AMTSO TEST PLAN

Venak Security Zero-Day AV/EDR Test

September–November 2026

Keywords	anti-malware; accreditation; assessment; testing; test plan; template; EDR; zero-day testing
Test Plan Creation Date	September 8, 2026
Version	1.3
Test Start Date	September 15, 2026
Final Report Delivery	November 1, 2026

AMTSO Test ID: [AMTSO-LS1-TP214]

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. (AMTSO) Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version 1.3 (the “Standard”). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version 2.5. Venak Security Test Lab is solely responsible for the content of this Test Plan.

1. Introduction

This Test Plan outlines Venak Security Test Lab’s September–November 2026 Zero-Day Evaluation of antivirus (AV) and Endpoint Detection and Response (EDR) solutions.

The objective is to evaluate whether selected endpoint security products can prevent execution of curated malicious and zero-day-style test samples under a simple, repeatable desktop execution methodology. The test is designed to be transparent, consistently applied across products, and aligned with AMTSO testing principles.

2. Scope

This test focuses on prevention and detection of malicious and zero-day-style samples by AV and AV/EDR endpoint security solutions.

Products Under Test

Category	Product
AV / Endpoint Security	AVG Anti-Virus
EDR / Endpoint Platform	Bitdefender Antivirus Plus
EDR / Endpoint Platform	Broadcom Carbon Black
EDR / Endpoint Platform	Check Point Endpoint Security
EDR / Endpoint Platform	Cisco Secure Endpoint
EDR / Endpoint Platform	CrowdStrike Falcon EDR
EDR / Endpoint Platform	Cybereason EDR
EDR / Endpoint Platform	eScan Enterprise EDR
AV / Endpoint Security	ESET NOD32 Antivirus
AV / Endpoint Security	F-Secure Internet Security
EDR / Endpoint Platform	FortiEDR
AV / Endpoint Security	G DATA Internet Security
EDR / Endpoint Platform	HP Wolf Security
AV / Endpoint Security	K7 Total Security
AV / Endpoint Security	Malwarebytes Premium Security
AV / Endpoint Security	McAfee Antivirus
EDR / Endpoint Platform	Net Protector Anti-Virus Pro
EDR / Endpoint Platform	Palo Alto Cortex Endpoint Security
AV / Endpoint Security	Panda Dome Antivirus
EDR / Endpoint Platform	Qualys Endpoint Protection
AV / Endpoint Security	Quick Heal Anti-Virus
EDR / Endpoint Platform	SentinelOne Singularity EDR
EDR / Endpoint Platform	Seqrite Endpoint Security
AV / Endpoint Security	Endpoint Detection and Response
AV / Endpoint Security	Surfshark Antivirus
AV / Endpoint Security	Total Defense Anti-Virus
AV / Endpoint Security	TotalAV Antivirus Pro
EDR / Endpoint Platform	Trellix Endpoint Security
AV / Endpoint Security	Trend Micro TrendAI Endpoint Security
AV / Endpoint Security	VIPRE ANTIVIRUS PLUS
EDR / Endpoint Platform	WatchGuard Endpoint Security
AV / Endpoint Security	Webroot Antivirus
EDR / Endpoint Platform	WithSecure Elements Endpoint Protection

Versioning Policy: Latest publicly available version as of September 15, 2026 (test start date).

Threat Type: Curated malicious samples and zero-day-style threats not previously used in this test campaign.

3. Methodology and Strategy

Overview

The test uses a deliberately simple execution methodology so that every product is evaluated under the same observable condition. Samples are executed on an isolated Windows desktop test system while the security product operates with its normal protection features enabled.

Simple AV/EDR Test Method

1. Prepare a clean, isolated Windows 11 virtual machine with the product installed and updated using the vendor's default settings.
2. Place the selected malicious test sample on the desktop of the test system.
3. Start the test recording and note the execution start time.
4. Run the malicious sample from the desktop.
5. Observe the endpoint security product for up to one minute (60 seconds) from execution start.
6. If the AV/EDR solution blocks, terminates, quarantines, or otherwise prevents the sample from continuing within 60 seconds, record the result as a Successful Detection/Block.
7. If the sample is not blocked within 60 seconds, record the result as Not Blocked Within Test Window.
8. Capture the alert, event log, screenshot/video evidence, and detection time when available, then reset the virtual machine to a clean snapshot before the next test.

Primary Success Criterion: If the AV/EDR solution blocks the sample within one minute (60 seconds) of execution, the test result is considered a successful detection/block.

Sample Sourcing

- Zero-day-style samples generated by Venak Security's AI Malware Simulator technology to create novel and polymorphic test artifacts for controlled laboratory evaluation.
- Samples include curated malicious artifacts selected by Venak Security Test Lab for the campaign.
- Sample provenance, hashes, timestamps, and test identifiers are logged for traceability. Where VirusTotal is used as a reference, its timestamps and detection history are recorded as supporting evidence rather than the sole basis for classification.

Evaluation Data Collected

- Block Result: whether the sample was blocked within 60 seconds.
- Detection/Block Latency: elapsed seconds from execution start to the observed block event.
- Alert Evidence: screenshots, event logs, product alerts, or other available evidence.
- Response Type: blocked, terminated, quarantined, prevented from launching, or not blocked within the test window.

Test Sample Delivery

Samples generated during the test are not free. These samples are generated by Venak Security's AI Malware Simulator. We would be happy to share the samples with vendors for a flat rate of $1,999 USD.

Updates

AV/EDR products will be permitted to auto-update according to vendor-default settings during testing to reflect real-world use.

Repeatability

- Each sample execution and result is logged and time-stamped.

- Virtual machine snapshots and standardized configurations are used to maintain consistent test conditions.
- The same one-minute observation window is applied to every product and sample.

4. Participation

Vendors: Products listed in Section 2.

Opt-Out Policy: Output is only available if there are technical difficulties during the testing period that could affect the vendor's reputation. Vendors may opt out by providing written notice no later than September 20, 2026.Written requests should be sent to info@Venaksecurity.com. Any voluntary removal request will be noted in the final participant list, and the public will be notified that your product has been removed at your request.

Notification: All vendors are scheduled to be notified on September 15, 2026.

Funding: Self-funded by Venak Security. No vendor sponsorship. No test fees.

Conflict of Interest: None identified.

5. Environment

Configuration

- Windows 11 Pro (latest patched build available at test start)
- Virtual Machines (VMware Workstation)
- 4 vCPU, 16 GB RAM, 120 GB SSD per instance
- Internet/cloud access enabled when required by the product's normal operation
- Vendor-default protection settings unless a documented exception is required for successful installation or activation

Sample Provenance: Venak Security AI Malware Simulator and curated malicious test samples maintained by Venak Security Test Lab.

Geographic Focus: Global, with no restrictions.

Curation Process: Samples are assigned unique identifiers and documented with available hash, timestamp, provenance, and validation information before use.

6. Schedule

Public Notification Date: September 9, 2026

Test Start Date: September 20, 2026

Final Report Delivery Date: November 1, 2026

Milestone	Date
AMTSO / Public Notification Published	September 9, 2026
Vendor Notification	September 15, 2026
Vendor Configuration Confirmation Period	September 9–14, 2026
Vendor Opt-Out Deadline	September 20, 2026
Test Period	September 15–October 16, 2026
Preliminary Results Shared	October 23, 2026
Draft Report Delivery	October 26, 2026
Dispute Window	October 26–31, 2026
Final Report Delivery / Publication	November 1, 2026

7. Control Procedures

- Cloud access is verified before each product test begins.
- Screen/video recording and relevant logs are collected during test execution.
- Vendor-default update settings are maintained.
- Each test virtual machine is reset to a clean snapshot between sample runs.
- The system clock is synchronized before testing so that one-minute detection timing is measured consistently.
- Only one sample is executed at a time in each test instance.

8. Dependencies

- Vendors confirm installation defaults and required cloud connectivity when requested.
- Configuration monitoring and validation occurs during September 9–14, 2026.
- Test systems must have working network access where the product requires cloud-assisted protection.
- Samples and evidence must remain isolated to the controlled test environment.

9. Scoring Process

Each AV/EDR product will be evaluated using the following primary measures:

1. Prevention Rate (%) – percentage of samples blocked within the 60-second test window.
2. Detection/Block Latency (seconds) – elapsed time from sample execution to the block event, up to a maximum recorded test window of 60 seconds.
3. Reporting Quality – availability and clarity of the product alert or event evidence associated with the block.

The principal protection result is the Prevention Rate. Detection latency and reporting quality are supporting measures. Any composite Final Protection Index (FPI), if published, will document its formula and weighting in the final report.

10. Dispute Process

Window: October 26–31, 2026

Written disputes must include technical evidence relevant to the reported test result. Examples may include:

- Basic evidence: hashes, product logs, alert screenshots, timestamps.
- Advanced evidence: packet captures, behavior traces, endpoint telemetry, or other technical artifacts that directly support the dispute.

11. Attestations

I, Nima Bagheri, representing Venak Security Test Lab, hereby attest that:

1. Public test notification is posted or submitted for publication through the applicable AMTSO process.
2. All participating vendors are treated equally under the same documented test methodology.
3. Any known test design imbalances or deviations will be disclosed.
4. No vendor paid to participate.
5. No conflicts of interest are known.
6. This test is fully self-funded by Venak Security.

Signature: /s/ Nima Bagheri

Name: Nima Bagheri

Test Lab: Venak Security Test Lab

Website: https://Venaksecurity.com

Email: info@Venaksecurity.com

Date: September 8, 2026

AMTSO Test ID: [AMTSO-LS-TP214]