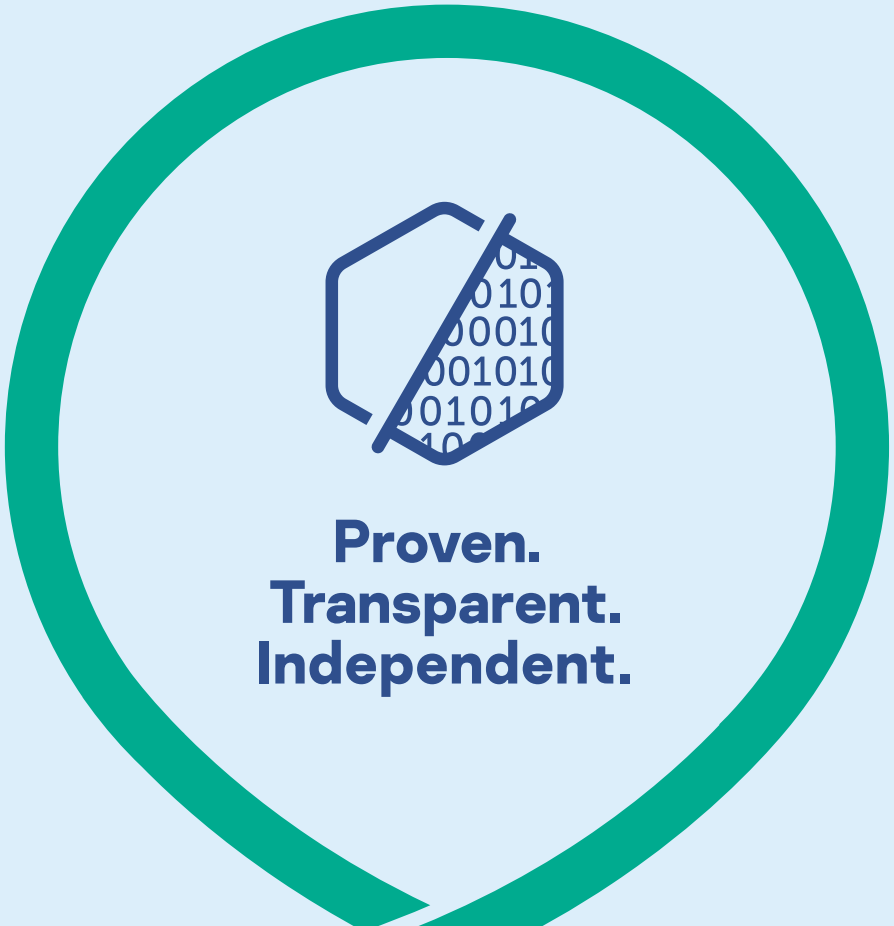
Global Transparency Initiative

Our goal is to provide the tools and conditions needed to validate the integrity and reliability of Kaspersky's products to corporate customers, partners and regulators.



What is the Global Transparency Initiative?

The Global Transparency Initiative (GTI) is a set of measures we have implemented to ensure the transparency and reliability of our products, as well as our development and business processes. Thanks to the GTI, our corporate customers, partners and regulators can visit our specialized centers to review the source code of the Company's products and learn more about our data processing principles. In addition, by receiving feedback from the expert community, our employees understand exactly what we need to improve in terms of transparency, process maturity and ensuring product safety.

How the GTI emerged and has evolved

Kaspersky initially initiated the GTI following requests from regulators seeking insight into the operational details of our products, including data processing methods, storage locations, and other aspects of our work. Since 2017, we have been working on a set of initiatives that aim to strengthen the trust of our corporate customers and partners. This includes opening Transparency Centers, independent audits of the security and reliability of our development processes, and an initiative to relocate the cyberthreat related data processing infrastructure to data centers in Switzerland.

Numerous other measures have subsequently been adopted as part of the GTI:

- Independent analysis of source code, software updates and threat detection rules.
- Regular independent assessment of the secure development process.
- The opening of Transparency Centers around the world.
- Updates of the bug bounty[1] program which includes an increase of the reward for identification of the most serious vulnerabilities in Kaspersky software.
- Training seminars on supply chain security and methods for assessing the reliability of ICT[2] products.
- Creation of additional infrastructure in Switzerland to store and process malicious or suspicious files from users opting in to participate in our Kaspersky Security Network cloud system.
- The continued publication of transparency reports showing how many requests for data the Company receives from law enforcement and government agencies.
- The continued development of educational programs, such as the Cyber Capacity Building Program, which aims to improve specialists' skills in the security of ICT products.

In 2023, Kaspersky celebrated the fifth anniversary of the GTI, which continues to evolve as it adapts to the changing conditions and demands of the cybersecurity market.

GTI results over five years

>US$8,4 million
investment in the development of GTI since 2018

2
data centers in Zurich

11
Transparency Centers around the world

60 reviews
of the Company's products at Transparency Centers

2
independent audits of SOC 2 and ISO 27001 annually

>US$81,000
paid for 59 bug bounty reports

[1] A software bug and vulnerability bounty program that is typically used by application and network platform developers to identify security problems in their products. The program generally rewards enthusiasts for reporting bugs that could be exploited by attackers. Sometimes the reward may consist of access to a paid online service or recognition in a professional community.

[2] ICT – information and communication technologies.

How the GTI works

GRI 3-3

Kaspersky's Global Transparency Initiative is not just a set of measures. It is a strategic focus that aims to create a reliable, secure and transparent digital space for all parties.

Essential components of the GTI

1

Source code review for corporate and regulators

- One of the key elements of the GTI is the ability for stakeholders to independently verify the source code of Kaspersky's products and our data practices.

2

Collaboration with experts

- Another important GTI element is the ability to actively collaborate with independent experts and organizations. We invite experts from around the world to test our systems and products, enhancing confidence in their reliability even further.

3

Training and education

- The GTI promotes cybersecurity education, something Kaspersky actively promotes through various global initiatives to raise awareness among its users and partners about the importance of security in the digital world.

How we ensure the transparency of our products and business processes

TC-SI-220-a.4

Objective

Strengthen public trust in the Kaspersky's products and activities

In an effort to reassure our corporate customers, users, partners and industry regulators of the security and high quality of our products and technologies, we constantly make improvements to the GTI by continuingly disclosing more data about our processes, and undergo audits and certifications. Feedback from our stakeholders enables us to understand which issues require special attention in terms of transparency, process maturity, while ensuring the safety of our products.

Solutions

Transfer data to secure data centers

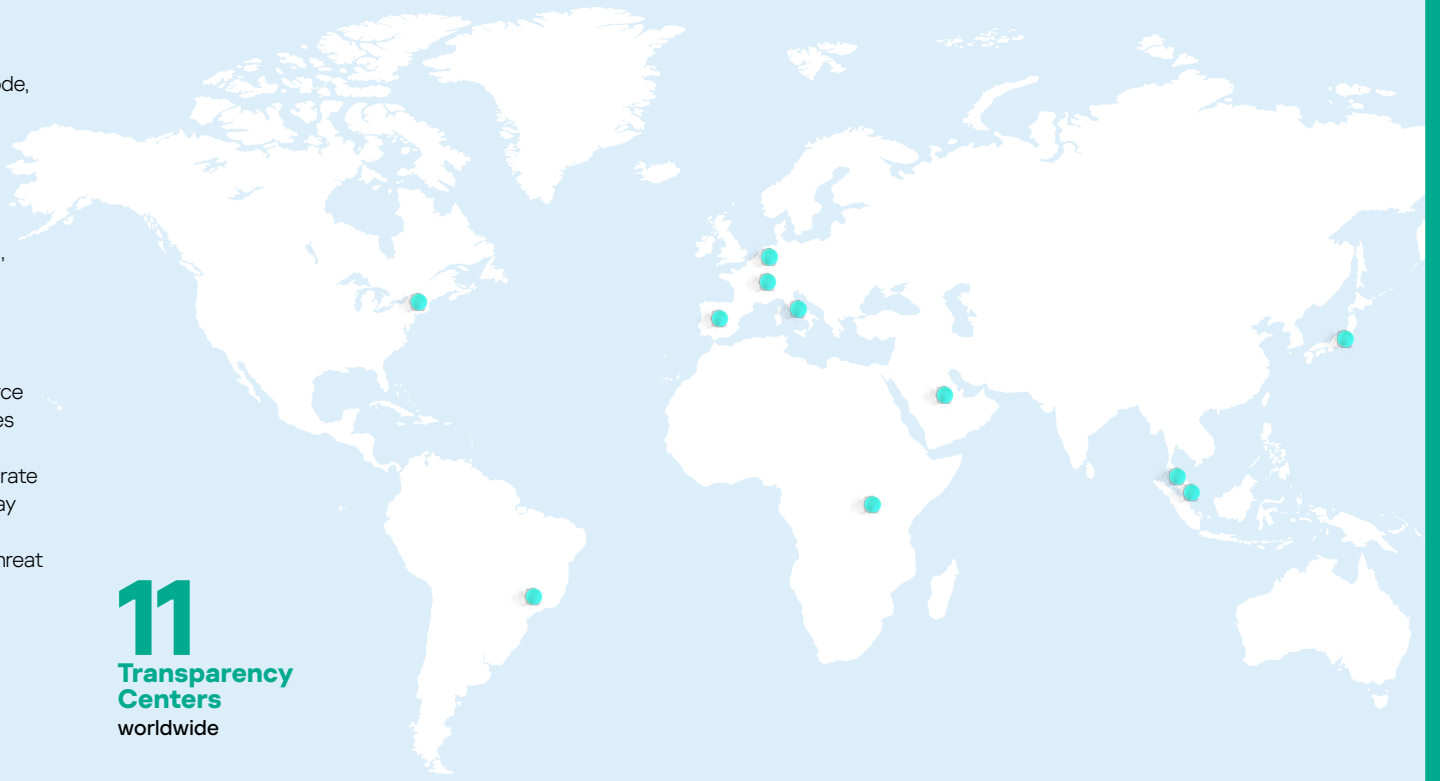
One of the first GTI steps was to commence the process of relocating Kaspersky's cyberthreat related data processing infrastructure and storage. To achieve this, we built two data centers in Switzerland in 2018, which are subject to strict data protection rules. Over five years, we have invested US$8.4m in equipping these centers, to which we transferred the data of its users. Today we have two data centers successfully operating in Zurich that process malicious files shared from users on a voluntary basis from the Kaspersky Security Network cloud system.The centers also process and store cyberthreat related data from users in Europe, North and Latin America, the Middle East and several countries in the Asia-Pacific region.

Open new Transparency Centers

We are building more Transparency Centers to offer our corporate customers, partners and government cybersecurity regulators the opportunity to verify the reliability of our solutions by examining our source code, and to learn more about our internal processes.

The first center opened in Zurich in November 2018 and since then over the five years of the GTI, the Company has built 11 such centers in Brazil, Italy, Japan, Malaysia, the Netherlands, Rwanda, Saudi Arabia, Singapore, Spain, Switzerland and U.S.A. Four opened between July 2022 and the end of 2023.

We are constantly expanding the range of capabilities the Transparency Centers offer. Previously, only the source code of flagship products for home users and businesses was offered for review. In July 2023, an overview of the source code of all on-premise solutions for corporate customers became available. The centers will soon display the results of the self-certification of the our products, including such elements as design documentation and threat models. This is all consistent with the recommendations of the draft European Cyber Resilience Act.



11
Transparency Centers
worldwide

RESULTS OF 2022–2023

4 **new Transparency Centers** opened in Rwanda, Saudi Arabia, Italy and the Netherlands

The Saudi Arabia Transparency Center is the **first in the Middle East**, while the Rwanda center is the **first in Africa**

34 **visits** to centers worldwide

Expanded list of products available for review at the Transparency Centers

U.S.A.	Brasil	Spain	Netherlands	Switzerland	Italy	Saudi Arabia	Singapore	Malaysia	Japan	Rwanda
Woburn	São Paulo	Madrid	Utrecht	Zurich	Rome	Riyadh	Singapore	Kuala Lumpur	Tokyo	Kigali

Conduct independent audits

In 2023, we successfully passed a

SOC 2

Type 2 audit

As part of the GTI, Kaspersky regularly undergoes independent audits of its internal processes. Since 2019, our data management systems have undergone annual certifications in accordance with ISO/IEC 27001:2013. The audit confirms the security of the Company's solutions. In addition, since 2019, Kaspersky has regularly undergone Service Organization Control for Service Organizations (SOC 2) audits.

In 2023, Kaspersky successfully passed a SOC 2 Type 2 audit, assesing the development and release of our antivirus bases, and how they are protected from unauthorized changes by security controls.

Collect data on vulnerabilities via the bug bounty program

59 reports
on minor vulnerabilities received over five years

US$81,750
paid out for reports

Since March 2018, Kaspersky has received 59 reports on minor vulnerabilities as part of the bug bounty program, eliminated them and paid out a total of US$81,750 in bounties to independent researchers.

The bug bounty program offers a maximum bounty of US$100,000 for discovering the most serious bugs in Kaspersky software. The Company has been running its public bug bounty program on the Yogosha platform since 2022. We also support the Disclose.io project, which provides a safe space for bug analysts who are concerned about possible negative legal consequences from their findings.

Teach how to assess cybersecurity levels

2 organizations
(a government agency and a private company) underwent training as part of the Cyber Capacity Building Program during the reporting period

Our Cyber Capacity Building educational program is designed for employees of private and public companies, as well as universities, who want to gain practical skills in assessing the security level of their IT infrastructure.

As part of the program, our experts provide recommendations on code auditing, creating procedures to handle vulnerabilities and code fuzzing techniques. Companies in the public and private sectors are interested in this offering. During the reporting period, two organizations underwent training: representatives of the Namibian Communications Regulatory Authority and a private organization.

Publish Transparency reports

Our mission is to protect users against cyberthreats, which is why we support our partners as well as international organizations and law enforcement agencies in the fight against cybercrime. We regularly process requests and, since 2020, every six months we have published reports detailing the jurisdictions from which we receive such requests, the number fulfilled, and the number declined. Kaspersky has an internal process for handling such requests and clear criteria for legally verifying them.

Kaspersky discloses the number of requests from law enforcement for user data, expert analyses, and technical details to investigate threats every six months. However, we do not provide any third parties with access to our system or network, including data processing infrastructure[1]. We report requests from our own users about their personal data, how we handle it and where it is stored with the same frequency.

[1] For more about how we work with requests, please see our transparency reports.

GTI development plans for 2024

The Company plans to expand its network of Transparency Centers by opening at least one additional center by mid-2024, arranging a minimum of five visits to these centers, and persisting in obtaining international independent certifications while publishing reports on its collaboration with law enforcement agencies.

Our call for development and usage of AI in cybersecurity

Presenting ethical principles for the development and use of systems employing artificial intelligence (AI) or machine learning (ML)

Artificial intelligence provides great benefits for the cybersecurity industry, but also poses risks to user privacy and freedom. In October 2023, at the Internet Governance Forum, which was held under the auspices of the United Nations in Kyoto, Kaspersky presented its ethical principles for the development and use of artificial intelligence or machine learning-based systems created as part of the GTI:

Transparency

The Company is committed to explaining principles of the way its solutions operate and utilize AI/MI technologies, developing AI/ML systems interpretable to the maximum extent possible and to introduce necessary safeguards to ensure the validity of outcomes provided by these systems.

Safety

For our AI/ML systems, we are committed to prioritizing safety in the development and use of AI/ML systems.

Human control

In order to provide the best protection, we are committed to maintaining human control as an essential element of all our AI/ML systems.

Privacy

Numerous technical and organizational measures need to be adopted to ensure the digital privacy of users.

Commitment to cybersecurity

Aligned with Kaspersky's core values centered around protecting individuals, organizations, and building a safe world, we are committed to utilizing AI/ML systems solely for defensive purposes.

Openness to dialogue

We are committed to promoting dialogue with all stakeholders in order to share best practice in the ethical use of AI. Kaspersky stands ready for discussions with all interested parties, including within the UN (Global Digital Compact, Open-ended Working Group, Internet Governance Forum etc.) and other leading global platforms.

What was the result?

We informed our partners, users and the professional community how we ensure the reliability of machine learning systems and encouraged other industry participants to join the dialogue and develop common ethical principles.