Independent TRACS 2025 Study Highlights Transparency and Data Practices in Leading Cybersecurity Products

Independent TRACS 2025 study evaluates cybersecurity vendors' transparency, compliance, and data practices across 14 enterprise solutions.

INNSBRUCK, AUSTRIA, December 5, 2025 /EINPresswire.com/ -- The Tyrol Chamber of Commerce (WKO), in collaboration with MCI | The Entrepreneurial School® and AV-Comparatives, has released the Transparency Review and Accountability in Cyber Security (TRACS) 2025, a comprehensive independent study examining how major cybersecurity vendors disclose data practices, implement compliance measures, and communicate transparency to their customers. The report aims to support enterprises, public institutions, and SMEs in making informed, evidence-based decisions when selecting cybersecurity solutions.

The study evaluates 14 widely used enterprise cybersecurity products. It combines a legal review of agreements and publicly available vendor information with a technical assessment of network traffic generated by installed security solutions.

Key Findings
The study identifies the differences across vendors in how they communicate transparency and data-handling policies. All solutions are closed-source, and while many confirm the use of third-party or open-source components, disclosures differ in depth and structure. A small number of vendors operate transparency centres that offer controlled inspection of source code and documentation.

All vendors confirm compliance with the EU GDPR, and most with the US CCPA. None yet claim compliance with the upcoming EU Cyber Resilience Act, which is expected due to the regulation's phased introduction. ISO/IEC 27001 and SOC 2 Type II certifications are commonly observed, though certification scopes vary and often require closer examination.
From a security posture perspective, all vendors offer vulnerability-reporting mechanisms, and several operate bug bounty programs. However, public disclosure of security advisories, incident-response details, and audit results remains inconsistent. Only a few vendors publish transparency reports detailing law enforcement data requests.
The technical analysis found that all evaluated products transmit some combination of device, network, environmental, or user-related metadata. Depending on configuration, some solutions also transmit usernames, hostnames, installed applications, and file names or hashes. A limited

number of products were observed transmitting benign file contents under certain conditions. All vendors provide options to configure telemetry, file submission, and reputation services, though the clarity and granularity of these settings differ significantly.

Implications for Organizations
The findings underscore the growing importance of transparency as a key procurement criterion. The study recommends that organizations verify certifications and compliance claims through official documentation rather than marketing statements; request SBOMs where available; examine incident-response obligations and Safe Harbor commitments; and carefully review telemetry, sample-submission, and privacy-related settings before deployment.
Enterprises operating in regulated or privacy-sensitive environments are advised to confirm offline capabilities, review data-retention policies, and validate data-centre locations to ensure compliance with internal and regulatory requirements.

Call to Action
Organizations seeking to strengthen their cybersecurity governance, compliance posture, and vendor risk management are encouraged to review the full TRACS 2025 report. The complete study provides detailed insights, data tables, and vendor-specific observations that can support more transparent and informed decision-making.
Read the full report for all findings and recommendations here.

Thomas Uhlemann
AV-Comparatives GmbH
+43 512 28778813
press@av-comparatives.org
Visit us on social media:
LinkedIn
Facebook
X