Access	Forge Web Credentials	Domain Trust Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Replication Through Removable Media	Shared Modules	Create or Modify System Process	Domain or Tenant Policy Modification	Domain or Tenant Policy Modification	Input Capture	File and Directory Discovery	Software Deployment Tools	Data from Information Repositories	Encrypted Channel	Exfiltration Over Web Service	Email Bombing
Supply Chain Compromise	Software Deployment Tools	Event Triggered Execution	Escape to Host	Email Spoofing	Modify Authentication Process	Group Policy Discovery	Taint Shared Content	Data from Local System	Fallback Channels	Scheduled Transfer	Endpoint Denial of Service
Trusted Relationship	System Services	Exclusive Control	Event Triggered Execution	Execution Guardrails	Multi-Factor Authentication Interception	Log Enumeration	Use Alternate Authentication Material	Data from Network Shared Drive	Hide Infrastructure		Financial Theft
Valid Accounts	User Execution	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	Network Service Discovery		Data from Removable Media	Ingress Tool Transfer		Firmware Corruption
Wi-Fi Networks	Windows Management Instrumentation	Hijack Execution Flow	Hijack Execution Flow	File and Directory Permissions Modification	Network Sniffing	Network Share Discovery		Data Staged	Multi-Stage Channels		Inhibit System Recovery
		Modify Authentication Process	Process Injection	Hide Artifacts	OS Credential Dumping	Network Sniffing		Email Collection	Non-Application Layer Protocol		Network Denial of Service
		Modify Registry	Scheduled Task/Job	Hijack Execution Flow	Steal or Forge Authentication Certificates	Password Policy Discovery		Input Capture	Non-Standard Port		Resource Hijacking
		Office Application Startup	Valid Accounts	Impair Defenses	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Screen Capture	Protocol Tunneling		Service Stop
		Power Settings		Impersonation	Steal Web Session Cookie	Permission Groups Discovery		Video Capture	Proxy		System Shutdown/Reboot
		Pre-OS Boot		Indicator Removal	Unsecured Credentials	Process Discovery			Remote Access Tools		
		Scheduled Task/Job		Indirect Command Execution		Query Registry			Traffic Signaling		
		Server Software Component		Masquerading		Remote System Discovery			Web Service		
		Software Extensions		Modify Authentication Process		Software Discovery					
		Traffic Signaling		Modify Registry		System Information Discovery					
		Valid Accounts		Obfuscated Files or Information		System Location Discovery					
				Pre-OS Boot		System Network Configuration Discovery					
				Process Injection		System Network Connections Discovery					
				Reflective Code Loading		System Owner/User Discovery					
				Rogue Domain Controller		System Service Discovery					
				Rootkit		System Time Discovery					
				Subvert Trust Controls		Virtual Machine Discovery					
				System Binary Proxy Execution		Virtualization/Sandbox Evasion					
				System Script Proxy Execution							
				Template Injection							
				Traffic Signaling							
				Trusted Developer Utilities Proxy Execution							
				Use Alternate Authentication Material							
				Valid Accounts							
				Virtualization/Sandbox Evasion							
				XSL Script Processing							

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

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	5-Year Product Cost (Per Agent)	Active Response	Passive Response	Combined Prevention/Response Capabilities Y-Axis	Operational Accuracy Costs	Workflow Delay Costs	5-Year TCO (Per Agent) X-Axis
Bitdefender	$100	100%	99.3%	99.7%	None	None	$210
Check Point	$190	96.0%	95.3%	95.7%	None	None	$1 620
CrowdStrike	$475	97.3%	98.0%	97.7%	None	None	$1 245
Elastic	$167	99.3%	99.3%	99.3%	Low	None	$739
ESET	$152	99.3%	99.3%	99.3%	Moderate	None	$2 132
Fortinet	$207	98.7%	98.7%	98.7%	None	None	$647
G Data	$80	95.3%	95.3%	95.3%	None	None	$1 620
Kaspersky	$206	95.3%	96.7%	96.0%	Moderate	None	$2 846
Palo Alto Networks	$200	99.3%	98.7%	99.0%	Low	None	$882
VIPRE	$120	99.3%	100%	99.7%	None	None	$230
Vendor A	$ 300	89.3%	90.0%	89.7%	None	None	$4 370
Vendor B	$ 195	91.3%	92.0%	91.7%	High	None	$6 135

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

Endpoint Compromise and Foothold

Initial Access
Execution
Persistence

Phase 2

Internal Propagation

Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement

Phase 3

Asset Breach

Collection
Command and Control
Exfiltration
Impact

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	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIIPRE	Vendor A	Vendor B
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	●▲	○△	●▲	●▲	●▲	●▲	○△	●▲	●▲	●▲	●▲	○△

Scenario	Framework	File Type	Description	Bitdefender	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIIPRE	Vendor A	Vendor B
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	●▲	●▲	●▲	●▲	○▲	○△	●▲	●▲	●▲	●▲	○△	●▲

Bitdefender, Check Point, and Palo Alto Networks had a silent block 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

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

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

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	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIIPRE	Vendor A	Vendor B
2	✓	✓	✓	✓	✓	✓	●▲	✓	✓	✓	✓	●▲
3	✓	✓	●▲	✓	✓	✓	✓	●▲	✓	✓	●▲	✓
4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲
9	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓
11	✓	✓	●▲	✓	✓	✓	✓	✓	✓	✓	●▲	✓
12	✓	✓	✓	✓	✓	✓	✓	●▲	✓	✓	✓	●▲
13	✓	✓	●▲	✓	✓	✓	●▲	●▲	✓	✓	●▲	✓
14	✓	●▲	✓	✓	●▲	✓	✓	✓	✓	✓	✓	●▲
19	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲	✓
21	✓	●▲	✓	✓	●▲	✓	●▲	●▲	✓	✓	●▲	●▲
22	✓	●▲	✓	✓	✓	✓	●▲	●▲	✓	✓	○△	○▲
23	✓	✓	✓	✓	●▲	✓	✓	✓	✓	✓	✓	✓
25	✓	●▲	✓	✓	✓	✓	●▲	✓	✓	✓	✓	○△
28	✓	✓	✓	✓	✓	●▲	●▲	✓	✓	✓	✓	✓
31	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲
33	✓	✓	●▲	●▲	✓	✓	✓	✓	✓	✓	✓	●▲
36	✓	●▲	✓	✓	✓	✓	✓	●▲	✓	✓	●▲	✓
41	✓	●▲	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓
46	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓	●▲	✓
47	✓	✓	✓	✓	✓	✓	●▲	✓	✓	✓	✓	○△
48	✓	✓	✓	✓	●▲	✓	✓	✓	✓	✓	○△	✓
49	✓	✓	✓	✓	✓	✓	✓	●▲	✓	✓	✓	✓
50	✓	✓	✓	✓	●▲	●▲	✓	✓	✓	✓	○△	✓

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

Scenario	Bitdefender	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIIPRE	Vendor A	Vendor B
22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	●▲
25	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲
47	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲
48	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓
50	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	●▲	✓

Although for **Vendor A** and **Vendor B** 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%
Check Point	88%	100%	100%
CrowdStrike	92%	100%	100%
Elastic	98%	100%	100%
ESET	90%	100%	100%
Fortinet	96%	100%	100%
G Data	86%	100%	100%
Kaspersky	86%	100%	100%
Palo Alto Networks	98%	100%	100%
VIPRE	98%	100%	100%
Vendor A	74%	94%	100%
Vendor B	80%	94%	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%
Check Point	86%	100%	100%
CrowdStrike	94%	100%	100%
Elastic	98%	100%	100%
ESET	98%	100%	100%
Fortinet	96%	100%	100%
G Data	86%	100%	100%
Kaspersky	90%	100%	100%
Palo Alto Networks	96%	100%	100%
VIPRE	100%	100%	100%
Vendor A	76%	94%	100%
Vendor B	80%	94%	100%

The following table shows the raw data, i.e. numbers of scenarios prevented/reported.

Product	Scenarios	Overall Active Prevention	Overall Passive Response	No Prevention/Response
Bitdefender	50	50	50	0
Check Point	50	50	50	0
CrowdStrike	50	50	50	0
Elastic	50	50	50	0
ESET	50	50	50	0
Fortinet	50	50	50	0
G Data	50	50	50	0
Kaspersky	50	50	50	0
Palo Alto Networks	50	50	50	0
VIPRE	50	50	50	0
Vendor A	50	50	50	0
Vendor B	50	50	50	0

EPR Cost Structure

Product costs are based on list prices in USD provided by vendors at the time of testing (summer 2025). The actual cost to end users might be lower, depending on different factors. In general, pricing may vary based on factors like volume discounts, negotiated discounts, geographic location, distribution channel, and partner margins.

The EPR Cost incorporates the product costs for 5,000 clients, based on a 5-year contract.

Product	EPR Cost 5,000 / 5 Years
Bitdefender	$ 500,777
Check Point	$ 950,000
CrowdStrike	$ 2,374,400
Elastic	$ 835,200
ESET	$ 760,833
Fortinet	$ 1,035,000
G Data	$ 397,750
Kaspersky	$ 1,032,000
Palo Alto Networks	$ 1,000,000
VIPRE	$ 600,000
Vendor A	$ 1,500,000
Vendor B	$ 975,000

Please note that each product has its own particular features and advantages. We suggest that readers consider each product in detail, rather than looking at these list prices alone. Some products might have additional / different features and services that make them particularly suitable for some organisations.

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 1.76 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	< 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 costs incurred.

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
Check Point	None	None	None
CrowdStrike	None	None	None
Elastic	Low	None	None
ESET	None	Moderate	None
Fortinet	None	None	None
G Data	None	None	None
Kaspersky	None	Moderate	None
Palo Alto Networks	Low	None	None
VIPRE	None	None	None
Vendor A	None	None	None
Vendor B	None	High	None

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.

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.

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.

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 2025	Bitdefender	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIPRE
Product Name	GravityZone Business Security Enterprise	Harmony Endpoint Advanced	Falcon Elite	Security	PROTECT Enterprise Cloud	FortiEDR	Endpoint Protection Business	EDR Expert (on-premises)	Cortex XDR Prevent	Endpoint Detection & Response
Version Number	7.9	88.70	7.16	9.0	6.3	5.2	15.8	7.0	8.8	13.2
Supported languages - endpoint client	English, Spanish, German, Romanian, French	English, German, Polish, Czech, Greek, Italian, Russian, French, Japanese, Spanish, Portuguese, Ukrainian	English	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	English, German, Polish, Czech, Greek, Italian, Russian, French, Japanese, Spanish, Portuguese, Ukrainian	Arabic, Czech, Chinese, Dutch, English, French, Japanese, Hungarian, Italian, German, Kazakh, Korean, Polish, Portuguese, Portuguese, Romanian, Russian, Spanish, Turkish, Vietnamese	English, German, Japanese, Spanish, French, Chinese	English
Supported languages - management console	English, Spanish, German, Romanian, French, Japanese, Vietnamese	English, Japanese, Chinese	English, Japanese	English	English, Spanish, German, Romanian, French, Japanese, Vietnamese	English, Japanese, Chinese, French	English, Japanese, Chinese	Arabic, German, English, Spanish, French, Italian, Japanese, Kazakh, Korean, Polish, Portuguese, Russian, Turkish, Chinese	English	English, Spanish, German, Romanian, French, Japanese, Vietnamese
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	Sophos	proprietary	proprietary	proprietary	proprietary	Bitdefender	proprietary	proprietary	Bitdefender
2-factor authentication	obligatory	obligatory	obligatory	obligatory	obligatory	optional	optional	optional	optional	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				•					•	
Test 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, 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, Spanish, German, Romanian, French, Italian, Portuguese, Polish, Russian, Czech, Chinese, Korean	All	English, Japanese, Spanish, Portuguese, French, Danish, Chinese, Hindi, Indonesian, Hebrew, Malay, Filipino, Swedish	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	English, French, German, Italian, Russian, Spanish, Japanese, Chinese, Turkish, Portuguese, Arabic	English	English, Swedish, Danish

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'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.

EDR Technology	Bitdefender	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIIPRE
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	Check Point	CrowdStrike	Elastic	ESET	Fortinet	G Data	Kaspersky	Palo Alto Networks	VIIPRE
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® Platform[6] and NIST platform, so that it becomes easier to operationalize the risk regarding a specific endpoint.

MITRE ATT&CK for Enterprise vs Seven Stage Cyber Attack LifeCycle[7]

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.

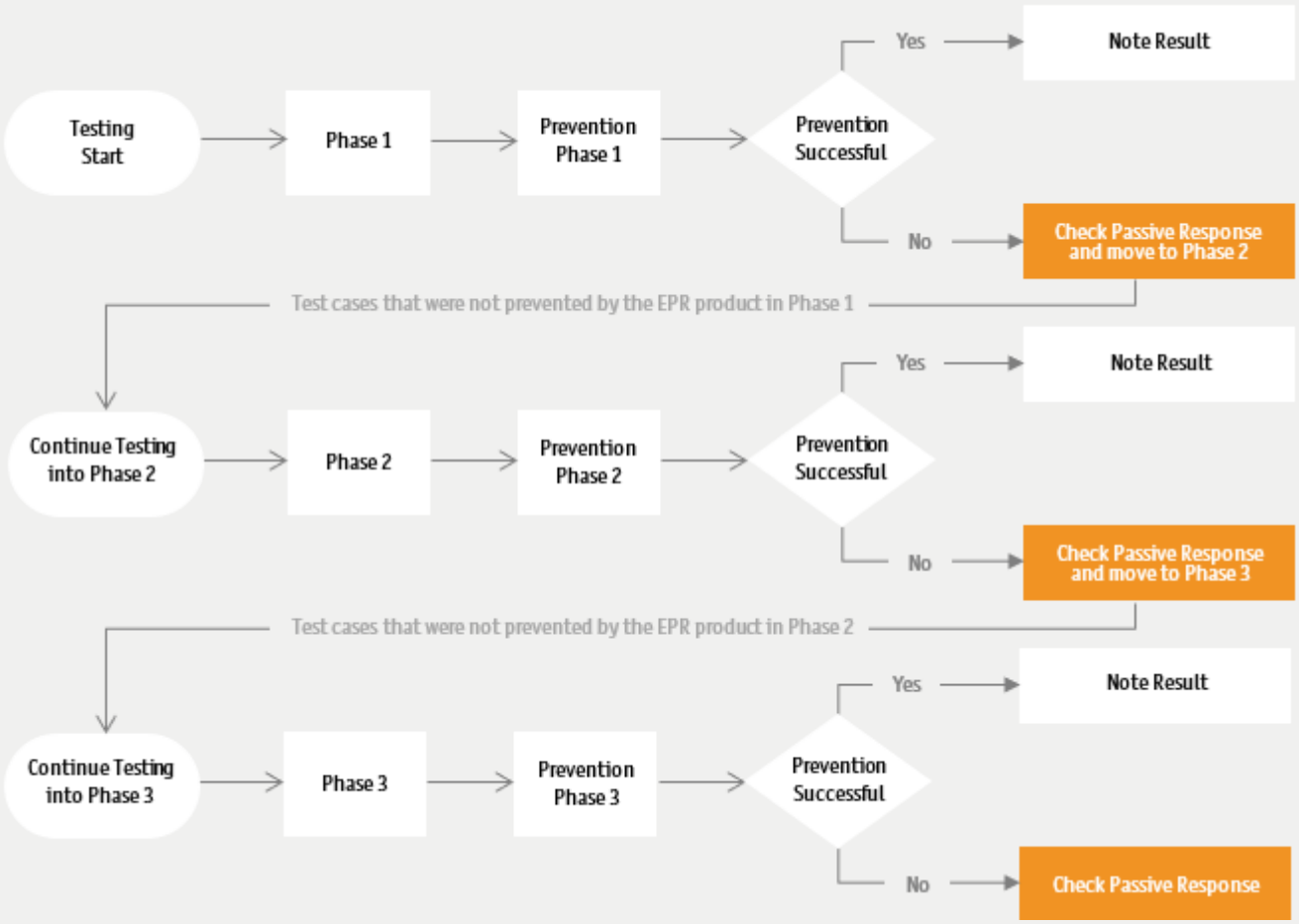
As illustrated in the graphic on the next page, we moved away from "atomic" testing, i.e. tests that only look at a particular component of the ATT&CK framework, and instead evaluated the EPR products from the context of the entire attack kill-chain, with workflows interconnecting at every stage from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

Please refer to the following article to learn about the differences between the AV-Comparatives EPR Test and the MITRE ATT&CK Engenuity Test: Link

[6] © 2015-2025, The MITRE Corporation. MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
[7] https://attack.mitre.org/resources/enterprise-introduction/

EPR Testing Workflow

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



Enterprise EPR Workflow Overview

Prevention (Active Response)

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

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

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

Detection (Passive Response)

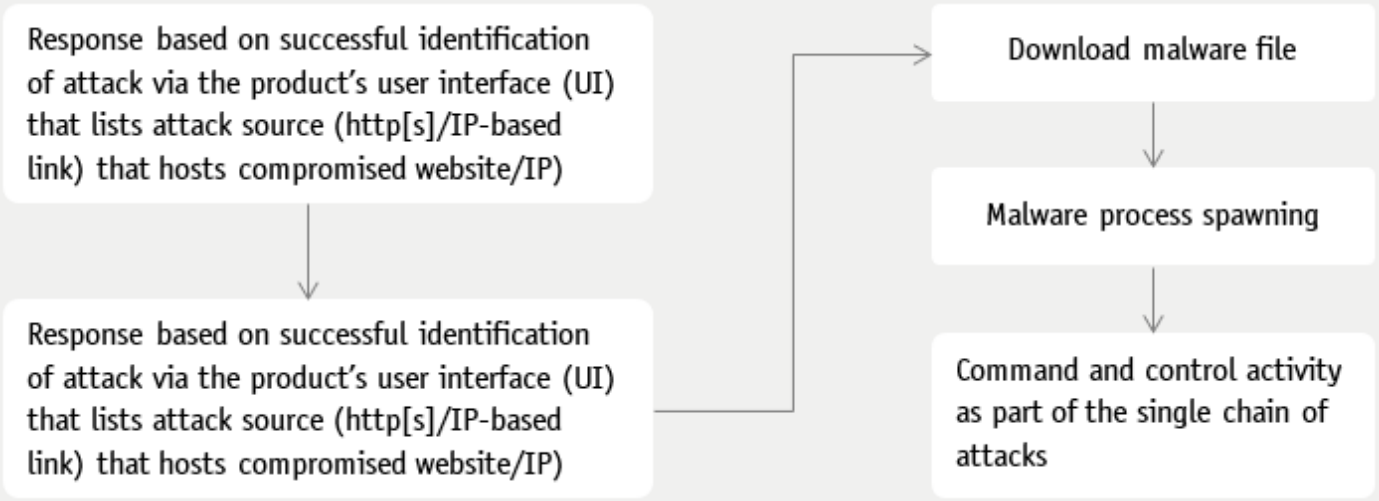
Passive response, as defined in this test, is a set of response mechanisms offered by the product with cohesive detection, correlation, reporting and actionable capabilities. Once an attacker is already inside the enterprise environment, traditional response mechanisms kick in, for example IOC and IOA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

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

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

Correlation of Process, Endpoint and Network

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



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 are able to do when deploying it in their infrastructure. The details of the configurations are included at the beginning of this report.

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

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

Test Objective

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

1.

In which attack phase did the prevention / detection occur? Phase 1 (Endpoint Compromise and Foothold), Phase 2 (Internal Propagation) or Phase 3 (Asset Breach)?

2.

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?

3.

Did the EPR product incur any additional costs due to imperfect Operational Accuracy or workflow delays?

Targeted Use-Cases

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

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

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

The test was conducted in summer 2025, 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 tools[8]/frameworks, and were developed using in-house expertise. The reason why we include commercial C2 frameworks[9] 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 it can be seen that the compromised User Account A has access to the C$ share on Workstation B, meaning that the account has local admin privileges on this workstation. With the knowledge gained from internal discovery, the attacker moves laterally from Workstation A to Workstation B. They then continue with internal discovery on Workstation B. This enables them to find a network administrator's open user session on Workstation B. To take advantage of this, the attacker dumps the LSASS process, and is thus able to steal the administrator's credentials. After doing this, they discover that the compromised administrator account has access to Server 1. The attacker then uses this compromised admin account to move laterally from Workstation B to Server 1, and then compromise this server. Here they perform further internal discovery, and also use some defence evasion techniques to bypass the installed security product (e.g. by patching AMSI and ETW). At the end of this procedure, they are able to identify credit-card data on Server 1, which they extract via an open C2 channel.

[8] https://attack.mitre.org/software/
[9] https://redfoxsec.com/blog/introduction-to-c2-frameworks/

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