ARTIFACT SECURITY

Consumer Real World Protection Testing Methodology

Document identifier	Version	Date of issue	Supersedes
RPT2025v1.0	**1.0**	**2025-04-07**	None, first public issue

Test environment	Issuing lab
Windows 11 Version 24H2 (OS Build 26100)	Artifact Security

Contents

Clause	Title	Test IDs	Page
1	Goal		3
2	Environment		3
3	Attack Corpus		3
3.1	Public Threats		3
3.2	Targeted Attacks		3
4	Legitimate Corpus		4
5	Attack Rating		4
5.1	Public Threats		4
5.2	Example Public threat rating		5
5.3	Targeted Attacks		5
5.4	Example Targeted Attack rating		5
6	Legitimate Rating		6
7	Total Rating		6
8	Configuration disclosure		7
9	Change Log		7

01 Goal

This test aims to evaluate the effectiveness of consumer antimalware endpoint security solutions against public malware and prevalent targeted attacks methods.

02 Environment

The environment consists of a Windows 11 Virtual Test PC. The base image Major version is upgraded biannually.

Current version: Windows 11 Version 24H2 (OS Build 26100).

Incremental updates are performed before each test exposure. The Endpoint Under Test (EUT) has constant unfiltered access to the internet.

03 Attack Corpus

The attack corpus is split into Public Threats and Targeted Attacks. Threats are collected and verified on a base clean image without any security product installed.

3.1 Public Threats

Public samples are sourced within 7 days of being exposed to the targeted security solution but must also be active within the 24 hours of exposure. These are served to the EUT using a similar attack vector as when captured.

3.2 Targeted Attacks

Targeted attacks are sourced and validated based on prevalent attack methods at the time of the test. Attacks are mapped to MITRE's ATT&CK matrix.

Attacks are split into two sequences *intrusion* and *infiltration*.

Intrusion	*Intrusion* is defined by the initial delivery mechanisms employed by the attacker against the victim. Example ATT&CK Tactic: Initial Access/Spearphishing link T1566.002
Infiltration	*Infiltration* is defined by the attacker executing and taking actions upon successful intrusion. Example ATT&CK Tactics: Execution, Persistence, Privilege Escalation.

04 Legitimate Corpus

The legitimate corpus is made to reflect a typical consumer machine. It is split into two sub-sets:

Set 1	Core set of applications from categories including but not limited to: Utilities, Office Processing, Web Browsers.
Set 2	Alternating legitimate applications & websites based on relevancy at the time of test. These change on a quarterly basis and will reflect popular scenarios for consumers.

05 Attack Rating

5.1 Public Threats

Prevented (+10)	No malicious code was executed on the EUT. Prevented rating includes the Cleaned rating points.
Disrupted (+8)	Significant malicious code started executing, the security product took action in blocking/quarantining the malicious processes later in the attack chain.
Compromised (-10)	The threat was successful in achieving its aim.
Partially Compromised (-8)	The threat was partially successful in achieving its goal.

Cleaned (+2)	The product took action to clean any significant traces of the threat.

5.2 Example Public threat rating

A threat containing a malicious web-download of a binary led to execution on the system, downloading an additional payload deploying Ransomware.

If the product prevents the download of the initial payload: **Prevented (+10)**

If the product intervenes by stopping at the point of Ransomware executing and reverts all changes on the system by deleting any files or threat artifacts: **Disrupted (+8) & Cleaned (+2)**. Failure to clean significant artifacts would yield: **Disrupted (+8)**.

5.3 Targeted Attacks

Intrusion Prevented (+10)	No malicious code was executed on the EUT. Prevented rating includes the Cleaned rating points.
Infiltration Disrupted (+8)	Significant malicious code started executing, the security product took action in blocking/quarantining the malicious processes later in the attack chain.
Compromised (-10)	The threat was successful in achieving its aim.
Partially Compromised (-8)	The threat was partially successful in achieving its goal.
Cleaned (+2)	The product took action to clean any significant traces of the threat.

5.4 Example Targeted Attack rating

A threat containing a malicious web-download of a binary led to execution on the system, downloading an additional payload deploying Ransomware.

If the product prevents the download of the initial payload: **Intrusion Prevented (+10)**

If the product intervenes by stopping at the point of Ransomware executing and reverts all changes on the system by deleting any files or threat artifacts: **Infiltration Disrupted (+8) & Cleaned (+2)**. Failure to clean significant artifacts would yield: **Disrupted (+8)**.

06 Legitimate Rating

Set 1 of applications are pre-installed on the EUT. During the legitimate test phase these are executed, and their core use case evaluated to ensure functionality. I.e. Browsers will navigate to a public webpage.

Set 2 scenarios are exposed while the product is already installed on the EUT. I.e. The user is installing a new application or visiting a clean new website.

Allowed (+10)	No Action taken/Clean verdict.
Blocked with suspicious attribution (-5)	the product raises suspicion during the test case and prevents the user from completing the use case.
Blocked with malicious Attribution (-10)	the product categorises the test case as malicious and prevents the user from completing the use case.

07 Total Rating

Total Rating is calculated as Attack Rating + Legitimate Rating. Grades are awarded based on the following thresholds:

Table 1 Grade thresholds

Grade	Threshold
S	96% - 100%
A	91% - 95%
B	86% - 90%
C	80% - 85%

08 Configuration disclosure

Products are deployed under default configuration. Any deviations from this. A full configuration and licencing disclosure is taken as part of any public report. If possible, this will be hosted under Artifact Security website. Linked references to the tested vendor resource are also acceptable.

09 Change Log

Table 2 Revision history

Date	Version · identifier	Change
2026-11	v1.0 · RPT2025v1.0	Reissued in the new methodology layout. Typographical corrections. No change to tests or scoring.
2025-04-07	v1.0 · RPT2025v1.0	Document created