Consumer Assessment & Certification
Powered by Tempus

Consumer Assessment & Certification Programme

09/2026

MRG Effitas

Copyright © 2026 MRG Effitas Ltd.

MRG Effitas

MRG Effitas Ltd.

MRG Effitas is a world-leading, independent IT security efficacy testing & assurance company. We are trusted by antimalware vendors across the world.

Management team:
Chris Pickard
Chief Executive Officer

Zsombor Kovacs
Chief Technical Officer

Website:
www.mrg-effitas.com

Email:
contact@mrg-effitas.com

Twitter:
@mrgeffitas

Contents

Introduction 3
Executive Summary 4
Tests Employed 5
- In-the-Wild Malware Test 5
- In-the-Wild Phishing Test 5
- False Positive Test 5

Test Results 7
- MRG Effitas Consumer Assessment Certification 09/2026 10
- Grading Criteria 11

Appendix 12

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

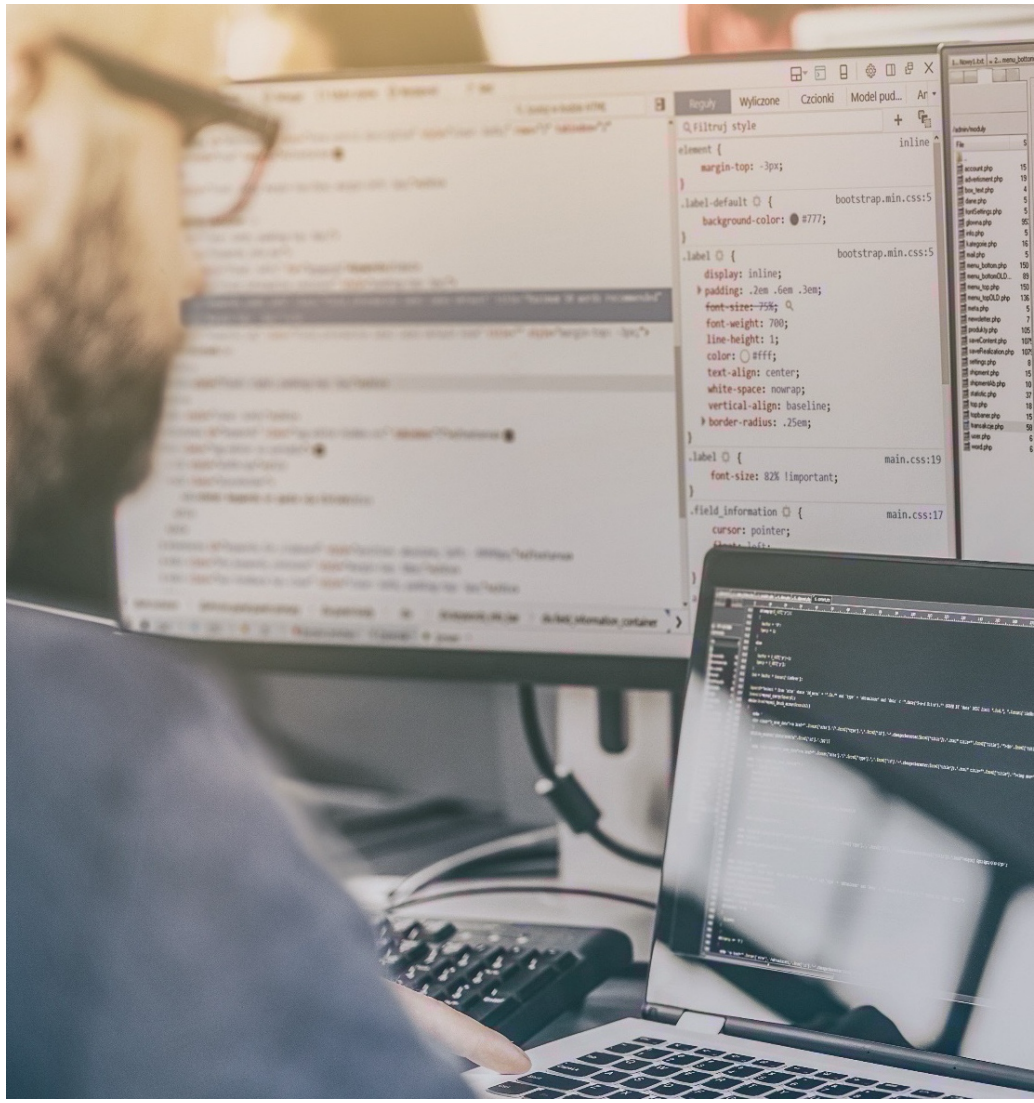
Introduction

Since its inception in 2009, MRG Effitas has specialised in evaluating how security products perform against real-world threats, with particular emphasis on malware and online fraud affecting everyday users.

This Consumer Assessment & Certification Programme is powered by the Tempus testing platform and is designed to closely reflect real-world usage scenarios on Windows systems. The methodology simulates the types of threats consumers are most likely to encounter, enabling an objective assessment of how effectively security products protect against modern attacks and supporting informed product selection.

Historically, security testing focused primarily on static malware detection rates. In recent years, however, methodologies have evolved significantly. Under the guidance of AMTSO, of which MRG Effitas is a member, testing organisations increasingly conduct Real-World testing based on transparent and standardised principles. Information regarding the AMTSO compliance status of this test is publicly available at:

https://www.amtso.org/amtso-ls1-tp213



Copyright © 2026 MRG Effitas Ltd.

While there is no single formal definition of Real-World testing, it generally involves introducing threats through realistic infection vectors, such as web downloads or removable media, and dynamically measuring a product's ability to prevent, block, or mitigate malicious activity during execution.

Building on this approach, MRG Effitas extends traditional Real-World testing by also evaluating time-to-detection and a product's ability to limit or prevent system damage.

To better reflect real-world user behaviour, no manual or on-demand scans are initiated during testing. Protection relies solely on each product's native, real-time capabilities.

Testing covers a full spectrum of in-the-wild threats, including trojans, backdoors, spyware, financial malware, ransomware, and other prevalent malicious applications. In addition to traditional ITW file-based attacks, the assessment also includes false-positive testing using clean files and phishing protection evaluation using live in-the-wild phishing URLs.

Modern malware is predominantly financially motivated. Whether through credential theft, fraud, ransomware, or data exfiltration, attackers benefit most when malicious activity remains undetected. As such, initial detection and response time are critical metrics, particularly for ransomware, where remediation after successful execution is often not possible.

Through this programme, MRG Effitas applies the same principles of accuracy, independence, and transparency that underpin its broader 360° Assessment & Certification initiatives, providing consumers and other stakeholders with a clear and reliable view of product effectiveness against the threats prevalent during the test period.

Executive Summary

This Certification Programme is designed to reflect real-world product efficacy based on what MRG Effitas refers to as "metrics that matter." Drawing on decades of IT security research, extensive historical testing, and access to large volumes of early-life malicious files and URLs, we recognise that no endpoint is immune to attack. In practice, the question is not if a system will encounter malware, but when.

While preventing initial infection remains critically important, it is not the only meaningful measure of protection. Equally important is how quickly malicious activity is detected and at what stage an infection or associated behaviour is identified. Delayed detection can significantly increase the impact of an attack, particularly for threats designed to steal data, commit fraud, or encrypt user files.

Testing is conducted to closely simulate normal user behaviour, recognising that expert-driven avoidance techniques do not reflect how most users interact with their systems. Particular attention is paid to how security products communicate risk to users. A test case is considered successfully protected only when alerts are clear, unambiguous, and actionable, guiding the user toward blocking the malicious activity.

During our 09/2026 Consumer Assessment, the following applications managed to attain our certification.

- Avast Premium Security
- Bitdefender Total Security
- ESET Internet Security
- Malwarebytes Premium Security
- Norton 360 AntiVirus Plus

Detailed results and certification criteria are presented in the sections that follow.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Tests Employed

In-the-Wild Malware Test

The majority of malicious URLs used in this test originated from compromised legitimate websites that were actively serving malware at the time of testing. We consider such URLs to pose a particularly high risk to users, as infections occur in environments where users least expect malicious activity. In these scenarios, traditional URL-based protection mechanisms may be less effective, as the domains themselves are often reputable.

Additional URLs were sourced from MRG Effitas honeypots and, in the case of ransomware and financial malware, from newly identified distribution infrastructures observed during the test period.

The malware delivered via these URLs was early-life and previously unseen by many security products at the time of testing, presenting a significant challenge for the participating solutions.

During the In-the-Wild (ITW) malware test, a total of 300 live samples were used. The sample set comprised 79 trojans, 47 backdoors, 14 financial malware samples, 36 ransomware samples, 64 spyware samples, 53 malicious scripts, 5 malicious documents, 2 other malicious samples.

In-the-Wild Phishing Test

To further extend the scope of the assessment, an In-the-Wild phishing test was conducted to evaluate the phishing protection capabilities of the security products, including secure browsers and browser extensions where provided.

During this test cycle, five live ITW phishing URLs were used. These URLs were actively hosting credential-harvesting phishing pages at the time of testing and were accessed using realistic user interaction scenarios.

False Positive Test

Effective malware protection must be balanced against the risk of false positives, which can disrupt legitimate user activity and, in enterprise environments, interfere with business operations. Overly aggressive detection mechanisms may successfully block malicious content but can also incorrectly flag legitimate applications, including newly developed or less widely distributed software.

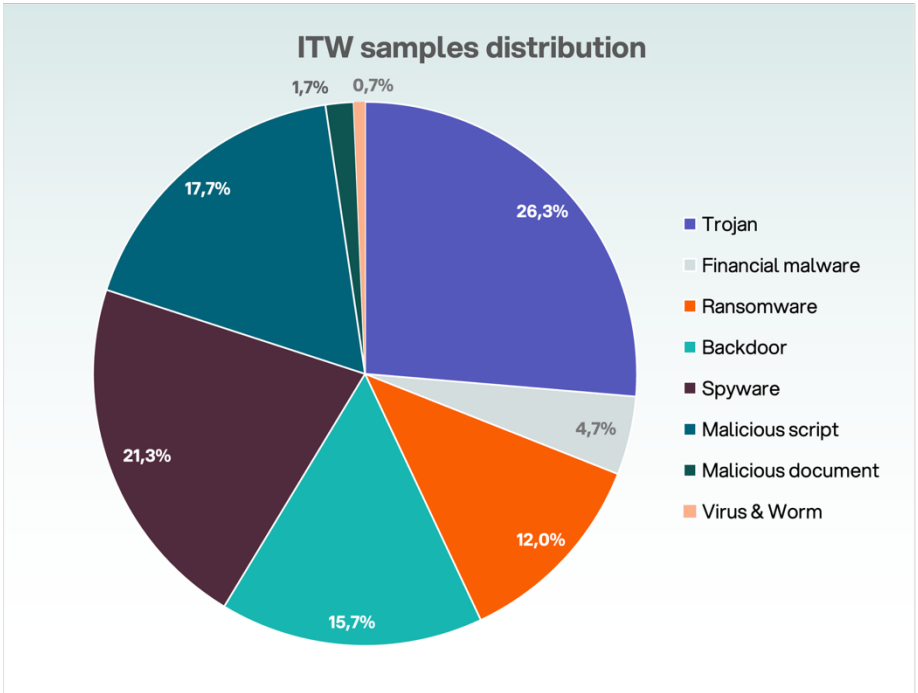
To assess false positive behaviour, the participating security products were tested against a set of clean, legitimate applications, which consisted of 100 clean application samples, with a focus on device drivers, media and content creation tools and other commonly used legitimate applications.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Security Applications Tested

- Avast Premium Security 26.9.11171.734
- Bitdefender Total Security 27.0.62.355
- ESET Internet Security 19.2.10.0
- G Data Internet Security 25.5.20.121
- Malwarebytes Premium Security 5.7.0
- McAfee Total Protection 1.40.161.1
- Norton 360 AntiVirus Plus 26.9.11171.0
- Sophos Home Premium 2025.2.3.67.0

Malware sample types used to conduct the test



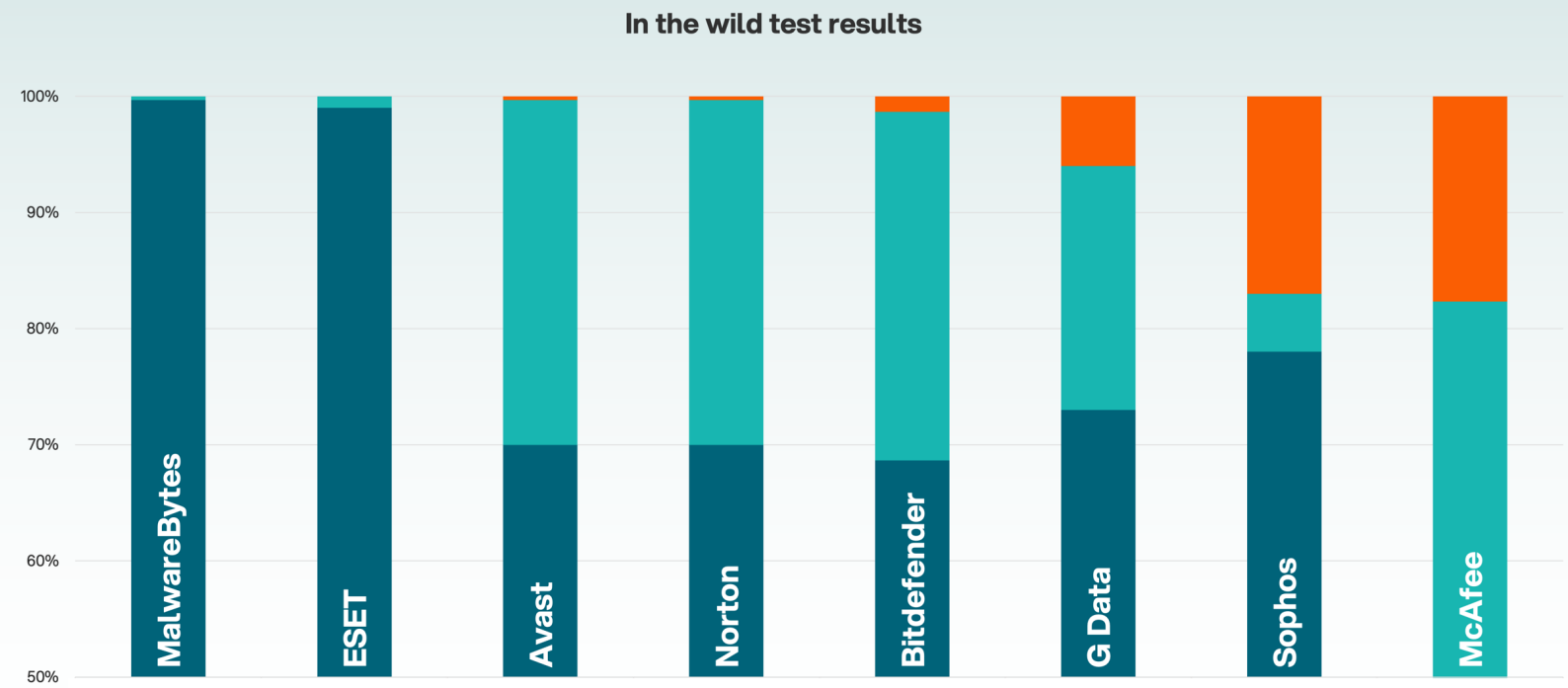
Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Test Results

The tables below show the results of testing under the Consumer Assessment Programme 09/2026.

In the Wild malware test results

The table below shows the detection rates of the participants for 300 ITW samples, sorted by the number of missed samples (lowest to highest).

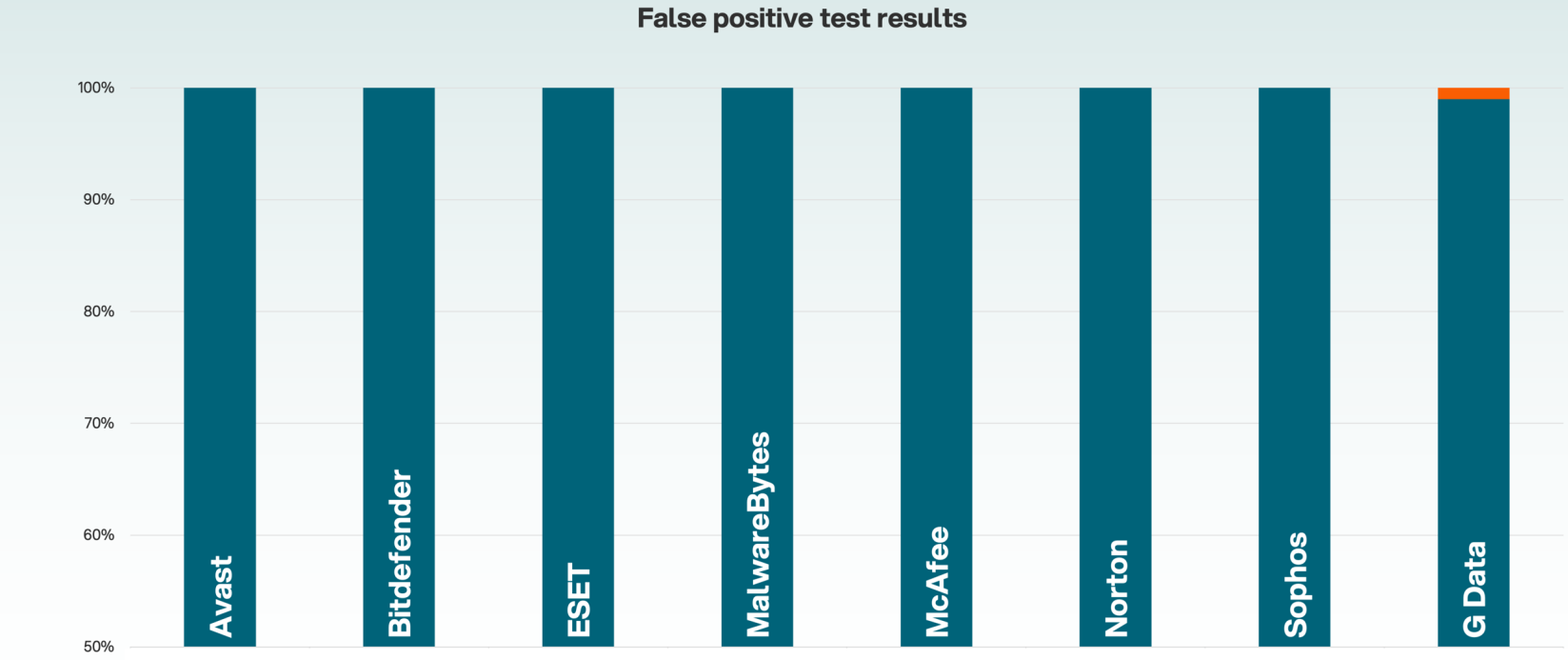


	MalwareBytes	ESET	Avast	Norton	Bitdefender	G Data	Sophos	McAfee
Miss	0,00%	0,00%	0,33%	0,33%	1,33%	6,00%	17,00%	17,67%
Behaviour block	0,33%	1,00%	29,67%	29,67%	30,00%	21,00%	5,00%	67,00%
Auto block	99,67%	99,00%	70,00%	70,00%	68,67%	73,00%	78,00%	15,33%

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

False positive samples test results

The table below shows the detection rates of the participants for False Positive (benign) samples, sorted by the number of missed samples (lowest to highest).

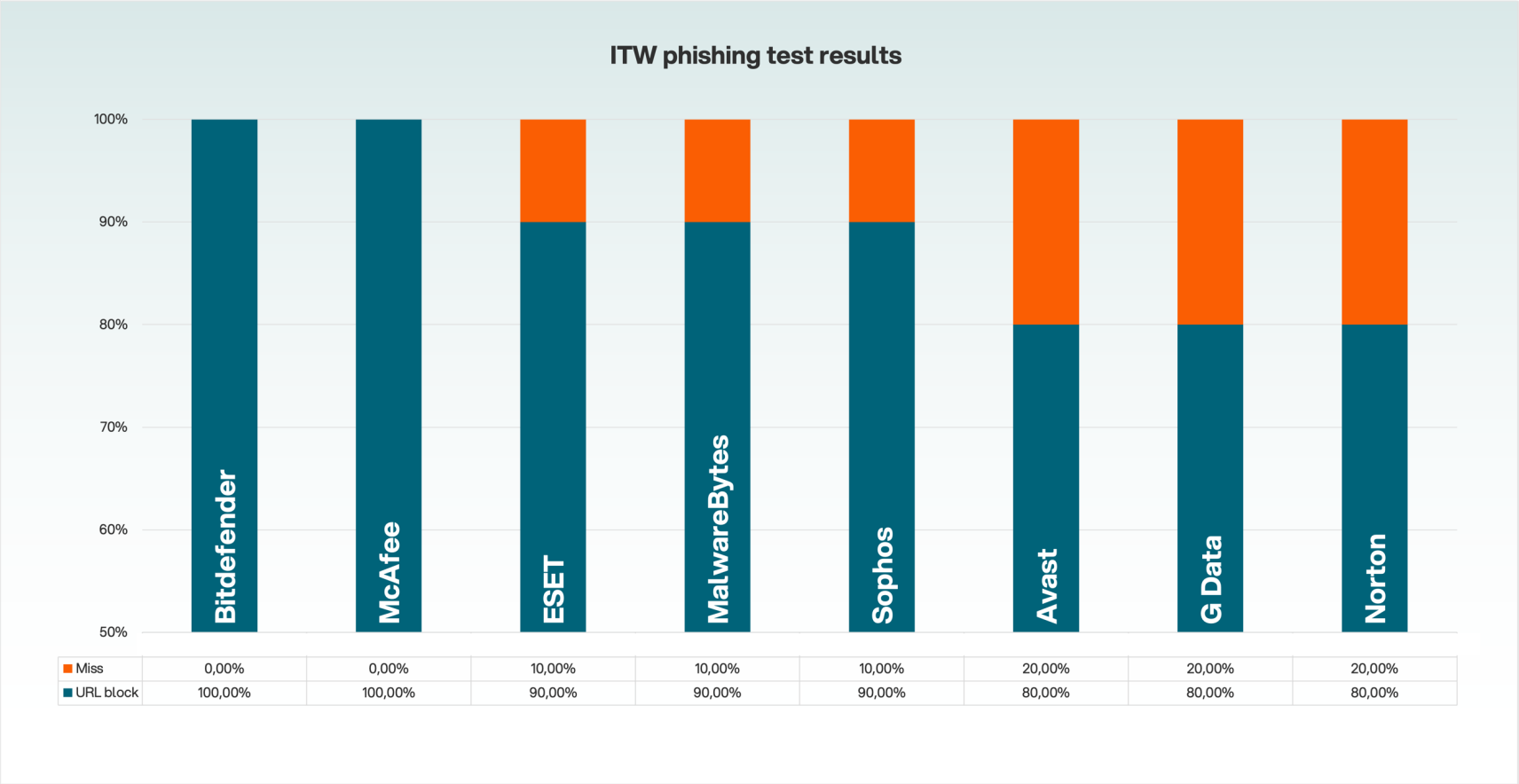


	Avast	Bitdefender	ESET	MalwareBytes	McAfee	Norton	Sophos	G Data
False block	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	1,00%
Allowed to run	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,00%

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

ITW phishing test results

The table below shows the detection rates of the security products for 10 ITW phishing sites.



	Bitdefender	McAfee	ESET	MalwareBytes	Sophos	Avast	G Data	Norton
Miss	0,00%	0,00%	10,00%	10,00%	10,00%	20,00%	20,00%	20,00%
URL block	100,00%	100,00%	90,00%	90,00%	90,00%	80,00%	80,00%	80,00%

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

MRG Effitas Consumer Assessment Certification 09/2026

To achieve an MRG Effitas Consumer Assessment **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 generate any false alert in FP test and must block at least 89% of the ITW phishing cases.

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.

Under the MRG Effitas Consumer Assessment & Certification, the following products were certified for 09/2026.

Certified (Level 1)

- ESET Internet Security
- Malwarebytes Premium Security

Certified (Level 2)

- Avast Premium Security
- Bitdefender Total Security
- Norton 360 AntiVirus Plus

MRG Effitas CERTIFIED CONSUMER TEST

09 / 2026

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Grading Criteria

Level 1 certified

All threats detected on first exposure or via behaviour protection, no false alert in FP test and block at least 89% of the ITW phishing case

- ESET Internet Security
- Malwarebytes Premium Security

Level 2 certified

At least 98% of the threats detected and neutralised less than 2% false alert in FP test and block at least 79% of the ITW phishing cases.

- Avast Premium Security
- Bitdefender Total Security
- Norton 360 AntiVirus Plus

Not certified

Security product failed to detect at least 98% of the infections and remediate the system during the test procedure, or more than 2% false alert in FP test or less block than 79% of the ITW phishing cases or at least one ransomware was missed.

- G Data Internet Security
- McAfee Total Protection
- Sophos Home Premium

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Appendix

Methodology used to create test environment

1. Windows 11 Enterprise operating system is installed on a hardened virtual machine, all updates are applied, and third-party applications installed and updated.
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) and then, where applicable, updated. 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.

Methodology used in the In The Wild testing

1. Downloading a single binary executable (or document, script, etc.) from its native URL using Chrome to the Downloads folder and then executing the binary in the clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test.

   1.1. The sample is selected for the test and tested in the systems where a security product is installed.
   - **The test case is marked as "Blocked"** if 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 machine.
   - **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 during both tests.
2. Tests are conducted with all systems having Internet access.
3. As no user-initiated scans are involved in this test, applications rely on various technologies to detect, block, and remediate threats. Some of these technologies are URL blacklisting, reputation, signature, machine learning, heuristics, behaviour, etc.

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Methodology used in the False Positive test

1. Downloading a single binary executable (or document, script, etc.) from URLs using Chrome to the Downloads folder and then executing the binary in the clean, unprotected system. If the sample works, the sample is saved in a replay proxy to provide the same binary throughout the test.
2. Executing the test samples.
    - **The test case is marked as "False block"** if the security application falsely identifies and blocks the binary at any stage during the test and retest.
    - **The test case is marked as "Allowed to run"** if the security application correctly identifies the binary as harmless and allows it to run.
3. Tests are conducted with all systems having Internet access.

Methodology used in the Phishing test

1. Starting an instance of Chrome (or the Safe Browser) and navigating to a phishing site. Where the security application offers a secured or dedicated banking browser, it is used.
    - **The test case is marked as blocked – a green checkmark** if the security application detects and blocks the URL.
    - **The test case is marked as missed – a red cross** if the security application fails to detect and block the URL.
2. Tests are conducted with all systems having Internet access.

Hardened virtual machine specification

- Browser: Google Chrome v151.0.7922.174
- OS: Windows 11 25H2
- CPU: 4 core processor
- Memory: 8GB
- Storage: 100GB SSD

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Version History

Nr.	Modify date	Comment
1.0	08.10.2026	Report published

Copyright © 2026 MRG Effitas Ltd. This article or any part thereof may not be published or reproduced without the consent of the copyright holder

Copyright © 2026 MRG Effitas Ltd.