Business & Enterprise Real World Protection Testing Methodology

Table of Contents

1. Goal

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

2. Environment

The environment consists of two Windows 11 Virtual Test PCs connected to a local Windows Server acting as a domain controller considered out of scope for threat testing.

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

The Endpoints Under Test (EUT) have constant unfiltered access to the internet. The base image Major version is upgraded biannually.

3. 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.

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.

Targeted Attacks

Targeted attacks are sourced and validated based on prevalent attack methods at the time of the test. Attacks are mapped to MITREs ATT&CK matrix. These are split into three sequences.

Sequence 1: Intrusion

This sequence is defined by the initial delivery mechanisms employed by the attacker against the target organisation.

ATT&CK Tactics applicable: Initial Access

Sequence 2: Infiltration

This sequence is defined by the attacker executing and taking actions on the initial target.

ATT&CK Tactics applicable: Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access

Sequence 3: Propagation

This sequence is defined by the attacker progressing past the first intrusion.

ATT&CK Tactics applicable: Discovery, Lateral Movement, Collection, Exfiltration, Impact

4. Legitimate Corpus

The legitimate corpus is made to reflect machines a business environment. 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.

5. Attack Rating

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 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.

Example Public threat rating

A threat containing a malicious web-download of a binary lead 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).

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 action in blocking/quarantining the malicious techniques during the infiltration sequence of the attack.

Propagation Disrupted (-5): Significant malicious code started executing, the security product took action in blocking/quarantining the malicious techniques after infiltration was successful but before propagation completed.

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.

Example Targeted Attack rating

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

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).

If the product intervenes by stopping the spreading the Ransomware propagating to the secondary endpoint but the initial EUT is compromised the attack is rated as: Propagation Disrupted (-5).

6. Legitimate Rating

Set 1 of applications are pre-installed on the EUT. During the legitimate test phase these 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.

7. Total Rating

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

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

8. Configuration disclosure

Products are deployed with recommended configuration, where possible vendor recommendations are made. Any configuration used in the test must be available to the public. 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.

9. Change Log

11/04/2025 – v1 Document created – Identifier – RPTBE2025v1.0