

TRANSPARENCY REVIEW AND ACCOUNTABILITY IN CYBER SECURITY

2025

CONTENTS

3	Foreword by Tyrol Chamber of Commerce (WKO)
4	Foreword by MCI The Entrepreneurial School®
5	Foreword by IT Security Experts Group
6	Foreword by Attorney at Law
7	Management Summary
9	Introduction
11	Test Procedure
14	Tested Products
15	Legal Review on Agreements, Compliance, and Transparency
27	Technical Analysis
38	Conclusion, Limitations, Remarks
41	Appendix: Survey Results



Foreword by Mag. Sybille Regensberger

Tyrol Chamber of Commerce (WKÖ)

Digitalization offers vast opportunities for businesses, but at the same time it creates increasingly complex challenges in IT security and data protection. For small and medium-sized enterprises in particular, it is crucial not only to rely on the protective capabilities of cybersecurity solutions, but also to understand their transparency, legal safeguards, and data handling practices.

The present study, *Transparency Review and Accountability in Cyber Security (TRACS)*, provides our member companies with an independent, practice-oriented assessment of leading international providers. Conducted in cooperation with the MCI | The Entrepreneurial School® and legal experts, it highlights the differing levels of openness among vendors and sets out key criteria that businesses should consider when selecting cybersecurity solutions.

**WE ARE PLEASED TO MAKE THIS STUDY FREELY AVAILABLE,
CONFIDENT THAT IT WILL FOSTER GREATER TRANSPARENCY,
SECURITY, AND TRUST IN THE DIGITAL ECONOMY**

What makes this study especially valuable are its concrete recommendations: from verifying certifications and requesting Software Bills of Materials (SBOMs) to carefully configuring telemetry and data flows. In doing so, it offers Austrian enterprises – and Tyrolean businesses in particular – practical guidance to strengthen their digital resilience while ensuring legal and organisational compliance.

As the UBIT Division of the Tyrol Chamber of Commerce, we are committed to providing our members with reliable knowledge and access to high-quality analyses in this vital field. We are therefore pleased to make this study freely available, confident that it will foster greater transparency, security, and trust in the digital economy.

Mag. Sybille Regensberger

Chairwoman of the UBIT Division, Tyrol Chamber of Commerce





Foreword by Prof. Dr. Pascal Schöttle

MCI | The Entrepreneurial School®, Innsbruck

In today's enterprise information systems landscape, cybersecurity solutions hold unprecedented access to the systems, data, and operations that sustain organizational resilience. This privileged position demands an equally high level of transparency and accountability – especially within the frameworks that govern their use. End User License Agreements (EULAs), often seen as formalities, are in fact critical instruments defining trust between providers and users of security products.

The study, *Transparency Review and Accountability in Cyber Security (TRACS)*, was launched to assess how clearly and responsibly such agreements communicate rights, obligations, and data-handling practices.

Advanced analytical methods – including large language models (LLMs) – were applied to evaluate transparency, compliance with data protection regulations, accessibility, and the vendors' commitments to secure development and operational openness.

THE RESEARCH FINDINGS CONTRIBUTE DIRECTLY TO IMPROVED GOVERNANCE, INFORMED PROCUREMENT, AND RESPONSIBLE DIGITAL RISK MANAGEMENT

The beneficiaries of this work extend to all enterprises deploying information systems and using one of the fourteen major enterprise security products examined in this study. By revealing how transparently these products communicate their terms of use and data practices, the findings contribute directly to improved governance, informed procurement, and responsible digital risk management.

This initiative also reflects the mission of MCI | The Entrepreneurial School®, which brings together academia, business, and consulting in a unique concept that bridges theory and practice, science and industry. As one of Austria's leading universities of applied sciences, MCI has a strong record in fostering innovation and entrepreneurial initiatives. This project illustrates the value of combining academic inquiry with industry engagement to promote transparency, accountability, and trust in enterprise cybersecurity solutions.

Prof. Dr. Pascal Schöttle

Professor for IT Security & Machine Learning, MCI | The Entrepreneurial School®, Innsbruck





Foreword by Peter Stelzhammer, MBA

**IT Security Experts Group, Tyrol Chamber of Commerce
Co-Founder of AV-Comparatives**

In today's interconnected world, data transparency is not just a principle; it is the foundation of digital trust. Whether in business, research, or government, decisions increasingly depend on the integrity and openness of data. Transparency in cybersecurity, in particular, has become essential to sustaining confidence in the technologies that protect our information and critical infrastructures. Beyond delivering effective protection, cybersecurity solutions must clearly demonstrate how they handle data, manage risks, and comply with evolving international regulations.

This study, *Transparency Review and Accountability in Cyber Security (TRACS)*, exemplifies this commitment. By combining legal review, technical analysis, and independent verification, it provides an unprecedented look into how major cybersecurity vendors communicate their data practices and operational integrity. In doing so, it establishes a benchmark for clarity and accountability that are indispensable for informed and responsible decision-making.

TRANSPARENCY IS NOT A REGULATORY BURDEN BUT A COMPETITIVE ADVANTAGE THAT BUILDS SUSTAINABLE TRUST AMONG VENDORS, CUSTOMERS, AND REGULATORS

As speaker of the IT Security Experts Group of the Tyrol Chamber of Commerce, I am proud that this initiative supports our shared goal: strengthening the resilience of Austrian enterprises by promoting transparent, evidence-based information security practices. Transparency is not a regulatory burden but a competitive advantage that builds sustainable trust among vendors, customers, and regulators.

My sincere thanks go to the students and academic team of MCI | The Entrepreneurial School® and to the researchers of AV-Comparatives. Their diligence, analytical precision, and scientific integrity reflect what can be achieved when academia and industry collaborate for the public good. Their contribution not only advances technical understanding but also helps ensure that cybersecurity remains anchored in transparency, ethics, and trust.

Peter Stelzhammer, MBA

IT Security Experts Group, Tyrol Chamber of Commerce | Co-Founder of AV-Comparatives





Foreword by Avv. Matteo Tremolada

Studio Legale Tremolada

This report provides a legal perspective on the contracts that shape the use of cybersecurity solutions, with particular attention to transparency, regulatory compliance, and data handling. In today's digital landscape, where technology evolves quickly and regulatory scrutiny is becoming stricter, especially in the EU, the legal aspects of these products have become as important as their technical strength. The agreements that support them are not just routine documents: they set out the rights and responsibilities of vendors and users, and they serve as the foundation for the trust that is needed in this contractual relationship. At the same time, the ability of these documents to be transparent, intelligible, and user-oriented has a direct impact on how effectively such trust can be established, preserved and maintained.

End-users, whether large corporations, SMEs, or public administrations, need to understand, among others, the scope of licenses, limits of liability, and vendor commitments with respect to security and privacy. Given that cybersecurity vendors often act as processors of personal and business-critical information, compliance with regulatory frameworks such as the GDPR and CCPA should also be considered as a matter of accountability and trust.

AS TECHNOLOGY EVOLVES AND REGULATORY SCRUTINY IS BECOMING STRICTER, ESPECIALLY IN THE EU, THE LEGAL ASPECTS OF THESE PRODUCTS HAVE BECOME AS IMPORTANT AS THEIR TECHNICAL STRENGTH

The value of this study lies not only in its findings but in its guidance. It provides a foundation for informed vendor selection, responsible risk management, and robust compliance. I commend this work as a timely and necessary contribution to the ongoing dialogue between law, technology, and enterprise trust.

Avv. Matteo Tremolada

Attorney at Law, Studio Legale Tremolada



MANAGEMENT SUMMARY



Cybersecurity solutions are essential for enterprise protection, but their deep system access and extensive data processing raise transparency, compliance, and trust challenges. To address growing concerns, the Tyrol Chamber of Commerce (WKO) commissioned an independent study by MCI | The Entrepreneurial School® with legal experts, supported by AV-Comparatives. Fourteen leading enterprise cybersecurity products were examined through legal review and technical network traffic analysis.

Key Findings

- **Transparency of Agreements:** All vendors use closed-source models. Some build trust via transparency centres and OSS disclosures, though legal texts often remain broad.
- **Compliance and Certifications:** All confirm GDPR compliance; most also CCPA. None yet claim EU Cyber Resilience Act alignment, though preparations are visible. ISO/IEC 27001 and SOC 2 are widespread, but coverage scopes vary.
- **Security Posture:** All vendors provide vulnerability reporting; several run bug bounty programs. Few consistently publish advisories or audit results; Safe Harbor is not universal.
- **Third-Party Risk Management:** Vendors acknowledge open-source and third-party use but rarely publish audit results or full SBOMs. Customers must request details.
- **Data Handling and Storage:** All support offline use and flexible deployments. Most disclose data centre locations (EU/NA at least) and commit to anonymization/deletion. Encryption in transit and at rest is standard, with some exceptions.
- **Technical Analysis:** All transmit machine, network, and environmental data. Many also send usernames, hostnames, and application lists. Some upload file names, hashes, or full content, even benign files, raising privacy concerns. Privacy settings exist but vary widely in scope and clarity.

TREAT TRANSPARENCY AND COMPLIANCE AS CORE CRITERIA, ALONGSIDE PROTECTION. INDEPENDENT VERIFICATION, CONTRACTUAL SAFEGUARDS, AND CAREFUL CONFIGURATION ARE ESSENTIAL

Implications for Enterprises

- **Vendor Selection:** Treat transparency and compliance as core criteria, alongside protection.
- **Due Diligence:** Request certifications, SBOMs, and retention policies; do not rely on generic claims.
- **Incident & Legal Readiness:** Review incident response, Safe Harbor, and jurisdiction clauses.
- **Privacy & Configuration:** Configure telemetry, file upload, and reputation features carefully to balance security and privacy.

Conclusion

All vendors meet a baseline of transparency and compliance, but practices differ in detail and openness. Enterprises should not rely solely on vendor assurances; independent verification, contractual safeguards, and careful configuration are essential. Vendors combining strong security with structured transparency provide the highest assurance of resilience, compliance, and trust.

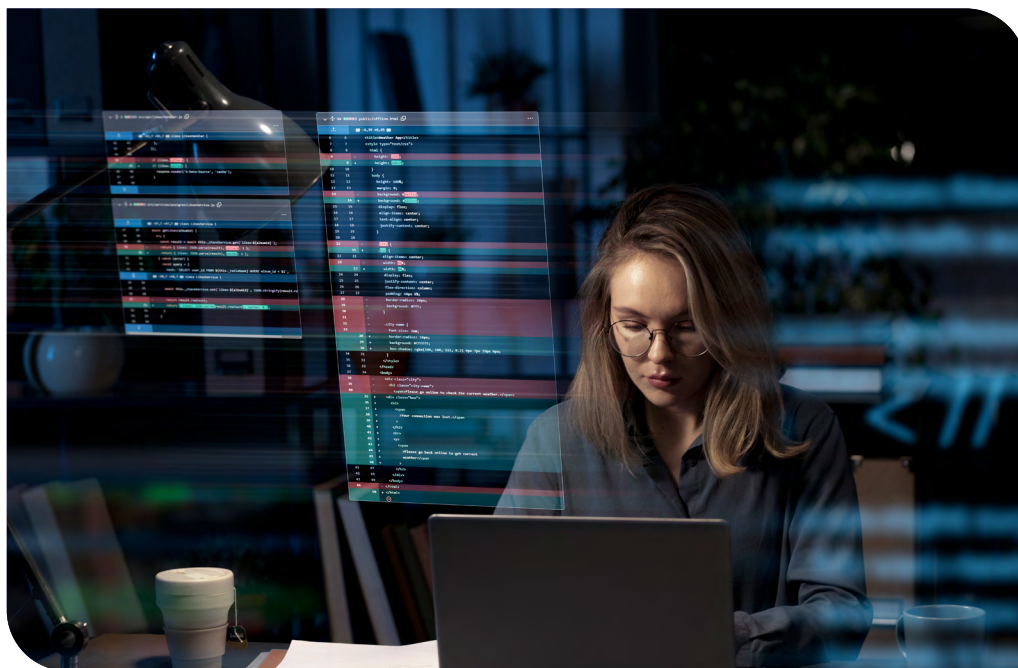
INTRODUCTION



INTRODUCTION

In recent years, businesses have increasingly turned to the **Tyrol Chamber of Commerce (WKO)**¹ with questions about transparency in the cybersecurity industry. Topics such as data handling, compliance, and legal clarity have become more pressing, particularly in light of new regulations (e.g., EU Cyber Resilience Act), data sovereignty, and geopolitical developments. To provide its members with reliable guidance, the WKO sought external expertise and initiated an independent study on this subject.

In addition to the legal work, technical examinations were carried out with the support of AV-Comparatives



The study was conducted by the **MCI | The Entrepreneurial School**² together with legal experts, who reviewed licensing terms, data protection measures, and adherence to international legal standards. To ensure the robustness and accuracy of the legal analysis, an additional **external law firm**³ was engaged to review and verify the findings. This independent verification strengthened the reliability of the study by providing a second expert perspective on licensing conditions, data protection obligations, and international compliance requirements. In addition to the legal work, technical examinations were carried out with the support of

TO ENSURE THE ROBUSTNESS AND ACCURACY OF THE LEGAL ANALYSIS, AN ADDITIONAL EXTERNAL LAW FIRM WAS ENGAGED TO REVIEW AND VERIFY THE FINDINGS

AV-Comparatives⁴. Their contribution included in-depth technical analysis of network traffic logging, metadata evaluation, and data transmission behaviour. AV-Comparatives also consolidated the findings, assisted in drafting the report, and is hosting the publication on behalf of the WKO. The aim is to deliver organizations clear and unbiased insights into how security vendors handle sensitive data, meet legal obligations, communicate transparency to their customers, and grant customers control over data processing.

¹ <https://www.wko.at/tirol>

² <https://www.mci.edu>

³ Studio Legale Tremolada – Avv. Matteo Tremolada, Attorney at Law

⁴ <https://www.av-comparatives.org>

TEST PROCEDURE



Scope and Objectives

This study aims to provide an objective comparison of cybersecurity vendors based on six key aspects:

1. **Transparency of Agreements** – Evaluating how clearly vendors communicate terms, obligations, and data-handling policies in their legal documents.
2. **Compliance with Data Protection Laws** – Reviewing adherence to global legal frameworks such as GDPR, CCPA, and other relevant regulations.
3. **Global vs. Local Consistency** – Investigating whether vendors maintain harmonized global agreements or introduce region-specific variations that may affect compliance.
4. **Accessibility of Legal Documents** – Assessing the public availability and ease of access to licensing agreements, privacy policies, and related legal materials.
5. **Security Posture and Openness** – Examining publicly available evidence of a vendor's commitment to secure development and operational transparency, including cybersecurity research, vulnerability management, incident response, source code publication and review, and standards-compliant software build processes and infrastructures.
6. **Technical Data Logging and Analysis** – Capturing network logs and metadata to analyse the data transmitted by cybersecurity products, comparing these findings with vendors' stated privacy policies, and assessing the possibilities to control the transmission behaviour through product settings.

The study was conducted over a **six-month period**, from April to September, and divided into two parts. The **Legal Review** (objectives 1 to 5) focused on evaluating vendors' legal documentation. The **Technical Analysis** (objective 6) aimed to validate these legal claims by capturing and analysing network traffic generated by the cybersecurity solutions. This dual approach ensures a comprehensive and practical assessment of vendor transparency and compliance in real-world conditions. The focused testing phase was followed by an extended evaluation period in which the findings were reviewed and verified to ensure accuracy, consistency, and objectivity.

OUR DUAL APPROACH ENSURES A COMPREHENSIVE AND PRACTICAL ASSESSMENT OF VENDOR TRANSPARENCY AND COMPLIANCE IN REAL-WORLD CONDITIONS

Legal Review

This part of the research focused on evaluating the transparency, accessibility, and legal soundness of cybersecurity vendors' documentation. The process began with the systematic collection of End User License Agreements (EULAs), privacy policies, and other relevant legal texts. In addition to general agreements, special attention was given to documents specific to the evaluated cybersecurity solutions. To allow for a structured, objective evaluation and a consistent comparison across vendors, a detailed questionnaire was developed based on the study objectives 1 to 5. Each objective was translated into a set of targeted questions covering key thematic topics, including:

- Source Code
- Product Updates
- Security Posture
- Transparency and Policies
- Third-party Risk Management
- Compliance and Certification
- Product Environment, Data Storage, and Telemetry

The evaluation process was supported and verified by legal experts to ensure that interpretations of complex legal language were accurate and aligned with current regulatory standards. This legal review was complemented and further refined by manual internet research, during which official vendor websites were examined for publicly available information relevant to the questionnaire. Sources included product documentation, data sheets, compliance reports, and other related materials made directly available by the vendors. The insights from this review provided the foundation for the technical analysis, enabling a comparison between vendors' stated policies and their actual product behaviour.

Technical Analysis

In addition to the legal review, the study incorporates a hands-on technical analysis of cybersecurity products. While the legal review is based on document analysis and internet research of vendor websites, the technical assessment requires direct access to the product, including installation on an endpoint. Therefore, all aspects of this report that require hands-on interaction with the product are covered in this section.

The configured endpoint was then integrated into a controlled network laboratory environment, designed to record all ingress and egress traffic associated with the endpoint.



The process began with the initialization of the web console (if any), applying typical configuration settings. Following this, an endpoint was provisioned with a typical configuration, reflecting standard deployment practices within operational environments.

The configured endpoint was then integrated into a controlled network laboratory environment, designed to record all ingress and egress traffic associated with the endpoint. The capture infrastructure supported the inspection of TLS-encrypted traffic as well, provided that no additional protective measures were in place. However, it must be noted that certain products implement anti-inspection countermeasures. These may include certificate pinning, mutual TLS, or proprietary encryption mechanisms, all of which can render TLS interception ineffective. In such cases, the encrypted portions of the traffic remained opaque to analysis. As a result, the dataset derived from the captured traffic might be incomplete, and any findings should be interpreted with this limitation in mind. To address this, the product's web console was examined for the same categories of data. If user-related information was found there, it was treated like it had been observed in transmission, since its presence in the console indicated that it must have been sent, even if it was not visible during traffic analysis.

The tested enterprise products are designed to collect and transmit data as part of their normal operation, and this analysis does not judge that functionality. The captured traffic was examined for potentially personal or company-related information, such as telemetry data, usage statistics, personal files, running processes, device identifiers, and hardware details. The following (not limited to) operations were performed on the endpoints, while recording the network traffic:

- Boot the machine and then let the machine idle
- Open the product's user console and update the virus definitions and policies (if possible)
- Browse websites using the browser
- Download files using the browser
- Navigate Windows Explorer to clean and malicious files of different types (on-access scanning)
- Run on-demand scans on clean and malicious files of different types
- Execute clean applications
- Let the machine idle for 24 hours

As part of the overall evaluation, observed data flows were compared with the vendors' published privacy policies and EULAs. This helps identify any discrepancies between documented practices and actual data transmissions, as well as activities not explicitly communicated to the user. Such gaps may indicate shortcomings in transparency, potential policy violations, or uncommunicated data handling practices.

The last section of this analysis includes an assessment of the availability and effectiveness of user-configurable privacy settings. This involves verifying whether such controls are easily accessible and comprehensive in limiting or preventing the collection and transmission of data. In addition, the clarity of these settings is evaluated to determine whether the implications of enabling or disabling a given product feature are clearly communicated to the user, ensuring informed decision-making.

Tested Products

The following up-to-date products were installed in Spring 2025 and evaluated in this study:

1.	Bitdefender GravityZone Business Security
2.	Broadcom Symantec Endpoint Security Complete
3.	Check Point Harmony Endpoint Prevent
4.	Cisco Secure Endpoint
5.	CrowdStrike Falcon Prevent
6.	ESET Protect Entry
7.	Kaspersky Next EDR Optimum
8.	Malwarebytes ThreatDown
9.	Microsoft Defender for Endpoint Plan 1
10.	Sophos Intercept X Essentials
11.	Trellix Endpoint Security ENS
12.	Trend Micro Vision One Core
13.	Webroot Endpoint Protection
14.	WithSecure Elements EDR and EPP for Computers Premium

LEGAL REVIEW ON AGREEMENTS, COMPLIANCE, AND TRANSPARENCY



LEGAL REVIEW ON AGREEMENTS, COMPLIANCE, AND TRANSPARENCY

This chapter is structured around the six thematic topics defined in the *Test Procedure*, each addressing a key aspect of cybersecurity vendor transparency and data handling practices. Sections begin with a brief introduction, followed by a discussion of vendor practices and observed differences. Where relevant, results are compiled in tables and practical implications for CISOs and enterprise stakeholders are highlighted. Each topic concludes with a concise summary to provide clear takeaways for vendors and customers. The text is written in a deliberately neutral style. Vendors are only named selectively to illustrate specific practices, while most findings are presented collectively. This ensures no vendor is unduly favoured or disadvantaged and a balanced, objective evaluation. Since many vendor agreements and policies, such as EULAs, are formulated in broad or ambiguous terms, leaving room for interpretation, the findings are presented at a higher level to maintain fairness, consistency, and comparability across all vendors.

● Publicly committed
or disclosed by vendor

○ Not publicly committed
or disclosed by vendor

Source Code

The handling of source code is a critical aspect of transparency in cybersecurity products. It determines how software is built, and security measures are implemented and maintained, directly influencing enterprise risk assessments, procurement decisions, and compliance strategies. Vendors, however, must balance customer visibility with protecting intellectual property and product integrity.

VENDOR	CLOSED-SOURCE PRODUCT CODE	THIRD-PARTY SOFTWARE DISCLOSURE	TRANSPARENCY CENTRES ADVERTISED
Bitdefender	●	●	○
Broadcom	●	●	○
Check Point	●	●	○
Cisco	●	●	● Link
CrowdStrike	●	●	○
ESET	●	○	○
Kaspersky	●	●	● Link
Malwarebytes	●	●	○
Microsoft	●	●	● Link
Sophos	●	●	○
Trellix	●	●	○
Trend Micro	●	●	○
Webroot	●	●	○
WithSecure	●	●	○

Proprietary and Closed Source

All tested products are proprietary and closed source, with End User License Agreements (EULAs) explicitly prohibiting reverse engineering, modification, or code examination. This protects vendors' intellectual property and ensures controlled, consistent product updates. However, it limits customers' ability to independently verify security or compliance with internal and regulatory requirements, shifting reliance to vendor assurances, third-party audits, and external certifications.

Third-party Software

All vendors except for ESET confirm that their product includes third-party or open-source software (OSS). ESET makes no explicit statement on the use of third-party or open-source code. Where disclosed, lists of OSS components are either published on the vendor's website or shipped with the product itself. This supports transparency and compliance with open-source licensing obligations. For enterprises, incomplete disclosure practices complicate supply chain risk management.

Transparency Centres

Cisco and Kaspersky advertise global transparency centres where enterprise customers and authorized stakeholders can review and rebuild source code, examine threat detection rules, Software Bill of Materials (SBOM), and development documentation to verify that builds match public releases. Microsoft, through its Government Security Program, offers national and federal agencies access to its transparency centres for source code review and technical documentation of selected products and services as well as threat intelligence information.

Summary

While the closed-source model remains the standard in enterprise cybersecurity, initiatives such as transparency centres and third-party software disclosure represent important steps toward greater trust and verifiability. Customers benefit from these measures by gaining additional assurance, while vendors can strengthen their credibility without fully exposing intellectual property.

Product Updates

The way vendors handle product and content (i.e., virus definition or signature) updates is central to both transparency and operational reliability in cybersecurity solutions. Regular, well-documented updates ensure timely delivery of new features, bug fixes, and security patches. For enterprises, the visibility of update processes and the ability to control deployment influence system stability and risk management. Vendors, in turn, must balance rapid distribution with adequate testing of updates.

VENDOR	PUBLIC UPDATE HISTORY	DOWNLOAD OF DEFINITION UPDATES	AUTOMATIC UPDATES	PRE-RELEASE TESTING OPTIONS	STAGED UPDATE ROLLOUT
Bitdefender	●	●	●	●	●
Broadcom	●	●	●	●	○
Check Point	●	○	●	●	○
Cisco	●	○	●	●	○
CrowdStrike	○	○	●	●	●
ESET	●	○	●	●	○
Kaspersky	●	●	●	●	●
Malwarebytes	●	○	●	●	●
Microsoft	●	●	●	●	●
Sophos	●	○	●	●	●
Trellix	●	●	●	●	●
Trend Micro	●	●	●	●	●
Webroot	●	○	●	●	○
WithSecure	●	○	●	●	○

Update History and Definition Updates

Most vendors publish detailed changelogs or release notes, outlining new features, resolved issues, and fixed vulnerabilities. In addition, **some vendors** provide virus definition histories and make the latest versions available for direct download. These practices enhance transparency by allowing customers to trace both product evolution and threat-detection improvements, while also supporting compliance teams in maintaining reliable audit trails. **CrowdStrike** is an exception, as its update history is accessible only to registered customers via its Falcon console or support portal, which reduces visibility for prospective customers or external reviewers.

Automatic Updates and Pre-release Testing

All tested products support automatic updates, with **most vendors** also enabling manual configuration via policies. This allows administrators to control when and from where updates are retrieved, and to test updates on a limited set of endpoints before company-wide rollout. However, product documentation is not always clear whether this process applies only to product updates, content updates, or both. As an alternative means of pre-release testing, **all vendors** provide Early-Access or beta programs. These programs allow customers to evaluate upcoming features before public release, improving preparedness and enabling proactive compatibility testing.

Update Rollout Practices

Many vendors emphasize best practices in update mechanisms, such as multi-phase staging, rigorous testing, and quality assurance. These measures reduce the risk of faulty updates disrupting production environments, an especially critical concern when automatic updates are enabled by default.

Summary

While most vendors demonstrate strong commitment to transparent and reliable update processes, differences remain in the scope of information disclosed and pre-release testing opportunities for customers. Enterprises should carefully review vendor update documentation, confirm testing practices, and apply phased deployment policies to mitigate risks from faulty updates.

Many vendors emphasize best practices in update mechanisms, such as multi-phase staging, rigorous testing, and quality assurance



Security Posture

A vendor's security posture reflects its commitment to safeguarding its products, services, and infrastructures. For enterprises, practices such as strong vulnerability management, clear disclosure, independent audits, and secure Software Development Life Cycle (SDLC) processes are key indicators of trustworthiness and long-term resilience.

VENDOR	VULNERABILITY REPORTING	SECURITY ADVISORIES	COLLABORATION & SAFE HARBOR	SECURITY AUDIT RESULTS	SECURE SDLC PRACTICES
Bitdefender	●	○	○	○	●
Broadcom	●	○	○	On request only	●
Check Point	●	○	○	On request only	●
Cisco	●	●	●	On request only	●
CrowdStrike	●	●	○	○	●
ESET	●	○	●	○	●
Kaspersky	●	●	●	On request only	●
Malwarebytes	●	○	●	○	●
Microsoft	●	●	●	On request only	●
Sophos	●	●	○	●	●
Trellix	●	○	●	○	●
Trend Micro	●	●	●	○	●
Webroot	●	○	○	On request only	●
WithSecure	●	●	○	○	●

Vulnerability Reporting

All vendors maintain a vulnerability reporting process, though the level of structure and detail varies considerably. **Webroot** relies on a simple reporting method through customer support without guidelines, while vendors such as **Broadcom**, **Check Point**, **ESET**, **Kaspersky**, and **Trellix** provide formalized policies with extensive step-by-step procedures. **Bitdefender**, **Cisco**, **CrowdStrike**, **Kaspersky**, **Malwarebytes**, **Microsoft**, **Sophos**, **Trend Micro**, and **WithSecure** also operate open bug bounty programs with financial rewards for responsible security researchers but may restrict the scope to selected products or vulnerability types. Acknowledging contributors on vendor websites further reinforces collaboration and transparency.

Security Advisories, Researcher Collaboration, and Safe Harbor

Some vendors publish "Security Advisories" listing publicly disclosed vulnerabilities in their products. This enables customers to track security issues and evaluate vendor responsiveness. However, **no vendor** consistently provides metrics on the average time between vulnerability reporting and patching in public disclosures. While understandable due to varying levels of severity and complexity, this lack of clarity makes it difficult to assess remediation speed. **All vendors** publicly commit to cooperating with security researchers. However, **only half** extend this commitment with a "Safe Harbor" statement, providing legal assurances that researchers acting in good faith will not face legal action, which fosters trust and encourages more active engagement from the research community.

Security Audit Results

Vendors regularly conduct internal and external audits, vulnerability assessments, and penetration testing of their products and infrastructures. However, **Sophos** is the only vendor that publishes attestation letters of these evaluations on its website but also offers more detailed reports to requesting customers. **Broadcom**, **Cisco**, **Kaspersky**, and **Microsoft** can provide

full reports of third-party audits and assessments upon request, whereas **Check Point** and **Webroot** provide only summaries or attestations when requested. This limits independent verification but ensures information can be obtained by enterprises during procurement.

Secure Software Development Life Cycle (SDLC) Practices

All vendors adhere to secure SDLC practices. **Check Point** does not make this commitment publicly, though they strongly emphasize "Security by Design" and promote secure SDLC best practices, suggesting that their products follow similar standards. Consistent SDLC adoption is an important assurance for customers, as it reduces the likelihood of introducing vulnerabilities during product design and development.

Summary

All vendors demonstrate baseline commitments to structured vulnerability reporting and researcher collaboration, but transparency on remediation timelines and audit outcomes remains inconsistent. Bug bounty programs, Safe Harbor statements, public security advisories, third-party certifications, and SDLC practices strengthen trust, but enterprises often must request further evidence to holistically evaluate vendor security posture.

Transparency and Policies

Public disclosure of cybersecurity incidents and responses to law enforcement requests are key indicators of vendor transparency. These practices directly influence customer trust, regulatory compliance, and enterprise risk assessments. While vendors must balance openness with security considerations and legal obligations, clear communication remains essential for customers.

VENDOR	INCIDENT RESPONSE	TIMELY, DETAILED DISCLOSURES	LAW ENFORCEMENT REQUEST RESPONSE	TRANSPARENCY REPORT
Bitdefender	●	n/a	○	○
Broadcom	●	n/a	●	○
Check Point	●	n/a	○	○
Cisco	●	●	●	● Link
CrowdStrike	●	●	●	○
ESET	●	n/a	○	○
Kaspersky	●	●	●	● Link
Malwarebytes	●	●	○	○
Microsoft	●	●	●	● Link
Sophos	●	●	●	○
Trellix	●	n/a	●	○
Trend Micro	●	●	●	On request only
Webroot	●	n/a	●	○
WithSecure	○	n/a	○	○

Incident Response

All vendors except WithSecure define contractual clauses that govern how they respond to and disclose cybersecurity incidents, particularly personal data breaches. These typically include commitments to notify customers without undue delay and provide details on the nature, scope, and impact of an incident. Where incidents were made public, **affected vendors** generally delivered timely and informative disclosures, including root-cause analysis, occasionally accompanied by detailed technical explanations, as well as remediation steps, and product or process improvements. At the same time, not every incident might be disclosed, and delays might occur due to ongoing forensic investigations or the need to prevent further exploitation.

Law Enforcement Requests

All vendors comply with lawful requests such as court orders, subpoenas, or government authority mandates, but **not all** explicitly commit to notifying affected customers. To increase openness regarding such data requests, **Cisco**, **Kaspersky**, and **Microsoft** publish regular transparency reports. **Trend Micro** provides them only to competent data protection authorities on request.

ALL VENDORS COMMIT TO PERFORM DUE DILIGENCE ON THEIR SUPPLIERS, ENFORCE CONTRACTUAL OBLIGATIONS

Summary

Most vendors commit to responsible disclosure of cybersecurity incidents and customer notification, but practices differ regarding communication of law enforcement requests and the availability of transparency reports. For CISOs, clear contractual obligations, breach reporting, and transparency reports are critical for compliance and risk management. Enterprises should prioritize vendors with consistent disclosure and reporting practices aligned with regulatory requirements (e.g., GDPR, CCPA).

Third-Party Risk Management

The growing reliance on third-party software, services, and open-source components makes supply chain security a critical concern. Vendors must manage external dependencies to protect product integrity and maintain compliance with industry and legal standards. Enterprises depend on vendors' transparency in managing their supply chains to assess risks, guide procurement, and meet regulatory requirements.

VENDOR	SUPPLY CHAIN MANAGEMENT	SUPPLY CHAIN AUDIT RESULTS	OSS DISCLOSURE	SBOM AVAILABILITY
Bitdefender	●	○	●	○
Broadcom	●	○	●	○
Check Point	●	○	●	○
Cisco	●	○	●	On request only
CrowdStrike	●	○	●	○
ESET	●	○	○	○
Kaspersky	●	○	●	On request only
Malwarebytes	●	○	●	○
Microsoft	●	○	●	○
Sophos	●	○	On request only	On request only
Trellix	●	○	●	○
Trend Micro	●	○	●	○
Webroot	●	○	○	○
WithSecure	●	○	●	○

Supply Chain Management

All vendors commit to perform due diligence on their suppliers, enforce contractual obligations, and regularly assess their compliance. However, audit results are not published, limiting independent visibility into these processes. While they claim to monitor third-party components to prevent shipping known vulnerabilities, there is no guarantee that current builds consistently rely on fully updated libraries.

Software Bill of Materials (SBOM)

Open-source software (OSS) components are commonly used in the products, with **most vendors** publishing lists online or shipping them with the product. **ESET** and **Webroot** do not provide such lists, while **Sophos** shares this information via SBOMs upon request. **Cisco** also makes SBOMs available to customers on request, and **Kaspersky** provides access through their transparency centres.

Summary

While vendor commitments to due diligence and monitoring of third-party components are valuable, the lack of published audit results and incomplete SBOMs restricts external validation. For CISOs, third-party risk management is a growing concern as regulations around software supply chain security, such as NIS2 and the EU Cyber Resilience Act, increase. Enterprises should request SBOMs during procurement, review how vendors track supply chain vulnerabilities, and include disclosure obligations in contracts.

Compliance and Certification

Compliance with international standards, regulatory frameworks, and legal governance is central to vendor transparency and trust. This study primarily focused on GDPR, CCPA, the upcoming EU Cyber Resilience Act (CRA), ISO/IEC 27001, and SOC 2, as these define key requirements for data protection, information security, and supply chain assurance. For vendors, certifications validate security maturity and facilitate global market entry. For enterprises, they provide independent assurance that vendors handle sensitive data responsibly, protect services and infrastructures, and align with global compliance expectations. Only certificates that were valid at the time of this review were included, ensuring that expired or outdated attestations did not influence the findings.

Beyond certifications, the place of jurisdiction specified in vendor contracts is another important factor for trust and accountability. It defines where legal disputes will be settled, and which laws apply. Vendors offering flexible jurisdiction options increase credibility with enterprise buyers across regions, while customers benefit from greater fairness and accessibility compared to a single foreign venue.

VENDOR	GDPR	CCPA	CRA	ISO/IEC 27001	SOC 2 TYPE II	MULTIPLE JURISDICTIONS
Bitdefender	●	○	○	●	●	●
Broadcom	●	●	○	●	●	●
Check Point	●	●	○	●	●	○
Cisco	●	●	○	●	●	●
CrowdStrike	●	●	○	●	●	●
ESET	●	●	○	●	●	●
Kaspersky	●	●	○	●	●	○
Malwarebytes	●	●	○	●	●	●
Microsoft	●	●	○	●	●	○
Sophos	●	●	○	●	●	●
Trellix	●	●	○	●	●	●
Trend Micro	●	●	○	●	●	●
Webroot	●	●	○	●	●	●
WithSecure	●	○	○	●	●	●

Data Protection Laws

All vendors confirm GDPR compliance. CCPA is also widely affirmed, **except for Bitdefender** and **WithSecure**, which have not published explicit confirmation. **None** currently claim compliance with CRA, which is expected given that the regulation is not yet fully in force and obligations will be phased in gradually. Several vendors appear to be preparing for CRA requirements but have not yet published official declarations.

ISO/IEC 27001 and SOC 2 Certification

ISO/IEC 27001 is widely adopted among cybersecurity vendors, though certification scopes vary, ranging from entire organizations to specific departments, products, services, facilities, or processes. This study examined whether vendor build systems, data centres, and managed data or cloud services fall under ISO/IEC 27001 certification, as these represent critical areas for product integrity, physical and operational security, and data security. Based on available certifications and legal agreements, **managed data or cloud services of all vendors** are ISO/IEC 27001 certified. However, in some cases it is unclear whether data centres and build systems are included in the certification scope, requiring enterprises to verify details directly with vendors. **All vendors** are SOC 2 Type II compliant, confirming independent assessment of their security, availability, and confidentiality controls.

ALL VENDORS PARTICIPATE IN REGULAR THIRD-PARTY COMPARATIVE PRODUCT TESTING, WHICH SUPPORTS TRANSPARENCY ON PERFORMANCE AND PROTECTION CAPABILITIES

Other Compliances and Certifications

All vendors participate in regular third-party comparative product testing, which supports transparency on performance and protection capabilities. **All vendors** have achieved additional certifications, including ISO/IEC 27017 (cloud security), ISO/IEC 27701 (privacy), and PCI DSS (payment card data security), or align with frameworks such as ISO/IEC 27032, ISO/IEC 27014, ISO/IEC 27034, DORA, and NIS2. These further strengthen customer trust and demonstrate readiness to operate in highly regulated environments. CISOs are advised to verify specific certifications and scopes directly on vendor websites.

Jurisdiction

The place of jurisdiction often depends on the customer's location or region. Vendors offering multiple jurisdiction options typically group customers into predictable legal hubs (e.g., Ireland for EU, Singapore for Asia-Pacific). This supports compliance with regional regulations, such as EU consumer law, facilitates international market entry, and enhances customer trust, fairness, and accessibility. The trade-off is increased complexity, exposure to unfamiliar legal systems, and additional contract management.

Summary

Most vendors confirm GDPR and CCPA compliance, though none yet claim CRA. ISO/IEC 27001 certification is widespread, especially for managed data and cloud services, but scope clarity varies. All vendors are SOC 2 Type II compliant and participate in regular independent product benchmarks. For CISOs, certifications and compliance declarations are a baseline for vendor selection, but scope must be verified through official certificates or attestation letters rather than logos or generic statements. Where scope is unclear, direct confirmation from

vendor compliance teams may be necessary. Organizations should also rely on accredited testing labs for credible product benchmarks.

Jurisdiction clauses deserve close review, as they determine where disputes are resolved and under which legal framework. Vendors with broader certification portfolios and regionally aligned jurisdictions provide greater assurance of security maturity, legal fairness, and regulatory compliance.

Product Environment, 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 clear data handling practices strengthen vendor credibility and broaden market access. Enterprises require visibility into how and where data is processed, retained, and protected to meet regulatory requirements and manage risks.

VENDOR	OFFLINE CAPABILITIES	ON-PREMISE REPUTATION SERVICE	REGULAR DATA DELETION	DATA ANONYMIZATION
Bitdefender	●	○	●	●
Broadcom	●	●	●	●
Check Point	●	●	●	●
Cisco	●	●	●	●
CrowdStrike	●	○	●	●
ESET	●	Dedicated solution	●	●
Kaspersky	●	●	●	●
Malwarebytes	●	○	●	●
Microsoft	●	●	●	●
Sophos	●	○	●	●
Trellix	●	●	●	●
Trend Micro	●	Dedicated solution	●	●
Webroot	●	○	●	●
WithSecure	●	○	●	●

Isolated Environments

All vendors confirm that their products provide threat protection even when disconnected from the cloud. Depending on the product and setup, offline or air-gapped environments can be supported through configurable policies, relay or proxy servers acting as private clouds, locally mirrored update repositories, or dedicated on-premise solutions. **Many vendors** also provide options for a local reputation service via the private server or on-premise alternative, enabling isolated environments to leverage threat intelligence without relying on external cloud connections. Highly regulated or privacy-conscious organizations should verify that offline capabilities are compatible with internal compliance frameworks before deployment.

Data Deletion and Retention

All vendors generally commit to deleting collected data, including personal information, when no longer needed. Some specify retention periods for different data types, providing greater clarity, while others use broader language such as retaining data "only as long as necessary" or "as required by law". In many cases, deletion is promised within a reasonable period following a deletion request or contract termination. **All vendors** also commit to anonymization, pseudonymization, or aggregation of personal data, though the level of detail in published policies varies.

Data Centre Locations

Almost all vendors disclose the locations of their data centres, either in policies or on their websites. Data centre allocation is typically determined automatically based on customer location or can be selected by the customer (e.g., at order or product setup). To comply with regulatory requirements, **all vendors** maintain facilities in both the EU and North America (NA), with **some** extending coverage to other regions, such as the Middle East (ME) as well as UK, Switzerland, Japan, Asia-Pacific, and Australia. **CrowdStrike** and **WithSecure** provide less clarity: **CrowdStrike** allows customers to choose EU or US hosting at order time, while **WithSecure** states that sensitive data is stored in Finland or the EEA but also uses backend servers outside the region.

VENDOR	PUBLIC DATA CENTRE LOCATIONS	EU DATA CENTRES	NA DATA CENTRES	ME DATA CENTRES
Bitdefender	●	●	●	○
Broadcom	●	●	●	○
Check Point	●	●	●	●
Cisco	●	●	●	○
CrowdStrike	●	●	●	○
ESET	●	●	●	○
Kaspersky	●	●	●	●
Malwarebytes	●	●	●	○
Microsoft	●	●	●	●
Sophos	●	●	●	○
Trellix	●	●	●	○
Trend Micro	●	●	●	●
Webroot	●	●	●	○
WithSecure	●	●	●	○

Data Encryption

Most vendors confirm that customer data is fully encrypted in transit and at rest. **Cisco** specifies that *Secure Endpoint* data is encrypted in transit but stored unencrypted with strict access controls at rest, while *Secure Cloud* data is encrypted both in transit and at rest. **Malwarebytes** provides only a general statement about protective measures without explicitly confirming encryption. **Kaspersky** does not state if data is encrypted at rest.

VENDOR	DATA ENCRYPTION IN TRANSIT	DATA ENCRYPTION AT REST
Bitdefender	Fully supported	Fully supported
Broadcom	Fully supported	Fully supported
Check Point	Fully supported	Fully supported
Cisco	Fully supported	Partially supported
CrowdStrike	Fully supported	Fully supported
ESET	Fully supported	Fully supported
Kaspersky	Fully supported	Not specified
Malwarebytes	Fully supported	Not specified
Microsoft	Fully supported	Fully supported
Sophos	Fully supported	Fully supported
Trellix	Fully supported	Fully supported
Trend Micro	Fully supported	Fully supported
Webroot	Fully supported	Fully supported
WithSecure	Fully supported	Fully supported

Summary

All vendors support offline protection through policies, proxies, local mirrors, or on-premise alternatives, making them suitable for isolated environments. Data retention practices differ, with some vendors specifying timelines, while others use broad legal terms. Most commit to anonymization of personal data. Data centre locations are disclosed by nearly all vendors, typically in the EU and North America (NA), with some extending to other regions. Encryption of data in transit and at rest is standard across most vendors. For enterprises, evaluating offline capabilities, retention policies, data centre locations, and encryption practices is essential for compliance with data protection frameworks. Vendors with clearer disclosures and flexible deployment options provide stronger assurance.

Final Legal Statement

Our legal review of license agreements across the evaluated cybersecurity products reveals several observations regarding the following areas.

Readability

The agreements generally adhere to a conventional legal drafting style. While most vendors employ structured documents with defined headings, the frequent use of complex legal language and lengthy clauses may reduce readability and make comprehension challenging for non-specialist readers.

Comprehensiveness

The agreements cover the essential areas expected in such instruments, but key provisions are often dispersed across multiple documents (commonly the EULA, Privacy Policy, and DPA). While this approach ensures substantive completeness, it creates fragmentation and frequent cross-referencing, limiting overall clarity.

Transparency

Transparency emerged as a relative strength. Most vendors explicitly address critical areas such as data handling, user obligations, applicable law and jurisdiction, and compliance with major frameworks (e.g., GDPR, CCPA). While the level of detail varies between vendors, these disclosures generally enhance legal certainty.

Accessibility

Practices differ significantly. Some vendors provide user-friendly “trust centres” or unified legal hubs that centralize relevant materials, while others scatter key terms across numerous webpages and documents, heavily relying on cross-references. In the latter case, identifying and extracting the relevant information could represent a challenge.

While the reviewed agreements demonstrate solid legal compliance and substantive coverage, their effectiveness could be enhanced by clearer drafting and a more unified presentation. For enterprise stakeholders, this implies that dedicated legal and compliance resources are still required to review and interpret vendor terms. Supplementing agreements with executive summaries, data-handling tables, and consistent terminology would further increase transparency and usability. Together, these measures would not only support enforceability but also foster greater trust and understanding between vendors and enterprise customers.

TECHNICAL ANALYSIS



The following chapters present notable findings regarding both data transmission and the available settings for configuring privacy-relevant aspects of the products.

Data Transmission Behaviour

We analysed the data traffic with a focus on four different categories of information, each of which can include a wide range of features. These categories are:

- Machine related information
- Network related information
- Environmental information
- Personal User data

The following section presents the observations for each category. The tables indicate whether a specific data fragment was observed, denoted by “yes”. **The inverse conclusion cannot be drawn: the absence of a “yes” in the table does not imply that the fragment was not transmitted, or will not be transmitted at any time, only that it was not observed during the testing.**

Machine Information

For machine information, this may involve details such as the machine's serial number, device manufacturer, CPU specifications, or firmware versions. There may be multiple reasons for a vendor to transmit machine-related information to the cloud. From a security perspective, such data can help identify potential weaknesses in specific firmware versions or hardware components. It can also support product improvement by providing insight into hardware-related limitations when analysing crashes or performance issues.

The analysis revealed that vendors transmitted different types of machine information. For instance, firmware versions were sent by **Broadcom**, **Check Point**, **ESET**, **Trend Micro**, and **WithSecure**, while CPU names were transmitted by **Check Point**, **ESET**, **Microsoft**, **Trellix**, **Trend Micro**, and **WithSecure**. In contrast, we were not able to see machine-related information being transmitted for **Cisco**, **Kaspersky**, **Sophos**, and **Webroot**.

	FIRMWARE VERSION	CPU NAME	RAM SIZE	MANUFACTURER NAME	DEVICE SERIAL NUMBER
Bitdefender			yes		
Broadcom	yes		yes	yes	yes
Check Point	yes	yes	yes	yes	
Cisco					
CrowdStrike				yes	yes
ESET	yes	yes	yes	yes	yes
Kaspersky					
Malwarebytes			yes	yes	yes
Microsoft		yes	yes	yes	
Sophos					
Trellix	yes	yes	yes	yes	
Trend Micro	yes	yes	yes	yes	yes
Webroot					
WithSecure	yes	yes	yes	yes	yes

Data fragments listed were identified either in network traffic or within the vendor's web console.

Network Information

Network information can include, for example, MAC addresses, local and public IP addresses, DNS server details, and network interface names. Security products may transmit network information to the cloud for several reasons. From a security perspective, it provides valuable context for detecting threats, for example by revealing unusual traffic sources. Network information also enables vendors to correlate events across multiple endpoints, which is important for identifying coordinated attacks or lateral movement within a company.

All tested products transmitted the local IP address. The external IP address was not explicitly seen for every product; however, since it is inherently required to communicate with the vendor’s cloud console, it is effectively transmitted by all. Concerning the MAC address of the network interface, this was observed for **all products except Kaspersky**. Finally, DNS server addresses were observed only in the data streams of **Broadcom** and **Webroot**.

	INTERNAL IP ADDRESS	EXTERNAL IP ADDRESS	MAC ADDRESS	DNS SERVER ADDRESS	NETWORK INTERFACE NAME
Bitdefender	yes		yes		
Broadcom	yes	yes	yes	yes	
Check Point	yes		yes		yes
Cisco	yes	yes	yes		yes
CrowdStrike	yes	yes	yes		
ESET	yes		yes		yes
Kaspersky	yes	yes			
Malwarebytes	yes		yes		yes
Microsoft	yes		yes		
Sophos	yes	yes	yes		
Trellix	yes		yes		
Trend Micro	yes		yes		
Webroot	yes		yes	yes	
WithSecure	yes	yes	yes		

Data fragments listed were identified either in network traffic or within the vendor’s web console.

Environmental Information

In the area of environmental information, examples range from host names, Windows user-names, Windows SIDs, and machine identification UUIDs to operating system versions, installed applications, running processes, scheduled tasks, or device location. This category can also extend to product-related data such as crash logs, licensing information, or unique endpoint identifiers.

ENTERPRISE CYBERSECURITY PRODUCTS MAY COLLECT ENVIRONMENT DETAILS TO UNIQUELY IDENTIFY DEVICES AND USER ACCOUNTS ACROSS LARGE NETWORKS FOR MANAGEMENT AND LICENSING

Enterprise cybersecurity products may collect such details to uniquely identify devices and user accounts across large networks for management and licensing. Information about operating system versions, installed applications, and scheduled tasks provides context for de-

TECHNICAL ANALYSIS

detecting vulnerabilities or attacks targeting specific software or configurations. Monitoring running processes helps distinguish between normal activity and malicious behaviour, improving detection accuracy. These data points also support incident response by allowing analysts to trace alerts back to specific machines, user accounts, or processes and understand how an attack unfolded. In addition, system and device information assists vendors in troubleshooting issues, ensuring product compatibility, and delivering effective customer support.

	CRASH LOGS	MACHINE UUID	OS VERSION	HOST-NAME	DEVICE / ENDPOINT ID	LIST OF INSTALLED APPLICATIONS	WINDOWS USERNAME	WINDOWS USER SID
Bitdefender		yes	yes	yes	yes		yes	
Broadcom			yes	yes	yes		yes	
Check Point	yes		yes	yes	yes		yes	yes
Cisco		yes	yes	yes	yes		yes	
CrowdStrike			yes	yes	yes		yes	yes
ESET			yes	yes	yes		yes	
Kaspersky			yes	yes	yes		yes	
Malwarebytes			yes	yes	yes	yes	yes	
Microsoft			yes	yes	yes	yes	yes	yes
Sophos			yes	yes	yes		yes	
Trellix			yes	yes	yes		yes	
Trend Micro			yes	yes	yes	yes	yes	yes
Webroot			yes	yes	yes		yes	
WithSecure			yes	yes	yes		yes	

Data fragments listed were identified either in network traffic or within the vendor's web console.

The hostname, the operating system version was transmitted by **all tested products**. This information is useful to identify the host within the corporate network. The Windows username was also transmitted by **all products** in the test. A list of all installed applications was transmitted by **Malwarebytes**, **Microsoft**, and **Trend Micro**.

THE HOSTNAME, THE OPERATING SYSTEM VERSION WAS TRANSMITTED BY ALL TESTED PRODUCTS

Personal User Data

Similarly, personal user data may comprise elements such as file paths and names, file hashes, file contents, or information about websites contacted (including domains, URLs, and query parameters). Enterprise cybersecurity products may collect file paths, names, hashes, and even contents to accurately identify suspicious files and enable deeper analysis for improved detection. Similarly, information about websites contacted, helps determine whether a system is communicating with malicious infrastructure or reveal an infection vector. This category also includes threat related information, like detection names when a file is detected as malicious.

Execution of benign executables on the machine

We saw multiple vendors submitting file names, paths and hashes of clean PE files, such as **Bitdefender**, **Broadcom**, **Check Point**, **Microsoft**, **Webroot**, and **WithSecure**.

We observed a file transmission of **WithSecure**. **Trellix** queried file hashes without providing the file name and file path.

TECHNICAL ANALYSIS

Check Point queried metadata for a locally stored, clean Excel file, including its file hashes and paths. For illustration, an example of such a request is shown below:

```
{
  "request": [
    {
      "resource": "a4562e51cdaaa1dbef3a544440ee2caa",
      "findings": true,
      "summary": true,
      "context": {
        "file_path": "C:\\Users\\User\\Documents\\my_document.xls",
        "file_name": "my_document.xls",
        "file_type": "xls",
        "ck": "CK-FC21104EE111",
        "md5": "a4562e51cdaaa1dbef3a544440ee2caa",
        "sha1": "7288edd0fc3fcb93a0cf06e3568e28521687bc"
      }
    }
  ]
}
```

Browsing websites and downloading benign files

Bitdefender, **Broadcom**, **Check Point**, **Microsoft**, **Sophos**, and **WithSecure** checked domains against a cloud endpoint. **Broadcom** transmitted the full URL, while **Check Point** and **Microsoft** also included query parameters. When files were downloaded via a browser, **Bitdefender**, **Broadcom**, **Check Point**, **Microsoft**, **Sophos**, and **WithSecure** checked the full download URI against the cloud. **Check Point**, **WithSecure**, and **Webroot** additionally checked the file hash of the downloaded file, and **Check Point** uploaded the downloaded Excel sheet to the vendor's cloud.

Malicious Files on the system

For malicious files, **all tested products** transmitted the file name and full path of the infected file. The file itself was uploaded by **Bitdefender**, **Check Point**, and **WithSecure**. In addition, **most solutions** transmitted the detection name to the vendor's cloud.

	FILENAME	FULL PATH	FILE HASH	FILE CONTENT	DETECTION NAME
Bitdefender	yes	yes	yes	yes	yes
Broadcom	yes	yes	yes		yes
Check Point	yes	yes	yes	yes	yes
Cisco	yes	yes	yes		yes
CrowdStrike	yes	yes	yes		
ESET	yes	yes	yes		yes
Kaspersky	yes	yes	yes		yes
Malwarebytes	yes	yes	yes		yes
Microsoft	yes	yes	yes		yes
Sophos	yes	yes	yes		yes
Trellix	yes	yes	yes		yes
Trend Micro	yes	yes			
Webroot	yes	yes	yes		yes
WithSecure	yes	yes	yes	yes	yes

Data fragments listed were identified either in network traffic or within the vendor's web console.

Privacy Related Settings & Transparency

Vendors typically provide administrators with configurable options that determine the extent of telemetry sharing, the reporting of suspicious files, and the integration of cloud-based analytics. These settings often define the balance between maximizing detection efficiency and minimizing the exposure of potentially sensitive organizational data. However, the degree of transparency and configurability varies across solutions, with some products offering granular administrative controls and others relying heavily on vendor-managed defaults.

Privacy Settings Scope

Testing revealed several common configuration options available across products from multiple vendors. These can generally be divided into two categories: global settings and policy-wide settings. Global settings apply to the customer's entire environment and cannot be customized for specific parts of the organization. Policy-wide settings, on the other hand, provide greater flexibility, as they allow certain features to be enabled or disabled within individual policies, which can then be assigned to selected groups of machines across the company.

Reputation Services

Configuration options related to reputation services were observed, which can be enabled or disabled as needed. These services provide additional contextual information about files or websites, such as verdicts or prevalence statistics. To achieve this, the endpoint sends a query to the service containing details about the object under analysis, for example, a file hash or a domain. The main advantage of reputation services is access to the most up-to-date intelligence about an object, extending beyond the boundaries of the company itself. A potential drawback, however, is that the service provider gains visibility into the domains accessed or file hashes present within the organization.

File Uploads & Sample Sharing

Settings related to the upload of detected files were also identified. For example, when the behaviour analysis of an antivirus solution flags a previously unknown file as malicious, the file may be uploaded to the vendor's cloud for further inspection. This approach offers several benefits. The vendor can perform an in-depth analysis, potentially creating new virus signatures that enhance protection for all customers. Additionally, the file may be executed in a secure sandbox environment, allowing the vendor to study its behaviour and intent without risking infection of production systems. Some vendors even provide administrators with the option to download quarantined files directly from the management console for internal analysis. However, file uploads also pose clear risks, as they may contain sensitive information that is then shared with a third party. To mitigate this, certain vendors allow restrictions on the types of files that can be uploaded, for example, permitting only PE files while excluding documents. Ultimately, a balance must be struck between privacy and security, since excluding certain file types (e.g., documents) could prevent the detection of malicious content, such as macro-based attacks, if those files are not uploaded to the sandbox.

Collection of Contextual Data

Continuously collecting contextual data during normal company operations helps differentiate between legitimate and malicious behaviour, and it provides valuable insight for responding more quickly to an active compromise. This approach is commonly associated with Endpoint Detection and Response (EDR). The drawback, however, is evident: unlike the previous examples where data is only collected and shared during detection events, EDR continuously gathers and uploads information, even when no malicious activity is present. In this test, the scope of EDR data collection was generally not configurable, with most solutions offering only a simple choice between enabling or disabling the feature.

Product Usage Statistics & Crash Reports

Finally, several products provide settings to enable or disable the sharing of product usage statistics and crash reports. Sharing this data helps vendors improve their products and detect software issues. Some vendors claim to anonymize the data before sharing, ensuring that personal information is not included.

The following sections present some privacy-related configuration options identified in the tested enterprise cybersecurity products, with attention to the level of control offered to administrators and the clarity of vendor communication.

Bitdefender

Some settings can be configured at the policy level, which allows different configurations for subsets of machines. These include checkboxes to: allow sending quarantined items to Bitdefender Labs, submit crash reports to Bitdefender, submit suspicious files for analysis, send feedback on the health of security agents, and use the Bitdefender Global Protective Network to enhance protection.

☒

Submit crash reports to Bitdefender

☒

Submit suspicious files for analysis

Changing this setting requires an endpoint restart.

☒

Send feedback regarding security agents' health

☒

Use Bitdefender Global Protective Network to enhance protection

Other settings apply globally. These include checkboxes to enable the submission of crash reports to Bitdefender, send feedback on the health of Security Servers, and “*use Bitdefender Global Protective Network to enhance protection.*”

Broadcom

The following settings can be configured at the policy level, allowing different configurations for subsets of machines. Users can choose to enable or disable the pseudonymous submission of suspicious files to Symantec to enhance threat intelligence. Within the Detection and Response section, users can turn the “Activity Recorder” on or off and configure its transmission intervals. Additionally, users can define exceptions, based on file hashes or file paths, to exclude specific files from the Activity Recorder.

Endpoint Activity Recorder Configuration ⓘ

Configure the global policy for Symantec Endpoint Security managed clients.

Database Size

1

GB

▼

Send Events interval

☒

Near real-time

☐ Hourly Upload

Show Advanced

Endpoint Activity Recorder Rules ⓘ

Configure the recorder rules for Symantec Endpoint Security managed clients.

GROUP BY

Windows

Linux

macOS

Rules list (Showing 0 to 0 of 0)

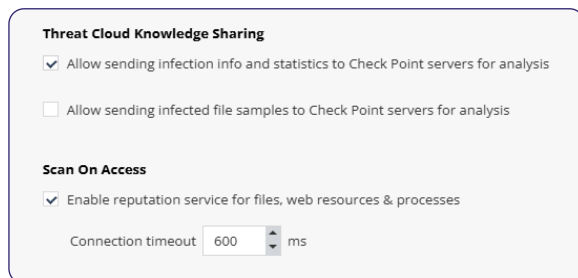
☒

PRIORITY

☐RULE TYPE

Check Point

The product includes several checkboxes, such as "Allow sending infection info and statistics to Check Point servers for analysis", "Allow sending infected file samples to Check Point servers for analysis", and "Enable reputation service for files, web resources and processes." In addition, Check Point provides automated attack analysis (forensics), which includes the Threat Hunting feature. Threat Hunting can be enabled or disabled, and the vendor explains this feature as follows: "With Threat Hunting enabled, Check Point securely maintains raw forensics data to facilitate additional personal security functionality for your use. You may opt-out of Threat Hunting at any time." A support mode can be enabled for the tennant.



Threat Cloud Knowledge Sharing

☒ Allow sending infection info and statistics to Check Point servers for analysis

☐ Allow sending infected file samples to Check Point servers for analysis

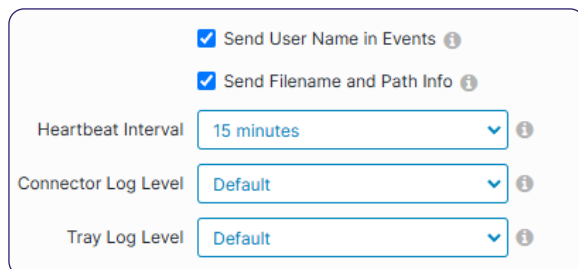
Scan On Access

☒ Enable reputation service for files, web resources & processes

Connection timeout ms

Cisco

The following settings can be configured at the policy level, allowing different configurations for subsets of machines. Users can choose whether to transmit usernames, filenames, and path information in events, enable automated crash dump uploads, or enable or disable the SPERO engine (the cloud-based heuristics engine). Additionally, users have the option to opt out of using Google Analytics.



☒ Send User Name in Events ⓘ

☒ Send Filename and Path Info ⓘ

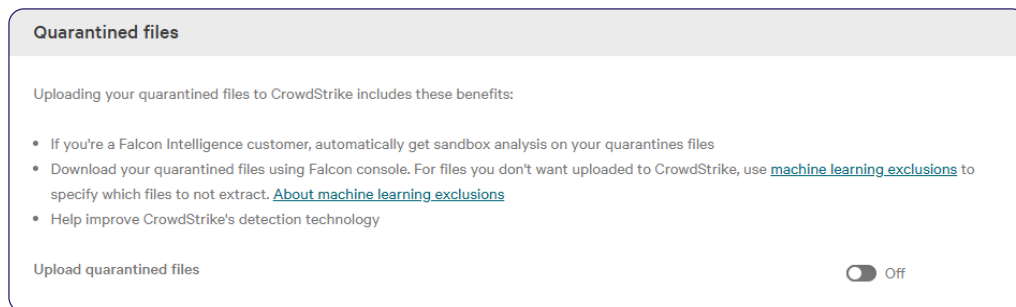
Heartbeat Interval ⓘ

Connector Log Level ⓘ

Tray Log Level ⓘ

CrowdStrike

Users can choose whether to upload quarantined files. This enables automated sandbox analysis, allows quarantined files to be downloaded from the console, and helps CrowdStrike improve its technology. At the policy level, users can also enable or disable the "Redacted HTTP" feature, which removes certain information from HTTP detection events, such as URLs, headers, and POST bodies, that may contain personal data.



Quarantined files

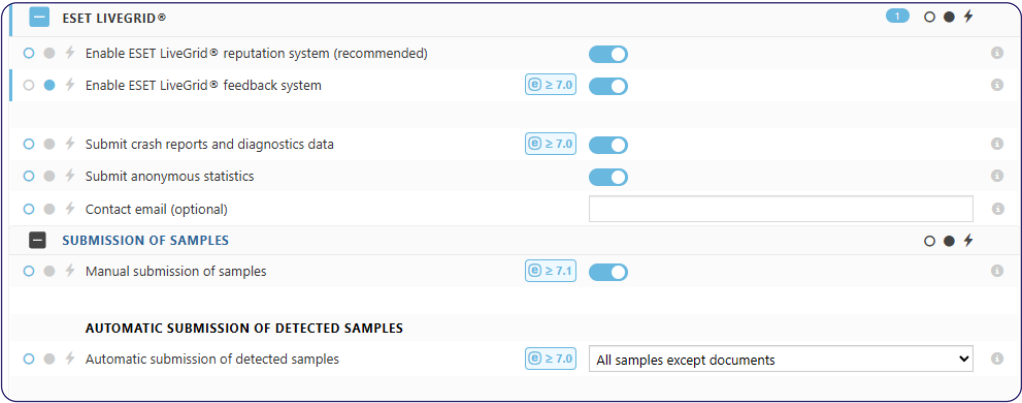
Uploading your quarantined files to CrowdStrike includes these benefits:

- If you're a Falcon Intelligence customer, automatically get sandbox analysis on your quarantined files
- Download your quarantined files using Falcon console. For files you don't want uploaded to CrowdStrike, use [machine learning exclusions](#) to specify which files to not extract. [About machine learning exclusions](#)
- Help improve CrowdStrike's detection technology

Upload quarantined files ☐ Off

ESET

The following settings can be configured at the policy level, allowing different configurations for subsets of machines. Users can choose to enable or disable the Live Grid reputation system (recommended by ESET), the Live Grid feedback system, the submission of crash reports and diagnostic data, and the submission of anonymous statistics. Administrators can allow users to manually submit files, and they can also enable or disable automatic submission of detected samples by ESET. Sample submission can be restricted by file type, including executables, archives, scripts, other files, or possible spam emails. It is also possible to define excluded file extensions and set a maximum file size for submissions. Additionally, the LiveGuard feature, a cloud-based layer for detecting never-before-seen samples, can be enabled or disabled, along with the option to submit documents to LiveGuard.



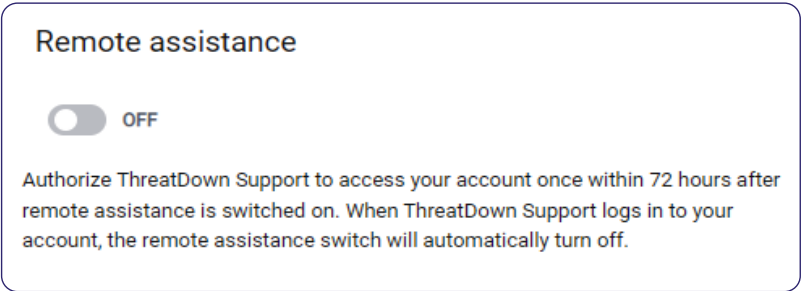
Kaspersky

The “Kaspersky Security Network (KSN)” feature can be disabled at the global level. Similarly, the “Endpoint Detection and Response” (EDR) component, which “monitors and analyses threat progression and provides you with information about possible attacks”, can also be disabled globally.



Malwarebytes

User can enable remote assistance to allow the ThreatDown support to access the account once within 72 hours.



Microsoft

The following settings can be configured at the policy level, allowing different configurations for subsets of machines. Users can choose whether to “*Allow Cloud Protection*”, in which case “*Windows Defender will send information to Microsoft about any problem it finds*”. For sample submission, multiple consent levels are available: “*Never send*”, “*Always prompt*”, “*Send safe samples automatically*”, and “*Send all samples automatically*”. It is also possible to disable the “*Core Service Telemetry*”. When using EDR, administrators can choose between sharing “*None*” of the samples or “*All*”.

The screenshot shows a configuration window with several settings:

- Submit Samples Consent**: A dropdown menu currently set to "Not configured". The expanded list shows options: "Not configured", "Always prompt.", "Send safe samples automatically. (Default)", "Never send.", and "Send all samples automatically."
- Disable Local Admin Merge**: A toggle switch with an information icon.
- Allow On Access Protection**: A toggle switch with an information icon.
- Threat Severity Default Action**: A section header.
- Remediation action for High severity threats**: A dropdown menu currently set to "Not configured".
- Remediation action for Severe threats**: A dropdown menu currently set to "Not configured".

Sophos

Sample submission can be turned on or off “*for improved security*”, with Sophos explicitly recommending that the feature remain enabled. Users also have the option to enable or disable uploads to the “*Data Lake*”, which is necessary to run queries on this data. Additionally, users can enable or disable “*Live Protection*” on a policy level, to access the latest threat information from SophosLabs online. A clear note next to this setting warns that “*the data may leave your geographic region and be shared with Sophos engineers*”.

The screenshot shows a toggle switch labeled “Submit sample files to Sophos automatically”. Below the toggle, a note states: “Some Sophos products can send us samples of suspicious files to help us protect you better. We recommend that you turn this option on. See [Sophos Group Privacy Notice](#).”

Trellix

Users can enable or disable “*cloud-based scanning*” and the option to “*send files not yet verified for analysis*”. They can also enable or disable Trellix GTI (Global Threat Intelligence), which is a reputation service, as well as the submission of anonymous diagnostic and usage data to Trellix via “*Trellix GTI feedback*” and “*Safety Pulse*”. Additionally, users can enable or disable sending events to “*Trellix ePO*” and control agent-to-server communication. Finally, users can choose whether to allow Trellix to collect usage, threat, and diagnostic data.

The screenshot shows a section titled “Proactive Data Analysis (Windows & Linux only)”. It contains the following settings:

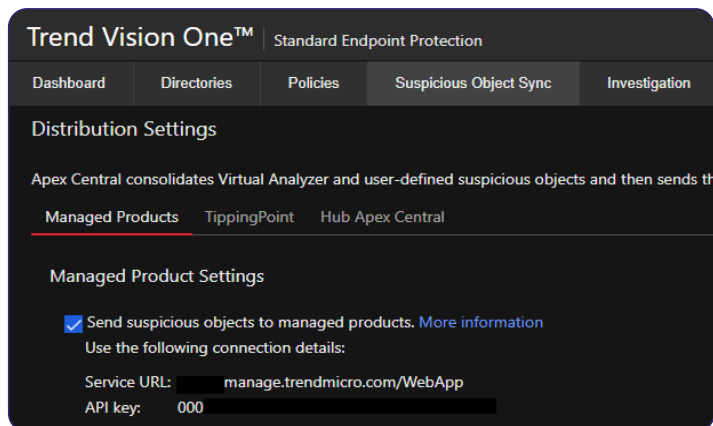
- Send anonymous diagnostic and usage data to Trellix:**
 - ☒ Trellix GTI feedback
 - ☒ Safety Pulse (Windows only)
- Check AMCore Content before installation:**
 - ☒ AMCore Content Reputation (Windows only)

Trend Micro

Users can enable or disable “*Endpoint Sensor Detection and Response*” as well as “*Advanced Risk Telemetry*”, a feature that analyses the endpoint for potential security weaknesses. Within the “*Suspicious Objects Sync*” section of the policy, users can enable or disable the option to “*send suspicious objects to managed products*”. Users can also choose whether to allow support staff to enable logging and access the console for troubleshooting, and whether Trend

TECHNICAL ANALYSIS

Micro support engineers are permitted to collect diagnostic packages from Endpoint Security. A note clarifies that this data will be stored in the Azure cloud in the US region and deleted after 21 days.



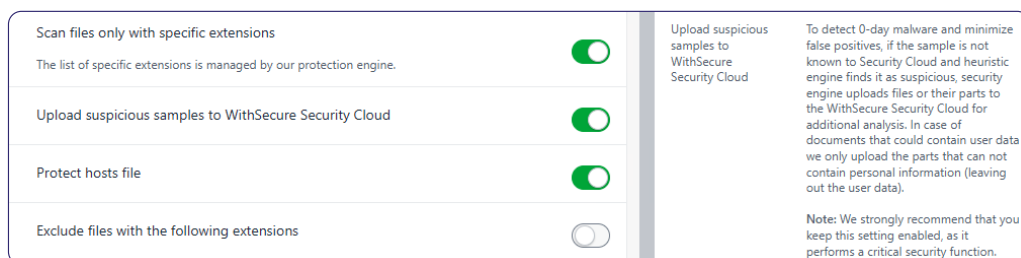
Webroot

The following settings can be configured at the policy level, allowing different configurations for subsets of machines. Users can enable or disable *Enhanced Support* and *Show Infected Scan Results*, although the user interface does not provide descriptions of what these settings entail. According to the documentation, enabling these options results in *logs being sent to customer support*. Users can also choose to enable or disable the upload of files for threat research.



WithSecure

Users can choose to enable *Advanced Response*, which allows administrators to investigate attacks occurring within the environment. A note indicates that this feature provides access to sensitive information and is disabled by default for that reason. Users must confirm that they are legally permitted and have the necessary consents to enable it. Additionally, users can enable or disable the upload of suspicious samples to the WithSecure Security Cloud. WithSecure notes that, for documents, only the parts not containing personal information are uploaded and recommends keeping this feature enabled. Users can also enable or disable *Reputation-based Browsing*, which evaluates a website's reputation using data collected by the WithSecure Security Cloud. It is possible to decide if the URL should be part of security events. The vendor notes, that some regional legislation may limit the right to enable the feature. Finally, users have the option to opt out of analytics on portal usage, with a note clarifying that no data is shared with third parties.



CONCLUSION, LIMITATIONS, REMARKS



Conclusion

Transparency is a cornerstone of trust between cybersecurity vendors and their customers. The topics examined in this study, ranging from source code and product updates to security posture, third-party risk management, compliance, and data handling, highlight the balance vendors must strike between openness and protecting intellectual property, market competitiveness, or legal obligations.

For vendors, greater transparency in areas such as update rollout processes, SBOM availability, data storage practices, and jurisdiction clauses can strengthen credibility, facilitate regulatory compliance, and foster long-term customer relationships. Publishing clear disclosures on vulnerabilities and customer data requests, certifications, and incident response allows customers to make informed decisions without undermining vendor security or business models. At the same time, maintaining limits on sensitive information such as source code is reasonable to prevent misuse.

For CISOs and enterprise stakeholders, transparency should be a key evaluation criterion in vendor selection. Practical steps include:

- **Verifying certifications and compliance** through official attestations rather than relying on logos or general claims.
- **Requesting SBOMs and retention policies** to improve supply chain assurance and privacy compliance.
- **Reviewing incident response and Safe Harbor commitments** to ensure vendors support timely, fair disclosure without discouraging researcher collaboration.
- **Checking jurisdiction clauses and data centre locations** to confirm that dispute resolution mechanisms and data storage align with organizational legal and regulatory requirements.
- **Assessing offline capabilities and deployment options** for suitability in air-gapped or regulated environments.

FOR CISOs AND ENTERPRISE STAKEHOLDERS, TRANSPARENCY SHOULD BE A KEY EVALUATION CRITERION IN VENDOR SELECTION

CISOs should make use of vendor online resources such as dedicated “trust centres” or “privacy centres”, where legal, compliance, and transparency information is often consolidated and easier to access. Vendors are encouraged to establish and maintain such pages to improve accessibility and strengthen customer confidence.

Ultimately, cybersecurity vendors that combine structured transparency with responsible limits provide the strongest assurance of maturity and accountability. Enterprises that conduct diligent verification and align vendor practices with internal and regulatory requirements will be best positioned to achieve effective protection, compliance, resilience, and lasting trust.

When configuring cybersecurity solutions for enterprises, administrators should carefully enable only those features that are truly required for their environment, rather than activating all available options by default. Each setting should be evaluated not only in terms of its security benefits but also with respect to its impact on privacy, as many features involve the collection or transmission of sensitive data. Striking the right balance between protection capabilities and data minimization is essential: enabling too little may leave the organization exposed, while enabling too much may unnecessarily compromise user privacy. Thoughtful configuration helps ensure that both security and privacy requirements are met in a responsible and effective manner.

Limitations

This study does not provide a comparative product ranking, as it would not meaningfully reflect the complexity of the subject. Contractual clauses and regulatory obligations can vary by customer region or jurisdiction, and many agreements are written in broad terms open to interpretation. Vendor practices also change over time in response to new regulations, audits, or product updates, so any static ranking would quickly lose relevance. In addition, certifications differ in scope and enterprises prioritize different factors, making direct comparison impractical. Finally, vendors balance transparency with confidentiality differently, withholding details to reduce security risks or misinterpretation. Instead of assigning scores or rankings, the analysis highlights vendor practices in a structured, thematic way, enabling stakeholders to interpret the findings in line with their own regulatory, operational, and risk management needs.

Technical limitations in the analysis of data transmission were anticipated, as described in the *Test Procedure*. Transmitted data may be encrypted, or other measures may hinder traffic inspection. The absence of a specific data fragment in the analysis does not necessarily indicate it was never transmitted, nor that it will not be transmitted at a later time. Moreover, only the traffic between the endpoint and the vendor cloud was observable, leaving it unclear whether data is shared with third parties or transferred to other geographic locations after reaching the vendor data centres.

THIS STUDY DOES NOT PROVIDE A COMPARATIVE PRODUCT RANKING, AS IT WOULD NOT MEANINGFULLY REFLECT THE COMPLEXITY OF THE SUBJECT

Legal agreements, such as EULAs, Privacy Policies, and Data Processing Agreements, do specify concrete categories of data collected and processed. However, these descriptions are often vague and presented as examples rather than exhaustive lists. As a result, direct comparison with the captured network traffic is not feasible, and the findings should be interpreted as thematic observations rather than precise one-to-one validations. Some vendors, including **Cisco**, **ESET**, **Kaspersky**, **Malwarebytes**, **Microsoft**, **Sophos**, **Trellix**, and **Trend Micro**, seem to provide more comprehensive data category descriptions regarding what may be transmitted.

In summary, the conclusions presented in this study represent one possible interpretation of the terminology used by vendors in their legal documentation. The technical analysis reflects data observed during specific test conditions; while the results are reliable, differing outcomes in future testing cannot be conclusively ruled out.

Remarks

In March 2022, the German Federal Office for Information Security (BSI) issued a public warning against the use of Kaspersky antivirus products, which continues to be referenced in inquiries to WKO. The warning was not based on identified technical vulnerabilities but was issued in light of the geopolitical situation. As any antivirus software operates with deep system-level privileges, the BSI considered the potential of Russian state influence over the company to be a security concern. In response, Kaspersky rejected the allegations, emphasizing that the decision was politically motivated rather than evidence-based. The company highlighted its measures to ensure transparency and independence, including relocating data processing to Switzerland and implementing independent source code audits. Within the scope of this study, no deviations in Kaspersky's practices compared to other vendors were observed.

APPENDIX: SURVEY RESULTS



To better understand the role of transparency and trust in enterprise cybersecurity products, qualitative expert interviews were conducted with a total of selected 60 participants to gain deeper insights into user perspectives. The majority of respondents were based in Austria, primarily drawn from members of the Chamber of Commerce (WKO), with Europe as the primary region of operations.

The survey captured viewpoints across a **wide spectrum of professional roles**, ranging from IT administrators and CISOs/CIOs to owners and C-level representatives. This diversity provides a comprehensive picture of both operational and strategic priorities in cybersecurity decision-making. Participants also represented a **mix of company sizes**, from small businesses (<25 employees) to large multinational corporations (>1,000 employees), ensuring the findings reflect the needs and challenges of organizations of different scales.

SURVEY DIVERSITY PROVIDES A COMPREHENSIVE PICTURE OF BOTH OPERATIONAL AND STRATEGIC PRIORITIES IN CYBERSECURITY DECISION-MAKING

Overall, the survey provides a solid foundation for evaluating how organizations assess cybersecurity products, what they value most, and where they see gaps or opportunities for improvement.

Regulatory Environment

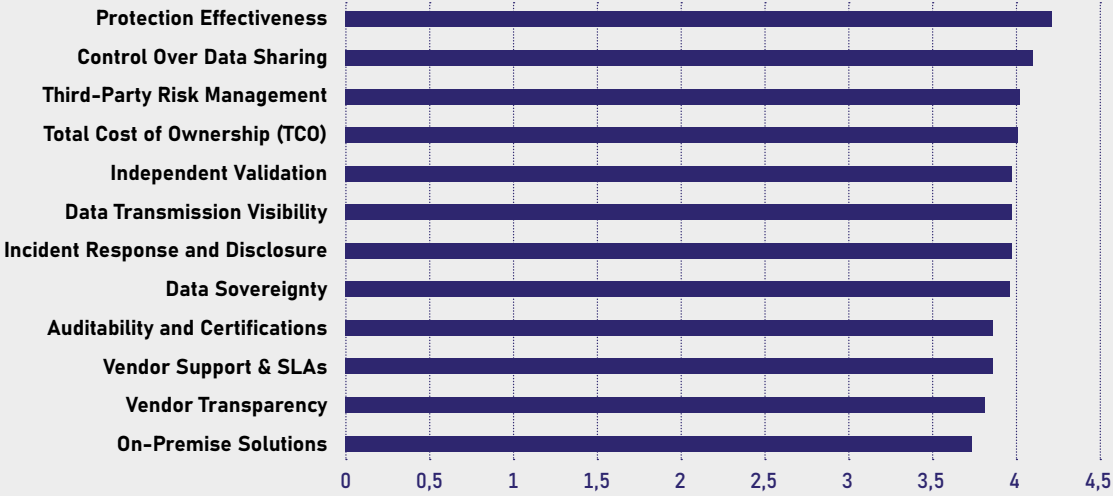
Participants were asked if their organization is subject to specific regulatory frameworks that affect IT security product choice. The survey results suggest that many have **only a limited understanding** of which regulatory frameworks apply to them, pointing to a noticeable knowledge gap. While C-level representatives often showed less familiarity with regulatory details, CISOs, IT managers, and administrators demonstrated a stronger grasp of compliance requirements. This contrast highlights how regulatory knowledge is concentrated at the operational and technical levels rather than at the strategic decision-making level. The findings indicate that although compliance is recognized as an important factor in cybersecurity, organizations may benefit from **improving awareness of regulatory frameworks** across all leadership levels to ensure that product choices and deployment strategies are aligned with legal and security obligations.

While C-level representatives often showed less familiarity with regulatory details, CISOs, IT managers, and administrators demonstrated a stronger grasp of compliance requirements



Priorities and Concerns

The survey reveals that organizations consistently rate cybersecurity product transparency and effectiveness highly, with average scores ranging from **3.75 to 4.23** (out of 5.0). The most critical considerations are **protection effectiveness** and **control over data sharing**, while **on-premise solutions** and **vendor transparency** are considered less important. More insights on these results, along with the specific questions asked, are provided below. Overall, respondents value core protection, data control, and risk management above all else, while cost and vendor-related aspects remain important but secondary.



Protection Effectiveness (4.23): *How important is the proven ability of a cybersecurity product to detect and block threats (e.g., malware, ransomware, phishing) in your organization?*
The highest-rated factor, reflecting that organizations prioritize solutions that provide strong, reliable protection against threats. This confirms that effectiveness in core security is the ultimate decision driver.

Control Over Data Sharing (4.11): *How critical is the ability to configure or limit what data is shared with the vendor (e.g., disable telemetry or sample submission)?*
Respondents strongly emphasize the ability to control how and what data is shared with the vendor. This highlights concerns about data misuse and the need for robust governance features.

Third-Party Risk Management (4.03): *How important is it that vendors disclose and manage their use of third-party and open-source components?*
Rated very highly, showing that organizations expect vendors to actively manage risks within their supply chains and partner ecosystems. This reflects the growing importance of resilience against indirect vulnerabilities.

Total Cost of Ownership (TCO) (4.02): *How important is transparency around licensing models, hidden costs, and long-term TCO?*
TCO is a key consideration, balancing financial sustainability with security effectiveness. Organizations clearly factor in long-term operational costs when evaluating solutions.

Independent Validation (3.99): *How valuable are independent third-party tests and benchmarks when assessing a product's protection and performance?*
While respondents see value in certifications and third-party validation, it is less decisive than direct security effectiveness. It is viewed as supportive rather than primary.

APPENDIX: SURVEY RESULTS

Data Transmission Visibility (3.98): *How important is full visibility into what data (e.g., telemetry, logs, threat samples) is transmitted from endpoints to the vendor?*

Transparency in data transfers is important to respondents, showing a need for monitoring and compliance with privacy regulations.

Incident Response and Disclosure (3.98): *How critical is it that vendors commit to transparent incident reporting, timely breach notifications, and disclosure of law enforcement data requests?*

Organizations value vendors who provide timely incident disclosure and clear response processes, underlining the importance of trust and accountability in crisis situations.

Data Sovereignty (3.97): *How important is the ability to ensure that customer data is stored and processed exclusively within designated regions (like the EU)?*

Knowing where data is stored and processed remains important, reflecting concerns about legal jurisdictions and compliance with national or regional data protection laws.

Auditability and Certifications (3.87): *How important is vendor compliance with recognized security standards (e.g., ISO/IEC 27001, SOC 2) and the availability of audit reports or attestations?*

Auditability is relevant but not as critical as proactive measures like data control and risk management. Organizations prefer real-time control over retrospective validation.

Vendor Support & SLAs (3.87): *How valuable is high-quality technical support and clear service-level agreements (response time, uptime guarantees)?*

Support quality and service-level agreements are valued, but respondents prioritize product performance and risk mitigation over contractual guarantees.

Vendor Transparency (3.82): *How valuable are vendor transparency resources (e.g., trust centres online and onsite, SBOMs, security practices, data retention, data centre locations) for your procurement decisions?*

Although important, vendor openness is considered less critical compared to technical and operational factors. This may reflect a focus on outcomes rather than promises.

On-Premise Solutions (3.75): *How important is it for your organization to have access to on-premise alternatives (e.g., management servers, private reputation services) instead of relying solely on vendor cloud services?*

The lowest-rated factor, indicating that traditional on-premise deployment is less of a priority. This aligns with the broader shift toward cloud-based and hybrid security solutions.

Improvements and Future Priorities

When asked participants what vendors should improve most regarding data transparency in cybersecurity products, the responses revealed a clear set of recurring themes. Most participants emphasized **transparency and visibility** as their top concern. This included calls for greater clarity on data collection, processing, storage, AI/ML model usage, third-party sharing, and the ability to track data flows in detail. Respondents also highlighted the importance of certifications, supply chain risk disclosures, and transparent incident reporting as trust-building measures.

Alongside transparency, participants also mentioned **cost and pricing**, calling for lower prices and more openness about hidden costs. Others highlighted the need for **stronger security and AI capabilities**, while some pointed to **better customer support and usability**, including clearer instructions and more responsive service. A notable portion of respondents indicated **no specific improvements** or stated they were unsure, suggesting either satisfaction with current practices or limited awareness of transparency issues.

Overall, the findings underscore that transparency is the dominant priority, with organizations demanding greater openness and accountability from vendors. At the same time, attention to pricing, usability, and security demonstrates that customers expect a balanced approach, combining trust and compliance with affordability, ease of use, and robust protection.

IMPRINT

Publisher

AV-Comparatives GmbH
Grabenweg 68, 6020 Innsbruck, Austria
www.av-comparatives.org

In Cooperation With

Tyrol Chamber of Commerce – Division of Management Consulting, Accounting, and IT (UBIT)
Wilhelm-Greil-Strasse 7, 6020 Innsbruck, Austria
www.wko.at/tirol

MCI | The Entrepreneurial School®
Universitätsstrasse 15, 6020 Innsbruck, Austria
www.mci.edu

Studio Legale Tremolada
Avv. Matteo Tremolada, Milan, Italy

©2025 AV-Comparatives GmbH, MCI | The Entrepreneurial School(R), and Studio Legale Tremolada.
All rights reserved.
Reproduction or distribution, in whole or in part, is permitted only with prior written consent of the publisher.
This publication is provided for informational purposes only and does not constitute legal advice.