Protection beyond detection

Why trust and transparency decide your cybersecurity future

kaspersky

Proven.
Transparent.
Independent.

Kaspersky leads in independent trust assessment

Transparency is a competitive advantage that builds sustainable trust among vendors, customers, and regulators

Key differentiators:

- Multiple transparency centers, SBOM and update inspection capabilities
- Multiple data residency regions
- Granular update control and flexible deployment options
- Choice of cloud, on-premise, or disabled reputation services
- No unnecessary telemetry collection

60 criteria assessed across user choice, data handling, and transparency

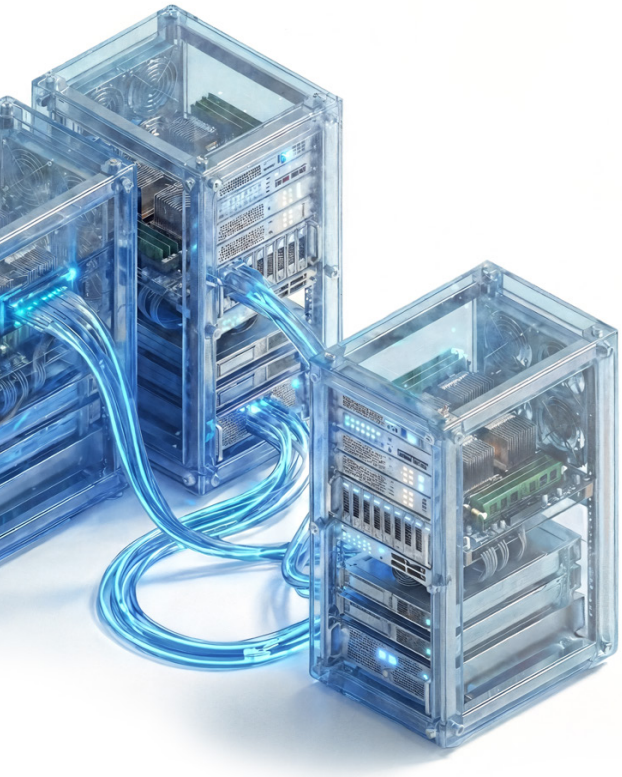
kaspersky

Proven.
Transparent.
Independent.

The trust equation: Critical questions your vendor must answer

Rising cyber risk costs, stringent regulatory requirements, and increasing supply chain attacks are forcing security leaders to re-assess the systems protecting their organizations. While EDR/EPP solutions form the foundation of cyber defense, their deep system access and extensive data processing capabilities raise critical questions about transparency, compliance, and trust.

Vendors pairing strong security with transparency ensure resilience, compliance, and trust



Key considerations include:

- What data do security solutions collect?
- Where and how is it stored?
- How much control do customers have over the solution's behavior?
- What tools does the vendor provide to verify product and manufacturer trustworthiness?

An independent study[1] commissioned by the Tyrol Chamber of Commerce (WKO) provides answers to these critical questions.

Study highlights

While all vendors meet baseline transparency and compliance requirements, their practices vary significantly in detail and openness. Vendors combining robust security with structured transparency provide the highest assurance of resilience, compliance, and trust.

Implications for enterprises

Vendor selection: Evaluate transparency and compliance as core criteria alongside protection capabilities.
Due diligence: Request certifications, SBOMs, and retention policies rather than accepting generic claims.
Incident & Legal readiness: Review incident response, Safe Harbor, and jurisdiction clauses.
Privacy & Configuration: Carefully configure telemetry, file upload, and reputation features to balance security and privacy.

[1] "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.

kaspersky

Proven.
Transparent.
Independent.

Kaspersky demonstrates clear leadership

Unique trust-defining features:

- Among the few vendors offering **Transparency Centers** for enterprise customers
- Provides **SBOM availability** and database update inspection capabilities
- Data facilities are present **across all regions** analyzed
- Complete **control over cloud/on-premise reputation** service deployment

Exceeding industry benchmarks:

- **Kaspersky excelled in the highest number of evaluation criteria,** meeting or exceeding industry standards in 57 of 60 categories[2]
- **Exceeded industry average in every third category** across user choice, transparency, update control, secure development, incident response, data handling, and data minimization

The research compared the transparency and accountability measures of leading cybersecurity vendors and evaluated their business practices, international legal standards adherence, and data protection measures. The legal analysis was underpinned by a technical to examine how the stated principles are implemented in the products. Kaspersky's product examined as part of the research — Kaspersky Next EDR Optimum.

Kaspersky exceeds industry standards in one-third of categories

[2] See the supplemental document for detailed category count and definitions.

kaspersky

Proven.
Transparent.
Independent.

A business mandate for transparency

While procurement questionnaires are already comprehensive, adding transparency and trust criteria addresses fundamental business risks. The "Transparency Review and Accountability in Cybersecurity" study reveals dramatic differences in vendor openness — from those offering transparency center visits and detailed security disclosures to others relying on broad contractual language and generic compliance claims[3].

This disparity represents more than a procurement preference; it directly impacts business risk. When cybersecurity incidents occur, an organization's ability to respond effectively, demonstrate regulatory due diligence, and maintain stakeholder trust depends on prior understanding of vendor practices. Vendor opacity translates directly to compliance vulnerabilities, legal exposure, and operational blind spots that can cripple incident response.

Modern business environments demand deeper accountability, and cybersecurity vendors cannot be exempt. The study demonstrates that transparency strongly correlates with operational maturity — vendors publishing audit results, maintaining current SBOMs, and providing granular privacy controls consistently demonstrate superior security practices overall.

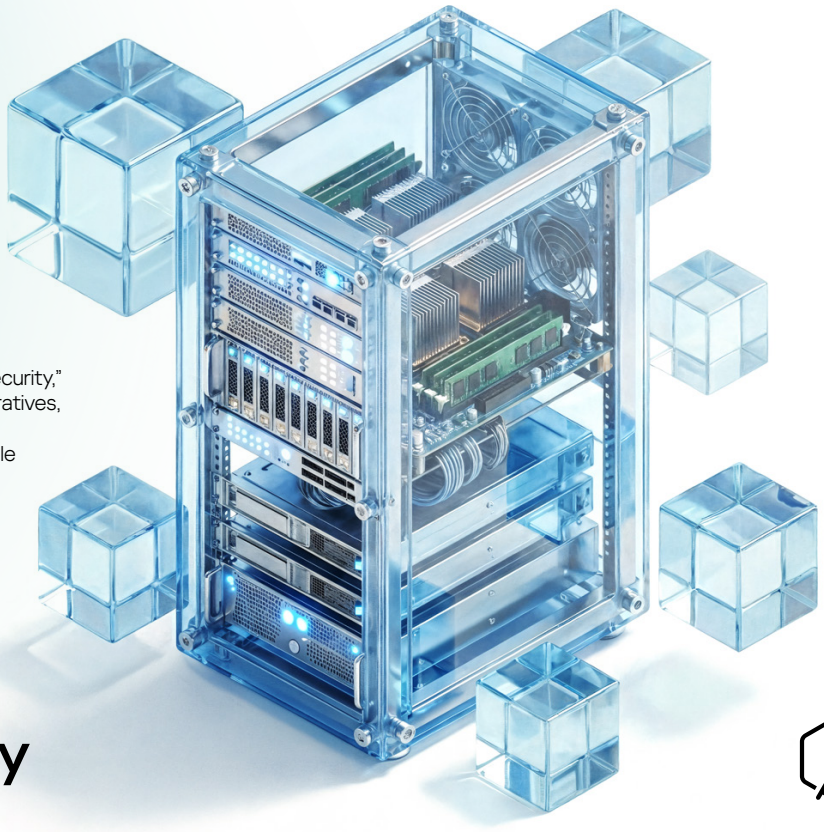
Business leaders must insist on vendor relationships supporting independent verification, detailed documentation, and clear accountability structures. This approach strengthens cyber resilience, ensures compliance with demanding regulations, and provides competitive advantage in an increasingly complex threat landscape.

The research findings contribute directly to improved governance, informed procurement, and responsible digital risk management

14

leading

endpoint security vendors were tested



[3] "Transparency Review and Accountability in Cybersecurity," 2025 edition, AV-Comparatives, MCI | The Entrepreneurial School®, and Studio Legale Tremolada, p. 39.

kaspersky

Proven.
Transparent.
Independent.

Industry benchmark overview

While many practices like SDLC adherence and GDPR compliance have become industry standard, some remain rare among the 14 leading security vendors evaluated:

Criteria	Industry adoption (number of vendors providing this feature)		Kaspersky
Transparency centers for source code reviews and data checks	3/14	Low	Yes ✓
Direct signatures/definitions download for inspection	6/14	Medium	Yes ✓
SBOM (Software Bill of Materials) provision	3/14	Low	Yes ✓
Regular transparency reports	4/14	Low	Yes ✓
On-premise reputation service	8/14	Medium	Yes ✓
Multiple data center options	4/14	Low	Yes ✓
Security advisories regularly published	7/14	Medium	Yes ✓
Independent security audit results available	7/14	Medium	Yes ✓
Options for staged update rollout	8/14	Medium	Yes ✓
Product update history is public	13/14	High	Yes ✓
Public reporting on law enforcement requests for data	9/14	Medium	Yes ✓
Verbose incident reporting	7/14	Medium	Yes ✓
Multiple jurisdictions for dispute resolution	11/14	Medium	No*
CCPA compliance	12/14	High	Yes ✓
CRA compliance	0		No

(*) It's possible to change jurisdiction for dispute resolution through a separate contract (see page 7 for more details).

Deep dive: Key practices

Source code and SBOM

All tested vendors use closed-source models, with 13 of 14 disclosing third-party OSS usage. However, only 3 vendors maintain transparency centers allowing enterprise customers to review source code.
Of these, one reserves access only to government customers, and another limits its scope to source code and unspecified intellectual property. Kaspersky stands out with the broadest Transparency Center offering, including threat detection rule examination and a verification check to confirm builds match public releases.
Only three vendors, including Kaspersky, provide SBOM access to customers.

Granular update control

Many vendors emphasize their update best practices, such as multi-phase staging, rigorous testing, and quality assurance. However, only 5 vendors, including Kaspersky, provide all the options to their customers:

Feature	Vendor adoption
Public update history	13/14
Definition update download	6/14
Automatic updates	14/14
Pre-release testing options	14/14
Staged update rollout	8/14

Inside the Transparency Center

Kaspersky operates over 10 global transparency facilities where government regulators and enterprise clients can independently review source code, threat detection rules, software updates, and development processes. Three assessment levels are available: “Blue Piste” for overview demonstrations, “Red Piste” for targeted code analysis, and “Black Piste” for comprehensive deep-dive reviews. Visitors can examine secure development documentation, rebuild source code to verify publicly available modules match builds, and review AV database updates with expert assistance.

Security posture

Strong vulnerability management, transparent disclosure, independent audits, and secure SDLC processes indicate vendor trustworthiness and resilience. Only Kaspersky and two other vendors provide all evaluated capabilities:

Feature	Vendor adoption	
Vulnerability reporting	14/14	
Security advisories	7/14	
Collaboration & Safe harbor	7/14	
Security audit results	7/14	
SDLC practices	14/14	

The research revealed that in addition to widely affirmed regulatory frameworks, several vendors appear to be preparing for Cyber Resilience Act (CRA) full enforcement. Having shared its inputs for the act during the legislation process open call, Kaspersky is closely monitoring the CRA phased implementation to be ready to meet regulatory obligations once it's in full applicability.

Transparency and policies

Public disclosure of incidents and law enforcement requests demonstrates vendor transparency. While most vendors contractually commit to incident disclosure, only 7 document detailed disclosures. Just 3 vendors, including Kaspersky, publish transparency reports with law enforcement request details:

Feature	Vendor adoption	
Contractual commitment to incident disclosure and response	13/14	
Timely, detailed incident disclosures documented	7/14	
Law enforcement request disclosure to affected customers	9/14	
Published transparency reports	3/14 public, 1 on-request	

Compliance and certification

Compliance with international standards, regulatory frameworks, and legal governance is central to vendor transparency and trust. The study found that all vendors confirm GDPR compliance and maintain ISO/IEC 27001 and SOC 2 Type II certifications. 12 of 14, including Kaspersky, comply with CCPA. Eleven vendors offer multiple dispute resolution jurisdictions. While Kaspersky's general agreement lacks this provision, it includes clauses enabling customers to supersede the general agreement with individual contractual agreements that address this need.

Telemetry and data storage

The way vendors manage product deployment environments, telemetry collection, and data storage is critical for both transparency and compliance. Flexible deployment options and transparent data handling strengthen vendor credibility. While offline operation is common, only half provide cloud reputation service alternatives, and just four maintain data facilities across all the regions analyzed — Kaspersky provides both:

Feature	Vendor adoption
Offline / air-gapped support	14/14
On-premise reputation service	8/14
Data anonymization and regular deletion	14/14
EU data centers are present	14/14
NA (North America) data centers are present	14/14
ME (Middle East) data centers are present	4/14

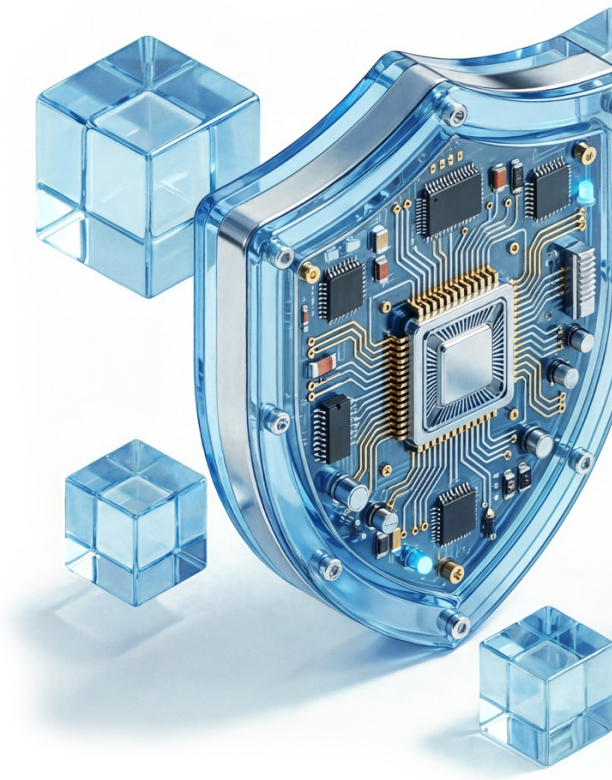
4
vendors
have data facilities across all regions

Data transmission analysis

The tested enterprise products are designed to collect and transmit data as part of their normal operation to be able to provide protection against threats. Each data element might be critical security telemetry, but it could also be viewed as sensitive information being transmitted to a third-party data center.
Organizations must align data collection with their risk profiles and priorities through available control options.

Kaspersky demonstrated minimal data collection in testing

The researchers observed the product transmitting most common indicators (hostname, Windows username, internal IP) on par with all competitors while avoiding sensitive data like crash logs.
Kaspersky also allows disabling Kaspersky Security Network (file reputation submission) and EDR functionality entirely.



kaspersky

Proven.
Transparent.
Independent.

Action items for CISOs

1. Source code & Product components

- ☐ Request detailed SBOM disclosure during procurement and for ongoing risk management
- ☐ Verify vendor processes for monitoring and mitigating supply chain vulnerabilities
- ☐ Seek transparency center access for source code and build verification

2. Product updates & Change management

- ☐ Require access to comprehensive changelogs and release notes
- ☐ Confirm staged rollout and beta testing programs for pre-deployment validation

3. Data storage, privacy, and telemetry

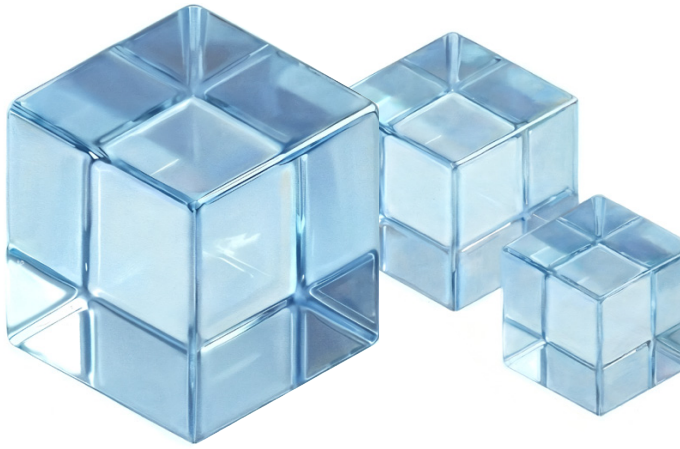
- ☐ Demand clear, configurable privacy settings for telemetry, file uploads, and data collection
- ☐ Require explicit data retention timelines, deletion procedures, and data center locations
- ☐ Verify support for offline or air-gapped deployments

4. Security posture, incident response, and policies

- ☐ Require transparent vulnerability reporting and public security advisories
- ☐ Request third-party audit results and SDLC documentation
- ☐ Ensure contractual obligations include prompt breach notification and detailed root-cause, scope, and remediation reporting
- ☐ Review vendor history of public incident disclosures and response clarity
- ☐ Seek regular transparency reports and law enforcement request policies

5. Compliance and Certification

- ☐ Verify certification scope (ISO/IEC 27001, SOC 2) through official documentation, not just logos or claims
- ☐ Ensure certifications explicitly cover data centers, build systems, and cloud services



kaspersky

Proven.
Transparent.
Independent.

Continue your transparency journey

Read the full report

Explore Kaspersky Next EDR Optimum

Schedule a transparency center visit

Review Kaspersky transparency report

Discover the complete Kaspersky enterprise portfolio

kaspersky

Proven.
Transparent.
Independent.