Keywords: anti-malware; compliance; assessment; testing; test plan; MRG Effitas; 360° Assessment

August 21, 2026
AMTSO Distribution: August 21, 2026

Version 1.1

MRG Effitas Test Plan for Q3 2026 360° Assessment and Certification

Sponsored and Authored by:
MRG Effitas (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.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

Table of Contents

1. Introduction 3
2. Scope 3
3. Methodology and Strategy 4
   - In-The-Wild malware test methodology 5
   - In-The-Wild PUA/Adware test methodology 5
   - False positive test methodology 6
   - Exploit / Fileless test methodology 7
   - Real botnet test methodology 8
   - Financial malware simulator test methodology 9
   - Ransomware simulator test methodology 10
   - In-The-Wild phishing test methodology 11
   - Phishing simulator test methodology 12
   - Performance & footprint test methodology 12
4. Participation 14
5. Environment 15
6. Schedule 16
7. Control Procedures 16
8. Dependencies 17
9. Scoring Process 17
10. Dispute Process 17
11. Attestations 17

©MRG Effitas Ltd, 2011-2026. All rights reserved.

MRG Effitas 360° Assessment and Certification Test Plan

Q3 2026

1. Introduction

A first-of-its-kind test that covers all angles, our pioneering 360° Protection Test targets the key threats faced by internet users. In each test case we employ the full spectrum of Early Life Malware.

MRG Effitas has a core focus on efficacy assessments in all variety of anti-malware evaluation with “Real World” detection testing. In today's fast-paced digital landscape, where threats evolve rapidly, it is crucial for organizations to adopt robust security measures. Real-time ITW testing offers the advantage of immediate feedback allowing our participants to update and correct their systems proactively.

This evaluation aims to determine the effectiveness of providing immediate information to users, allowing them to promptly respond and rectify any issues encountered within their system.

This Programme is called a “360° Assessment” since it deals with the full spectrum of malware instead of just one specific type. In the 360° Assessments, trojans, backdoors, ransomware, financial malware, scripts, Office documents and “other” malware are used.

2. Scope

This Certification Programme is designed to serve as a reflection of product efficacy based on what we have previously termed “metrics that matter”. Being one of the world’s largest supplier of early-life malicious binaries and malicious URLs, and from our own simulator developments, we know that all endpoints can be infected, regardless of the security solutions employed.

For us, a product’s ability to block initial infection (although critical in most cases) is not the only metric that matters. When conducting these tests, we try to simulate normal user behaviour. We are aware that a “Real World” test cannot be conducted by a team of professionals inside a lab because we understand how certain types of malware work, how malware attacks and how such attacks could be prevented. Simulating normal user behaviour means that we pay special attention to all alerts given by security applications.

A pass is given only when alerts are straightforward and clearly suggested that malicious action should be blocked. Meanwhile when a threat is detected but not blocked, is counted as detected. With these, it is very important to note that the best choice for an average user is to keep things very simple and for the product not to present many pop-up alerts or questions. We test a group of internet security suites and complementary security applications.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

In our next execution of this test, eight test subjects are to be included. Companies are represented by their products as follows.

- Avast Business Antivirus
- Avira Antivirus Pro - Business edition
- Bitdefender Gravityzone Advanced Business Security
- ESET Endpoint Security
- ThreatDown Endpoint Protection
- Microsoft Defender Antivirus Enterprise
- Symantec Endpoint Protection

Final Test Subject Vendors and Participants will be determined after the Public Test Notification has been issued.

3. Methodology and Strategy

Since its inception in 2009, MRG Effitas has strived to differentiate itself from traditional testing houses by having its primary focus on providing “efficacy assessments” and not just performing “tests”. Traditionally, testing of security software has centred on measuring a product’s ability to detect malware.

Testing has evolved rapidly over the last few years as most labs, under the guidance of AMTSO (of which MRG Effitas is a member) strived to conduct “Real World” testing. Although there is no absolute definition of this kind of testing, loosely speaking, it involves the introduction of malware to an endpoint through a realistic vector, such as a browser, mail server or USB memory stick. Real World testing mostly involves “dynamic testing” (i.e. the malware is executed and then the ability of the security product to block the malware is measured). Several testing labs also conduct “System Rescue” tests, which assess a security product’s ability to remediate a pre-infected endpoint.

Whilst both types of tests are useful and yield valid and meaningful data, MRG Effitas wanted to merge these tests and go one step further by providing all test information to our users immediately. Measuring initial detection rates is important, particularly in today’s threat landscape with the mix of malware that is prevalent. Continuous ITW testing and instant access to the logs, screenshots, samples and intel data after the test is the next step to support our users rapid response capabilities.

In providing quarterly certifications, the MRG Effitas 360° Assessment & Certification Programme is the de facto standard by which security vendors, financial institutions and other corporations can attain the most rigorous and accurate determination of a product’s efficacy against the full spectrum of malware that is prevalent during the period.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

In-The-Wild malware test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. Test samples (binary or document, email, script, etc.) are downloaded from its URL using Google Chrome to the Downloads folder and then executed in a clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test systems created in (4).

Live binary, document and script testing is conducted by the following procedure.

5.1. The sample is selected for the test and tested in the systems where a security product is installed (4).

Malicious e-mail attachment test is conducted by the following procedure.

5.2 Microsoft Office Outlook client downloading a single email from its server to the victim system created in (4).

5.3 Opening the e-mail, saving the attachment to the Downloads folder, and then executing the binary.

- **The test case is marked as "Blocked"** by either the security application blocks the URL where the malicious binary was located. Or the security application blocks the malicious binary whilst it was being downloaded to the desktop.
- **The test case is marked as "Behaviour Blocked"** if the security application blocks the malicious binary when it is executed and either automatically blocks it or postpones its execution and warns the user that the file is malicious and awaiting user input.
- **The test case is marked as "Detected"** if the security application detects the threat and sends an alert to the central console or notifies the user, but the sample is allowed to run.
- **The test case is marked as "Missed"** if the security application fails to block or behaviour block the malicious sample.

6. Tests are conducted with all systems having internet access.
7. As no user-initiated scans are involved in this test, applications rely on their own built-in technologies to detect, block and remediate threats. Some of these technologies are URL blacklisting, reputation, signature checking, heuristics, behaviour scanning, machine learning, etc.

In-The-Wild PUA/Adware test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. Test samples (binary or document, email, script, etc.) are downloaded from its URL using Google Chrome to the Downloads folder and then executed in a clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test systems created in (4).

- **The test case is marked as "Blocked"** by either the security application blocks the URL where the malicious binary was located. Or the security application blocks the malicious binary whilst it was being downloaded to the desktop.
- **The test case is marked as "Behaviour Blocked"** if the security application blocks the malicious binary when it is executed and either automatically blocks it or postpones its execution and warns the user that the file is malicious and awaiting user input.
- **The test case is marked as "Detected"** if the security application detects the threat and sends an alert to the central console or notifies the user, but the sample is allowed to run.
- **The test case is marked as "Missed"** if the security application fails to block or behaviour block the malicious sample.

6. Tests are conducted with all systems having internet access.
7. As no user-initiated scans are involved in this test, applications rely on their own built-in technologies to detect, block, and remediate threats. Some of these technologies are URL blacklisting, reputation, signature checking, heuristics, behaviour scanning, machine learning, etc.

False positive test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. Test samples (binary or document, email, script, etc.) are downloaded from its URL using Google Chrome to the Downloads folder and then executed in a clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test systems created in (4).

- **The test case is marked as "False Positive"** if the security application falsely identifies and blocks the binary at any stage during the test.
- **The test case is marked as "Detected"** if the security application falsely identifies and the

©MRG Effitas Ltd, 2011-2026. All rights reserved.

binary at any stage during the test and retest but allows it to run.

- **The test case is marked as "Allowed to run"** if the security application correctly identifies the binary as harmless and allows it to run.

6. Tests are conducted with all systems having internet access.

Exploit / Fileless test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.

Exploit / Fileless test is conducted by the following procedure.

1. The payloads use an exploit for the one of an installed vulnerable application. In order to simulate a realistic attack scenario, the payload is constructed to include at least one of the common CnC frameworks.
2. The opening stage of the exploit is introduced to the system and we monitor if the vulnerable application starts the initial stage payload, for a session to be established to our CnC server.
3. After navigating to the exploit site, the system is supervised if there are any new processes, loaded DLLs or CnC traffic. If the exploitation is successful, the following actions are executed.
   3.1. Upload a file to the victim.
   3.2. Download a file from the victim.
   3.3. Create a process remotely.
   3.4. Read the contents of a file on the victim.
4. When user interaction is needed from the endpoint protection (e.g. site visit not recommended, etc.) the default action is chosen. When user interaction is needed from the operating system, we chose the run/allow options.
5. Throughout the test, the Process Monitor from the Sysinternals Suite and Wireshark are running (both installed to non-default directories and modified not to be detected by default anti-debugging tools).

- **The test case is marked as "Signature Block"** if the security application blocks the URL (infected URL, exploit kit URL, redirection URL, malware URL) by its URL database.
- **The test case is marked as "Blocked"** if the security application blocks the page containing malicious HTML code, JavaScript (redirects, iframes, obfuscated JavaScript, etc.). Or if the security application blocks the downloaded payload by analysing the malware before it can be started. (reputation-based block or heuristic based block).

©MRG Effitas Ltd, 2011-2026. All rights reserved.

- **The test case is marked as "Behaviour Blocked"** if the security application blocks the downloaded payload after it has been started.
- **The test case is marked as "Detected"** if the security application detects the threat and sends an alert to the central console or notifies the user, but the attack is allowed to run.
- **The test case is marked as "Missed"** if the security application fails to detect, block or behaviour block the attack and it can be carried out.

6. Tests are conducted with all systems having internet access.
7. As no user-initiated scans are involved in this test, applications rely on their own built-in technologies to detect, block, and remediate threats. Some of these technologies are URL blacklisting, reputation, signature checking, heuristics, behaviour scanning, machine learning, etc.

Real botnet test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A Real botnet dropper is run on the clean, unprotected system, thus simulating a pre-infected state.
4. A clone of the imaged system (3) is made for each of the security applications to be used in the test.
5. An individual security application is installed using default settings on each of the systems created in (4). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
6. A clone of the system as at the end of (5) is created.

Real botnet test is conducted by the following procedure.

6.1. Starting a new instance of Firefox or Google Chrome (or the Safe Browser) and navigating to a financial website. Where the security application offers a secured or dedicated banking browser, this is used.

6.2. Text is entered into the Account login page of the financial website using the keyboard or using a virtual keyboard if the application under test provides such functionality, and then the "log in" button is pressed.

- **The test case is marked as passed – a green checkmark** if the security application detects the financial malware when the security application is installed, and a mandatory scan is made. Or the security application detects the real financial malware when it is executed according to the following criteria:
  - It identifies the real financial malware as being malicious and either automatically blocks it or postpones its execution, warns the user that the file is malicious and awaits user input.
  - It identifies the real financial malware as suspicious or unknown and gives the option to run in a sandbox or safe restricted mode, which prevents the real financial malware from

©MRG Effitas Ltd, 2011-2026. All rights reserved.

capturing and sending the logon data to the MRG CnC, whilst giving no alerts or giving informational alerts only. Or The security application intercepts the action of the real financial malware and displays warnings and user action input requests that are clearly different from those displayed in response to legitimate applications.

- **The test case is marked as missed – a orange cross** if the security application fails to detect the real financial malware according to the following criteria:
    - The security application fails to prevent the real financial malware from capturing and sending the logon data to the MRG CnC and gives no alert or provides informational alerts only.
    - The security application intercepts the action of the real financial malware but displays warnings and user action input requests that are indistinguishable in meaning from those displayed in response to legitimate applications.
    - The security application identifies the malware and gives the option to run in a sandbox or safe restricted mode which fails to prevent the real financial malware from capturing and sending the logon data to the MRG CnC and gives no alert or provides informational alerts only.

7. Testing is conducted with all systems having internet access.

Financial malware simulator test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.

Financial malware simulator test is conducted by the following procedure.

6. Where the security application offers a secured or dedicated banking browser, this is used.

    6.1. The simulator specific process is started.

    - **The test case is marked as passed – a green checkmark** if the security application identifies the simulator as being malicious and either automatically blocks it or postpones its execution, warns the user that the file is malicious and awaits user input. Or, it identifies the simulator as suspicious or unknown and gives the option to run in a sandbox or safe restricted mode which does not allow the hooking/redirection, or even with successful hooking, the personal data cannot be captured from the browser.
    - **The test case is marked as missed – a orange cross** if the security application fails to identify the simulator based on the following criteria:
        - The security application allows the hooking/redirection of the event, and the personal data can be captured from the browser. Or, it fails to prevent the simulator

©MRG Effitas Ltd, 2011-2026. All rights reserved.

from injecting itself into the browser process and gives no alert or provides informational alerts only.

- The security application identifies the simulator as malware or unknown and gives the option to run in a sandbox or safe restricted mode which fails to prevent the simulator from injecting itself into the browser process and gives no alert or provides informational alerts only. Or, the security application allows the hooking/redirection of the event, and the personal data can be captured from the browser.

7. Testing is conducted with all systems having internet access.

Ransomware simulator test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.
6. Downloading a single binary executable (or document, script, etc.) using Chrome to the Downloads folder and then executing the test sample in the clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same sample throughout the test.
7. The sample is selected for the test and introduced to the system where a security product is installed.

- **The test case is marked as "Blocked"** by either the security application blocks the URL where the malicious sample is located. Or the security application blocks the malicious data whilst it was being downloaded to the desktop.
- **The test case is marked as "Behaviour Blocked"** if the security application blocks the malicious sample when it is executed and either automatically blocks it or postpones its execution and warns the user that the file is malicious and awaiting user input.
- **The test case is marked as "Detected"** if the security application detects the threat and sends an alert to the central console or notifies the user, but the sample is allowed to run.
- **The test case is marked as "Missed"** if the security application fails to block or behaviour block the malicious sample during the test.

8. Tests are conducted with all systems having internet access.
9. As no user-initiated scans are involved in this test, applications rely on their own built-in technologies to detect, block, and remediate threats. Some of these technologies are URL blacklisting, reputation, signature checking, heuristics, behaviour scanning, machine learning, etc.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

Ransomware simulator false positive test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. A clone of the system as at the end of (4) is created.
6. Introducing the binary executables (or documents, scripts, etc.) to the clean, unprotected system via disk image or network share. If the sample works, the sample is saved to a different disk image or network share.

Ransomware simulator false positive test is conducted by the following procedure.

6.1. Scanning the binary executables (or documents, scripts, etc.) on the disk image or on the network share.

6.2. Executing the test samples.

- **The test case is marked as "False Positive"** if the security application falsely identifies and blocks the binary at any stage during the test.
- **The test case is marked as "Detected"** if the security application falsely identifies and the binary at any stage during the test and retest but allows it to run.
- **The test case is marked as "Allowed to run"** if the security application correctly identifies the binary as harmless and allows it to run.

7. Testing is conducted with all systems having internet access.
8. As no user-initiated scans are involved in this test, applications rely on their own built-in technologies to detect, block, and remediate threats. Some of these technologies are URL blacklisting, reputation, signature checking, heuristics, behaviour scanning, machine learning, etc.

In-The-Wild phishing test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. Where the security application offers a secured or dedicated browser or plugin, this is used/installed. Otherwise, Google Chrome is used and all anti-phishing features in the

©MRG Effitas Ltd, 2011-2026. All rights reserved.

browser are deactivated. If the browser can't support the anti-phishing deactivation and the user has the option to open the URL, we will click on that option. The scope of the test is to measure the security product detection capabilities.

6. In-The-Wild URL, which presents a phishing site with credential capturing capabilities is opened in the browser.
    - **The test case is marked as "Blocked"** by either the security application blocks the URL or warn the user that the URL is malicious and awaits user input.
    - **The test case is marked as "Missed"** if the security application fails to block the URL and fails to warn the user that the URL is malicious and awaits user input.

Phishing simulator test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a hardened virtual machine.
2. An image of the operating system is created.
3. A clone of the imaged systems is made for each of the security applications used in the test.
4. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
5. Where the security application offers a secured or dedicated browser or plugin, this is used/installed. Otherwise, Google Chrome is used and all anti-phishing features in the browser are deactivated. If the browser can't support the anti-phishing deactivation and the user has the option to open the URL, we will click on that option. The scope of the test is to measure the security product detection capabilities.
6. Specially crafted URL, which presents a phishing site with credential capturing capabilities is opened in the browser.
7. Sensitive data is entered into the fields (login identifiers, credentials, bank details, etc.)
    - **The test case is marked as "Blocked"** by either the security application blocks the URL or prevents the submission of the affected data.
    - **The test case is marked as "Missed"** if the security application fails to block the URL and fails to prevent the phishing site to receive the sensitive data.

Performance & footprint test methodology

1. Windows 11 Enterprise 64-bit operating system is installed on a physical machine.
2. A backup image of the operating system is created.
3. An individual security application is installed using default settings on each of the systems created in (3). Updated and where applicable, PUA settings enabled. If the vendor provided a non-default setting, this setting is checked whether it is realistic. If yes, the changes are documented, applied, and added to the appendix section of the report.
4. **The following performance metrics are measured.**

©MRG Effitas Ltd, 2011-2026. All rights reserved.

- Operating system boot time
- Size of the files installed and created by the security application. (The size is measured at least one week after the installation, after virus definition updates, scans, simulating normal computer usage.)
- Copy time of files
- Archive operation time
- Opening time for (clean) files in Office applications
- Downloading files through browser
- Website loading time in browser. The browser should fully load a popular, complex website, from a local network URL or replay proxy to eliminate network latency.
- AV product update time – informational
- AV product update CPU usage (%) – informational
- AV product update memory usage (Mb) – informational
- AV product update physical disk usage (%) – informational
- AV product update network interface usage (%) – informational
- System disk scan time – informational
- System disk scan CPU usage (%) – informational
- System disk scan memory usage (Mb) – informational
- System disk scan physical disk usage (%) – informational
- System disk scan physical disk usage (%) – informational
- System disk scan network interface usage (%) – informational

Every performance result is a calculated average of at least three measurements.

Additionally, for informational purposes, footprint data is collected during IDLE system status.

- CPU usage (%)
  % Processor Time is the percentage of elapsed time that all of process threads used the processor to execution instructions. An instruction is the basic unit of execution in a computer, a thread is the object that executes instructions, and a process is the object created when a program is run. Code executed to handle some hardware interrupts and trap conditions are included in this count.

- Memory - Allocated bytes
  Private Bytes is the current size, in bytes, of memory that this process has allocated that cannot be shared with other processes.

- I/O Data Bytes/sec
  The rate at which the process is reading and writing bytes in I/O operations. This counter counts all I/O activity generated by the process to include file, network and device I/Os.

IDLE test results are displayed as an average of the system running for 1 hour.

5. Scoring

©MRG Effitas Ltd, 2011-2026. All rights reserved.

The security product reaching the best result in the category is rewarded with the highest achievable points, the second receives one point less, and so on. Once every performance category was measured, the points were summed up, and the final calculation was made by dividing the total points by the number of tests.

The following performance metrics are used to calculate "Performance test results".

- Operating system boot time
- Size of the files installed and created by the security application. (The size is measured at least one week after the installation, after virus definition updates, scans, simulating normal computer usage.)
- Copy time of files
- Archive operation time
- Opening time for (clean) files in Office applications
- Downloading files through browser
- Website loading time in browser. The browser should fully load a popular, complex website, from a local network URL or replay proxy to eliminate network latency.

AV product update time, System disk scan time and IDLE metrics are only informational.

4. Participation

AMTSO's goal with having Participants is that in exchange for cooperating (engaging with Testers and following disclosure requirements), Participants have additional rights to audit their configuration and provide commentary on Test results without additional costs. If a Tester charges to participate in a Public Test or any related services, and a Test Subject Vendor chooses to not pay the fee, that Vendor must be able to choose to be a Participant and follow this AMTSO standard.

Partial participation is allowed for the Vendors for these test sections:

- Expolit/fileless test,

- Online Banking test (Real botnet test, Financial malware simulator test, financial malware In-The-Wild test),

- Ransomware test (Ransomware In-The-Wild test, Ransomware simulator test, Ransomware false positive simulator test),

- Phishing tests (In-the-wild phishing test and/or Phishing simulator test).

Opt-Out Policy: Vendors can opt out if Vendor can prove that the test system or the Product was misconfigured in a way which greatly changes the test results. E.g. important modules were unnecessarily turned off compared to default configuration, or during the test the system could never reach the cloud.

Conflict of Interest Disclosure: There is no known conflict of interest.

Funding: Funding of this project is achieved by vendors subscribing to participate in this project, this gives them more in-depth information on how their product(s) performed and, if there are

©MRG Effitas Ltd, 2011-2026. All rights reserved.

any issues discovered in the product during testing, our technical team provides all the data necessary to help improve the product.

If the vendor wants to participate only in one or more partial test sections, they must subscribe to the selected section.

Part of the funding comes from subscribing vendors who can be use the report for marketing purposes.

Vendors often silently enter testing, sometimes with their newly developed product or a product in BETA or Pre-Release phase.

Finally, part of our funding comes from third parties, who commission us to include certain product into testing, both public and private.

5. Environment

Test hardware and configuration details as follows.

Hardened virtual machine specification:	OS: Windows 11 x64 CPU: 4 core Intel CPU Memory: 8GB Storage: 100GB SSD Networking: Intel Gigabit Network Connection
Physical machine specification:	OS: Windows 11 x64 CPU: Intel Core i5 Memory: 8GB Storage: 100GB SSD Networking: Intel Gigabit Network Connection

Sample Relevance: In the Wild 360 / Full Spectrum Test, majority of the malicious samples used in this test are from compromised, legitimate websites which served malware. We believe that such samples pose the greatest danger to users as they are often disguised as valid binaries (or documents, scripts or emails downloaded from usually used mail servers). The remaining of the samples come from our regular honeypots.

Geographic Limitations: There are no geographic limitations in terms of samples.

Curation Process: Voluntary Participants are given equal opportunities to participate in such Curation for all their respective Test Subjects.

Malware used in this test can be considered as Zero Day in the true meaning of that phrase. Based on the wide spectrum of malware used in this project and our previous experiences, we consider ransomware to be the greatest threats to the users.

Applications that didn't protect the system from file encrypting ransomware or wiper cannot be certified because they could not remediate the threat as files usually cannot be decrypted or restored.

Our hardened virtual testing environment supports the use of VM aware malware, this is the reason why we were able to use more sophisticated threats which wouldn't run on Virtual Machines.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

Distribution of Test Data: We send all failed samples to subscribed participants, along with detailed test logs.

6. Schedule

Start Date Range: The test commencement date is August 21, 2026.

Test Duration and Calculated End Date: The test is expected to require approximately nine weeks (without installation of products) and is forecast to conclude on October 23, 2026.

Milestones: Delivery milestones appear in the following chart.

MRG-Effitas 360° Enterprise Assessment and Certification Test Project Schedule Milestones

Index	Test Activity	Start Date Range	Dependencies
1	*Test Commencement*	*August 21, 2026*	
2	*Confirm Vendor Configuration Feedback*	*August 24, 2026*	
3	*Feedback and Dispute Resolution – Retests as Needed*	*October 26, 2026 - November 2 , 2026*	
4	*Issue Final Report – End Date for Test*	*November 6, 2026*	

Communications: Whenever there are significant deviations from this schedule (more than 5 workdays), we will notify all affected vendors within 3 business days.

Risks and Risk Management: We could not identify any risks with the test.

7. Control Procedures

Connectivity Validation: Tests are conducted with all systems having internet access. All security applications are fully functional registered versions Each vendor can supply a utility or another in-product feature to validate proper cloud-connectivity functionality.

Logging: In the first initial email to the vendors, we will ask if they require any special logging during the test. We expect these methods and tools to be working, otherwise we cannot guarantee the result of these logs.

Updates: Each individual security application will be installed using default settings on each of the test systems defined in the Environment section of this Test Plans and then, where applicable, updated.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

8. Dependencies

Participant Actions: As this test scope are consumer Test Subjects, we do not require any Vendor specific actions.

9. Scoring Process

In order to attain a quarterly MRG Effitas 360° Level 1 certification award, a security application must entirely protect the system from initial ITW infection (autoblock or behaviour protection) and a product must pass the Botnet test during the quarter.

Level 2 certification is given if the application blocks (autoblock or behaviour protection) any ITW malware in at least 98% of all cases.

If an ITW ransomware/wiper successfully runs and the files are not available anymore, certification is not available.

In order to attain a quarterly MRG Effitas 360° Exploit certification award, a security application must entirely protect the system from initial infection of every Exploit / Fileless test case (autoblock or signature block or detected or behaviour protection).

In order to attain a quarterly MRG Effitas 360° Online Banking certification award, a security application must entirely protect the system from In-the-wild financial malware initial infection (autoblock or behaviour protection) and the product must pass the Botnet and Financial malware simulator tests during the quarter.

In order to attain a quarterly MRG Effitas 360° Ransomware certification award, a security application must entirely protect the system from In-the-wild ransomware malware initial infection (autoblock or behaviour protection) and the product must pass the Ransomware simulator (autoblock or behaviour protection) and Ransomware false positive simulator tests during the quarter.

10. Dispute Process

The ITW test runs continuously. After the vendors receive the test results and the logs, Vendors can dispute individual test cases if they can prove that their disagreement is justified. The subscribed vendors receive detailed disputes with the categorization of the malware (type and family names) immediately after the test via email and they can download the samples. The other vendors can use their limited access for the dispute site during the date range defined in section 6, point 4: "*Feedback and Dispute Resolution Time for other tests".*

11. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to "I" or "me" or "we", similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

©MRG Effitas Ltd, 2011-2026. All rights reserved.

1. I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test.
2. All products included in this Test will be analysed fairly and equally.
3. I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test.
4. Although I may charge for participation in a Test although, I will not charge any additional fees for a vendor to be a test subject under the Standards.
5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test.
6. I will disclose how the Test was funded.

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards (v 1.3), as of the date hereof.

Signature: /s/ Lorand Lajsz

Name: Lorand Lajsz

Test Lab: MRG Effitas

AMTSO Test ID: [AMTSO-LS1-TP210]

©MRG Effitas Ltd, 2011-2026. All rights reserved.