MRG Effitas 360° Consumer Assessment and Certification

Test plan – 05/2026

Sponsored and Authored by
MRG Effitas Ltd. (Lorand Lajsz)

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 [2.3]. Effitas Ltd. is solely responsible for the content of this Test Plan

Table of Contents

MRG Effitas 360° Consumer Assessment and Certification
Test Plan – 05/2026

1. Introduction

The MRG Effitas 360° Consumer Assessment and Certification is a first-of-its-kind testing programme designed to evaluate the real-world security posture of consumer endpoint protection products. Unlike traditional tests that focus on a narrow slice of threats or rely solely on static detection metrics, the 360° Assessment measures protection against the full spectrum of early-life malware circulating in the wild.

Today's threat landscape evolves rapidly, and consumer users are often the most vulnerable. This programme emphasizes real-time, in-the-wild (ITW) testing, which provides timely insights into product performance and reflects how effectively users are protected at the moment of exposure. Vendors receive immediate access to test telemetry, enabling transparent, proactive remediation if issues are discovered during the cycle.

The “360°” name reflects the breadth of threats included: trojans, backdoors, ransomware, banking malware, malicious scripts, Office documents, phishing attacks, and other prevalent consumer-focused malware families.

2. Scope

The purpose of this certification programme is to measure and publicly reflect the efficacy of consumer security products based on “metrics that matter” to real users.

While preventing initial infection is essential, real-world user behavior must also be considered. Users often make mistakes, ignore warnings, or interact with malicious content unintentionally. Therefore, our evaluation looks not only at binary detection but also at:

- clarity and usability of alerts
- blocking capability at all stages of execution
- phishing protection
- false positive reliability

A product passes only when it clearly communicates threat severity and blocks malicious activity without requiring sophisticated decision-making from the user.

The proposed list of consumer products for the MRG Effitas 360° Consumer Assessment and Certification 01/2026 includes:

- Avast Premium Security
- Bitdefender Total Security
- ESET Internet Security
- Gdata Internet Security
- Malwarebytes Premium Security
- McAfee Total Protection
- Microsoft Defender
- Norton 360 AntiVirus Plus
- Sophos Home Premium

The final list of participants will be defined after the Public Test Notification is issued.

3. Methodology and Strategy

Since 2009, MRG Effitas has focused on efficacy assessments, not merely detection testing. Our methodology aligns with AMTSO guidelines for Real World Testing while incorporating MRG's own continuous ITW testing standards and immediate transparency model. Real World testing introduces threats as they appear in a genuine consumer environment: through browsers, email clients, downloaded documents, malicious URLs, and other user-facing vectors. We execute malware on endpoints to assess blocking, behavioural protection, and system remediation. We also simulate everyday user behavior, including opening attachments, visiting phishing pages, or running downloaded files.

In-The-Wild malware test methodology

1. **Environment Preparation**
   - Windows 11 Pro 64-bit installed on a hardened virtual machine
   - A clean base image is created

- Clones are prepared for each product under test

2. **Installing Security Applications**
   - Consumer products are installed with default settings
   - All components updated
   - PUA/PUP detection enabled where available
   - Vendor-recommended non-default settings may be applied if realistic, and documented
3. **Sample Collection & Validation**
   - Malware samples are collected from live ITW sources
   - Each sample is validated on a clean system to confirm that it executes correctly
   - Samples are replayed identically across all product installations via replay proxy
   - Samples are downloaded via Google Chrome into the user's Downloads folder
4. **Execution Process**
   - Samples are launched by double-clicking, consistent with normal user behavior

Outcome Categories

- **Blocked**
  Threat blocked at URL or download stage
- **Behaviour Blocked**
  Threat detected and stopped upon execution (automatic or via clear user warning)
- **Detected**
  Threat raised an alert, but execution was allowed to proceed
- **Missed**
  Product failed to block or behavior-block the malware

5. **Tests are conducted with all systems having internet access.**
6. **As no user-initiated scans are involved in this test, applications rely entirely on their built-in technologies to detect, block, and remediate threats. These include:**

- URL blacklisting
- Reputation services
- Signature-based detection
- Heuristics
- Behaviour monitoring
- Other proprietary protection mechanisms

False positive test methodology

1. **Environment Preparation**
   - Windows 11 Pro 64-bit installed on a hardened virtual machine
   - A clean base image is created
   - Clones are prepared for each product under test
2. **Installing Security Applications**
   - Consumer products are installed with default settings
   - All components updated
   - PUA/PUP detection enabled where available
   - Vendor-recommended non-default settings may be applied if realistic, and documented
3. **Sample Collection & Validation**
   - Clean / False positive samples are collected from live ITW sources
   - Each sample is validated on a clean system to confirm that it executes correctly
   - Samples are replayed identically across all product installations via replay proxy
   - Samples are downloaded via Chrome into the user's Downloads folder
4. **Execution Process**
   - Samples are launched by double-clicking, consistent with normal user behavior

Outcome Categories

- **False Positive**

Sample is falsely identified as malicious and blocked at any stage of the test

- **Detected**
  Sample is falsely identified as malicious at any stage of the test, but execution is not blocked
- **Allowed to run**
  Sample is correctly identified as harmless and allowed to run

5. **Tests are conducted with all systems having internet access.**
6. **As no user-initiated scans are involved in this test, applications rely entirely on their built-in technologies to detect, block, and remediate threats. These include:**
   - URL blacklisting
   - Reputation services
   - Signature-based detection
   - Heuristics
   - Behaviour monitoring
   - Other proprietary protection mechanisms

In-The-Wild phishing test methodology

1. **Environment Preparation**
   - Windows 11 Pro 64-bit installed on a hardened virtual machine
   - A clean base image is created
   - Clones are prepared for each product under test
2. **Installing Security Applications**
   - Consumer products are installed with default settings
   - All components updated
   - PUA/PUP detection enabled where available
   - Vendor-recommended non-default settings may be applied if realistic, and documented

3. **Sample Collection & Validation**
   - Phishing samples are collected from live ITW sources
   - Each sample is validated on a clean system to confirm that it executes correctly
   - Samples are replayed identically across all product installations via replay proxy
4. **Execution Process**
   - Samples are executed in the application's dedicated secure browser when available; otherwise, they are opened in Google Chrome with all built-in anti-phishing features disabled. This ensures that the test measures the phishing-blocking capabilities of the security product itself, without assistance from external protections.

Outcome Categories

- **Blocked**
  Phishing site is identified as malicious and blocked from loading
- **Detected**
  Phishing site is identified as malicious, there is a warning, but it is allowed to load awaiting user input
- **Missed**
  Phishing site is not identified as malicious and allowed to load without any warning awaiting user input

5. **Tests are conducted with all systems having internet access.**
6. **As no user-initiated scans are involved in this test, applications rely entirely on their built-in technologies to detect, block, and remediate threats. These include:**
   - URL blacklisting
   - Reputation services
   - Signature-based detection
   - Heuristics
   - Behaviour monitoring
   - Other proprietary protection mechanisms

4. Participation

Participation follows AMTSO Public Test Requirements

- Vendors may participate voluntarily without additional cost
- Vendors may subscribe for enhanced access, including detailed logs, telemetry, and disputed sample data
- Opt-out is permitted only if the vendor demonstrates proven misconfiguration or connectivity failure

5. Environment

Hardened virtual machine configuration

- OS: Windows 10 x64
- CPU: 4 core Intel CPU
- Memory: 8GB
- Storage: 100GB SSD
- Networking: Intel Gigabit Network Connection

Sample Relevance

Most malware is sourced from compromised legitimate websites and consumer infection chains. Remaining samples come from MRG Effitas honeypots.

Some malware is VM-aware; our hardened testing environment supports execution of advanced threats.

Geographic Limitations

There are no geographic limitations in terms of samples.

Curation Process

Voluntary Participants are given equal opportunity to take part in the curation process for all of their respective Test Subjects.

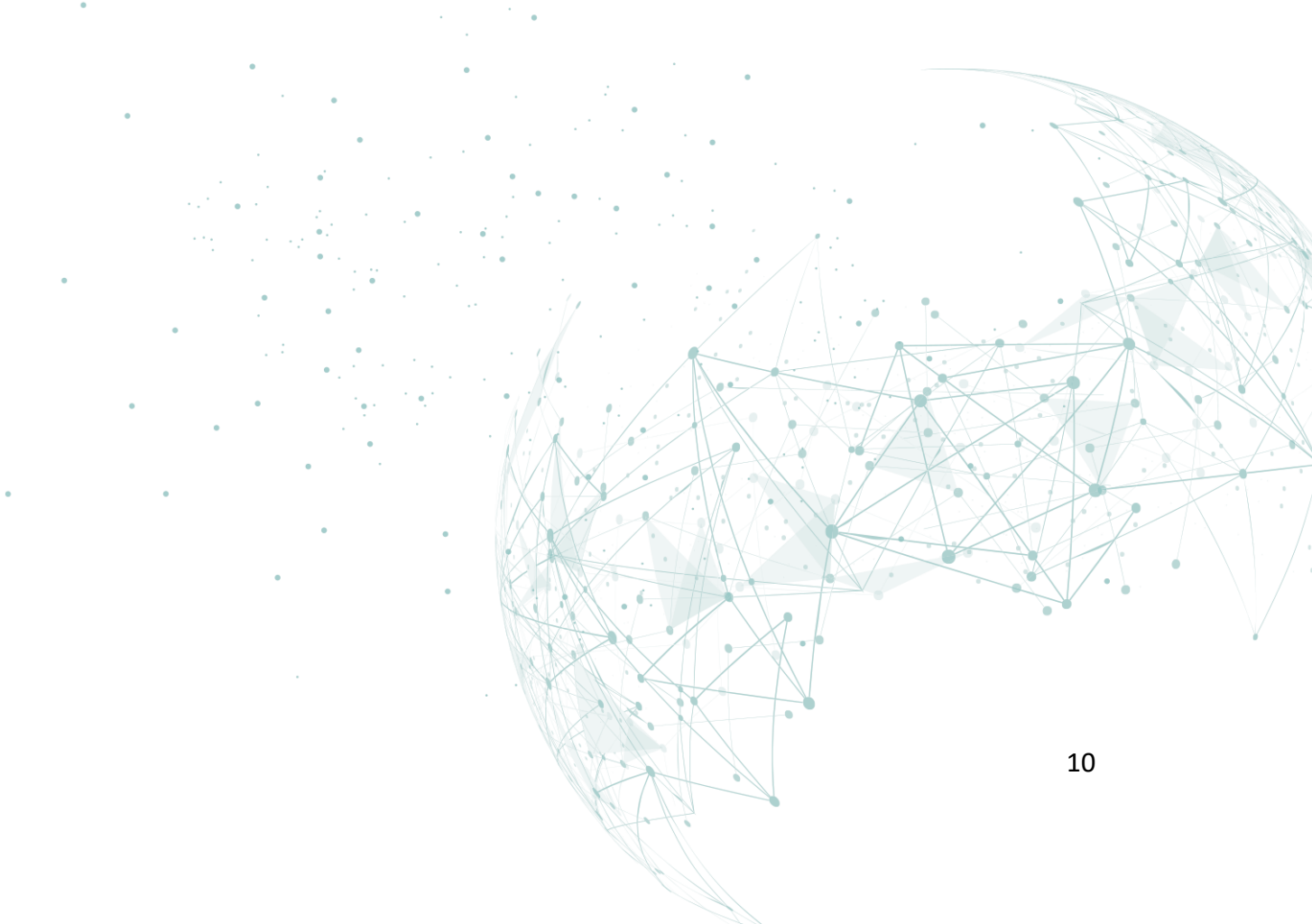
The malware used in this assessment can be considered true zero-day in nature. Based on the broad spectrum of threats included and our long-term experience, ransomware remains the most significant risk to consumer users. Applications that fail to protect the system

from file-encrypting ransomware or wipers cannot be certified, as successful execution typically results in irreversible data loss and no possibility of remediation.

Our hardened virtual testing environment is designed to support the execution of VM-aware malware. This enables us to include more sophisticated threats that would not normally run in standard virtual machine environments.

Distribution of Test Data

All failed samples are provided to subscribed participants together with the corresponding detailed test logs.



6. Schedule

MRG Effitas 360° Consumer Assessment and Certification – 01/2026 Schedule Milestones

Index	Test Activity	Date / Date Range	Dependencies
1	Test Commencement	May 01, 2026	None
2	Test Start Date	May 04, 2026	Completion of Activity 1
3	Test End Date	May 22, 2026	Completion of Activity 2
4	Feedback and Dispute Resolution Window	May 25. – June 01. 2026	Completion of Activity 3
5	Final Report Publication	June 05, 2026	Completion of Activity 4
—	**Testing Period**	**~3 weeks**	**Activities 1–3**
—	**Total Assessment Duration**	**~4 weeks**	**Activities 1–5**

Communications

If there are any significant deviations from this schedule (greater than 10 working days), MRG Effitas will notify all affected vendors within three business days.

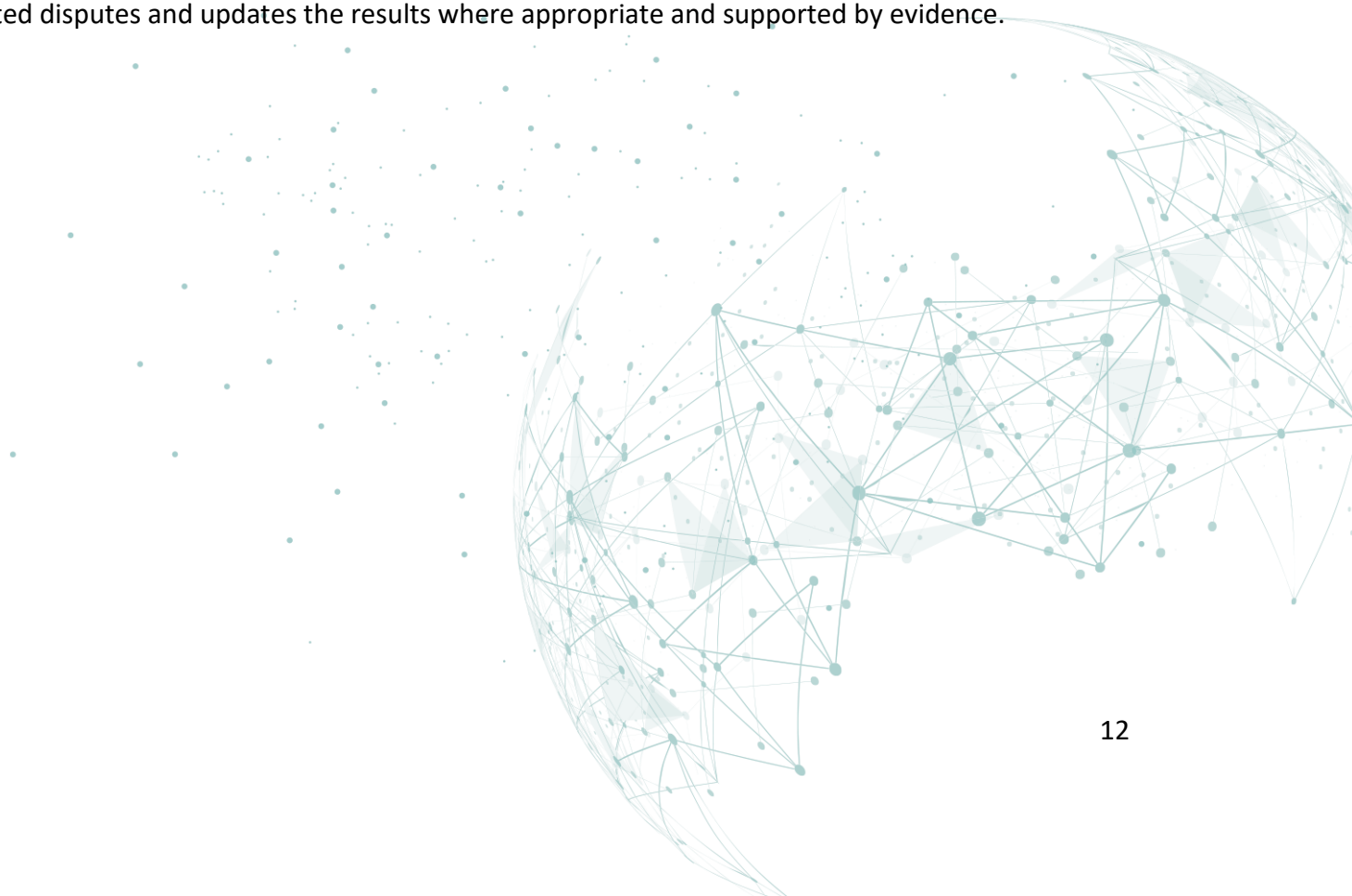
7. Scoring Process

- To achieve an MRG Effitas 360° **Level 1 Certification**, a security application **must fully protect the system from all initial in-the-wild (ITW) infections**, without any compromise to system integrity or user data, **must not provide any false alert in FP test** and **must block at least 79% of the ITW phishing** cases.
- A **Level 2 Certification** is awarded when the application **blocks** (either automatically or through behaviour-based protection) **at least 98% of all ITW malware** test cases, **must not provide more than 2% false alert in FP test** and **must block at least 79% of the ITW phishing** cases.

- If an ITW ransomware or wiper sample executes successfully and results in permanent loss of user files or irreversible system damage, the product cannot be certified, regardless of its overall block rate.

8. Dispute Process

- Subscribed participants receive near-immediate (typically within 24 hours) notification of test outcomes, along with instant access to sample files, logs, and telemetry data.
- Non-subscribed vendors receive their results and associated logs during the designated dispute phase defined in the test schedule.
- Vendors wishing to dispute a result must provide supporting evidence, such as portal logs, detection events, or relevant timestamps, to demonstrate that the dispute is justified.
- MRG Effitas reviews all submitted disputes and updates the results where appropriate and supported by evidence.



9. Attestations

By submitting this Test Plan, MRG Effitas attests:

- The public test notification will be posted on the AMTSO website
- All products will be analysed fairly and equally
- Any known imbalance or design limitation will be disclosed
- No additional fees will be charged for inclusion as a Test Subject
- Any conflict of interest will be disclosed
- Funding sources for the test will be transparently disclosed

MRG Effitas Ltd. affirms that this Test Plan complies with AMTSO Testing Standards version [1.3].

Signature: /s/ Lorand Lajsz

Name: Lorand Lajsz

Test Lab: MRG Effitas

AMTSO Test ID: [AMTSO-LS1-TP200]