AMTSO Test Plan

Keywords: anti-malware; accreditation; assessment; testing; test plan; template; EDR; zero-day testing

Test Plan Creation Date: January 12, 2026

Version: 1.2

Tester's Test Plan Title: Venak Security Zero-Day AV/EDR Test

January 2026

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.

AMTSO Test ID: AMTSO-LS1-TP182

1. Introduction

This Test Plan outlines Venak Security Test Lab's January 2026 Zero-Day Evaluation of AV and Endpoint Detection and Response (EDR) and solutions.

The objective is to evaluate the detection, prevention, and response capabilities of selected AV/EDR products against curated zero-day threats. The testing methodology is structured to be repeatable, transparent, and compliant with AMTSO Testing Protocol Standards.

2. Scope

This test will focus on Zero-Day Malware and Exploit Detection in AV/EDR solutions.

Products Under Test (AV/EDRs):
- Sophos Endpoint Detection and Response (EDR)
- CrowdStrike Falcon EDR
- Huntress Managed EDR
- Sentinel One's Singularity EDR
- McAfee Antivirus
- ESET Smart Security Premium
- Watchdog Anti-Malware
- G Data Internet Security
- Avast Premium Security
- Malwarebytes Premium Security
- Quick Heal Internet Security

Versioning Policy: Latest publicly available version as of February 7, 2026 (test start date).

Threat Type: Zero-day malware, exploits, and attack vectors not seen in prior vendor signature databases.

3. Methodology and Strategy

Overview:
The zero-day malware samples utilized in this evaluation are predominantly generated using Venak Security's proprietary **AI Malware Simulator technology**. This cutting-edge system employs advanced artificial intelligence and machine learning techniques to autonomously create novel, polymorphic malware strains that simulate realistic attack behaviors seen in the wild.

Unlike traditional sample collections relying solely on captured threats, the AI Malware Simulator actively generates previously unseen malware variants by learning from known attack patterns and extrapolating new malicious code that evades current detection mechanisms. This approach enables the creation of **highly sophisticated zero-day threats** that are specifically designed to challenge Endpoint Detection and Response (EDR) solutions under realistic, continuously evolving threat landscapes.

The AI-generated samples mimic real-world delivery vectors such as phishing payloads, drive-by downloads, dropper-based infections, and lateral movement techniques. By leveraging AI, the simulator provides an ongoing pipeline of fresh, evasive threats which enhances the rigor and relevance of the test.

Sample Sourcing:

- Zero-day malware created using Venak Security's **AI Malware Simulator technology**, generating new and polymorphic threats designed to evade existing detection
- All samples are validated as genuine "zero-day" through VirusTotal (VT) timestamp comparison and internal forensic analysis

EDR Evaluation Criteria:

- **Blocking Effectiveness:** Ability to prevent execution or lateral propagation of AI-simulated and other zero-day malware
- **Detection Speed:** Rapid identification and alerting of novel malicious activities
- **Behavioral Response:** Quality and accuracy of automated or manual containment, quarantine, and remediation
- **Alert Reporting:** Completeness, clarity, and technical accuracy of security event logs and forensic information

Updates:
AV/EDR products will be permitted to auto-update per vendor default settings during testing, to reflect real-world conditions.

Repeatability:

- Each test sample and execution step is fully logged and time-stamped for traceability
- Virtual machine snapshots and standardized configuration protocols ensure consistent and reproducible environments

4. Participation

Vendors: Listed in Section 2.

Opt-Out Policy:
Vendors may opt out by providing written notice by February 7, 2026. Written request to info@venaksecurity.com or Nima@venaksecurity.com ,We will list your request in our final list, noting that you requested to be removed voluntarily.

Notification:
All vendors notified on January 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)
- Virtual Machines (VMWare Workstation)
- 4 vCPU, 16GB RAM, 120GB SSD per instance

Sample Provenance: Using our own AI Malware Simulator.

Geographic Focus: Global, with no restrictions.

Curation Process: All samples validated as “zero-day” by timestamp comparison against vendor detection feeds.

6. Schedule

Public Notification Date: January 12, 2026
Test Start Date: February 7, 2026

Milestone	Date
AMTSO Notification Published	January 12, 2026
Vendor Opt-Out Deadline	February 7, 2026
Vendor Config Confirmation Period	February 7–13, 2026
Test Period	February 7–18, 2026
Preliminary Results Shared	February 21, 2026
Draft Report Delivery	February 24, 2026
Dispute Window	February 24– March 3, 2026
Final Report Published	March 7, 2026

7. Control Procedures

- Cloud access verified before test start
- Logs/Videos collected automatically
- Default vendor updates settings maintained
- Each test VM independently reset between runs

8. Dependencies

- Vendors confirm installation defaults and connectivity
- Configuration monitoring and validation: February 7–13, 2026

9. Scoring Process

Each AV/EDR will be scored across:
1. Prevention Rate (%) – successful blocking of zero-day threats.
2. Detection Latency (seconds) – time to flag/block suspicious activity.
3. Reporting Accuracy – correctness and clarity of alerts.

Scores will be aggregated into a Final Protection Index (FPI).

10. Dispute Process

Window: February 24–March 3, 2026

- Written disputes must include technical evidence
- Evidence tiers:
    - Basic (hashes, logs)
    - Advanced (PCAPs, behavior traces)

11. Attestations

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

1. Public test notification is posted to AMTSO website
2. All vendors are treated equally
3. Any test design imbalances will be disclosed
4. No vendor paid to participate
5. No conflicts of interest exist
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: January 2, 2026
AMTSO Test ID: AMTSO-LS1-TP182