

# Calculation methodology for the whitepaper

## “Protection beyond detection: Why trust and transparency decide your cybersecurity future”

The [whitepaper](#) draws on findings from the [report](#) “Transparency Review and Accountability in Cybersecurity,” 2025 edition, commissioned by WKO (Tyrol Chamber of Commerce) and conducted by AV-Comparatives, MCI | The Entrepreneurial School®, and Studio Legale Tremolada.

The study itself doesn’t provide comparative product rankings. However, each specific category reveals the prevalence of concrete practices among evaluated cybersecurity vendors.

For each category, we define practice adoption as “High” if confirmed for 12 or more vendors/products, “Low” if confirmed for fewer than 5 vendors/products, “None” if no vendors disclose the practice, and “Medium” in other cases.

We consider Kaspersky “exceeding industry standards” if Kaspersky demonstrates an evaluated practice while industry adoption is medium or low. For telemetry collection, we consider Kaspersky “exceeding industry standards” if specific telemetry item collection is common (High to Medium prevalence) among tested products, but Kaspersky’s product hasn’t demonstrated collection during the study.

The whitepaper doesn’t include any cumulative/aggregate rating, following the original study’s logic that emphasizes different importance and relevance of each specific category for different organizations. According to this methodology, the 60 formally defined categories of the study break down as follows:

	<b>Number of evaluation categories</b>	<b>Kaspersky exceeds industry baseline</b>	<b>Kaspersky follows industry norms</b>
Legal and technology policy	37	12	23
Telemetry analysis	23	6	16
Total categories	60	18	39

# The complete list of categories where Kaspersky exceeds industry standards

(in the order of appearance in the report)

## Policy categories:

TRANSPARENCY CENTRES ADVERTISED (p. 16)  
DOWNLOAD OF DEFINITION UPDATES (p. 17)  
STAGED UPDATE ROLLOUT (p. 17)  
SECURITY ADVISORIES (p.19)  
COLLABORATION & SAFE HARBOR (p. 19)  
SECURITY AUDIT RESULTS (p. 19)  
LAW ENFORCEMENT REQUEST RESPONSE (p. 20)  
TRANSPARENCY REPORT (p. 20)  
OSS DISCLOSURE (p. 21)  
SBOM AVAILABILITY (p. 21)  
ON-PREMISE REPUTATION SERVICE (p. 24)  
REGION-DIVERSE DATA CENTRES (p. 25)

## Telemetry categories:

FIRMWARE VERSION (p. 28)  
CPU NAME (p. 28)  
RAM SIZE (p. 28)  
MANUFACTURER NAME (p.28)  
DEVICE SERIAL NUMBER (p. 28)  
MAC ADDRESS (p. 29)

