Scaling Security

Kaspersky's 2024-2025
Sustainability report

kaspersky.com

kaspersky

Contents

Chief Executive Officer's Address

GRI 2-22

Dear Friends,

With each passing year, the digital environment grows more complex, threats become more diverse, and the dependence of individuals, businesses and governments on technology deepens. In light of this, it is particularly important for us to respond to emerging challenges and to expand opportunities for the secure development of the digital world. The approach underpinning our work remains unchanged: true security can only be achieved through Cyber Immunity.

For nearly three decades now, Kaspersky has been developing information security technologies that enable both individuals and organizations to benefit from digitalization and grow without unnecessary risk.

Kaspersky continues to expand, strengthen its expertise, and broaden its international presence: today we have companies in more than 30 countries, protecting organizations and users in more than 200 countries all over the world. In August 2024, our office in Bogotá began operations to become our third in Latin America, and at the end of 2025 we further strengthened our presence in Southeast Asia by opening a new representative office in Vietnam. During the reporting period, new Transparency Centers were also opened in Turkey, South Korea and Colombia. For us, these steps mean that more customers around the world gain direct access to our expertise, technologies, and principles of openness.

This growth reflects not only the scale of our business, but also the scope of our responsibility: the broader our geographic presence and the greater the number of customers relying on our technologies, the higher the expectations placed upon us in terms of reliability, transparency, and quality of protection. The foundation of this remains our technologies, our international expertise, and our continuous readiness to adapt our approach in response to an evolving threat landscape.

Our product portfolio continues to evolve in line with the needs of the digital world. By the end of 2025 it comprised 43 products. We are consistently expanding our ecosystem of solutions for home and business users, for industrial enterprises and critical infrastructure, and for organizations requiring systemic resilience against a wide range of threats.

We place particular emphasis on developing the industry's human capital. We continue to invest in digital education, and to engage with school pupils, students, young professionals, and experienced specialists. Kaspersky collaborates with approximately 200 universities across 45 countries – including more than 70 institutions in Russia and the CIS. This forms part of our long-term contribution to the resilience of the entire industry: a strong digital environment begins with skilled professionals capable of designing, implementing, and securing the technologies of the future.

In recent years, artificial intelligence has emerged both as a new challenge and as an opportunity for our world, alongside the need for its responsible development and use. We have long applied such technologies in our own products and research; however, today it is essential not only to enhance their capabilities, but also to establish principles for their safe use. In December 2024, at the United Nations Internet Governance Forum in Riyadh, we presented our guidelines for the secure development and deployment of artificial intelligence systems. Their purpose is to help organizations take cyber risks associated with such technologies into account and to mitigate them at the design and implementation stages. Kaspersky has also joined the Russian Artificial Intelligence Alliance, which supports the responsible development of technologies, as well as the United Nations Industrial Development Organization's Global Alliance on AI for Industry and Manufacturing.

At the same time, sustainable development for us extends beyond the technological agenda. We continue to advance all key areas of our strategy: strengthening cyber resilience, investing in innovation, enhancing transparency and business ethics practices, reducing our environmental footprint, supporting our employees, and contributing to societal development.

Today, it is clear to us that security cannot be regarded as a state that is achieved once and for all. It must be continuously developed, strengthened, and made accessible across industries, regions, and user groups. This is how we understand our mission: step by step, to expand the space in which people and organizations can confidently use digital technologies, grow, and build the future.

On behalf of Kaspersky, I would like to thank our employees, partners, customers, and all those who share our values for their trust, professionalism and willingness to move forward together with us. I am confident that only by combining expertise, responsibility, and openness can we make the digital world truly secure and sustainable for all.

Eugene Kaspersky
CEO, Kaspersky

About the Company

Kaspersky ("the Company") is an international company that develops innovative cybersecurity, data protection, and digital privacy solutions. We strive to make the digital world safe for everyone and build a future where technology works for the benefit of humanity.

>1 billion

devices[1] protected from widespread cyberthreats and targeted attacks in more than 200 countries and territories

>2 billion threats

detected since the Company's inception

~200,000

corporate clients

[1] According to Kaspersky Security Network (KSN) data from automated analysis of malware, including information dating back to 2011.

Key facts about Kaspersky

Amid the widespread transition to the digital economy, cybersecurity has become a basic need for global sustainable development. Since 1997, Kaspersky has been working to scale reliable protection and make it available to everyone.

>200

countries and territories

where the Company's cybersecurity solutions are used

~5,700

employees

43

products for home and business users

5

Expertise Centers

Mission and values

Kaspersky's mission is to build a secure and sustainable digital world where technology helps improve life on Earth.

We realize our mission through three key areas:

- **increasing resilience in digital environments, including by developing Cyber Immunity and inherently secure systems**
- **promoting social development and the well-being of society**
- **protecting the environment and the planet's resources**

Read more about Cyber Immunity on page 36

Be there for you

Our clients, partners, and our team are always our focus. We base our decisions on their objectives and listen to their needs. We provide security at a level that meets the highest requirements. The people we work for feel our support in every situation and know they are choosing the best protection, which was created just for them.

Be clearly inventive

We bolster our leading position every day by creating cutting-edge technologies that make the world a safer place. We never stop working on ourselves and growing our expertise. We are unrivaled in cybersecurity, as confirmed by independent industry experts. Clients, partners and users trust us. In turn, we believe it is our professional duty to vindicate this trust by remaining honest with them and with ourselves.

Be committed experts

We are constantly thinking about how to make our products even better and strive to surpass our own achievements by implementing new technologies and anticipating new threats.

We persistently test the strength of our own products and always find ways to move one step closer to perfection. We never stand still and are constantly growing, while maintaining our values. This is what repeatedly takes our solutions to a new level of performance.

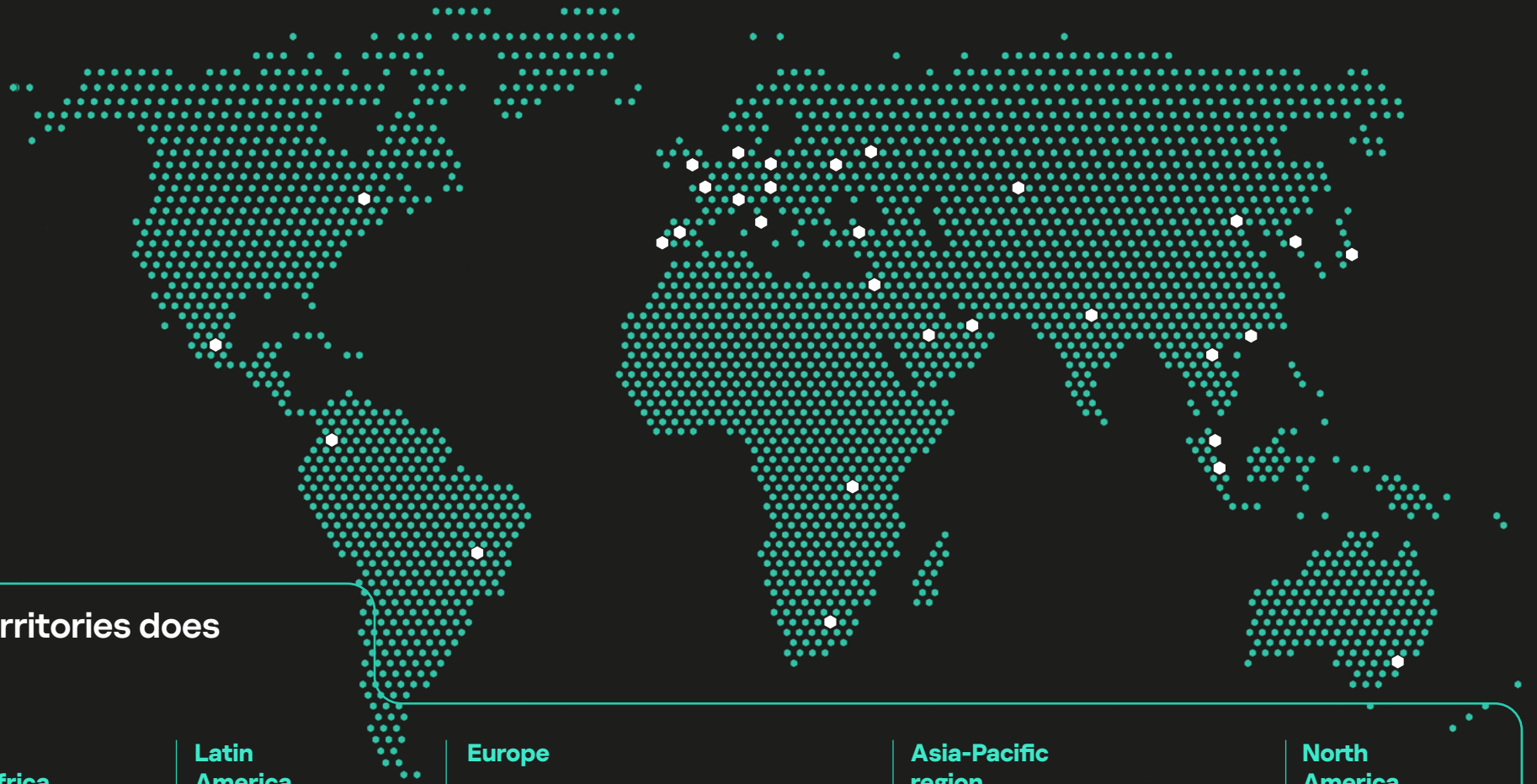
Be powered by challenges

No matter how much or how often we are challenged, we only become stronger. We do what others cannot do and dare to do what we have not done before. We stand out, make our own rules, and are proud of what sets us apart from others. We don't look for easy paths or simple tasks, because we know how to turn challenges into opportunities. We find creative solutions even in difficult situations, and we do so our own way.

Geography

GRI 2-1

With companies in 30 countries and territories, Kaspersky protects organizations and users in more than 200 countries and territories all over the world.



In which countries and territories does Kaspersky operate?

CIS

- Belarus
- Kazakhstan
- Russian Federation

Middle East, Turkey and Africa

- Israel
- Rwanda
- Saudi Arabia
- South Africa
- Turkey
- UAE

Latin America

- Brazil
- Colombia
- Mexico

Europe

- Czech Republic
- France
- Germany
- Italy
- Netherlands
- Portugal
- Spain
- Switzerland
- United Kingdom

Asia-Pacific region

- Australia
- China and Hong Kong
- India
- Japan
- Malaysia
- Singapore
- South Korea
- Vietnam

North America

- Canada

Business model

GRI 2-6

Cybersecurity Global Market[1]

B2B

$83.3 B
B2B cybersecurity market size in 2025

$136 B
B2B cybersecurity market size forecast in 2029

+13%
compound annual growth rate of the B2B-market

B2C

$6.3 B
B2C cybersecurity market size in 2025

$7.6 B
B2C cybersecurity market size forecast in 2029

+5%
compound annual growth rate of the B2C-market

kaspersky

$836 M
revenue in 2025

+4%
YoY growth in 2025

Business Areas and Product Lines B2B

Endpoint Security
Next Foundations, Next EDR Optimum/ Expert, Small Office Security, Mobile Security

Cloud & Virtual Infrastructure Security
Cloud Workload Protection (incl. Hybrid Cloud, Container Security), Security for Storage, Scan Engine

Network and Mail Security
NDR (Anti Targeted Attack), Mail Security Gateway, Security for Office 365 / MS Exchange, SD-WAN, Anti-DDoS, Web Traffic Security

Unified Security Platform (Security Operations) — Open Single Management Platform

Platform for Detection and Response to Advanced Threats
Next XDR Optimum / Expert

Monitoring and Cybersecurity Events Management
SIEM (Unified Monitoring and Analysis Platform)

Platform and Intelligence Services / Security analytics
Threat Intelligence

AI-assistant

Industrial Cybersecurity
Industrial CyberSecurity — native OT XDR platform (nodes, networks)

Cybersecurity Services
MDR, Incident response, Security Assessment, Premium support & Professional services, etc.

Cybersecurity Trainings
Automated Security Awareness Platform, Cybersecurity Trainings, etc

Operating System Solutions based on Kaspersky OS: Thin Client, OS Mobile, Automotive Secure Gateway

Business Areas and Product Lines B2C

Core Offer

Three-tiered offering:
- Kaspersky Standard
- Kaspersky Plus
- Kaspersky Premium

Standalone Solutions
- Kaspersky VPN
- Kaspersky Password Manager
- Kaspersky Who Calls (Spam calls protection)[2]
- Kaspersky Safe Kids (Parental Control)
- Kaspersky eSIM Store (eSIM services)

Partner offers with service providers and resellers
- Kaspersky Safe Web (Web-based)
- Kaspersky Smart Home (Router-based)

Sales Channels B2B

- Partner Network: Distributors, Resellers, System Integrators, Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), and others
- Technology Alliances (integration with partner products)
- Digital channel

Sales Channels B2C

- Digital channel
- Retail channels (stores, resellers)
- Partners: Internet providers, mobile operators, banks, etc., offering protection "bundled" with their services

Promotion

- Integrated advertising campaigns to promote the brand and solutions (outdoor advertising, digital promotion, community collaborations, social media, podcasts, and PR)
- Co-marketing with partners and collaborations with other brands
- Participation in industry and professional conferences and exhibitions
- Content marketing and threat analysis (GReAT research), publications, blogs, webinars
- Building trust through Transparency Centers, bug bounty programs, international SAS (Security Analyst Summit) conferences, etc.
- Participation in social projects to develop a culture of security and cyber hygiene
- Engaging schoolchildren and students in the IT / security industry

Customers Globally

~1 B
devices protected by Kaspersky to date

~200 thousand
corporate clients worldwide choose our protection


Government sector


Enterprises


Industrial companies


Small and Medium Business (SMBs)


Private PC and smartphone users

[1] The assessment is based on an internal market evaluation methodology. The assessment only includes cybersecurity areas where Kaspersky is present

[2] WhoCalls is available in Russia, Kazakhstan, Indonesia, and Latin America

Products

Kaspersky solutions provide reliable protection against cyberthreats for individuals, small and medium-sized businesses, and large enterprises, earning recognition year after year from leading independent experts.

GRI 2-6

The Company's portfolio includes 43 information security products for home and business[1]. From 2013 to 2025, Kaspersky solutions participated in 1,122 independent tests and reviews. Several independent organizations, including AV-Comparatives, AV-TEST, and SE Labs, evaluated the Company's products, ranking them first place in 861 cases and placing them among the top three in 965 cases. Kaspersky achieved top-three finishes in 86% of evaluations throughout this period.

Solutions for home users

- Kaspersky Standard
- Kaspersky Plus
- Kaspersky Premium
- Kaspersky Safe Kids
- Kaspersky VPN
- Kaspersky Who Calls
- Kaspersky Password Manager
- Kaspersky eSIM Store

Learn more about products for home users

Solutions based on KasperskyOS

- Kaspersky Automotive Secure Gateway
- Kaspersky Hybrid Cloud Security
- Kaspersky Thin Client
- Kaspersky Container Security
- Kaspersky Security for Mail Server

Learn more about KasperskyOS-based solutions

In 2025, Kaspersky products:

participated in **100** independent tests and reviews

in **90** cases, they took first place

achieved **94** top three finishes

ranked among the top 3 in **94%** of evaluations for the year

Key solutions for business

- Kaspersky Next
- Kaspersky Small Office Security
- Kaspersky Next EDR Expert/ Optimum
- Kaspersky Next XDR Expert/ Optimum
- Kaspersky Industrial CyberSecurity
- Kaspersky MDR
- Kaspersky Ant-Targeted Attack
- Kaspersky Automated Security Awareness &Training
- Kaspersky SIEM
- Kaspersky Threat Intelligence
- Kaspersky Digital Footprint Intelligence

Learn more about these and other business solutions

43 products in our portfolio

[1] The list of products includes the security solutions presented on the website kaspersky.com. These products are available under a wide range of licenses to meet the needs of various customers. The Company's price list includes more than 1,500 entries.

Brief history of the Company

Over nearly 30 years of operation, Kaspersky has become a leader in the development of cybersecurity and digital privacy technologies that protect individual users, businesses, industry, and government agencies in more than 200 countries and territories worldwide.

1997
- Kaspersky is founded

1999
- The Company's first overseas office is opened in the UK

2001
- Antivirus software for portable devices is developed

2007
- The business product line is launched

2008
- The Kaspersky Global Research and Analysis Team (GReAT) is created

2013
- Cooperation with INTERPOL begins

2015
- A specialized solution for protecting critical infrastructure and industrial facilities is launched

2016
- Together with Europol and Intel Security, Kaspersky partakes in the launch of the No More Ransom project to help victims of ransomware
- Kaspersky ICS-CERT, computer incident response center for industrial and mission-critical facilities, is opened

2017
- Kaspersky's own operating system is unveiled

2018
- Kaspersky's Global Transparency Initiative (GTI) is launched

2019
- Kaspersky undergoes rebranding and unveils a new mission: "Building a safer world"

2021
- The Company opens access to the Software Bill of Materials (SBOM) so that customers and partners understand what is inside Kaspersky products and software
- The Company concludes a deal with Brain4Net to further develop a full-scale XDR system

2023
- AV-Comparatives awards "Product of the Year" for Kaspersky Standard

2024
- Kaspersky concludes a cooperation agreement with AFRIPOL

2025
- The Company enters new business areas with the launch of the Kaspersky eSIM Store

Key events in the reporting period

Business expansion

- **Three new Transparency Centers opened in key regions.** Kaspersky continued to expand its Global Transparency Initiative in 2024, opening Transparency Centers in Turkey, South Korea, and Colombia.
- **Presence expands in Latin America and Southeast Asia.** In August 2024, Kaspersky opened an office in Bogota, Colombia — its third location in Latin America. And in October 2025, the Company opened an office in Vietnam and appointed a new General Manager for Southeast Asia.

Innovations

- **Kaspersky Cloud Workload Security.** Kaspersky launched a comprehensive solution for protecting cloud workloads, consisting of Kaspersky Hybrid Cloud Security and Kaspersky Container Security. Joint installation of the systems can protect infrastructure wherever it resides: on servers or virtual machines, or in private, public, or hybrid clouds, etc.
- **Kaspersky Next Line.** Kaspersky released a new line of flagship business products that combine endpoint protection, the visibility and speed of EDR[1],and powerful XDR[2] tools. The solution is built on AI technologies and is available in both cloud and on-premises versions.
- **Kaspersky Thin Client 2.0.** The Company presented an updated operating system for thin clients that offers enhanced connectivity, higher speed of applications delivery, lower total cost of ownership, user-friendly graphical interface and quick deployment.
- **Launch of new consumer solutions.** In 2025, the Company entered new market segments with the launch of the Kaspersky eSIM Store, an app for selecting, purchasing, and activating eSIMs, available in more than 150 countries.

[1] Endpoint Detection and Response encompasses solutions for continuous monitoring of threat data on workstations and other endpoints, incident detection, and rapid incident response.

[2] XDR (Extended Detection and Response) is a unified security incident platform powered by AI and automation that provides organizations with a comprehensive and effective way to protect against and respond to sophisticated cyberattacks.

Standards and certificates

- **New ISO international standard for IoT devices.** Kaspersky helped develop a standard describing factors that determine the trustworthiness and reliability of IoT devices. It was prepared jointly with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
- **Guide to safe AI development.** At the UN Internet Governance Forum in Riyadh, the Company presented the guidelines for the secure development of AI-driven systems aimed at helping organizations mitigate cyber risks associated with the use of AI technologies.
- **Re-certification against ISO/IEC 27001:2022 standard.** In 2025, Kaspersky reinforced its security credentials by re-certifying its information security management system (ISMS) against ISO/IEC 27001:2022, an international standard which outlines the best practices for establishing, implementing and continuously improving these systems.

International cooperation

- **Cooperation with AFRIPOL.** Kaspersky signed a five-year agreement with AFRIPOL to jointly combat cyberthreats on the African continent.
- **Operation Serengeti with INTERPOL and AFRIPOL.** The Company participated in an operation that resulted in the arrest of more than one thousand cybercrime suspects in African countries. Over 134,000 malicious infrastructure objects were neutralized.
- **Participation in INTERPOL's Operation Synergia II.** The Company assisted INTERPOL in an operation aimed at combating the spread of malware and phishing attacks worldwide. The operation resulted in 41 arrests.
- **Assisting INTERPOL in the fight against Grandoreiro.** Kaspersky assisted INTERPOL in apprehending five administrators of the Grandoreiro malware, a banking trojan that is believed to have caused over €3.5 million in damage.

Education and social responsibility

- **Cooperation with Boğaziçi University.** A memorandum of understanding was signed to establish a Transparency Lab and develop joint training programs in cybersecurity and information transparency.
- **Cybersecurity training for universities.** A free online course, "Cybersecurity: Entry Level," designed to introduce first- and second-year university students of all technical and non-technical specialties to the fundamental concepts of information security.
- **Kaspersky Capture the Flag (CTF) competitions.** The Company held Security Analyst Summit (SAS) CTF and the Kaspersky{CTF} contests focused on skills development and building cyber capacities.

Awards and recognitions

Our solutions continue to receive high praise from independent experts and win awards in prestigious international tests and competitions.

For 2024–2025, we can highlight the following achievements of our solutions.

Kaspersky EDR Expert:

- demonstrated 100% effectiveness against targeted attacks in the AV-Comparatives Endpoint Prevention and Response Test study, earning the esteemed **Strategic Leader 2024** and **Certified 2025** awards (in 2022–2025, the solution received the Strategic Leader award three times in a row and the Certified award once after the tester cancelled all other award gradations in 2025)
- was the first in the industry to successfully pass all tests in the AV-Comparatives EDR Detection Validation Certification Test 2025 study, earning the **Certified EDR Detection 2025** award
- demonstrated high results in detecting and classifying advanced attack tactics and techniques in AV-TEST Advanced EDR Tests and earned the **Approved Advanced EDR 2024** award

Kaspersky Small Office Security earned:

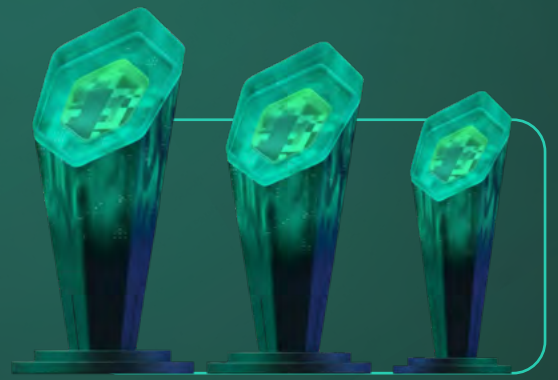
- the annual **AV-TEST BEST Protection 2024** award for the best results in all two-month tests in 2024
- the **AV-TEST BEST Advanced Protection 2024 + 2025** annual awards for absolute performance in tests of protection against complex threats during each year
- the **AV-TEST Best Usability 2024 + 2025** annual awards for the best resistance to false positives in each year
- the annual **SE Labs Winner Small Business Endpoint 2025** award for high results in quarterly tests, including the best result for the Total Accuracy Rating during Q3 2023 – Q3 2025

Kaspersky Endpoint Security earned:

- the annual **AV-TEST BEST Protection 2024** award for the best results in all two-month tests in 2024
- the **AV-TEST BEST Advanced Protection 2024 + 2025** annual awards for absolute performance in tests of protection against complex threats during each year
- the **AV-TEST Best Usability 2024 + 2025** annual awards for the best resistance to false positives in each year
- the **Approved Anti-Tampering 2025** award for successfully preventing all tampering attempts in the AV-Comparatives: Anti-Tampering Test 2025
- the **Approved Credential Dumping 2024** award, having successfully prevented unsanctioned access in the AV-Comparatives: Credential Dumping Test 2024
- the **Approved Process Injection 2024** award for successfully preventing 14 out of 15 unauthorized injections of malicious code in the AV-Comparatives: Process Injection Test 2024
- the annual **SE Labs Winner Enterprise Endpoint 2025** award for high results in quarterly tests, including the best result for the Total Accuracy Rating during Q3 2023 – Q3 2025

Kaspersky Premium for protecting home users earned:

- the annual **Top Rated Product** award for 2024 and 2025 from AV-Comparatives for outstanding test performance in each year. Moreover, the product has received the most annual awards from AV-Comparatives since testing began in 2004
- the annual **AV-TEST BEST Protection 2024** award for the best results in all two-month tests in the year
- the **AV-TEST Best Usability 2024 and 2025** annual award for the best resistance to false positives in the year
- the annual **AV-TEST BEST MacOS Security 2024 + 2025** awards for high performance in quarterly tests in each year
- the annual **SE Labs Winner Consumer Endpoint 2025** award for high results in quarterly tests, including the best result for the Total Accuracy Rating during Q3 2023 – Q3 2025
- the annual **SE Labs Best Home Anti-Malware 2024** award for high results in quarterly tests
- the **Approved Fake Shops Detection 2025** award from AV-Comparatives
- the **Approved Anti-Phishing 2024** award from AV-Comparatives, having ranked first in AV-Comparatives: Anti-Phishing Certification 2024



Kaspersky VPN:

- In 2024, Kaspersky Premium and Kaspersky VPN successfully passed all tests in an AV-TEST study and received **AV-TEST Approved VPN 2024** certificates
- In 2025, Kaspersky Premium and Kaspersky VPN confidently outperformed the other eight competing solutions in Combined Score Ranking and received AV-TEST Approved VPN 2025 certificates.

Kaspersky Safe Kids (KSK):

- In 2024, KSK demonstrated a high detection rate and zero false positives, becoming the only one of the five tested solutions to meet the certification criteria and receive **Approved Parental Control 2024** status from AV-Comparatives
- In 2025, KSK again demonstrated the highest detection rate among all participants as well as zero false positives, fulfilling the certification criteria and receiving **Approved Parental Control 2025** status from AV-Comparatives.

2024

- In 2024, Kaspersky products participated in a total of 95 independent tests and reviews, taking first place 91 times and entering the top three 92 times. Overall, the products ranked among the Top 3 with a record 97% rate.
- Kaspersky's business solutions, Kaspersky Small Office Security and Kaspersky Plus, received the highest scores in the SE Labs test. They demonstrated 100% effectiveness against cyberthreats in all four tests.
- Kaspersky is once again a leader in the global managed solutions market according to Quadrant Knowledge Solutions.
- Kaspersky Standard achieved one of the best results in AV-Comparatives tests, receiving a total of 100 points out of a possible 105.
- Kaspersky received nine BEST 2024 awards from AV-TEST for its outstanding level of protection. Three of these awards were for solutions for personal Windows and Mac devices, and six were for corporate security products.
- Kaspersky once again successfully passed an independent Service and Organization Controls 2 Type 2 (SOC 2 Type 2) audit. The audit confirms that the processes used by the Company to develop and release antivirus databases are safe and reliably protected from unauthorized interference.
- Kaspersky Safe Kids, our parental control app, was recognized once again as one of the most effective solutions for protecting children online. The product received certificates from AV-TEST and AV-Comparatives for its effectiveness in blocking inappropriate content.

2025

- In 2025, Kaspersky products participated in 100 independent tests and reviews. In 90 cases they took first place, and ranked among the top three 94 times. The Company placed among the top 3 94% of the time during the year.
- VDC Research named Kaspersky a key player in the global industrial information security market, highlighting its Kaspersky Industrial CyberSecurity (KICS) XDR platform and the opening of new transparency centers.
- Kaspersky EDR Expert was the first in the industry to successfully pass all tests in the AV-Comparatives EDR Detection Validation Certification test 2025, earning a Certified EDR Detection 2025.
- Kaspersky Premium achieved the highest score in AV-Comparatives tests, receiving a total of 105 points out of a possible 105.
- Kaspersky won in three main categories at the SE Labs Security Awards. Awards were given to the Company's solutions for protecting individual users, small businesses, and large companies.
- Kaspersky Endpoint Security, a security solution for business, once again demonstrated full effectiveness against cyberattacks in the Anti-Tampering Test 2025 of AV-Comparatives.
- Frost & Sullivan and QKS Group have recognized Kaspersky as a leader in the global threat intelligence market, citing the Company's global presence, technological prowess and innovation, extensive product portfolio, and high-quality customer service.
- Kaspersky VPN received an award for its high performance at the annual AV-TEST certification. The "Approved" certificate recognizes Kaspersky VPN's stable connection, highly effective protection of user privacy, and low impact on system performance.
- ISG noted Kaspersky's effective advanced detection and response. The Company received Global Product Challenger and Market Leader awards in Brazil for its XDR technology.

Key results

+4%
increase in global sales

$836 million
global revenue for 2025 in fixed exchange rates[1]

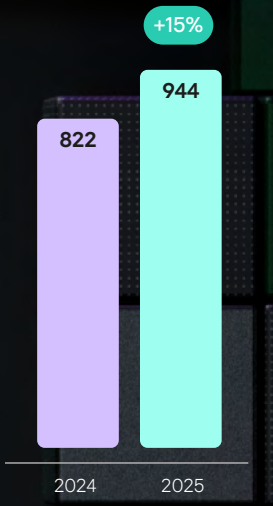
+21%
increase in enterprise sales

+85%
growth in global sales of KasperskyOS-based solutions

+29%
increase in non-endpoint solutions sales

+16%
increase in B2B sales globally

Global revenue for 2025 in actual rates[2], $ million



1 Combined sales of the Kaspersky companies from their IT business presented, in USD, using fixed 2025 exchange rates.
2 Actual rates: The Company-wide results in actual rates.

Managing Sustainable Development

10 UN SDGs
Kaspersky's contribution to achieving

5
key strategic priorities in sustainable development

Sustainable Development Management System

GRI 2-9, GRI 2-12

Kaspersky addresses sustainable development and its impacts comprehensively and at multiple levels of management.

The Board of Directors is involved at the highest level in approving overall strategic directions and goals for sustainable development. The Sustainability Department works together with project team leaders across the company to implement initiatives and monitor results. These teams provide methodological support, analyze results, and regularly update data for internal reporting.

Strategic priorities in sustainable development

Kaspersky pursues five key strategic directions related to sustainable development. They are determined based on the specifics of the Company's activities and the nature of its positive and negative impacts, and shape how key ESG initiatives are developed and implemented.

Sustainable and responsible business practices

- Developing business ethics and enhancing business sustainability;
- Protecting data and respecting privacy rights;
- Ensuring transparency and reliability of our products and business processes.

Contributing to social development

- Social and charitable projects;
- Developing talent for the IT industry;
- Promoting inclusivity in the cyberspace;
- Improving general digital literacy.

Reducing impact on the environment

- Reducing carbon footprint and improving energy efficiency of our infrastructure;
- Optimizing resource consumption;
- Developing environmental awareness and supporting environmental initiatives.

Advancing global cyber resilience and a secure digital future:

- Protecting users, businesses and critical infrastructure from cyberthreats;
- Developing cyber immunity for new technologies;
- Strengthening international cooperation against cybercrime;
- Creating a secure digital environment.
- Implementing innovations, including artificial intelligence.

A human-centered approach to HR management

- Creating a supportive, inclusive and safe work environment for our employees;
- Supporting talent development;
- Promoting women in IT.

GRI 2-23, GRI 2-24

1. Anti-Corruption Policy
2. Procurement Policy
3. Contract Policy
4. Occupational Safety and Health Policy

Key internal documents are posted in internal information systems and are accessible to all Kaspersky employees. The obligations set out in these documents are communicated to employees during the hiring process and through regular training within the Company.

The Company's impacts related to sustainable development

Kaspersky's activities have a multifaceted impact on the economy, the environment, and society. The Company aims to enhance positive impacts and reduce potential negative effects related to its operations and the development of digital technologies.

GRI 203-1, GRI 203-2

Economy

+ Positive impacts

- Improved digital security for businesses and organizations: protection from cyberattacks and reduced financial losses.
- Creating solutions for industrial security and critical infrastructure to support a more stable economy

– Negative impacts

- The Company's significant market share and high level of technological expertise may create barriers to entry for new or niche players, potentially limiting competition in certain segments of the cybersecurity market
- Improved digital security may require organizations to invest more in software infrastructure and staff training, which can increase operating costs
- The deployment of complex cybersecurity solutions can widen the gap between organizations with a high level of digital maturity and those with limited financial and technological resources

Environment

+ Positive impacts

- Fewer physically packaged products and more digital licenses: less resource consumption
- Blocking illegal mining, which reduces energy consumption and, according to the Company's estimates, reduces CO_2-eq emissions by up to 3,000 tons annually.
- Optimized resource consumption in offices and data centers

– Negative impacts

- High carbon footprint from employee air travel related to international projects, partnership meetings, and events
- High energy consumption of data centers and servers

For more information on reducing negative impacts, see the "We reduce our carbon footprint" and "We improve energy efficiency" section on page 90 and 92

People

+ Positive impacts

- New job creation
- Employee benefits package
- Support for parents
- Programs on digital literacy and inclusion, support for employees with disabilities, participation in educational projects

– Negative impacts

- Digital divide: Part of the population is lagging behind technological developments, which makes people without digital skills more vulnerable
- Increasing complexity of digital life: Cybersecurity requirements make everyday activities more difficult, which is especially challenging for older adults and people with cognitive disabilities

For more information on reducing negative impacts, see the "Inclusivity in cyberspace" and "Digital awareness" sections on page 79 and 86

Contribution to solving shared problems

Kaspersky is committed to helping achieve global and national sustainable development priorities. The Company supports achieving the UN Sustainable Development Goals (SDGs) and focuses on those where its influence is greatest.

Contribution to achieving UN SDGs

Kaspersky develops educational projects for both employees and local communities.

For more information on educational projects, see the "Employee development," "Training IT personnel," and "Digital awareness" sections on page 67, 81 and 86

Kaspersky promotes women in the IT industry.

For more information on gender equality programs, see the "Women in IT" section on page 62

The Company implements initiatives to reduce energy consumption.

Detailed information is available in the "We improve energy efficiency" section on page 91

Our employees are our greatest asset, and their job satisfaction is of particular importance to the Company.

For more information on the creation of decent working conditions, see the "People at Kaspersky" section on page 55

Kaspersky develops and implements unique innovative cybersecurity solutions.

For more information on innovative projects, see the "Digital security" section on page 48

The Company's projects contribute to the safe and sustainable development of cities and the economy as a whole.

For more information on protecting urban infrastructure, see the "Protecting critical infrastructure" section on page 30

The Company strives to reduce its environmental impact and resource consumption throughout its supply chain.

For more information on responsible production and consumption initiatives, see the "Environment" section on page 88

Kaspersky supports projects of the Nature and People Foundation, including programs to protect sea otters and monitor the health of marine ecosystems.

For more information on the initiatives, see the "We cultivate environmental awareness" section on page 97

The Company supports efforts to conserve the Arctic fox and other species, as well as conservation expeditions and projects of partner non-profit organizations to reduce the number of abandoned pets.

For more information on the initiatives, see the "We cultivate environmental awareness" section on page 98

Interaction with stakeholders

GRI 2-29

Kaspersky's approach is based on respect, open dialogue, and accountability, striving to maintain stable and trustbased relationships with all stakeholders.

Employees

Group interests

- Stable employment and career growth
- Fair wages and social security
- Comfortable and safe working conditions
- Training and development
- No discrimination

Methods of interaction

- Internal corporate communications system
- Meetings with the Company's management
- Joint conferences, cultural and sports events
- Corporate website

Results of interaction in the reporting period

For more information about the Company's interaction with its employees, see the "People at Kaspersky" section on page 55

Users

Group interests

- Personal data protection
- High quality products
- High level of service
- Reasonably priced products

Methods of interaction

- Feedback system and services
- Press releases, advertising and promotional materials

Results of interaction in the reporting period

For more information on the Company's interaction with users, see the "Safeguarding users' trust" section on page 107

Partners and suppliers

Group interests

- Transparency and openness in competitive procedures
- Product quality control
- Compliance with business ethics
- Anti-corruption measures
- Timely and accurate fulfillment of contractual obligations

Methods of interaction

- Open competitive procedures
- Prompt handling of claims
- Business meetings, conferences and exhibitions
- Information disclosure

Results of interaction in the reporting period

For more information on the Company's interactions with partners, see the "Sustainable supply chain" section on page 116

Government authorities and law enforcement agencies

Group interests

- Compliance with legal requirements and standards
- Timely payment of all applicable taxes and fees
- Investments in developing regions where the Company has a presence
- Employment assistance and support for entrepreneurs
- Protection of critical infrastructure
- Assistance in the fight against cybercrime

Methods of interaction

- Consultations with law enforcement officials
- Software development and licensing
- Consultations on legislative matters

Results of interaction in the reporting period

For more information on the Company's interactions with government and law enforcement agencies, see the "How we combat cybercrime" section on page 25

Local communities

Group interests

- Creation of jobs for local residents, development of human capital
- Contribution to developing social infrastructure
- Development of local production and supplier networks
- Charitable projects and social investments
- Minimizing negative environmental impact in areas where the Company has a presence
- Good communication and transparent operations

Methods of interaction

- Recruitment of staff from local communities
- Internships for students
- Development and professional growth programs for staff
- Training programs for a wide range of users
- Procurement from local suppliers

Results of interaction in the reporting period

For more information on the Company's interaction with local communities, see the "Contribution to community development" section on page 72

Groups vulnerable to information security threats

Group interests

- Internet safety

Methods of interaction

- Training activities to improve digital literacy

Results of interaction in the reporting period

For more information on the Company's interaction with vulnerable groups, see the "Digital awareness" section on page 86

Non-profit organizations

Group interests

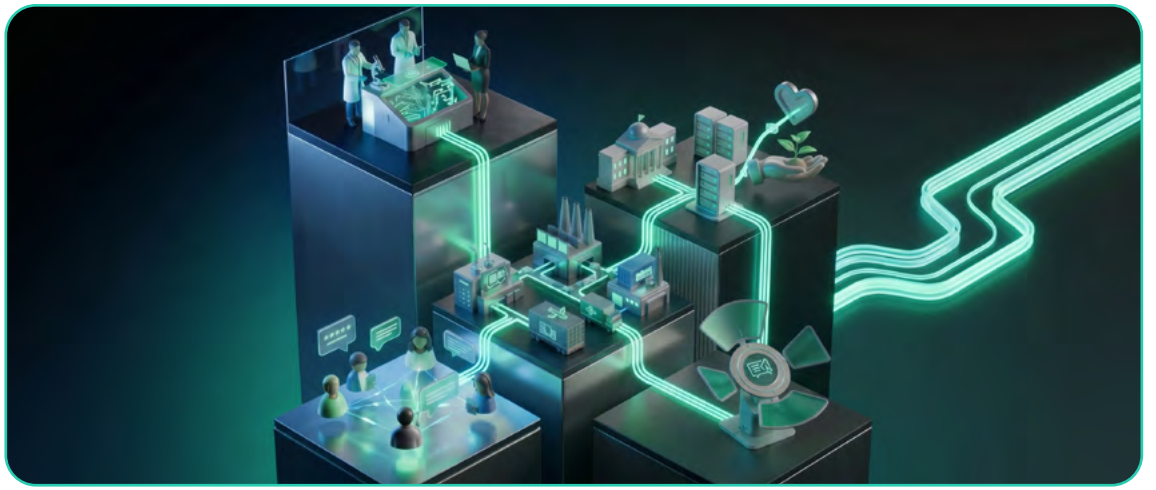
- Assistance in organizing and implementing environmental and social programs

Methods of interaction

- Development, support and implementation of joint environmental and social projects

Results of interaction in the reporting period

For more information on the Company's interaction with non-profit organizations, see the "Social and charitable projects" section on page 74



Digital Security

500,000

new malicious files detected each day in 2025

>554 million

attempts to follow phishing links thwarted by our Anti-Phishing system

>1.4 billion

clicks on phishing links worldwide blocked in 2024–2025

We scale security by combining knowledge and experience

GRI 3-3

Our goal is to protect users and organizations from cyberthreats using advanced technologies and our accumulated expertise.

At Kaspersky, countering modern cyberthreats begins with an analysis of how the modern digital world is structured, what threats arise there, and how they evolve. Accordingly, all our activities in this area are underpinned by the work of our Expertise Centers – multidisciplinary teams whose work we are truly proud of.

They bring together researchers, analysts, engineers and practitioners, who study cyberthreats, investigate cyberattacks, develop new security technologies, and help organizations around the world manage incidents.

Kaspersky solutions:

In 2025, Kaspersky solutions blocked a worldwide total of

>14 million

attacks involving malware, adware or unwanted mobile software.

>144 million

malicious email attachments blocked by Kaspersky Mail Anti-Virus

Detected and blocked web threats[1] on the devices of

34%

of users globally in 2025

Detected local threats[2] (on-device threats) on the devices of

37%

of users globally

[1] Web threats are cyberthreats that penetrate devices via the internet.

[2] Here we mean cyberthreats that are spread via removable USB drives, CDs and DVDs, or that initially get on the computer in a disguised form, for example, in installation files or encrypted files.

Kaspersky's five Expertise Centers

Today, Kaspersky concentrates its expertise in five specialized centers, each of which addresses its own tasks but also works closely with all the others. Together, they let us not only respond to threats, but also understand their nature, anticipate how attacks will unfold, and transform knowledge into reliable protection.

1. Kaspersky Global Research and Analysis Team (GReAT)

As well as researching the most complex APTs and the actors behind them, GReAT experts investigate organized cybercriminal groups and lead the way in exploring the security risks of cutting-edge technologies – often before anyone else has even attempted to compromise them.

Thanks to the joint effort of GReAT and other Threat Research teams, our clients receive access to enhanced mechanisms of protection against advanced threats and exclusive reports on APT threats and threats specific to financial crime which feature a breakdown of tactics, techniques, and procedures (TTP) employed by attackers and indicators of compromise (IoC) necessary for the creation of a robust security system.

GReAT experts also provide unique threat research tools to their colleagues from other centers, aiding both internal and commercial services.

2. Kaspersky Threat Research

Kaspersky Threat Research experts focus on deep analysis of all types of cyberthreats, and develop protective technologies and threat intelligence data that allow organizations to monitor and counter the broadest range of malicious activities.

They shape technological and methodological foundations that make our solutions resilient against compromise.

3. Kaspersky AI Technology Research

The AI Technology Research team explores one of the most significant technological breakthroughs of the 21st century. They excel in driving AI-powered technologies to tackle real-world cybersecurity challenges, navigate the unchartered territory of GenerativeAI applications – in cybersecurity and beyond – and strengthen the security of existing AI-based systems against compromise.

4. Kaspersky Security Services

Renowned for delivering Security Services globally, the team goes beyond customer engagements, uncovering new TTPs, enriching the MITRE ATT&CK framework, developing proprietary tools and enhancing detection capabilities in Kaspersky products.

They also share their expertise through webinars, reports and training to help professionals stay ahead of threats.

5. Kaspersky ICS CERT

Kaspersky ICS CERT leverages deep expertise to combat ICS-specific cyberthreats, identify vulnerabilities in disruption-sensitive environments, and serve as trusted analysts and thought leaders in global industrial associations.

The results of this expertise underpin our Industrial (ICS) Threat Intelligence[1] services, which are available through the TIP[2]. These include research reports, machine-readable feeds of indicators of compromise (IoC), and information about vulnerabilities.

Another important area for ICS CERT is assisting software and hardware vendors. The center helps check the level of cybersecurity maturity of their solutions and make these solutions more secure.

[1] Specialized cyberthreat analytics focused on industrial systems and critical infrastructure.
[2] TIP (Threat Intelligence Platform) is a platform for working with threat analytics.

How we combat cybercrime

GRI 3-3

As we scale security, we develop global cooperation with law enforcement agencies and the professional community, enhancing our expertise and helping improve anti-cybercrime legislation.

We cultivate international cooperation to combat digital offenses

Modern cybercrime knows no boundaries. No single country or organization can cope with this threat alone. A unified effort is required to fight it. That's why we actively cooperate with international organizations, government bodies and law enforcement agencies, helping protect people and companies from cyberthreats.

Kaspersky brings transparency and accountability to this cooperation. Our internal policies establish a clear procedure for handling requests from law enforcement and government bodies. Each request undergoes a legal review according to established criteria and, if necessary, may be rejected or challenged. Moreover, we never provide access to our infrastructure or systems storing user data.

Key documents

- Kaspersky's internal policy governing how law enforcement requests are to be handled (approved in September 2021 by the Company's top managers)
- Agreement with INTERPOL on jointly combating cybercrime under the Gateway project
- Agreement with AFRIPOL on cooperation in preventing and combating cybercrime
- Memorandums of cooperation with various cybersecurity agencies and law enforcement agencies

We conduct joint operations with INTERPOL and AFRIPOL

Kaspersky has been cooperating with INTERPOL in the fight against cybercrime since 2014. In 2019, we also signed an agreement to join the Gateway project.

The support we provide to law enforcement organizations includes:

- exchange of expert information on the latest types of malware and cyberattack methods
- participating in joint operations around the world to identify and combat cybercrime
- cybersecurity training and consulting for INTERPOL and other law enforcement agencies

In 2024, we also formalized our collaboration with AFRIPOL by signing a five-year agreement to combat cybercrime in Africa.

Results of joint operations

>2,600

suspected criminals arrested in 2024–2025

During the reporting period, Kaspersky announced the results of seven joint operations with INTERPOL and AFRIPOL, which resulted in the arrest of over 2,600 suspected criminals.

Operation Synergia

September – November 2023

- More than 50 INTERPOL member states helped identify and block infrastructure used for phishing, malware distribution, and ransomware attacks.
- 31 people were detained.
- 26 arrests in Europe, where most of the servers were taken down.
- Hong Kong police took down 153 servers, Singapore police — 86 servers.
- Authorities in South Sudan and Zimbabwe took down the largest number of servers on the African continent and arrested four people.

Operation Synergia II

April – August 2024

This operation targeted spear phishing, ransomware and stealers[1] around the world. The affected countries were mainly in Europe, Africa and the Asia-Pacific region.

- More than 100 suspects were identified, 41 of whom were arrested.
- Around 30,000 suspicious IP addresses and servers were detected (more than 75% were blocked).
- 59 servers and 43 electronic devices were seized.

Operation Red Card

March 2025

This operation was carried out as part of AFJOC[3], an INTERPOL project to combat cybercrime in Africa, and brought together law enforcement agencies from seven countries (Benin, Côte d'Ivoire, Nigeria, Rwanda, South Africa, Togo and Zambia). Criminals victimized more than 5,000 people.

- There were 306 arrests in the region.
- Approximately 2,000 devices were seized.

Operation Serengeti 2.0

June – August 2025

This operation brought together law enforcement agencies from 18 African countries and the UK to combat ransomware, BEC attacks and online scams. About 88,000 people fell victim to the attackers.

- More than 1,200 suspects were detained.
- 11,432 malicious infrastructure objects were neutralized.
- $97.4 million in damages were recovered.

During this operation, experts from our Threat Research Center provided findings on a cryptocurrency investment scam that led 65,000 people to lose $300 million. As a result, Zambian authorities arrested 15 individuals.

Operation against Grandoreiro

March 2024

We assisted an INTERPOL-coordinated action that led to the arrest of five administrators who ran the Grandoreiro banking trojan, which targeted over 900 financial institutions in more than 40 countries in North and Latin America, as well as Europe. The banking trojan operators are believed to have defrauded victims of more than €3.5 million

Operation Serengeti

September – October 2024

An operation to combat ransomware, BEC attacks[2] perpetrated via corporate email, and other crimes, which caused damage totaling $193 million. More than 35,000 people were identified as victims of these malicious activities.

- More than 1,000 suspects were detained.
- 134,089 malicious infrastructure objects were neutralized

Operation Secure

January – April 2025

An operation to detect and block malicious activity involving infostealing malware in the Asia-Pacific region.

- Law enforcement agencies from 26 participating countries and INTERPOL private sector partners joined the operation.
- More than 30 suspects were detained (including 18 in Vietnam).
- More than 20,000 illegitimate IP addresses and domains were blocked.
- More than 40 servers were seized.
- More than 216,000 victims were warned to take immediate protective measures.

1 A stealer is a malicious program that silently collects large amounts of confidential information from infected devices, such as logins, passwords and payment card details.
2 In a BEC (Business Email Compromise) attack, criminals initiate correspondence with a company employee in order to gain their trust and convince them to take actions that are harmful to the interests of the company or its clients.
3 African Joint Operations against Cybercrime.

We expand our partner ecosystem

Together with INTERPOL, Kaspersky provided cybersecurity for major events.

- 2024 Summer Olympics in Paris — Our experts helped detect phishing attacks and other fraudulent activity. We provided cyberthreat intelligence to INTERPOL as part of Project Stadia, INTERPOL's initiative to protect major international events.
- Singapore Grand Prix, as part of the 2025 Formula One World Championship — We provided cyberthreat intelligence to protect participants from digital risks.

In addition to INTERPOL and AFRIPOL, our partners in combating cybercrime include:

- No More Ransom (jointly with Europol) — Over nine years of work, this alliance has helped more than 6 million users recover their data without paying ransom
- Coalition Against Stalkerware
- Geneva Dialogue
- Paris Call for Trust and Security in Cyberspace
- Council of Europe
- World Internet Conference (member of the High Level Advisory Council)
- International Telecommunication Union
- International Organization for Standardization (ISO)
- Smart Africa Alliance and many other organizations

In 2025, the Company became a member of the International Telecommunication Union's Telecommunication Development Sector (ITU-D) and actively participated in global cybersecurity forums.

We research targeted attacks and advanced threats

According to our Kaspersky Managed Detection and Response (MDR) report, in 2025, advanced targeted attacks (APTs) were detected in 25% of companies and accounted for 43% of all high-severity incidents. APTs were detected in all sectors except telecommunications, with IT and the public sector being the hardest hit.

Moreover, the number of APTs has increased significantly —

by 74%

compared to 2023

In 2025, we identified and helped fix a critical zero-day vulnerability in Google Chrome (CVE-2025-2783) used in Operation ForumTroll, a series of sophisticated cyberattacks against Russian organizations. During the research, experts from Kaspersky GReAT discovered for the first time that spyware created by the Italian company Memento Labs (formerly HackingTeam) was being used in real-world attacks.

Additionally, Kaspersky GReAT experts discovered a new PassiveNeuron cyberespionage campaign targeting Windows Server systems in government, financial, and industrial organizations in Asia, Africa and Latin America (from December 2024 to August 2025).

Key trends in cyberthreat landscape

Phishing and spam campaigns

In 2024–2025, we blocked more than 1.4 billion clicks on phishing and scam links worldwide. Attackers prolifically create fake pages impersonating major brands in order to steal users' credentials and money.

Threats in the financial sector and sophisticated attacks

In 2025, the financial sector faced multi-layered threats: attacks on users' smartphones with banking Trojans as well as NFC-relay attacks, attacks through instant messaging apps and telephone fraud and supply chain attacks.

Increased financially-motivated crime

In 2025, the number of unique financial-sector users encountering ransomware increased by 35.7% compared to 2023[1].

Automated attacks and the use of AI

Attackers actively use machine learning and automation to spread malware more efficiently and evade detection by security solutions.

Threats to mobile devices

The number of Trojan banker attacks on Android smartphones increased by 56% in 2025 compared to 2024.

Supply chain attacks

Almost 19,500 malicious packages were found in open-source projects by the end of 2025, representing a 37% increase compared to the end of 2024.

We help develop legislation

With our extensive expertise in critical infrastructure protection, cybercrime, and data protection, we regularly participate in working groups and public consultations to develop international and national regulations aimed at ensuring global cybersecurity.

Kaspersky was an active participant in the development of the UN Convention against Cybercrime, the first-ever universal international treaty on information security, adopted in December 2024. In October 2025, Eugene Kaspersky spoke at a panel discussion on global cooperation in cybersecurity capacity-building programs, which was held as part of the convention signing ceremony in Hanoi.

We also presented our proposals during discussions of the UN Global Digital Compact (adopted in September 2024), focusing on improving digital literacy, training specialists, the safe use of AI and countering stalkerware.

We help develop standards

Kaspersky contributes to the development of international and national standards related to cybersecurity and the secure development of digital solutions.

During the reporting period, Kaspersky experts helped develop an ISO international standard for the Internet of Things.

It describes the key factors that contribute to the reliability and trust of IoT devices and establishes the basis for more secure and sustainable development of IoT ecosystems.

[1] Data for the period November 2024 to October 2025 compared to November 2022 to October 2023.

We share our expertise

We are passionate about sharing our cybersecurity expertise by speaking at major events and organizing our own conferences, such as the Security Analyst Summit, with representatives from law enforcement agencies, government bodies and the academic community.
We publish information about cyberthreats in our own blog, threat intelligence reports, malware research, APT analysis and statistics via our securelist blog and conduct free webinars on cybersecurity.

In 2024–2025, our experts participated in numerous cybersecurity forums and conferences, including:

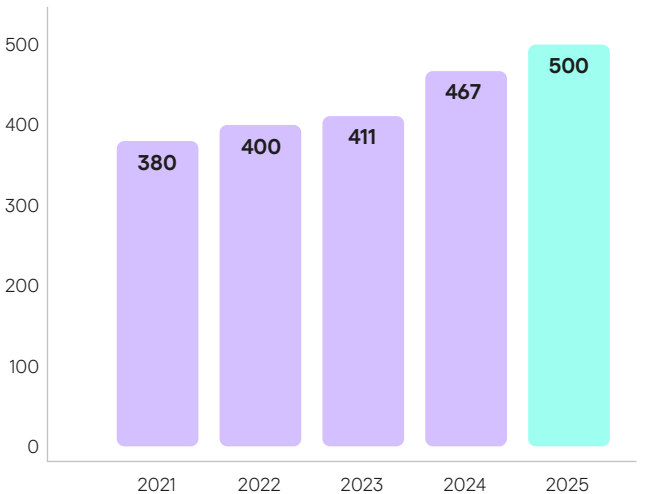
- UN Open-Ended Working Group on Information and Communication Technologies (within an informal dialogue under the auspices of the Chair of the OEWG)
- consultations of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.
- UN Internet Governance Forum, UN Global Digital Compact
- African Cyber Defense Forum.
- Geneva Dialogue working groups
- INTERPOL expert working groups
- World Internet Conference (China)
- Cyber Security Summit (China)
- it-sa Expo&Congress (Germany)
- Singapore International Cyber Week (Singapore)

From November 2025 to March 2026, Kaspersky experts conducted the "Security Operations and Threat Hunting" online training course for around 40 law enforcement officers from 23 AFRIPOL member states.

Results of work combating threat actors

In 2025, Kaspersky's cyberthreat detection systems detected an average of 500,000 malicious files per day—7% more than in 2024[1].

Number of malicious files detected each day by Kaspersky, thousands



- GReAT has uncovered evidence linking the HackingTeam successor, Memento Labs, to a new wave of cyberespionage attacks using Dante spyware. The discovery stems from an investigation into Operation ForumTroll, an Advanced Persistent Threat (APT) campaign that exploited a zero-day vulnerability in Google Chrome. The research was presented at the Security Analyst Summit 2025, taking place in Thailand.
- Kaspersky Threat Research expertise center has discovered a new data-stealing Trojan, SparkCat, active in AppStore and Google Play since at least March 2024. This is the first known instance of optical recognition-based malware appearing in AppStore. SparkCat uses machine learning to scan image galleries and steal screenshots containing cryptocurrency wallet recovery phrases.
- Kaspersky's Global Research and Analysis Team (GReAT) have uncovered an ongoing cyberespionage PassiveNeuron campaign, that targets Windows Server systems in government, financial and industrial organizations across Asia, Africa and Latin America. The activity has been observed since December 2024 and continued through August 2025.
- Kaspersky's Global Emergency Response Team has identified a previously unseen ransomware strain in active use, deployed in an attack following the theft of employee credentials. The ransomware, dubbed "Ymir," employs advanced stealth and encryption methods. It also selectively targets files and attempts to evade detection.

Our plans for 2026

- Help shape the legal framework for combating cybercrime.
- Train and upskill experts, conduct training sessions on relevant cybersecurity topics.
- Collaborate with external organizations and establish partnerships with government institutions to share information on cyberthreats.
- Regularly update software and technology for reliable protection against cyberthreats.

[1] See the Kaspersky Security Bulletin 2025. The statistics in the report cover the period from November 2024 to October 2025.

How we protect critical infrastructure

Our goal is to ensure that cyber-physical systems can operate without interruption at critical infrastructure facilities and in industry through the use of modern technologies, knowledge, and experience.

Protected by Kaspersky solutions

>130
completed projects in the oil and gas sector

>40
companies in the energy and utility industries

12%
of global oil production

>80
completed projects in the electric power industry (nuclear, thermal, renewable energy)

Top 5
global renewable energy producers

>60
oil and gas companies

Critical infrastructure is systems that directly influence the sustainable functioning of the economy, state, and society.

Examples of critical infrastructure

- Energy
- Water supply
- Transport
- Mining
- Metallurgy
- Mechanical engineering
- Food
- Chemical
- Pharmaceutical industries
- Housing and communal services
- Logistics
- Electronics production, etc.

Why this matters

Modern industrial automation systems are increasingly digital, connected, and intelligent, utilizing the cloud, AI, the Internet of Things, and digital twins. This makes production more efficient but also increases risks: the attack surface grows, and the critical infrastructure facilities themselves become attractive targets for attackers. Moreover, many critical systems were originally designed to operate in an isolated environment but are now forced to operate in a highly open and connected environment.

Today, the world faces a growing number of cyberattacks on critical infrastructure, and these attacks are becoming increasingly sophisticated.

Key researches in 2024–2025

- At the beginning of 2025, Kaspersky ICS CERT announced it discovered SalmonSlalom - a campaign targeting industrial organizations in the Asia-Pacific region. The attackers used legitimate cloud services to manage malware and employed a complicated multi-stage malware delivery scheme using legitimate software to avoid detection. As a result, they could spread malware over victim organizations' networks, install remote administration tools, manipulate devices, steal and delete confidential information.
- At the Security Analyst Summit 2025, Kaspersky ICS CERT presented the results of a security audit that has exposed a significant security flaw enabling unauthorized access to all connected vehicles of one automotive manufacturer. By exploiting a zero-day vulnerability in a contractor's publicly accessible application, it was possible to gain control over the vehicle telematics system, compromising the physical safety of drivers and passengers. For instance, attackers could force gear shifts or turn off the engine when the vehicle is driving. The findings highlight potential cybersecurity weaknesses in the automotive industry, prompting calls for enhanced security measures.
- In 2025, Kaspersky ICS CERT discovered a hardware-level vulnerability affecting Qualcomm chipsets that are widely used in a range of consumer and industrial devices, including smartphones and tablets, car components, IoT devices and more. The vulnerability resides in the BootROM – firmware embedded at the hardware level. Attackers could potentially get access to any data stored on the device or device sensors like camera and microphone, implement complicated attack scenarios and in some circumstances get full control of the device.

Energy, water supply, and transport—sectors that directly impact people's daily lives and a country's sustainable development—are increasingly vulnerable.

At the same time, the manufacturing sector remains the main target of attackers. According to our quarterly reports of the main incidents in industrial cybersecurity, the vast majority of organizations attacked in 2024–2025 were in manufacturing.

Our approach to protecting critical infrastructure

We view cybersecurity as a continuous cycle: preparation, monitoring and early detection, response, rapid recovery.

Today, cyber resilience goes beyond traditional cybersecurity. This means that simply blocking attacks is no longer enough: the entire OT infrastructure[1] must be kept stable even during incidents.

Therefore, we are building a security platform for cyber-physical systems, where Kaspersky solutions protect IT, OT and IIoT[2] environments and help organizations implement digital technologies without compromising business stability, human safety, or the environment.

We help minimize risks and evaluate the benefits of investments in protecting critical infrastructure.

How our solutions help businesses save money and make informed decisions

By disrupting industrial operations, cyberattacks can cause significant losses, ranging from equipment downtime to product loss and reputational damage. To help companies more accurately assess the risks and effectiveness of cybersecurity investments, we conducted an international study, together with VDC Research, an analytics firm.

What was the result?

The joint study found that implementing a comprehensive solution (protecting industrial nodes and monitoring network traffic) can reduce the potential damage from cyber incidents:

- **by up to 45%** for energy firms and enterprises offering housing and communal services
- **by up to 76%** for the manufacturing sector.

1 OT (Operational Technology) infrastructure is the systems, equipment, and software that directly control physical processes in industry and at critical infrastructure facilities.
2 Industrial Internet of Things.

We protect at every level

Kaspersky OT CyberSecurity

Kaspersky offers a dedicated OT CyberSecurity Ecosystem that delivers comprehensive protection for industrial environments. At the heart of this ecosystem lies Kaspersky Industrial CyberSecurity (KICS) — a native Extended Detection and Response platform that protects all levels of industrial and critical infrastructure systems and networks.

Level 2

Monitoring and management

- IIoT[1], perimeter protection and upper-level automation (SCADA)
- Access control, auditing, and increased visibility of OT systems
- Expert support on the customer's side

Level 3

Enterprise systems

- Convergence of IT and OT, correlation of data from all available sources
- Unified security processes and approaches using Hybrid XDR
- Training programs, consulting and advanced threat intelligence

Level 1

Controllers and protection

- Detection of intrusions, hacking attempts and compromised microprocessor equipment in low-level automation
- Deep packet inspection (DPI), protection of embedded operating systems from network threats and attempts to change process parameters
- Machine learning for detecting anomalies in industrial processes

Level 0

Industrial process

- Monitoring cyber-physical threats to key equipment
- Ensuring the security of connected vehicles and other physical objects

[1] The Industrial Internet of Things (IIoT) is a multi-level system that includes sensors and controllers installed on components and assemblies at an industrial facility, data transmission and visualization tools, powerful analytical tools for interpreting received information, and many other components.

Key areas of application

- Oil, gas and chemical industries
- Electric power industry, including nuclear power, and housing and communal services
- Metallurgy and mining
- Industrial production, including microelectronics

Promising areas of application of Kaspersky OT CyberSecurity

- Pharmaceuticals and medical equipment
- Transport and logistics, including airports
- Telecommunications
- Large infrastructure facilities (stadiums, business centers, shopping centers, residential complexes)

Kaspersky Next XDR Expert — **IT — OT Convergence**

Specialized solutions

- Kaspersky SD-WAN
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky Antidrone

Kaspersky Industrial CyberSecurity

Native XDR

KICS for Nodes
Endpoint protection, detection and response

×

KICS for Networks
Network traffic analysis, detection and response

Solutions based on KasperskyOS

- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

Knowledge

Cyber hygiene	Threat Intelligence	Training
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

Expertise

Diagnostics	Response	Managed service
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Kaspersky Industrial CyberSecurity (KICS) is the foundation of the Kaspersky OT CyberSecurity ecosystem

Today, KICS protects

12%
of global oil and gas production

10%
of petrochemical production

Up to 15–25%
of the extraction and processing of various metals

15%
of commercial nuclear generation

20%
of nitrogen and phosphorus fertilizer production

The core of the cyber-physical industrial security ecosystem is Kaspersky Industrial CyberSecurity (KICS). This native OT XDR platform provides situational awareness, cyber resilience, visibility into industrial network events, and powerful protection for core automation systems without affecting the availability of industrial processes.

KICS helps prevent costly downtime, security incidents, data theft, and sabotage caused by mass threats, targeted attacks, ransomware, or insider activity, while also protecting legacy equipment, extending its service life, and supporting compliance with national and international standards and information security best practices.

The platform consists of:

- KICS for Nodes — protection of servers, workstations, and operator panels running Linux and Windows
- KICS for Networks — network traffic analysis, asset inventory, anomaly and intrusion detection, and network threat response.

Geographic distribution of KICS

During the reporting period, we significantly strengthened our relationships with companies specializing in energy storage systems and the manufacture of electric vehicles and solar panels. Our clients include five manufacturing companies, each of which is among the top 5 global leaders in their industries, according to independent sources.

In 2025, these relationships gave the business a boost that led to the organization of KICS Con China 2025 in Shenzhen, an innovative region known for its technology cluster. This conference brought together more than 100 participants. Industry roundtables for the oil and gas sector in the META[1] region were also held.

We consistently expand our technology partnership program. The KICS platform has been tested for interoperability with industrial automation vendors in Latin America, East Asia, and China, including Altus, Chint, Consen, Supcon and HollySys, helping customers build resilient supply chains and make responsible technology choices.

Our new KICS-protected clients:

- Nuevo Hospital de Toledo (Spain) — the largest hospital in the Iberia region
- Birla Sugar Group — India's largest sugar producer
- Holy Stone — a leader in China's cement industry
- Atlas Tapes (Greece) — the largest manufacturer of electrical tape in the European Union
- OLED — China's largest OLED display manufacturer

The KICS platform is compatible with a wide range of process control systems from

70+ vendors

>50
successful cases implementing KICS

[1] Middle East, Turkey, Africa.

Native OT XDR platform

Kaspersky Industrial CyberSecurity for Networks

Network traffic analysis, detection and response

Kaspersky Industrial CyberSecurity for Nodes

Endpoint protection, detection and response

- Asset discovery
- Vulnerabilities and risks
- Network visibility
- Traffic analysis toolkit

- Intrusion detection
- Anomaly detection
- Deep packet inspection (DPI)
- Event correlation
- Smart incident prioritization

Several integrations with third-party solutions and synergies within the Kaspersky OT Cybersecurity ecosystem

- Advanced host monitoring
- Hardware and software inventory
- Blind spot coverage (spanless mode)

- Incidents at the host-network interface
- Investigation graph
- Alert enrichment
- Manual response actions
- Restricted network access

- Vulnerability scanning
- Compliance audit
- Configuration change monitoring

- Real-time threat prevention
- Local activity monitoring
- Network activity monitoring
- System Watcher

- Endpoint telemetry (processes, files and network activity)
- Threat development chain
- Response measures

- Malware Scan
- Vulnerabilities
- Compliance
- Traffic capture
- Host inventory

We build Cyber Immunity

Why this matters

A Cyber Immune system is an approach to building IT systems with innate protection against cyberattacks. We believe that such systems can be created using KasperskyOS. To achieve this, KasperskyOS combines best practices in information system development with a focus on secure architecture, secure system design principles and patterns, quality control, secure software development methodology, industry standards, and mandatory penetration testing. This is how we draw closer to a wonderful future where systems solve security problems out of the box.

We propose to build systems so they are secure-by-design by separating them into isolated parts and controlling the interactions between those parts.

As a result, even if an attacker manages to penetrate one line of defense, the rest of the system continues to operate securely. This is especially important for industrial automation, wearable devices, the Internet of Things (IoT), and remote access to critical infrastructure.

KasperskyOS

The KasperskyOS operating system, consisting of a microkernel and the Kaspersky Security System subsystem, provides standard security and enables the development of Cyber Immune solutions.

By combining a microkernel architecture with concepts of MILS (Multiple Independent Levels of Security) and FLASK (Flux Advanced Security Kernel), KasperskyOS creates a fundamentally new level of cybersecurity, significantly increasing a system's resilience to cyberattacks.

In 2024–2025, we took a significant step in our development of KasperskyOS: we adjusted our strategy and began expanding the scope of its use as a full-fledged general-purpose operating system.

Flagship release: Kaspersky Thin Client 2.3

During the reporting period, the key product was the new commercial version of Kaspersky Thin Client 2.3, which combined the achievements of 2024 with new features from 2025:

- extended support for peripherals (webcams, headsets, scanners)
- centralized management of monitor settings via Kaspersky Security Center
- Technical support through remote administration
- Secure Boot mode.

This is the first release certified on the Dell Wyse 3040 platform, marking a significant step in expanding hardware compatibility.

Examples of successful deployment of Kaspersky Thin Client

- Aswant Distribution, an international partner, became the exclusive distributor of Kaspersky Thin Client in Malaysia and Indonesia. Between 2024 and 2025, it delivered cyberimmune thin clients to government bodies, industrial enterprises, and financial and educational institutions in the region.
- The Kulim Municipal Council's deployment of the system reduced operating costs by 20% and increased the cyber resilience of infrastructure.

We create products that help track ESG indicators

Kaspersky Automotive Secure Gateway

Kaspersky Automotive Secure Gateway is a solution for protecting connected vehicles, including a security gateway, an intrusion detection and prevention system (in-vehicle IDPS), telemetry services, remote control, and a navigation system.

Human safety

Our solution and its development processes and individual software components are certified as compliant with ISO 26262 (ASIL B). This functional safety standard for the automotive industry minimizes the risk of harm to human life and health resulting from vehicle system failures.

Accounting for data security and functional safety requirements opens the way to remote business scenarios (remote maintenance, autonomous transportation, flexible operating models for access to vehicles) without compromising on human safety and cyber risks.

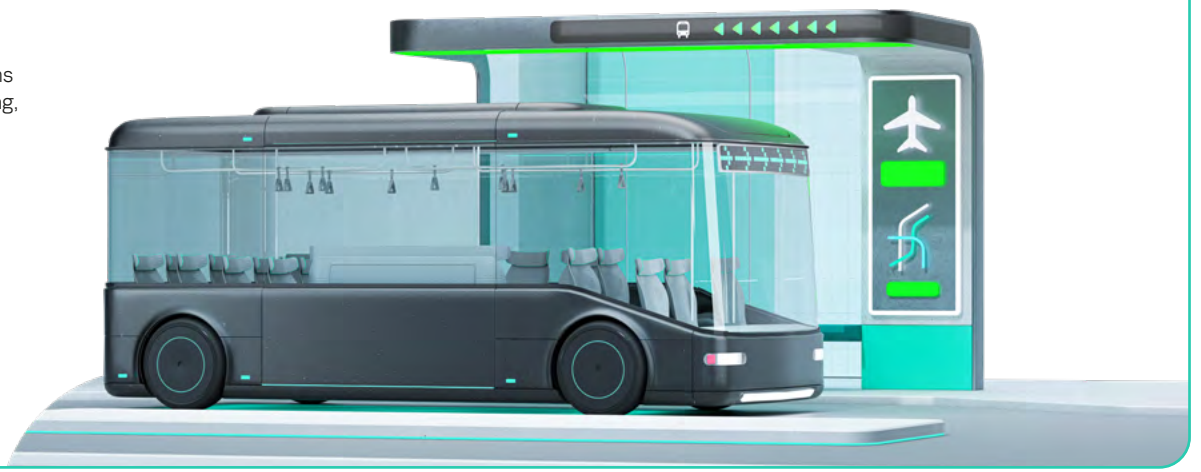
Management quality

Kaspersky Automotive Secure Gateway helps automakers comply with international vehicle cybersecurity standards, including by monitoring information security events and sending them to the Vehicle Security Operations Center (VSOC) for a prompt response and incident investigation.

These features of Kaspersky Automotive Secure Gateway facilitate the implementation of ESG principles in the transportation industry.

Care for the environment

Our solution can continuously monitor vehicle systems (battery, electronics, driving parameters, etc.), enabling, for example, optimized charging and extended battery life, as well as fewer service vehicle trips and, consequently, reduced CO_2 emissions, thanks to predictive diagnostic data.



We comply with requirements and standards when developing solutions

Kaspersky guarantees that its products comply with industrial cybersecurity standards and legal requirements worldwide.

For more information about the legal and industry requirements we account for when developing our products and solutions, please see Appendix 5 on page 135

KICS is the world's first XDR platform certified as compliant with the IEC 62443-4-1 industrial standard.

Both products within the KICS platform—KICS for Nodes and KICS for Network—have been certified as compliant with key international cybersecurity standards and also address or help meet the requirements of other international laws and industry standards.

Our results

Kaspersky OT CyberSecurity in 2024–2025

The Kaspersky OT CyberSecurity platform and Kaspersky Industrial CyberSecurity, one of the solutions included in the platform, showed strong sales growth in the reporting period. Interest in these solutions increased due to:

- market factors, including increased attacks on industrial enterprises, tighter regional regulations, import substitution, a focus on cyber sovereignty and diversification of security suppliers, and increased customer maturity
- Kaspersky's long-term strategy to strengthen its position in domestic markets and expand geographically
- a strategic approach to cross-product ecosystem sales for public sector and critical infrastructure customers

2nd place

in Kaspersky's portfolio in terms of total sales of all ecosystem products

+20%

CAGR (compound annual growth rate) year-on-year

16%

of Kaspersky's revenue comes from industrial customers (second place after the public sector)

KICS in 2025

The KICS platform has demonstrated 25% annual business growth, demonstrating strong momentum in all key markets, including regions affected by geopolitical issues. International sales are growing by more than 50% year-on-year thanks to Kaspersky's strategy to expand its geographic reach.

KasperskyOS

In 2024–2025, the KasperskyOS ecosystem demonstrated sustainable growth and expanded into new markets. The portfolio of KasperskyOS-based solutions has expanded, covering the corporate, transport, and embedded segments. During this period, the platform achieved double-digit growth in the number of installations worldwide and triple-digit growth rates in the Russian market (as percentages).

+25%

growth in sales compared to 2024

Top 5

domains among Kaspersky's B2B products

>540

protected networks of large customers with structural economic importance

+20%

increase in ARPC (average revenue per customer) due to cross-selling and up-selling solutions (cross-selling and increasing sales to existing customers)

>330,000

licenses sold

Our plans for 2026–2027

Industrial cybersecurity

Industrial companies around the world are moving from closed (proprietary) solutions to open architectures and software-defined automation.

Accordingly, our plans for industrial cybersecurity for 2026-2027 include:

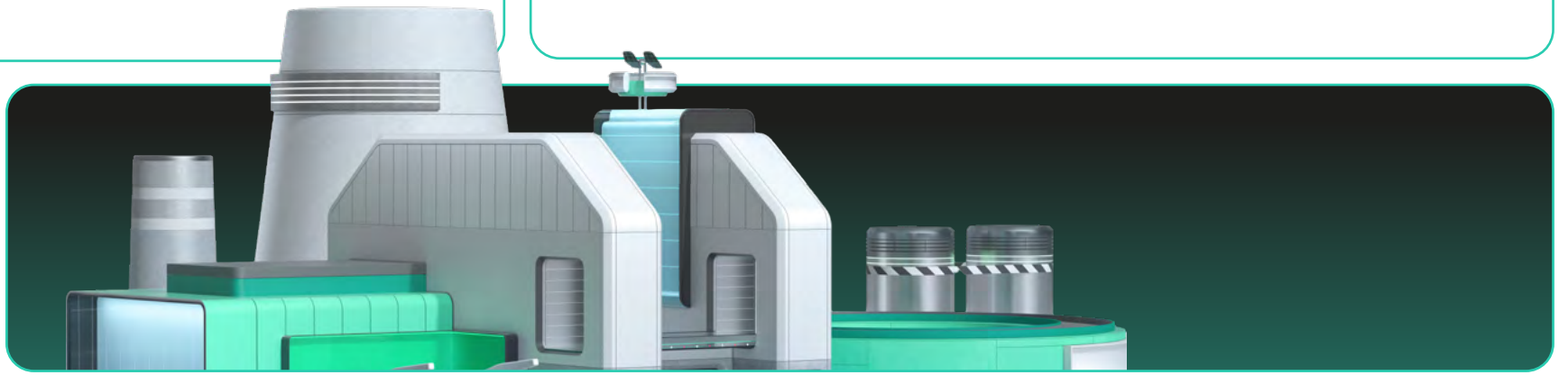
1. **Integrate and develop KICS.** Regarding the development of Kaspersky OT CyberSecurity, we plan to continue integrating KICS with Kaspersky Cloud Workload Security, our solution for protecting cloud and container environments, while simultaneously expanding its functionality and integration with other products. KICS already uses AI technologies for monitoring (device profiling, process analysis), and we are developing protections against future AI-based cyberattacks.
2. **Develop cyberimmune devices and new technologies**. Another area of KOTCS development is the creation of Cyber Immune devices that run KasperskyOS: thin clients. We also plan to progress from connected car gateways to V2X[1] data control devices for highly automated vehicles.
3. **Train specialists**. Together with Kaspersky Academy, we plan to develop collaboration with leading technical universities that have departments or academic laboratories that research automated process control systems or information security. By offering students the opportunity to gain relevant, hands-on experience, we are already building a pipeline of engineers who will protect mission-critical enterprises for decades to come.

Develop KasperskyOS

In the coming years, KasperskyOS will focus on moving beyond its niche as an embedded solution to become a fully-fledged technical foundation for secure, next-generation digital ecosystems.

Main areas for ecosystem development

1. **Expand areas of application**. KasperskyOS will become a universal secure platform for the digital ecosystems of companies, government bodies, and industrial organizations.
2. **Further the technological development of the kernel and SDK**. Improvements to the microkernel architecture, performance optimization, and expansion of developer tools (KasperskyOS SDK) will allow partners and developers to more quickly create new solutions based on the operating system.
3. **Grow the ecosystem**. Build a community of integrators and developers who use KasperskyOS, expand educational programs and startup accelerators related to cyberimmune security.
4. **Expand internationally**. Scale deployment of KasperskyOS in Asia, the Middle East, Turkey and Latin America, creating regional centers of excellence, and developing localized versions of products.
5. **Gain regulatory and industry recognition**. Continue to collaborate with regulators and industry associations to develop standards for a new class of devices and systems whose built-in cyberimmunity is proven by architecture.
6. **Contribute to the ESG agenda**. Use KasperskyOS as a foundation for building secure and energy-efficient solutions in transportation, industry, energy and IT to help reduce carbon footprints and improve equipment efficiency.



[1] Vehicle-to-everything — Real-time communication between a connected vehicle and any other object (other vehicles, road infrastructure objects: traffic lights, pedestrians, networks, etc.) via wireless communication technologies.

How we protect from malware

To protect users from cyberthreats, we develop technological solutions and conduct educational activities, helping people and businesses better understand digital risks and how to protect themselves from them.

Why this matters

As technology evolves, the number of cyberthreats also grows. In 2025, Kaspersky solutions detected an average of 500,000 new malicious files daily, a 7% increase from 2024. These figures clearly illustrate the scale of the threats facing users and organizations.

Experts note that cyberattacks are becoming increasingly sophisticated, with attackers exploiting software vulnerabilities, stolen credentials, increasingly targeting supply chains, and using AI-based tools. In these circumstances, incorrect approach to cybersecurity can lead to extended business downtime and serious financial losses. For private users, it can result in the loss of data and funds.

Main types of cyberthreats

Our solutions protect users and organizations from a wide range of cyberthreats. These include, for example, various types of malware: viruses, worms, Trojans.

Malware can also be classified according to its purposes. For example:

- **Spyware** can track the victim's location, record their screen, and monitor the victim's activity in instant messengers and browsers, as well as record the victim's surroundings using a camera and microphone.
- **Infostealers (password stealers)** can collect and send large amounts of confidential information from infected devices to attackers, such as user's logins and passwords, payment card data, and cryptocurrency wallets.
- **Ransomware** encrypts data on a private or corporate device and then demands a ransom for decryption. Wipers are another type of malware that permanently destroys data, making it impossible to recover from the attack.

Cyberthreats can also be classified according to how they are distributed:

- **Web threats** are malicious software that infects devices via the internet.
- **Local threats** are distributed via removable USB drives, CDs and DVDs or disguised installers.

In 2025, web threats were detected on the devices of 27% of users globally, and local threats were detected on the devices of 33% of users globally. Windows remains attackers' primary target: 48% of users were targeted by different types of threats throughout 2025. For macOS, this figure was 29%.

Globally, compared to 2024, in 2025, detections of password stealers increased by 59%, spyware by 51%, and backdoors by 6%.

Individual users and businesses can also fall victim to phishing, scams, phone fraud and DoS attacks.

Alexander Liskin

Head of Cyber Threat Research at Kaspersky

"Vulnerabilities remain the most popular way for attackers to penetrate corporate networks, followed by the use of stolen credentials. Hence the increase in both password stealers and spyware we have seen this year. Supply chain attacks are also common, including attacks on open source software. This year, the number of such attacks increased significantly, and we even saw the first widespread NPM worm, Shai-Hulud."

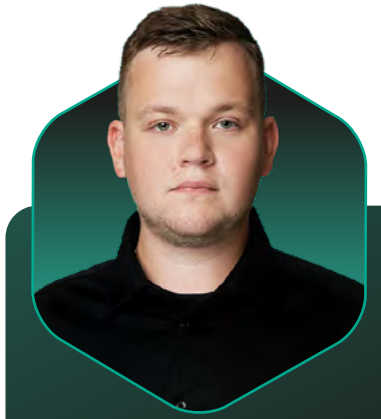
We are responding to the rise in mobile threats

Attackers are increasingly targeting data on smartphones. In 2025, Kaspersky solutions blocked a worldwide total of 14 million attacks involving malware, adware or unwanted mobile software.

Adware remains the most widespread mobile threat, accounting for 62% of all detections in 2025. Over 815 thousand new unique installation packages including 255 thousand mobile banking Trojans were observed in 2025, showing a decrease compared to the previous year. We observed a massive surge in activity from Mamont banking Trojans.

During the reporting period, new complex mobile threats were also identified: SparkCat and SparkKitty for iOS and Android, as well as LunaSpy for Android disguise themselves as legitimate applications - these malware programs stole user data, including passwords and cryptowallet seed phrases. For example, SparkCat malware is spreading through both infected legitimate apps and lures – messengers, AI assistants, food delivery, crypto-related apps, and primarily targets users in the UAE and countries in Europe and Asia. It scans image galleries for keywords in multiple languages, including Chinese, Japanese, Korean, English, Czech, French, Italian, Polish, and Portuguese.

Modifications of known mobile malware families also appeared. For example, updated versions of the banking Necro Trojan and the infamous Triada Trojan, which can modify cryptocurrency wallet addresses during transfer attempts, replace links in browsers, send arbitrary text messages and intercept replies, and steal login credentials for messaging and social media apps. These facts show how quickly mobile threats are evolving.



Dmitry Galov

Head of Kaspersky GReAT in Russia and the CIS

"Lately attackers actively spread mobile malware through instant messaging apps, disguised as photographs, delivery trackers, support apps for telecom operators, medical assistance services, and more."

To protect smartphones from cyberthreats, we recommend that smartphone owners download apps only from official sources and use our reliable protection solutions: Kaspersky for Android and Kaspersky for iOS.

We protect against ransomware

Risks for businesses and individuals

Ransomware is one of the most dangerous types of cyberthreats to organizations. Ransomware programs are called cryptors because they gain access to a device, encrypt data, and then the attackers demand a ransom from the victims.

Such attacks can cripple companies of all sizes, from large corporations to small businesses, and cause damage in all regions. For example, in 2025 Latin America had the highest share of organizations with ransomware attacks detected (8.13%), followed by the Asia-Pacific region (7.89%), Africa (7.62%), Middle East (7.27%), the Commonwealth of Independent States (CIS, 5.91%) and Europe (3.82%).

A successful attack costs a business far more than the ransom. The downtime, supply chain disruptions, reputational damage and subsequent recovery costs can all be many times greater than the direct payments to the attackers.

Together with VDC Research, we calculated the potential losses to industrial companies globally from downtime due to ransomware attacks in the first three quarters of 2025. We estimate that they could have exceeded $18 billion — and this is only the potential damage caused by the halt of production.

$18 billion

is the potential global cost of ransomware attacks on organizations in the manufacturing sector globally in just the first 9 months of 2025

14 million attacks

involving malware, adware or unwated mobile software blocked by Kaspersky solutions in 2025

New ransomware tactics

In 2024–2025, we noted several alarming trends related to cryptors:

- **active use of AI** in the creation of malware
- **prevalence of the RaaS** (Ransomware as a Service) model, where individual groups develop cryptors and rent them out to other hackers for a share of the ransom
- **shifting attacks to non-standard penetration points**. Instead of sending phishing emails or searching for vulnerabilities in a web server, attackers are now looking for non-trivial entry points: webcams, IoT devices, and other poorly protected equipment
- **increased average ransom amount** even as threat actors' total income decreases. For example, in 2024, the average ransom size increased by approximately 50% compared to the previous year, reaching $4 million[1].

Our solutions

Kaspersky helps its customers protect themselves from the increasingly complex cyberthreat landscape.

We have developed various cybersecurity solutions and recommendations for organizations to help reduce the cyber risks of attacks and minimize damage.

We have also developed products that demonstrate high effectiveness against various types of malware. Independent tests confirm that users are effectively protected by Kaspersky Security for Business, Kaspersky Small Office Security, and Kaspersky consumer suite: Kaspersky Standard, Kaspersky Plus, and Kaspersky Premium.

During the reporting period, Kaspersky Standard received the Top-Rated Product award for 2024 from the independent lab AV-Comparatives, scoring a total of 100 points out of a possible 105. Kaspersky has been awarded this title six times already, and in 2023 the solution was recognized as Product of the Year for the seventh time.

In 2025, Kaspersky Premium for Windows received an "Approved" certificate of quality based on annual anti-phishing testing by AV-Comparatives. It detected 93% of all phishing links and successfully passed the false positive check.

Kaspersky Security for Business achieved 100% protection in AV-Comparatives' tests of protection against unauthorized use of credentials, passing all 15 tests. Kaspersky EDR Expert was highly rated for achieving a 100% cumulative Active Response rate in the Endpoint Prevention and Response Test and was certified and awarded Strategic Leader status for the third consecutive year.

In 2025, Kaspersky received the Cybersecurity Leaders award in three categories. The jury noted the development of Kaspersky Container Security (KCS), a solution for protecting container environments at all stages of their lifecycle (by the end of the year, more than 30 KCS deployment projects had been completed), and Kaspersky Unified Monitoring and Analysis Platform (KUMA), a SIEM platform with the integrated AI-powered Kaspersky Investigation and Response Assistant (KIRA).

Kaspersky also received awards for its achievements in cyberthreat analytics—in its Kaspersky Threat Intelligence suite of services—and its work in providing organizations with up-to-date data on attacker techniques and tactics for building proactive defenses.

In addition, Kaspersky continues to actively participate in No More Ransom, an international initiative that it helped to found. This project was created in 2016 with the aim of helping ransomware victims regain access to their encrypted data without paying money to the attackers.

Members of the alliance, including Europol, the Dutch police and cybersecurity vendors, share expertise, knowledge, and decryption tools that help recover data encrypted by ransomware.

How we closed a loophole for attackers

Our incident response experts regularly identify and address vulnerabilities exploited by ransomware.

We participate in incident investigations, helping to close vulnerabilities before they can be exploited.

In 2025, while analyzing a MedusaLocker ransomware attack on a company in Brazil, Kaspersky specialists identified a vulnerability in ThrottleStop, a legitimate utility that the virus used to gain privileged access to the system.

Result
We immediately reported the issue to the utility's developer and quickly added detection for the new exploit to our products, thereby closing another hole used by ransomware.

[1] According to a report published by Sophos, a software development company.

We provide the latest information on cyberthreats

To effectively combat cyberthreats, we provide organizations with access to the Kaspersky Threat Intelligence suite of services, which delivers up-to-date data on attackers' tactics, techniques, and procedures. The Kaspersky Threat Intelligence Portal is a single point of access to reliable threat intelligence. Users can also access a free version of the portal: Kaspersky Open TIP. You can request access to this service here.

>200

private cyberthreat reports published annually

>900

APT groups and operations continuously monitored by Kaspersky

We regularly share insights into cyberattacks at industry events and in the media. For example, GReAT experts analyzed the activities of the FunkSec ransomware group and published a report on its methods. They discovered that it features a unique password-based mechanism that controls its operation modes. Without a password, the malware performs basic file encryption, while providing a password activates a more aggressive data exfiltration process in addition to encryption to steal sensitive data. Notably, code analysis showed that FunkSec was actively using generative artificial intelligence to create its tools.

We improve digital literacy

Kaspersky conducts special research and surveys aw well as lifestyle guides and tips to raise awareness about cyberthreats that people face in real life, often without even realizing it:

- Scams targeting lovers or the lovelorn. With Valentine's Day coming up, we examined a special breed of scams aimed at lovers, married couples, and single people.
- Is this love or stalking? Kaspersky privacy experts explained how to spot red flags in digital relationships
- Travel safely and comfortably. Ahead of summer we shared a guide on the best apps for travelers to help them plan a comfortable vacation trip, focusing on tips how to stay connected, find bearings in a new place or good food and get around safely.
- Growing up online. In collaboration with the UAE Cyber Security Council we released a report on the online behavior of parents and children in the UAE, aiming to uncover trends, habits, and concerns associated with internet usage. One of the key findings showcased that 33% of children in the UAE play computer games that are not suitable for their age.
- The digital illusion: millennials and the risks of online trust. Our research revealed a concerning stat – 70% of millennials rarely verify the authenticity of the people they engage with online, leaving them vulnerable to cyberrisks such as identity fraud, misinformation, and emotional deception.

In 2024–2025, in partnership with other organizations, we released several interesting studies to the general public.

Our plans for 2026–2027

- Research various schemes and cyberthreats and provide relevant analytics in new reports
- Conduct and publish research and surveys to inform users about the various cyberthreats they may face
- Release our annual global reports on ransomware attacks, mobile threat landscape, etc.

How we protect various user groups

GRI 3-3

Protecting various user groups is an important part of our work to create a safer digital space.

We combat cyberstalking

What is stalkerware and why is it dangerous?

Modern technologies have become an important part of life and help us in many ways, but sometimes they are used to our detriment. One such threat is digital stalking or cyberstalking.

Attackers can install a special kind of application, known as stalkerware, on the victim's smartphone. This software operates covertly and secretly monitors a person through their device: it collects location information, reads correspondence, and gains access to photos and other personal data without the smartphone owner's knowledge. This is a serious problem, both as technical and a social one, as it violates a person's right to privacy and can often be linked to domestic violence.

The scale of the problem

23%

of online dating service users worldwide have experienced online stalking

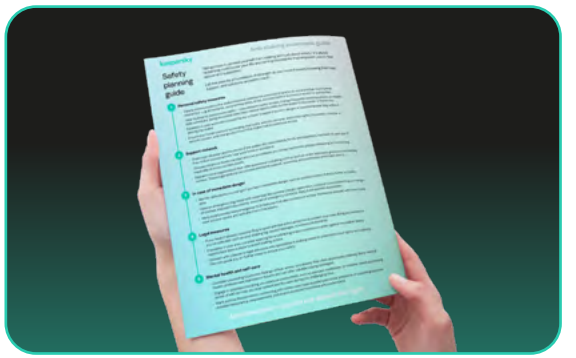
34,000

users worldwide encountered stalkerware in 2024–2025

Research by Kaspersky shows that digital stalking is an urgent threat.

According to the results of a global study by the Company[1], approximately one in four users (23%) have experienced some form of digital stalking from a person they were newly dating. The types of abuse varied, with 39% of respondents having reported some form of violence or abuse from a current or previous partner: 10% admitted they had had their location tracked, 10% that their social media accounts or emails had been hacked, and worryingly, 7% having had stalkerware installed on their devices without their consent.

It is very difficult to detect stalkerware without special tools. If you discover a suspicious app, experts advise not to delete it immediately (the stalker might quickly find out it has been deleted), but to seek help from professionals, a crisis center or the police.



We help users protect themselves

Kaspersky has been protecting users from digital stalking for many years, leading the fight against cyberstalking. In 2019, we implemented a stalkerware detection feature in our mobile app. Our Kaspersky for Android solution scans the device and alerts the user when hidden surveillance apps are detected.

In 2024, we went further and added a new feature – Who's Spying on Me, extending its protection against digital stalking. In addition to the stalkerware detection, the new feature provides protection from offline stalking by detecting suspicious devices tracking the location of a person or object via Bluetooth technology.

In addition to technical solutions against stalking, Kaspersky strongly emphasizes education and cooperation.

In November 2024, we published the Anti-Stalking Awareness Guide, which was created in collaboration with international experts and victims of stalking. The initiative aims to support victims and their families, raise awareness of the problem, and provide practical tools for protection. This guide helps users understand stalking, debunks common myths, and describes the manipulative methods used by stalkers. It focuses on two practical checklists covering both digital and physical security.

[1] The study involved 21,000 people worldwide.

The first checklist includes recommendations for creating a safety plan, a form for documenting incidents, and tips for family and friends who support victims. It was created with the help of:

- Olimpia Coral Melo Cruz, an activist who initiated "Olimpia's Law" in Latin America, which has become the foundation for the fight against digital violence
- Marcela Hernández, co-founder of Red Latinoamericana de Defensoras Digitales, a support network for digital rights defenders
- Janaina Campos, a Brazilian psychoanalyst who works with dysfunctional relationships
- Acacia Diana and Yulia Pavlova, victims of stalking who shared their personal stories to raise awareness among other women

The second checklist, our Digital Security Guide, which was developed by Kaspersky expert Anna Larkina, contains recommendations for protecting personal data, configuring privacy on devices and reducing digital risks that can make a person vulnerable to online harassment. Together, these materials form a holistic approach to supporting victims, encompassing both physical and digital security, and underscore Kaspersky's commitment to creating a safer digital space for everyone.

Additionally, Kaspersky experts regularly share tips on digital security. For example, we recommend using complex, unique passwords and not sharing them, carefully managing privacy on social media, and not disclosing too much personal information online. These simple measures reduce risks and help users feel more confident.

We join forces and help victims

>40

organizations are part of the international Coalition Against Stalkerware, co-founded by Kaspersky

Combating cyberstalking requires the combined efforts of many participants, and Kaspersky actively works to bring stakeholders together. In 2019, we co-founded the international Coalition Against Stalkerware, which today unites more than 40 organizations—from IT companies to law enforcement agencies. Together with our partners, we raise awareness about digital violence and help victims.

Kaspersky participates in international initiatives to combat digital violence, such as Europe's DeStalk project. Another joint project is "Revolutionizing Online Safety: Tackling Technology-Facilitated Abuse to Protect Victims and Survivors of Intimate Partner Violence"[1]. In addition to Kaspersky, other international companies, representatives of the academic community, and non-profit organizations are participants. This project is being implemented in partnership with the British agency UKRI from 2023 to 2026. Kaspersky supports the project by sharing its expertise in combating cyberbullying and stalking, and by participating in additional events.

[1] Research on how to protect victims / survivors of intimate partner violence (IPV) from the risks created by digital technologies.

A safe space for people who need protection

We support the Nizhny Novgorod Women's Crisis Center

We understand every statistic represents real lives, so we strive to participate in initiatives to help victims in real life.

Problem
Women and children who face domestic violence and stalking often need safe shelter urgently. Moreover, sometimes victims do not even have access to their own documents and money. In these circumstances, they have no chance of finding emergency shelter in many regions.

What we did
Since 2022, Kaspersky has supported the Nizhny Novgorod Women's Crisis Center's Safe Apartment project. It offers secret housing that victims can move in to on the same day they apply. Beneficiaries receive basic necessities: accommodations, food, clothing, means of communication, as well as psychological, legal and social assistance. The project imposes no formal barriers, offering help even in the absence of documents.

Result
Over four years, with our support the center has managed to provide shelter and assistance to 32 women with children.

We ensure children's online safety

Creating a safe online environment for children is a priority, and our future depends on it. Kaspersky is working on this both internally and in partnership with ministries, agencies and other organizations around the world.

Why this matters

Children today begin using the internet from a very early age — for study, communication and entertainment. The online environment offers many opportunities for growth, but at the same time, it also carries real risks: threats of fraud, cyberbullying, dangerous content, attempts to manipulate and pressure. Children often encounter these threats before they have time to understand how to resist them, and adults don't always know what exactly is happening to their child in digital spaces.

We believe that technology alone is not enough to protect children online. It's important to understand children's online lives, what they trust, what they fear, and what problems they face. That's why Kaspersky has been conducting surveys on the digital habits of children and parents for many years and then turning knowledge we gain into practical solutions: educational programs, useful materials, and initiatives available to families, schools, and communities around the world.

What does our research say?

One of our key projects in the area of children's digital safety is a regular survey that we use to prepare our annual report on kids' digital interests. On International Children's Day we issued an analysis, covering the period from May 2024 to April 2025, revealing a growing fascination with AI-powered chatbots, the viral rise of Italian brainrot memes like "tralalero tralala," and growing attention to Sprunki — a rhythm-based game combining music and motion. YouTube remains the most popular app among children globally, while WhatsApp overtook TikTok for second place.

We continued to analyze children's digital habits using anonymized data from our Kaspersky Safe Kids solution The data show that children are spending more and more time on online games, video platforms, and social platforms, are using mobile devices more often, and are actively interested in gaming and video content.

At the same time, they continue to face key risks: fraud, unwanted content and pressure from unknown users. These findings confirm the need for a comprehensive approach to children's online safety that combines technology-based protection, education, and improved digital literacy among children and parents.

We also studied how attackers exploit the popularity of children's brands. For example, in the reporting period, our experts analyzed threats that use references to well-known games, toys, and cartoons (Minecraft, Roblox, LEGO, Disney, etc.) as bait. The study found that in the first quarter of 2024 alone, the number of such attacks increased by 35% compared to the previous year.

We educate and support children, parents, and teachers

We believe that developing digital literacy should be accessible, clear, and engaging. That is why Kaspersky actively participates in educational and awareness-raising projects.

Easy-to-understand materials for the whole family

To discuss digital literacy and other complex topics in simple terms, we create special publications for children and adults.

- Cybersecurity Alphabet is an educational book about technology and digital threats, built around the alphabet. It helps children and parents understand new terms and learn safe online behavior. Between 2024 and 2025, we translated the book into 15 languages, and in October 2024, Cybersecurity Alphabet was commercially released in Russian.
- Digital Schoolbag is a practical guide for parents, offering tips on how to protect children both online and offline: from setting up devices to conversations about safety and trust. The guide is available for free and is aimed at parents without a technical background.

Regional initiatives

Our work to protect children online extends far beyond the borders of one country.

- In **Italy**, as part of the Privacy Tour organized by the Italian Data Protection Authority, we distributed 500 copies of Cybersecurity Alphabet to people participating in educational events.
- In **Germany**, at the largest IT industry exhibition, it-sa Expo&Congress in Nuremberg, participants received 500 copies of these books.
- In **Morocco**, Kaspersky experts participated in a family day at the Cadi Ayad School in Casablanca, where they spoke to children and parents about digital risks and ways to protect themselves. They also presented Cybersecurity Alphabet. About 50 children and their parents participated in the event.

KidZania: Safety through play and experience

In March 2025, we opened the Cyber Research Center at KidZania Santa Fe in Mexico. Here, in this renowned entertainment capital, children learn the basics of cybersecurity by playing, completing practical tasks, and learning to recognize digital risks. Kaspersky's Cyber Research Center at KidZania will allow visitors to become cyber investigators, tackling challenges such as digital fraud, online espionage, and identity theft. Children will also develop key skills like critical thinking and problem-solving while learning how to protect their privacy and security on the internet.

Our plans for 2026–2027

- Publish analytical reports and educational materials on children's online safety
- Participate in educational and awareness-raising projects to improve digital literacy among children, parents and teachers
- Open new cyber research centers at KidZania, an educational theme park for kids, in India and the UAE.
- Develop partnerships with international law enforcement organizations, coalitions, and non-profit organizations to combat stalking.

How we turn knowledge into protection

GRI 3-3

By investing in R&D and creating innovative technologies, we transform knowledge and expertise into new practical solutions for protecting the digital world.

We invest in research and new products

~3,000
Kaspersky employees work in R&D

373
unique research publications for 2024–2025

We believe that to effectively protect people and businesses from cyberthreats, we must constantly evolve and stay one step ahead of attackers. Accordingly, research and work to improve security solutions are among the key areas we focus on at Kaspersky.

Kaspersky's R&D departments employ approximately 3,000 specialists — engineers, analysts, researchers and developers. Their shared mission is to transform cyberthreat expertise and knowledge into practical security solutions that help clients feel more confident in the digital environment.

During 2024–2025, our experts prepared 373 unique research and analytical publications. In them, we share research findings, observations about emerging threats, approaches to protection, and practices that help the market and community better understand the modern cyber-risk landscape.

Main areas of development

In the reporting period, Kaspersky primarily invested in three new and extremely promising areas:
- We enhance corporate network security protection with NGFW
- development and sales of Kaspersky Container Security
- creation of cloud products for the international market (XDR Optimum, Cloud XDR)

Kaspersky also develops innovative solutions at the intersection of the cybersecurity and physical security of industrial facilities. For example, our Kaspersky Antidrone system is designed to detect and protect against drones.

The Kaspersky Antidrone project has four patents in Russia, two patents in the United States, and three patents in Europe. The system has been awarded the AGBA Cybersecurity Innovation Award and the Industrial Design Award.

We enhance corporate network security protection with NGFW

We developed and launched a next-generation firewall (NGFW) based on our global expertise and advanced technologies.

This solution helps businesses:
- protect the corporate network from a wide range of cyberthreats
- monitor the activity of applications and services
- manage traffic effectively to ensure a more stable network
- optimize infrastructure performance, reducing the risk of downtime and incidents.

We make container and cloud environments more secure with Kaspersky Container Security

Kaspersky Container Security (KCS) is a solution that protects containerized applications at all stages of their life cycle, from development to operation.

KCS helps organizations:

- protect business processes and reduce the likelihood of incidents
- comply with security standards and regulations
- build security into development processes and follow DevSecOps principles, according to which security is implemented from the very beginning, at all stages of the product life cycle
- free up information security resources for other tasks by automating certain checks and controls
- reduce time to market by enabling faster development and faster releases while complying with security requirements

Kaspersky Container Security is designed with container environments in mind and provides protection at multiple levels: from container images to the host operating system—the environment the containers run on.

KCS is part of Kaspersky Cloud Workload Security, our comprehensive solution for protecting cloud workloads. As part of this platform, KCS helps reliably protect against cyberattacks and reduce the time required to detect threats in cloud environments and respond to them.

We make it simpler to detect sophisticated attacks with cloud-based XDR products

We create cloud-based XDR products, XDR Optimum and Cloud XDR, for the international market to make it easier for companies to detect and stop sophisticated cyberattacks.

XDR is an information security concept that helps:

- proactively identify threats at various levels of infrastructure
- respond quickly to incidents
- repel complex attacks that are not always noticeable by a single indicator

XDR combines endpoint device protection (EDR) capabilities with other security tools from a single vendor and connects additional data sources. As a result, specialists get:

- a single point for decision making
- a user-friendly interface
- advanced capabilities for investigating complex cyber incidents

For the international market, we are developing this product as a cloud-based service—this format helps companies significantly reduce the cost of using the solution and achieve benefits faster without complicating their infrastructure.

AI's role in cybersecurity

Using artificial intelligence and machine learning, we help people and organizations detect cyberthreats faster, mitigate risks, and confidently use digital technologies in their daily lives and work.

Why this matters

Attackers are increasingly using AI to automate attacks. Our experts regularly see AI used to generate phishing pages, ransomware, malware for advanced targeted attacks (such as Bluenoroff), and in campaigns targeting Russian organizations, such as Librarian Likho.

Attackers are automating more and more steps in the attack chain. However, it is important to note that AI does not radically change the threat landscape.

AI is also actively used in cyber defense: it can significantly improve threat detection performance, including detection of complex attack techniques such as DLL hijacking[1].

That said, reliable protection still relies on a multi-layered approach: endpoint and network protection, managed services (e.g. MDR), advanced end-to-end solutions such as XDR, and high-quality threat analytics (Threat Intelligence). AI plays a different role: it improves the response speed, scalability and accuracy of security technologies, helping to resist cyberattacks.

How we use AI in cyber defense

~20 years

Kaspersky has been using AI and ML technologies

135 AI-related patents

Kaspersky's intellectual property portfolio

Kaspersky has been using AI and ML technologies in its products and services for almost 20 years.

Each day, artificial intelligence helps analyze hundreds of thousands of suspicious and malicious files, identifying patterns and anomalies in a split second. At the same time, we view AI not as a replacement for human specialists, but as a support tool: algorithms take on routine signal processing, freeing up experts to analyze complex, targeted, and unconventional attacks.

Our Kaspersky AI Technology Research Center brings together data scientists, machine learning engineers, and experts on threat intelligence and infrastructure to solve the most ambitious challenges at the intersection of AI/ML and cybersecurity. This work includes developing and improving applied technologies, research into the safety of AI algorithms, raising awareness of AI risks, and much more.

We expand threat detection capabilities

Kaspersky has developed many AI/ML-based threat detection technologies, primarily for identifying malware, but also to detect attackers' suspicious activity. For example, in 2025, our experts trained an ML model to detect attempts to use DLL-hijacking techniques and used it to improve the KUMA SIEM system. Our solutions use not a monolithic algorithm that does everything, but a set of specialized models that each perform a particular task. This approach makes our protection more robust and accurate.

Key applications of AI/ML[2]

- Early file checks. Deep neural networks help identify malicious executable files based on static characteristics at early stages, even before the files are launched.
- Automatic creation of detection rules. Machine learning (ML) technologies based on decision trees help generate threat detection rules that can run directly on the user's device. This is important when it comes to quickly translating threat knowledge into practical defenses.
- Behavioral analysis. Even if a file appears safe, malicious activity can occur while the program is running. Behavioral patterns help identify such threats through their atypical actions.
- Identification of malicious internet resources based on anonymous telemetry received from solutions installed on clients and other sources.
- Protection from phishing and spam. We reduce risks to users by applying specialized models, including an ML model for detecting fraudulent web pages and DeepQuarantine for quarantining emails suspected of spam.

Thanks to our cloud infrastructure, AI results are available to users almost instantly, and new threats are blocked immediately upon detection.

[1] An attack technique in which an attacker injects a malicious dynamic-link library (DLL), causing a legitimate program to load and execute malicious code.

[2] Read more about these technologies in our whitepaper Machine Learning for Malware Detection.

We combat phishing and online fraud

Online fraud has become more sophisticated over the years: modern phishing sites look neat, their text is often error-free, and the visual elements mimic the interfaces of well-known services. To combat these threats, we use machine learning and content analysis.

In particular, Kaspersky protects against phishing through:

- optical character recognition (OCR) to identify malicious text hidden within images
- proprietary ML models that identify the telltale signs of fraud, having been trained on datasets of legitimate and counterfeit websites.

This is especially important as scammers increasingly use images and visual bait to try to bypass simple filters.

We help SOC specialists be more effective

In corporate environments, security professionals often encounter excessive "noise," i.e. a large number of alerts that do not represent real incidents. This wastes a lot of time.

Our Managed Detection and Response (MDR) services use AI algorithms to automatically analyze event streams and filter out false positives, allowing tens and hundreds of thousands of benign incidents to be resolved each year without human intervention. As a result, security operations center (SOC) specialists can focus on truly important attacks and respond more quickly to real threats.

Our enterprise monitoring and response solutions (Kaspersky SIEM and Kaspersky XDR) use machine learning for risk scoring when evaluating the behavior of devices and servers within the infrastructure. This helps identify hidden attacks and anomalies without sharing data outside the company, which is especially important for organizations with stringent confidentiality requirements.

We develop AI for industry and physical objects

Artificial intelligence is used for more than just protecting computers and networks. In industry, equipment failures and errors can lead to downtime, accidents and serious financial losses.

Machine learning-based solutions such as Kaspersky MLAD (Machine Learning for Anomaly Detection), which provides predictive analytics, are used to address such scenarios. These solutions analyze equipment telemetry and help identify early (hidden) signs of impending equipment failure, process disruptions, cyberattacks and human errors. By continuously training the neural network, MLAD analyzes the stream of "atomic" events from an object, structures the stream into patterns, and identifies abnormal behavior.

We prevent AI from being abused by malicious actors

Attackers actively use artificial intelligence to automate their work: creating phishing resources, accelerating the creation of malicious code, scaling up fraudulent schemes and creating audio and video deepfakes.

Our analysis of detected threats created using AI lets our specialists improve the effectiveness of protection against malware, phishing and scams, and then share recommendations with users. For example, Kaspersky experts recommend that users be suspicious of any unexpected messages, audio, and video, always double-checking information, and using reliable security solutions.

We research large language models

Generative AI and large language models have already become part of digital reality. We are developing infrastructure for researching and safely using their capabilities and for rapid prototyping. We deploy LLM tools, such as ChatGPT, in this environment, where they are available to employees across all departments for day-to-day tasks while also serving as a foundation for developing new solutions.

A key practical scenario is using language models to assist analysts. In particular, the Kaspersky Threat Lookup service (part of the Kaspersky Threat Intelligence Portal) now enables AI-enhanced open-source intelligence search, providing customers with summaries and article abstracts related to analyzed objects in the OSINT (Open-Source Intelligence)[1] tab, saving them time when searching for IoCs (Indicators of Compromise) or researching cybersecurity reports.

[1] Open-Source Intelligence - a branch of intelligence that analyzes information about people or organizations from sources available to the public

Examples of detected malware that was created using AI or that has an AI theme

- FunkSec. Our analysis of the ransomware revealed signs of automated code generation. The targets include public sector, IT, financial, and educational organizations in Europe and Asia.
- RevengeHotels. We detected a new wave of attacks on hotels that aims to steal bank card data. Samples created using AI have been identified in the campaign.
- Malware disguised as DeepSeek and Grok. Campaigns with fake pages that distributed a stealer, a malicious PowerShell script[1], and a backdoor. Links to one of the malicious resources were posted online, including on the social network X (formerly Twitter).
- BrowserVenom. A phishing resource imitating the DeepSeek website invited visitors to download a model for Windows, but in reality, it distributed a Trojan that intercepts traffic.
- Jarka. Malicious packages distributed through the Python Package Index (PyPI) repository under the guise of tools for neural network-based chatbots infected devices with a stealer.
- Gipy. The downloader was distributed under the guise of a neural network-based voice-changing app.

Our AI research

Loose-lipped neural networks and lazy scammers:

we analyzed the artifacts that LLMs may leave behind on phishing and scam pages (including characteristic phrases as well as traces in markup).

Why and how people manipulate neural networks:

we found out how and why people use indirect prompt injections[2] — for example, to point large language models at their resumes, etc.

Deepfake Services Are Now 400 Times Cheaper and More Accessible:

we analyzed multiple Russian- and English-language platforms and uncovered ads on darknet offering real-time video and audio deepfake services.

How we manage AI safety

We view AI safety as a complex issue that extends far beyond AI technologies themselves. It isn't just about protecting algorithms and models, but also about how AI is used at Kaspersky, what data it processes, what risks it creates, and how these risks are managed.

AI safety is multifaceted. It involves:

- legal and compliance issues—for example, what data is permissible to use and send to cloud-based AI services
- IT and information security processes, including access management, configuration control, and preventing the use of so-called "shadow AI," i.e. when employees use external AI tools without approval;
- processes used to develop and train models, where it is important to understand data sources, possible biases, model vulnerabilities, and scenarios where models could be abused.

Effective management of these risks requires specialists from various fields: information security, IT, and legal teams, as well as data science and machine learning experts. Ideally, dedicated AI security specialists would coordinate the work of these teams.

We also recognize AI security is a very rapidly evolving field. New approaches, vulnerabilities, attack methods and security tools are constantly emerging. Therefore, we believe AI risk management is an ongoing process that requires knowledge, practices and training materials to be regularly updated.

[1] A PowerShell script used by attackers to covertly execute commands, download malicious code or control an infected system.

[2] A method of manipulating AI in which instructions for the model are hidden within the data it is working with, rather than being fed to it directly.

We foster cooperation and share expertise

We grow our AI expertise systematically, performing fundamental research, building infrastructure for model training, and implementing practical applications in products and services. We believe that sustainable AI development is only possible with the active exchange of knowledge. Accordingly, Kaspersky participates in international initiatives and industry alliances, collaborates with the professional and academic communities, and appears in industry rankings.

In 2024, Kaspersky joined the Global Community on Artificial Intelligence for Industry and Manufacturing (AIM Global), which was created in 2023. AIM Global brings together governments, international organizations, commercial companies and industry leaders. By participating in AIM Global, we are able to exchange expertise, help develop unified approaches to applying AI, and support the development of technologies that reflect ethical, social, and technological considerations.

In 2025, Kaspersky joined the ranks of organizations supporting the UN Global Digital Compact. The document sets out objectives and principles that will help achieve an inclusive, open and sustainable digital future.

We share our AI expertise with communities. Some research, such as our work on monotonic machine learning algorithms or the application of neural networks to spam detection, is published as academic papers at leading machine learning conferences, and other research is published on specialized portals and at information security conferences.

For example, we publish research on the security of our own AI algorithms, including by writing about simulated attacks on spam detection and malware detection algorithms. We research the use of neural networks for time series analysis.

We also release training materials and courses, including for information security professionals and developers, to help them safely implement AI solutions and consider potential risks.

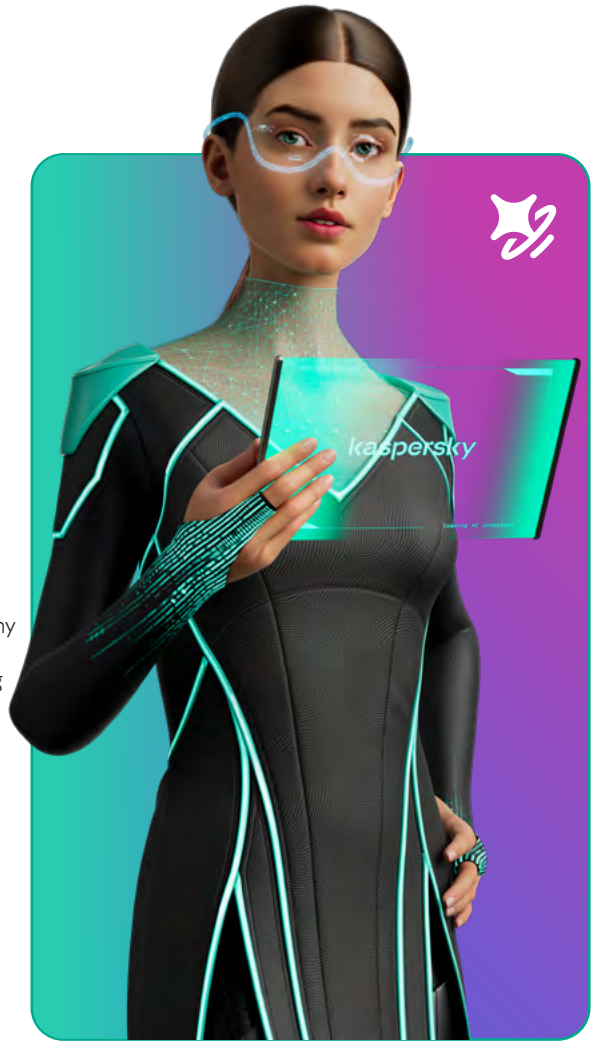
In 2025, Kaspersky released a course to train developers and information security specialists in the fundamentals of protecting systems based on large language models. We also continually update our expert training portfolio to ensure our training materials meet the needs of businesses, government agencies and academic institutions.

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky's AI and ML expertise is also recognized externally. In 2025, Kaspersky won the IT Leader award in the Artificial Intelligence category. The award was given to our SIEM system: Kaspersky Unified Monitoring and Analysis Platform (KUMA) with the built-in AI-powered Kaspersky Investigation and Response Assistant (KIRA).

Smart Ranking

In 2025, Kaspersky also placed fifth in the Russian company Smart Ranking's ranking of AI firms, having demonstrated significant growth in revenue from sales of solutions using AI and machine learning. And in 2024, Kaspersky was recognized among key employers in Russia's AI sector based on the results of a TAdviser study.



We adhere to principles for responsible and ethical use of AI

We believe that artificial intelligence should be used responsibly and transparently, especially in such a sensitive area as cybersecurity. Accordingly, Kaspersky regularly participates in the development of legislation, policies, and other documents covering various aspects of security in working with new technologies, including AI.

At the 2024 UN Internet Governance Forum (IGF), Kaspersky presented the Guidelines for Secure Development and Deployment of AI Systems.

Earlier, in 2023, we formulated and then publicly presented at the IGF the first principles for the ethical use of AI in cybersecurity, which we adhere to in our work.

- **Transparency**. We explain how AI works: clients have the right to understand where and why machine learning technologies are used.
- **Security**. We make security a priority: all AI systems undergo validation, testing, and specialized audits. We are taking measures to minimize dependence on third-party datasets in the training of AI-powered solutions.
- **Human control**. Human experts can always intervene, check, and adjust the algorithms when analyzing complex threats.
- **Confidentiality**. We take steps to protect data and systems to ensure the digital privacy of our clients.
- **Commitment to cybersecurity goals**. By focusing exclusively on security technologies, we fulfill our mission to build a safer world and demonstrate our commitment to protecting users and their data.
- **Openness to dialogue**. We share best practices related to the ethical use of machine learning algorithms with all stakeholders.

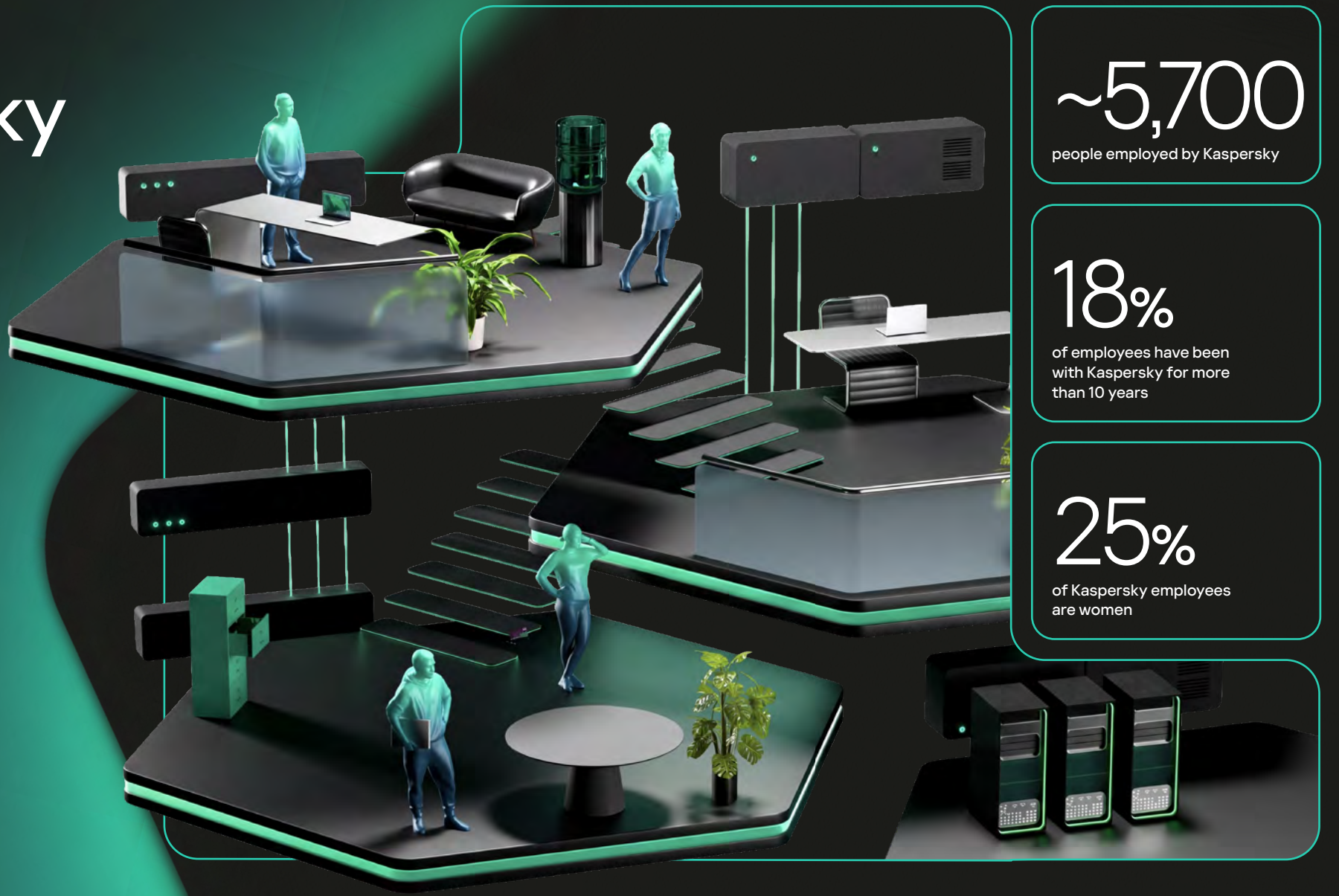
Plans for 2026–2027

Kaspersky plans to expand its portfolio of machine learning-based solutions, complementing it with technologies that cover the full cycle of work with cybersecurity solutions. We seek a reasonable balance between resources used and results achieved: we use AI methods that are as reliable and fast as possible, while also being effective and understandable.

Our highest-priority plans include:

- develop classic statistical and ML models for detecting various types of malware, content attacks and anomalies, including searching for attacks involving lateral movement and unauthorized use of accounts.
- apply generative AI to new kinds of tasks inaccessible to traditional ML algorithms, primarily by expanding KIRA's skills and KIRA's use in various products—from Kaspersky SIEM to Kaspersky Container Security.
- develop a paradigm for agentic AI: create KIRA skills that combine existing decision functions and help in multi-step investigation and response scenarios without a pre-defined script. Such deep integration may require the creation of MCP (Model Context Protocol) interfaces to provide the AI model with access to our solutions' built-in tools.
- enter the market for vulnerability management solutions. A new AI-powered product will help organizations quickly identify and fix vulnerabilities and configuration errors in their IT infrastructure.

People at Kaspersky



~5,700
people employed by Kaspersky

18%
of employees have been with Kaspersky for more than 10 years

25%
of Kaspersky employees are women

Human resources management

GRI 3-3

Employees are Kaspersky's most important asset. We aim to make working at Kaspersky comfortable and engaging, so everyone can be productive, feel secure, grow, and contribute to the company.

~1,000

new employees joined us

including

>200 interns

13%

of our Russian employees, including two top managers, started as interns and rose through the ranks at the company

Key documents

- Labor Code of the Russian Federation
- Internal labor regulations
- Regulations on Compensatory Payments
- Regulations on Wages
- Personal Data Processing Policy

Our approach to personnel management

We build relationships with our employees based on trust and mutual respect. Our approach is to continuously analyze work processes and the work environment. We strive to listen to employees' needs and support them in every situation. This helps create the conditions necessary for productive work and professional development and, as a result, for the growth of the business as a whole.

Our key objectives:

- ensure decent working conditions and professional development, including competitive pay and a generous benefits package;
- invest in employee training and development, implement new educational programs
- create conditions that foster career growth, expand professional experience, and allow employees to change their career path.

Human Resources Management System

Personnel management is handled by a dedicated department comprising eight functional streams, each narrowly focused on specific tasks. This division of responsibilities helps structure HR management processes and adapt them to the needs of a large international business.

Among other things, this structure includes a separate function associated with international operations.

In addition, Kaspersky regards employee development and investment in its people as a distinct and important function, with several teams specifically dedicated to these matters.

Corporate culture and business ethics

We maintain high standards of governance and business ethics by implementing corporate best practices. Kaspersky's corporate culture supports employee development, career advancement, and personal well-being.

Key documents

- Labor Code of the Russian Federation
- Corporate Code of Ethics
- Guiding Principles on Business and Human Rights

Personnel headcount and structure

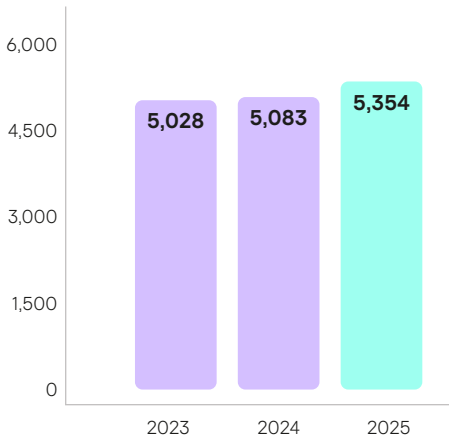
GRI 2-7, GRI 401-1

In 2025, the total number of Kaspersky employees grew by 11.3% year-on-year, reaching 5,691.

In 2025, approximately 1000 new employees joined us, including more than 200 interns. Additionally, 18% of employees have been with Kaspersky for more than 10 years, and 13% of our Russian employees, including two top managers, started as interns and rose through the ranks at the company.

We expect staff turnover to drop significantly, by 5 percentage points, from 15% in 2024 to 10% in 2025. Kaspersky ensures business continuity through human resources management, implements new HR practices, and improves existing ones. We believe in long-term relationships with people and in developing opportunities for their growth within the company. Furthermore, we believe that interesting and challenging tasks, being part of expert teams, and sharing a corporate culture play a key role in retaining talent.

Average number of Kaspersky[1] employees



+11.3%

growth in total employee headcount in 2025 compared to 2024

[1] The previously published figure for 2023 has been adjusted due to a change in the calculation methodology.

Our incentive system

Kaspersky creates a comfortable and motivating environment where employees feel supported, see opportunities for growth, and understand the value of their contribution.

We pay close attention to all aspects of working life, from office conditions to performance reviews. We believe that skilled professionals should be rewarded for their contribution to Kaspersky's growth. Therefore, we maintain competitive salaries, offer employees one of the broadest benefits packages on the market, and actively implement and improve professional development and training programs.

Financial incentives

We strive to pay highly competitive and fair compensation that can attract and retain the best professionals and motivate them to achieve results.

In building our compensation programs, we are guided by the following principles:

1. **Rewards for results.** Kaspersky does not automatically index wages, but there is an annual salary review process. This lets us maintain competitive employee salaries and accelerate the growth of employees who perform at a high level.
2. **External competitiveness.** We regularly review the market and ensure that our total compensation packages remain highly competitive.
3. **Transparency.** We communicate openly with employees about how we approach putting together a compensation package to ensure they understand our compensation philosophy.

At Kaspersky, Total Target Cash Compensation (TTCC) includes a fixed component (salary) and a target bonus.

Kaspersky reviews employee salaries annually. Globally, Kaspersky employees' salaries increased by an average of 6% in 2024 and by 7% in 2025.

Average year-on-year increase in salaries of Kaspersky employees:

6%	7%
in 2024	in 2025

Social policy and care for people

GRI 401-2

We support our employees throughout their time at Kaspersky and do everything possible to ensure they feel confident in various life situations.

We offer our employees a comprehensive benefits package and medical care as part of our insurance program and provide financial assistance to those dealing with unforeseen difficulties. Elements of the benefits package differ from region to region of Kaspersky's presence.

At the office, employees can access the services of a general practitioner, massage therapists, and psychologists, and also use a gym and sauna. We also created an online mental health support line for employees. In addition, Kaspersky develops corporate sports programs and reimburses employees for fitness expenses.

Regular internal communications help us gather employee feedback on various employment issues: we hold AMA sessions and kickoff[1] meetings with management, share results and plans, and discuss strategy. Each year, we assess employee satisfaction through an internal survey and hold our Annual Kaspersky Awards ceremony, where we recognize key individual and team achievements across all departments.

We help all employees whose families have children, whether biological parents, adoptive parents, or guardians. They have access to parental leave. In Russia we supplement the state maternity benefit with our corporate benefit of up to the employee's full salary for the entire duration of maternity leave (usually 140 calendar days).

[1] An introductory meeting.

For more information on how we support mothers with children, see the "Supporting female employees' parenthood and well-being" subsection on page 64

Career development and internships

We see personnel development as the foundation for business growth. Kaspersky encourages career mobility—both vertical and horizontal—between positions, teams, and departments. This broadens employees' experience, improves cooperation between departments, and increases motivation.

In 2025, we launched several initiatives designed to support career growth:

- **Grow Lab** — a space for knowledge sharing and expertise development, where employees can learn from each other and work with mentors
- **Internal Mobility** — a program aimed at cultivating internal job transitions, helping employees try new roles and projects within the company if they are ready for a change
- **Career advice** — individual support for employees in choosing their next steps in professional development: from deepening their current expertise to changing their direction.

We pay special attention to young professionals. Since 2016, we have run Kaspersky SafeBoard, a paid internship program for Russian university students. About half of our interns become full-time employees upon completion of their internship. Many of them now occupy leadership positions at various levels and are now using the SafeBoard program to recruit interns for their own teams.

For more information about the SafeBoard program, see "Training personnel for the IT industry" section on page 85

Equal opportunities

Kaspersky provides equal opportunities to all employees and does not tolerate discrimination in any form.

This is a key corporate principle for us and aligns with the UN Guiding Principles on Business and Human Rights, as well as the UN Sustainable Development Goals, including SDGs 4.5, 5.1 and 8.5.

For more information on the Company's contribution to achieving the UN SDGs, see the "Sustainable development" section on page 19

We strictly comply with legal requirements and make decisions about hiring, developing, and rewarding employees solely based on their professional qualities, experience and achievements—without any restrictions on gender, age, or other characteristics.

Respect and a safe work environment

Kaspersky's adopted rules and standards of conduct are based on our values and principles. Every employee is important to Kaspersky and deserves respect. We strive to maintain a healthy, open, and welcoming work environment where people feel comfortable collaborating, sharing ideas, and growing.

Kaspersky does not tolerate any form of discrimination, humiliation, insults, any pressure, or violation of personal boundaries. We adhere to generally accepted standards of business ethics and expect professional, proper, and respectful behavior from our employees and partners.

How we support employees

We build relationships within Kaspersky based on trust and mutual respect. To ensure a comfortable work environment for everyone, we regularly review working conditions, performance evaluation processes, and employee feedback. We listen to everyone's needs and do everything we can to ensure Kaspersky employees feel supported and cared for in every situation.

As Kaspersky, human resources management includes a business partnership function. HR business partners help build dialogue between the business and employees, support teams in challenging situations, and facilitate solutions that account for the interests of all parties.

If an employee experiences discrimination or unethical behavior, they can report it to the HR Support team or their HR business partner. In addition, the HR Support team is always ready to assist employees with any questions, from administrative procedures to consultations on corporate training and development.

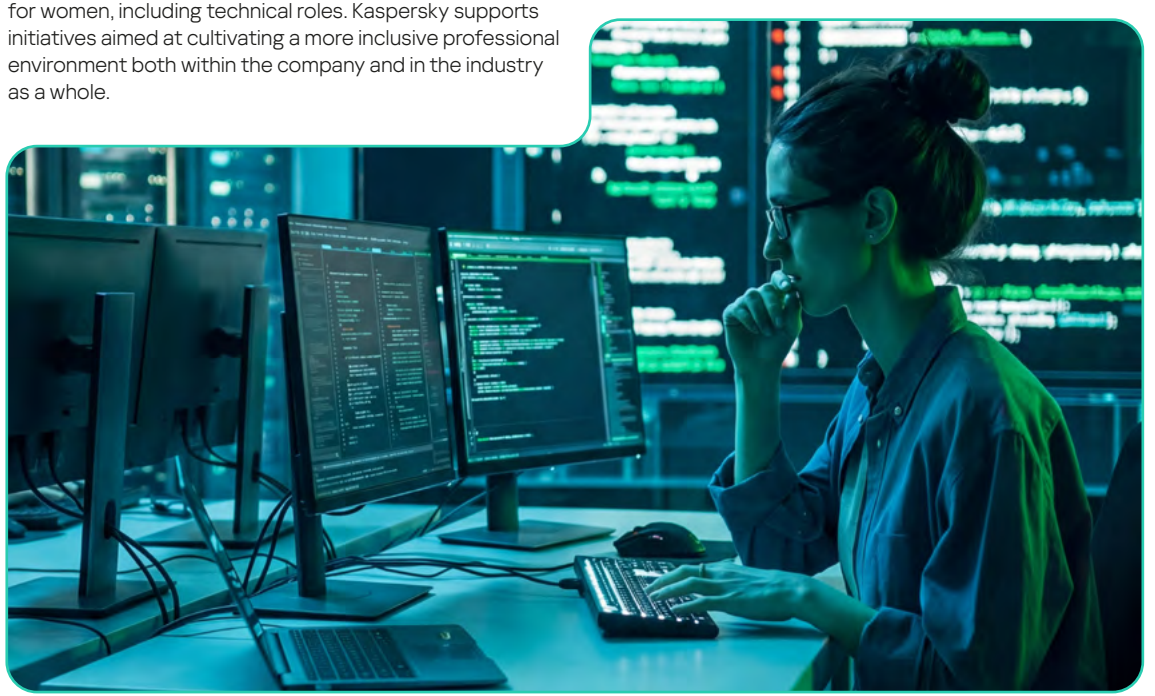
Women in IT

Kaspersky consistently works to demonstrate the diversity of IT career opportunities and create an environment in which people with different experiences and professional paths who share our values can realize their professional potential. This work is carried out across Kaspersky's global markets.

We focus on overcoming persistent stereotypes about women's role in the technology sector and on expanding opportunities for professional and career advancement for women, including technical roles. Kaspersky supports initiatives aimed at cultivating a more inclusive professional environment both within the company and in the industry as a whole.

Our approach to supporting women

We believe that sustainable innovation is only possible in an environment where all employees, regardless of gender, have equal access to opportunities, support and recognition. Our initiatives are part of a long-term strategy to create a safer and more inclusive digital world through the diversity of experiences and perspectives of our teams, which include both men and women. This is how we envision the future of IT and cybersecurity: diverse and built on the strength of different voices.



We start with schools and universities

We are committed to making IT education accessible and open to everyone from an early age. Accordingly, Kaspersky partners with schools and universities around the world, conducting lectures, master classes, and internship programs so that all schoolchildren and university students, regardless of gender, can better understand the technology sector and see their own opportunities in IT and cybersecurity.

We foster a women's IT community within the company

Involving and supporting women in the IT industry is an important part of Kaspersky's corporate culture, which is shaped at the level of the board of directors and senior management. Additionally, women who have already achieved success at various levels actively participate in support programs: they communicate with colleagues and subordinates, share experiences, and inspire beginning IT specialists by their example.

Moreover, we support our internal women's tech community and initiatives aimed at increasing women's representation in technology and related roles.

We ensure equal access to career opportunities

Kaspersky strives to be as fair and open as possible to prevent gender discrimination.

We apply a skills-based approach when recruiting new employees for our team. We are primarily interested in candidates' professional skills, qualifications, and relevant experience. We evaluate competencies without regard to gender, focusing on a candidate's motivation and the extent to which they share our values and are willing to contribute to the overall mission. This approach helps to minimize the risk of discrimination and maintain a fair and transparent hiring system.

25%

of Kaspersky employees are women

26.7%

Women make up of the global tech industry in 2025[1]

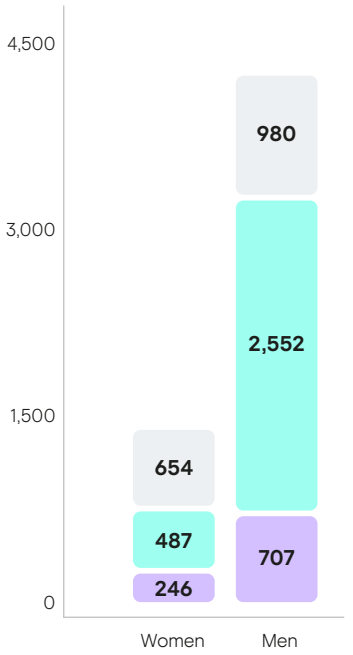
26%

of women at the company hold leadership positions

[1] According to research by Exploding Topics. The tech sector includes companies working in IT, cybersecurity, AI, cloud technologies and others.

SASB TC-SI-330-a.3

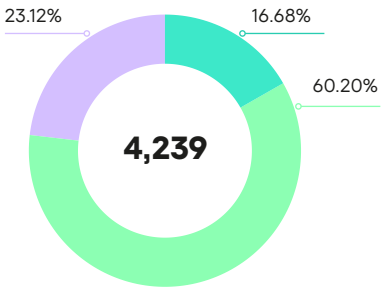
Total number of employees by gender and role category[1]



GRI 405-1

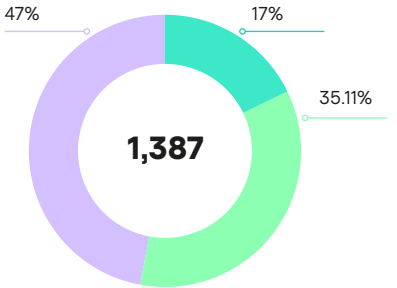
Total number of employees by gender and role category[3]

Men



Managers[2]	707
Technical specialists	2,552
Other specialists	980

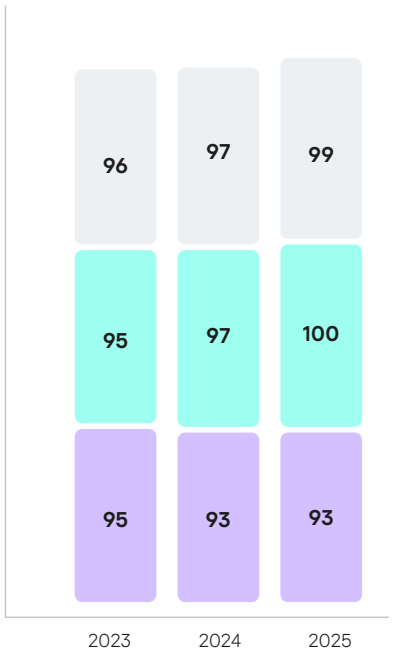
Women



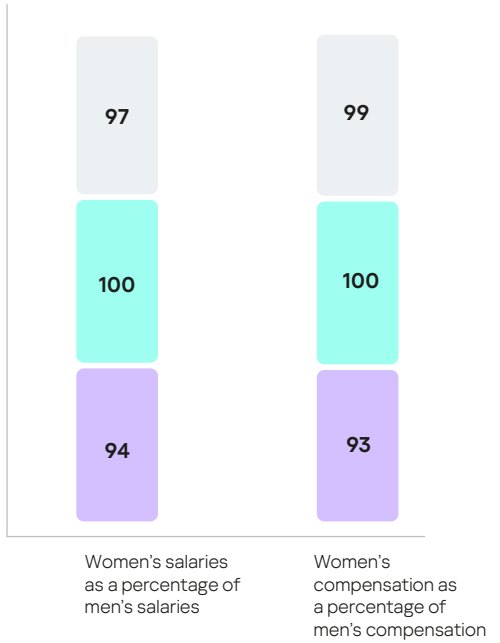
Managers	246
Technical specialists	487
Other specialists	654

GRI 405-2

Ratio of total target cash compensation[4] of women and men[5], %



Ratio of base salary[6] and total target cash compensation[4] of women and men in 2025[1], %



1 The provided data for Kaspersky's Moscow office as of December 31, 2025.
2 Employees who have at least one person reporting to them.
3 As of December 31, 2025.
4 Total Target Cash Compensation consists of base salary and a target bonus.
5 The provided data for Kaspersky's Moscow office as of December, 31 for the years: 2023, 2024 and 2025.
6 Base salary represents the fixed, guaranteed component of employees' compensation.

We support female employees' parenthood and well-being

In all countries where we operate, we strive to inspire our female employees along their career paths and support them at the most important moments in their lives. Kaspersky offers support programs for parents in every region where we operate, but specifics may vary depending on the laws of a given country.

We bring women together in online communities

In 2021, Kaspersky launched its Empower Women project, an online worldwide platform about women in cybersecurity and technology that brings together research from various regions, news, and the inspiring Women in IT podcast, which features female employees. During the reporting period, ten Kaspersky employees in various countries shared stories of their professional and personal development on the platform, and four opinion round-ups and six special projects appeared on the website.

In 2024, we launched our Letters To The Past project, where our employees share personal and professional stories in the form of letters to their younger selves, describing the challenges they overcame and the lessons that helped them become who they are today.

We inspire the next generation of women in IT

To help the upcoming generation of women in technology, Kaspersky launched the Future You in Tech global initiative, an online quiz aimed at schoolgirls and female university students choosing their career path. The project helps girls and young women understand the scope of cybersecurity, available roles and career opportunities, and which ones might be right for them based on their personal interests and talents. It also lowers barriers to entry to the profession.

In 2025, we actively promoted the project internationally: we worked with Africaines in Tech to present the quiz at the Transform Africa Summit, organized by Smart Africa in Conakry, Guinea, and at the Women in Tech special online session of the ATDA[1] conference in Rabat, Morocco. This helped attract more young women from African countries who are considering a career in IT. At the time of writing, more than 180 young women had taken the quiz, and this number continues to grow as the initiative expands its geographic reach.

Special projects about women in tech

Kaspersky implements several global themed projects dedicated to women's role, past and present, in the IT industry.

Our initiatives for 2025 included Women in the History of Tech, which highlights women who helped advance technology in a wide range of fields — from cybersecurity, IT entrepreneurship, and digital education to telecommunications, public digital policy, e-commerce, and public safety. The project's participants included female professionals with experience in tech businesses, startups, the public sector, and educational initiatives, demonstrating the diversity of career paths in the digital industry.

Another initiative is Mothers in Tech, dedicated to our female employees who combine their professional careers with motherhood. The project shows that self-actualization can take different forms and can be tailored to individual life circumstances and priorities.

That same year, we launched another new project: Confronting IT's Career Barriers, an interactive quiz that shows the obstacles that specialists face in technology fields. Participants decide what barriers they are willing to tolerate and learn how these compromises can hinder growth and why they cannot be ignored. The quiz also provides recommendations on how to overcome these barriers and explains their significance in the technology sector.

In total, more than 400 men and women from all over the world took the quiz. They helped identify the most pressing barriers, which included a toxic or unhealthy work environment, overwork, limited career advancement opportunities, insufficiently transparent promotion criteria, and biased employee evaluations. The results demonstrate the importance of changes in corporate culture.

[1] ATDA — Assises de la Transformation Digitale en Afrique, a major industry event on digital transformation in Africa.

Partnerships, events and activities

Kaspersky builds long-term partnerships and actively participates in initiatives that help strengthen women's position in IT and cybersecurity worldwide. We focus on supporting career growth, developing leadership, sharing experiences, and expanding access to digital opportunities for women and girls.

In 2024, Kaspersky sponsored the 100 Women Face to Face project. This initiative included offline and online meetings, as well as a series of webinars on developing women's tech career opportunities. Additionally, BTHaber magazine published an introductory column by Ilkem Özar, Kaspersky's General Manager in Turkey, in which she discussed the project's goals and significance.

The Turkish magazine CIO Update dedicated a special issue to women leaders in IT for International Women's Day. Ilkem Özar, Kaspersky's General Manager in Turkey, joined leading women in the industry in a group photo on the magazine's cover and gave an interview for the print and video editions, discussing her career path and the importance of inclusion in the tech industry.

In March 2024, Kaspersky held a press conference in Mexico to present its State of Stalkerware report and raise awareness about the problem of digital stalking. The discussion featured Olimpia Coral, a well-known digital rights advocate, and Judith Tapia, Kaspersky's consumer product manager in Mexico. The speakers discussed the impact of stalkerware on users and presented practical recommendations for detecting and preventing it.

As part of a summer boot camp for 800 students from various Turkish universities, organized by BÜSİBER (Boğaziçi University MIS Cybersecurity Center) and Cyber Technology Clubs, Kaspersky held a training day and panel titled "Women in Technology," dedicated to women's growing role in cybersecurity. Ilkem Özar, Kaspersky's General Manager in Turkey, moderated the event, where invited industry experts discussed how to strengthen women's positions in IT and the career opportunities available to them.

Anna Pavlovskaya, Digital Footprint Intelligence Analysis Team Lead at Kaspersky, spoke at the European Women in Tech forum. She presented her research on the psychological profiles of cybercriminals, based on an analysis of informal conversations on darknet forums.

Gladys Yiadom, Kaspersky's Senior Public Affairs Manager, participated in Future Forward Paris, an event organized by the Wonder Women Tech project. During a panel discussion titled "Impact and Resilience: Building a Better Future," she discussed how Kaspersky helps make the world a safer place through educational projects for vulnerable groups and initiatives aimed at supporting women.

Kaspersky served as a consulting partner at the Women Empowerment Conference (WEC) in West Africa, which brings together women leaders, entrepreneurs, and technology innovators from across the region. The event focused on inclusion, leadership, and women's access to digital opportunities.

In 2025, Kaspersky signed a three-year memorandum of understanding with Smart Africa. This important partnership aims to advance cybersecurity across the African continent and reduce the gender gap in STEM/ICT through dedicated programs for women and girls.

In 2024–2025, Kaspersky employees served as mentors, conducted webinars, and provided free access to training for Outreachy interns and other early-career professionals. These activities help young professionals, including women, gain initial skills and experience in IT and cybersecurity.

In July 2025, in collaboration with the Women in Tech Russia community, we organized an online conference: "How to Prove Yourself in IT: Personal Branding and Digital Reputation for Career Growth." The first part featured a roundtable discussion titled "How an IT Specialist's Image is Formed in the Eyes of Employers—From GitHub to LinkedIn, From Old Forums to Conferences," featuring Elena Mikheeva, Talent Development Director at Kaspersky. The second part featured TED talk-style presentations, including one by Anna Pavlovskaya, Digital Footprint Intelligence Analysis Team Lead at Kaspersky, titled "Stack Overflow, Habr, and Internal Wikis: Digital Footprint or Digital Trail." More than 150 participants attended the online conference.

Kristin McDonald, Kaspersky's Senior Enterprise Marketing Manager for the META region, was recognized with an industry award for Senior Marketing Leader of the Year at the Women in Technology Forum and Awards 2025. The award recognizes her contribution to the development of the technology sector and the advancement of women in it.

Kaspersky funded and supported the production of a special Africaines in Tech podcast episode that was recorded in February 2025 and published in November. In the episode, Gladys Yiadom, our Senior Public Affairs Manager, discusses Kaspersky's vision and the steps the company is taking to strengthen women's inclusion in cybersecurity in French-speaking Africa.

In September 2025, Kaspersky and GRAMAX, a trusted partner in protecting critical information infrastructure, held a special session: "Resilience in Action: The Women Beyond the Firewalls." It focused on supporting and advancing women in cybersecurity, examining women's current status in the industry, the progress made, and the challenges that remain. Jaydeep Singh, Kaspersky's General Manager in India, presented the Women in Tech initiative. The program also included keynote speeches and panel discussions on the role of women in the tech sector.

Plans for 2026

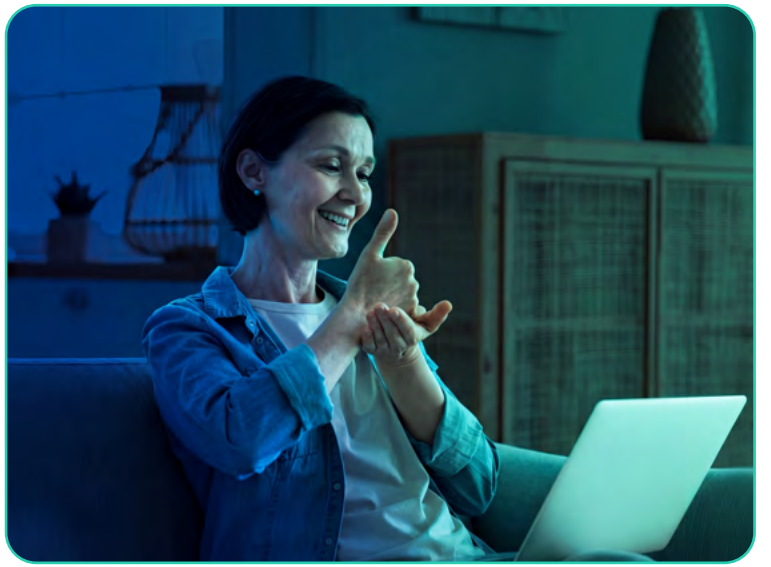
In 2026, we will continue to develop current projects and launch new programs aimed at providing women with equal opportunities for career development in various areas of IT and information security. We plan to continue participating in industry conferences and forums, publishing employees' success stories, expanding educational initiatives, and strengthening mentoring and career development programs for women around the world.

Support for employees with disabilities

Kaspersky supports job seekers and employees with disabilities and strives to create an accessible and inclusive work environment. What matters to us is the person and their potential, not their limitations.

When hiring, we evaluate candidates solely on their professional skills, experience, and expertise. Remote work is available for several positions at Kaspersky, and if necessary, a workplace can be adapted to an individual rehabilitation program.

For employees with disabilities, we create all necessary conditions for them to fully realize their potential.



Employee development

We create the necessary conditions for our employees' professional growth and development, both individually and in teams, thereby supporting the growth of the entire business.

Additionally, Kaspersky is constantly improving its training methodology and increasing investments in employees' development at all stages of their careers. For example, in 2025, expenditures on personnel training and development increased by 12.6% compared to the previous year, and average training time per employee increased by 14%, reaching 12.9 hours.

Average number of training hours per employee[1]

GRI 404-1

Employee category	2023	2024	2025
Average number of training hours for all employees, including:	9.2	12.1	11.4
■ managers	11.4	10.2	9.9
■ technical specialists[2]	7.8	9.8	9.6
■ other specialists	11.4	14	13

Our employees have access to both internal and external training opportunities. At Kaspersky, they can take online courses on products and technologies, complete programs to develop business skills and boost sales and personal competencies, choose a convenient format for learning foreign languages, find a professional growth mentor, and submit applications to participate in external trainings and events.

Training is flexible: in addition to mandatory programs, we offer additional corporate educational programs that employees can take at their discretion.

Kaspersky emphasizes development of leadership skills. In 2025, we reimagined our approach to training and combined our programs into a single "Leadership Programs" system. It includes two levels:

- Start — for new managers, team leads, and employees preparing for leadership roles. We completely revamped the content of this program and relaunched it as part of our training ecosystem.
- Pro — for more experienced mid-level managers whose teams already have team leads. The pilot group for this new program began in 2025.

Based on practical case studies and modern management frameworks, the training aims to create a unified system for developing leadership skills, fostering continuity within the company, aligning and strengthening managerial expertise, increasing motivation, and strengthening a culture of leadership and strategic partnership.

63 team leads

and 17 middle managers

participated in Leadership Programs in 2025

In addition, we are developing a corporate culture of sharing experience within the company. To this end, in 2024, Kaspersky launched Grow Lab, an internal mentoring program that helps employees find mentors and internal experts to develop applied skills and solve complex professional problems. Since its launch, 94 mentor-mentee pairs have participated in the program, and we plan to expand the project in 2026.

$2.23 million

in total expenses for employee training in 2024–2025

14%

increase in average training time per employee in 2025

[1] The data in the table does not include data from MOOC (massive open online courses) platforms.
[2] IT specialists + all R&D employees.

Required courses

GRI 404–2

Mandatory employee training at Kaspersky includes the following courses:

Information security

Information security. No matter what security measures we implement, a human is ultimately the most important participant in a system. The human factor is the most vulnerable element of information security. All Kaspersky employees undergo training in cybersecurity basics, even if they are not directly involved in the development or promotion of our solutions. Through a series of information security courses, our employees learn how to handle confidential information, securely store passwords and account information, and identify phishing emails and websites.

Rules of conduct during emergencies

Fire, smoke, sparking electrical wiring and equipment, breakdowns and other incidents can inflict serious financial losses and, more importantly, they can harm health and take lives. Safety training is mandatory for all Kaspersky employees and is designed to prepare them for appropriate and coordinated action during potential emergencies.

Anti-corruption behavior

Anti-corruption behavior. Employees at any cutting-edge company need to understand and comply with anti-corruption legislation. By following the rules taught in this course, our employees can maintain Kaspersky's reputation and integrity, as well as avoid personal liability and potential fines against the company.

Additional training programs and tools for developing expertise

In addition to mandatory educational programs, employees can independently choose additional training options to develop their professional expertise. Kaspersky offers remote learning courses on its internal educational platform, as well as in-person training programs aimed at developing soft skills, managerial competencies, and applied professional competencies.

Our employees can:

- take training on external online platforms such as Udemy, LinkedIn Learning, Pluralsight, and CBT
- attend in-person trainings and webinars on our internal e-Queo training portal
- participate in the GrowLab mentoring program
- participate in external professional conferences
- if necessary, receive training from external providers to maintain and develop professional expertise (within departmental budgets)
- learn foreign languages in a convenient format that accounts for individual goals and work duties.

In 2025, we updated our communications training. The main benefit was the inclusion of expert case studies that were as closely related to our business as possible.

Plans for 2026

Our immediate plans include a major relaunch of the GrowLab mentoring program, expansion of Kaspersky Academy's catalog of online courses, including foreign language instruction, and the creation of educational pathways for comprehensive professional development—both on specific topics (for example, channel sales or communication skills) and content associated with certain roles and positions.

Performance reviews and compensation

Kaspersky has built a comprehensive and transparent ecosystem for managing performance and developing talent. It is designed to achieve our strategic goals by unlocking each employee's potential. This ecosystem consists of three interconnected elements: regular performance reviews, transparent compensation, and career mobility.

The annual cycle of our employee performance review process includes several stages:
- annual goals are set
- the employee submits an end-of-year self-assessment
- the employee's immediate supervisor submits a final assessment

Progress is constantly monitored throughout the year, allowing employee goals, as well as the plans for achieving them, to be promptly adjusted.

GRI 404-3

We constantly evaluate the quality of work of Kaspersky personnel. In 2025, 90% of employees underwent regular performance reviews and career prospects assessments (88% in 2024).

The annual adjustment of employee compensation is based on the results of the annual performance review cycle. The following criteria are taken into account:
- individual employee performance
- current income level relative to the market
- labor market conditions
- Kaspersky's performance and plans.

Personnel development

When it comes to compensation, one of our guiding principles is "rewards for results." Performance reviews influence adjustments to employees' compensation and their career mobility.

After reaching a certain length of service at Kaspersky (from six months to one year), all employees become eligible to join our internal mobility program. The program offers support at every stage of development and opens up additional professional growth opportunities that let employees flourish in a team of like-minded individuals.

Employee productivity

The performance review process is a comprehensive system that aims to simultaneously develop employees and achieve business goals. It includes:
- setting and evaluating goals (performance review)
- regular collection of employee feedback (one-on-one meetings, 360-degree surveys, self-assessments and other tools)
- assessment of competencies and formation of individual development plans

Performance reviews influence employees' career advancement, their financial compensation, the amount of investment in training and development, and more.

We continuously track over 800 different HR and business metrics and use them to make management decisions. The goal of our HR function is to increase our return on investment in people. This strategic metric helps us assess how effective our investments in people are, make more informed personnel decisions, and find answers to complex management questions.

Employee engagement

Every year, we assess employee satisfaction levels through an anonymous YourVoice survey. The survey helps us understand employee attitudes toward internal corporate changes, and strategy adjustments, and evaluate the impact of various factors, such as pay, benefits, work-life balance, career growth prospects, team atmosphere, etc.

We focus mainly on the Employee Net Promoter Score (eNPS), which measures the percentage of employees who would recommend the company as an employer.

In 2024, eNPS increased by 0.4 percentage points year-on-year, reaching 57.2, and in 2025, by 8 percentage points, reaching a record 65.

The survey results are available to managers at every level. This helps them analyze the situation across teams, regions, and divisions and identify areas for growth.

We regularly inform employees about news, plans, and internal changes. We engage employees in corporate initiatives through digital and offline tools:
- articles and publications on our internal portal
- posts in a private channel on a social network
- email newsletters.

SASB TC-SI-330a.2

We also hold AMA (Ask Me Anything) sessions with Kaspersky's top managers and representatives of various business functions. During these meetings, we share the results of our work, discuss plans, and answer employee questions live.

Occupational health and safety

We strive to ensure that every workplace at Kaspersky is comfortable and safe, and that employees have access to high-quality medical care and support.

Key documents

GRI 403-1

- Labor Code of the Russian Federation
- Regulations on Hazard Identification and Occupational Risk Classification
- Fire Safety Instructions
- Internal Labor Regulations
- Regulations on Access Control and Facility Security
- Mandatory interactive training course on emergency procedures at Kaspersky offices
- Occupational Safety and Health Policy

GRI 403-9

0 accidents

related to occupational risks in 2024 and 2025

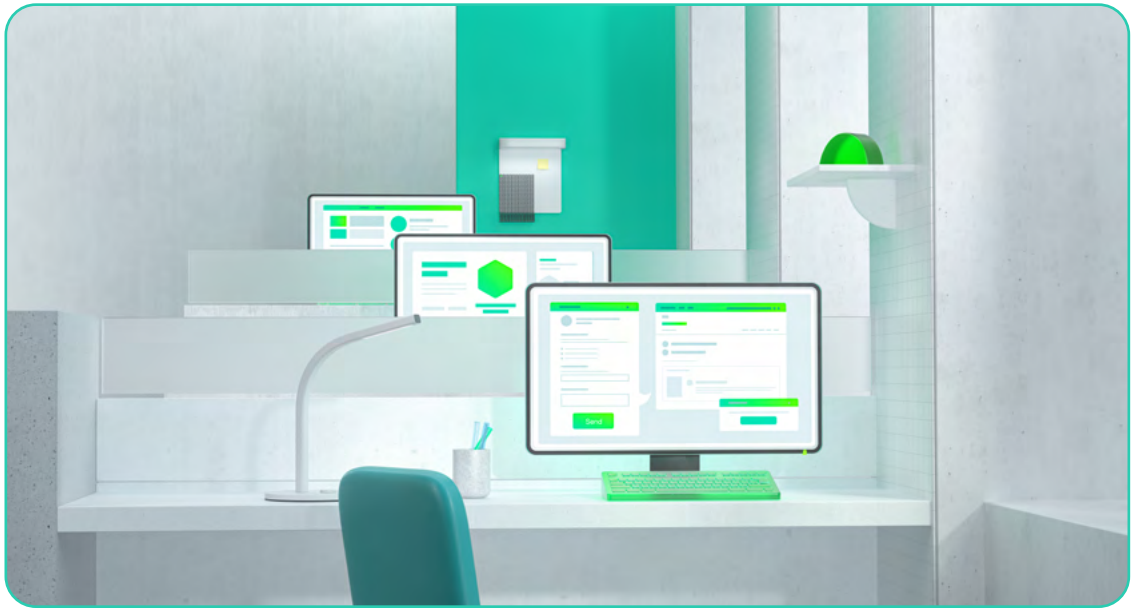
Managing occupational health and safety

GRI 403-2, GRI 403-5

The HR Department, with the support of external consultants, is responsible for occupational safety at Kaspersky. The department includes a personnel administration group that oversees issues related to the occupational safety and health of employees.

Within the disclosures in this report, the occupational health and safety management system at all Kaspersky offices complies with current labor legislation requirements everywhere Kaspersky operates. This system includes:

- regular instruction
- regular special assessment of workplaces in all departments
- a system for managing risks and investigating accidents
- measures to improve working conditions



Our occupational health and safety training includes introductory training for new Kaspersky employees when they are hired.

Kaspersky currently has the following occupational health and safety programs in place:

- introductory training on occupational safety and fire safety
- training on general occupational safety and health issues and how the occupational safety and health management system works
- emergency response training

Kaspersky managers also undergo training at the training center.

The key performance indicator here is the absence of workplace injuries.

GRI 403-9

Most employees work in the office. During the reporting period, not a single workplace injury or occupational illness was recorded.

Work on weekends and holidays

When approved by the personnel department and the head of the relevant department, employees may be required to work on weekends or non-working holidays. This arrangement is formalized with the employee's written consent, and the performed work is recorded in the timesheet.

Employees who are pregnant or on vacation or sick leave are not allowed to work on weekends and non-working holidays. Work on weekends must not exceed eight hours per week. When working two consecutive weekend days, employees must not work more than four hours per day.

Employees who are required to work on a weekend or non-working holiday are given a choice of two types of compensation:

- increased pay
- extra vacation time

How we care for our employees' health and well-being

GRI 403-6

Kaspersky employees in Russia and their children aged 16 and under are covered by our corporate voluntary health insurance program. The program also provides accident insurance for employees. If an accident occurs, employees can submit relevant information to the insurance company through the HR department.

Our voluntary health insurance program includes cancer treatment, inpatient care, online and offline psychological support, annual medical examinations for getting a health resort pass, and seasonal vaccinations.

Kaspersky's headquarters features a gym and sauna, and in-office appointments with a doctor, psychologist, and massage therapist are available. We also offer an online psychological support line for our employees. We reimburse some expenses on healthy living, including fitness classes and children's health camps. Employees also get a corporate discount at Rigla pharmacies.

GRI 403-4

Employees can provide feedback after completing the mandatory emergency response training course. We also measure employees' perceptions of their physical, emotional, and social well-being through an anonymous employee satisfaction survey each year.

GRI 403-2

As an employer, Kaspersky provides its personnel with safe working conditions in accordance with state occupational safety regulations. During the reporting period, we did not record a single incident related to occupational safety violations.

Of course, Kaspersky still provides accessible options for responding to potential incidents. In particular, employees can:

- contact the employee support hotline (HR Support)
- submit a request through our internal portal for the administrative team
- schedule an appointment with an in-office doctor or psychologist
- contact their HR business partner directly

Contribution to Social Development

>$760,000

in direct charitable expenditures for 2024–2025

>200 universities

in 45 countries cooperate with Kaspersky Academy

~400

corporate volunteers at Kaspersky

Support beyond the digital world

GRI 203-1, GRI 203-2

We believe that social impact activities are an extension of our core mission: at Kaspersky, our commitment to making the environment we live in safer and more sustainable extends beyond the digital world.

>$760,000

(71.3 million rubles) in direct charitable expenditures for 2024–2025

13,500 licenses

donated to charitable foundations

>$172,000

(>16 million rubles) saved by non-profit organizations over two years thanks to free security product licenses provided by the Company

Kaspersky's social projects are systematic, long-term work based on an understanding of the real needs of society.

We strive to support those who are particularly vulnerable in the digital and real world by creating an inclusive and safe online environment. We want people to feel confident online, understand how technology works, and know how to use it. Training personnel for the IT industry is another key aspect of our philosophy—as we cultivate expertise, deliver educational initiatives, and transfer knowledge to the next generation of specialists.

Our support goes beyond direct charity. We create a positive economic impact on local communities and economies. A significant part of Kaspersky's contribution to social development comes through indirect economic effects. Our products and services help companies, government organizations, non-profit organizations, and individuals reduce financial losses caused by cyber incidents, improve the resilience of digital processes, and build trust in the online economy.

How we help foundations and non-profits save money

- The Company provided free cybersecurity to **more than 100 foundations during the reporting period**.
- NPOs saved >$172,000 (>16 million rubles) over two years thanks to free security product licenses issued by the Company

Kaspersky regularly helps charities and non-profits by protecting their digital operations from cyberattacks, data breaches, and malware. We provide free licenses to these organizations for their desktop PCs, laptops, and, if necessary, employee phones and servers.

Here are examples of the annual savings enjoyed by charitable foundations:

- up to **$9,250 (860,000 rubles)** for the Vera Hospice Charity Fund
- up to **$6,850 (637,000 rubles)** for the Gift of Life Charity Foundation
- up to **$2,900 (270,000 rubles)** for the Deti Nashi Foundation
- up to **$2,100 (196,000 rubles)** for the Perspectiva Regional Public Organization of Disabled Persons
- up to **$1,700 (160,000 rubles)** for the So-edinenie Deafblind Support Foundation

What was the result?

Such significant savings allow organizations, especially small non-profits, to spend more time and money on the needs of their beneficiaries and their statutory activities.

We also make an impact by investing in digital infrastructure, research, expertise, and educational initiatives in the field of cybersecurity. These investments have both immediate and long-term positive effects on local communities and the economies of the regions where the Company operates. New high value-added jobs are created, and the number of personnel qualified for the IT industry grows. At the same time, our partner ecosystem is growing, supporting small and medium-sized businesses in the IT and information security services sector.

We also consider potential downsides. For example, increased cybersecurity requirements could increase costs for small businesses and non-profit organizations. But these effects are limited and manageable thanks to our educational programs, consultations, accessible services, and free products for vulnerable groups. Overall, we assess all impacts as predominantly positive, consistent with sustainable development goals and reducing the digital divide.

Social and charitable projects

Our approach to social investments

Kaspersky's social and charitable programs help those in the greatest need and strengthen the Company's ties to people and communities in various regions.

Kaspersky's charitable activities aim to advance the Company's core mission: building a safe and sustainable world where people can use technology to improve life on the planet.

The main objectives of our social and charitable programs are:

- build and develop long-term partnerships with charitable foundations, non-profit organizations and educational institutions;
- cultivate corporate volunteering, including sports volunteering, donor initiatives and pro bono initiatives;
- provide free security solutions to non-profits and vulnerable groups;
- involve employees in charitable projects and corporate fundraising;
- support inclusive projects, including employment and mentoring for young professionals with disabilities;
- foster digital literacy and safe use of technology among vulnerable groups;
- support social, environmental and inclusive activities both inside and outside of the Company.

Main areas of charitable activities

The company has supported social projects for over 15 years. In Russia, we support more than ten foundations and non-profit organizations, including federal ones, such as Gift of Life, Vera, and Syndrome of Love, and regional ones, such as the Nizhny Novgorod Women's Crisis Center and Zhivi. We support patients with serious illnesses, socially vulnerable citizens, disaster victims and the elderly.

Corporate fundraising plays a key role in this activity—we support our non-profit partners' fundraising efforts and organize our own fundraising events in conjunction with important dates and holidays. In 2024, Kaspersky employees raised over $5,400 (500,000 rubles) through internal fundraising events, and over $10,800 (1 million rubles) in 2025. These donations went to the following foundations: Syndrome of Love, Igra, Gift of Life, Dom s mayakom, Podarok Angelu, Nika, Nature and People, and Second Wind.

Company employees raised

$16,100

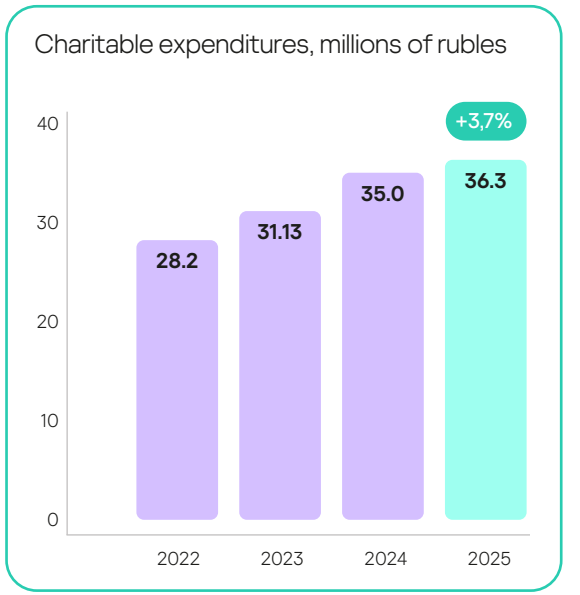
(1.5 million rubles) for charitable foundations in 2024–2025

How we support foundations and non-profit organizations

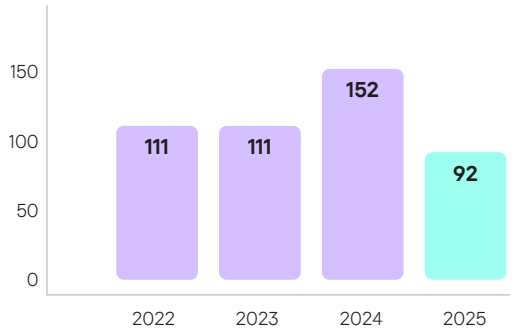
One of the key areas of our social work is technological support for the non-profit sector. The Company participates in the Technologies for Good Russian federal project, which helps NPOs access digital products and services free of charge or on preferential terms. This project is implemented by PJSC Sovcombank and Skolkovo Fintech Hub.

During the reporting period, we donated over 13,500 security product licenses to more than 100 charitable foundations and non-profits. We also provided free licenses to more than 200 individuals—people with disabilities, large families, and people in difficult life situations.

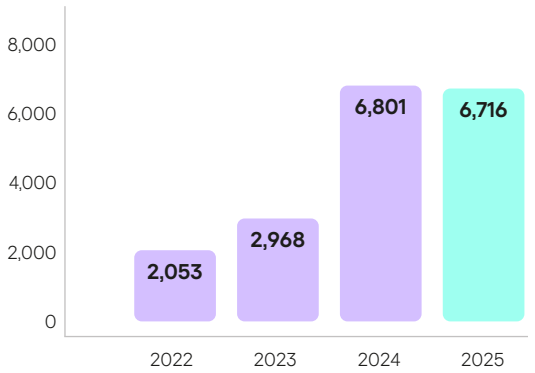
In 2024, Kaspersky began cooperating with the Russian Red Cross, providing it with solutions for protecting infrastructure and online resources: Kaspersky Endpoint Detection and Response Optimum and Kaspersky DDoS Protection. Since the start of the collaboration, the Russian Red Cross's website has not suffered any problems with availability, despite facing cyberattacks previously.



Free licenses provided to individuals in need



Product licenses donated to charitable foundations



How we support the Igra Foundation

We help increase the knowledge of young specialists in Russia and develop state-of-the-art approaches to treating movement disorders in children.

Since 2022, Kaspersky has supported the Igra Foundation, which helps children with motor disabilities live more active and independent lives. This work is not only about targeted assistance to families, but also about improving the entire support system by training specialists and ensuring access to cutting-edge knowledge.

In 2022, the foundation requested the Company's assistance in purchasing an internationally-recognized therapeutic methodology that helps specialists set treatment goals and evaluate the results of treatment. In Russia, similar resources were available only sporadically and most often in the form of unofficial translations.

With support from Kaspersky, the foundation translated relevant materials into Russian, obtained an educational license, and launched a training course for doctors and rehabilitation specialists. The program focused on a client-centered approach, SMART goal-setting in therapy, and assessing changes in children's quality of life following treatment.

What was the result?

- **~300** specialists were trained in modern therapy methods by the end of 2025
- **45** rehabilitation organizations participated in the program
- **3** service providers serving children with movement disorders from birth to three years implemented early intervention assessments into their routine work
- **2** specialists began a one-year retraining program to learn occupational therapy—the most in-demand skill set for helping children with disabilities
- **33** regions of Russia are covered by the initiative

For many doctors, this was a significant opportunity to take a fresh look at their work and apply more gentle and modern methods of helping children. And it allows families to receive high-quality therapy closer to home, without having to travel to major federal centers.

In 2025, the acquired rights to the methodological materials became the foundation of an IT platform for doctors and rehabilitation specialists, which won Global CIO's IT community competition. The platform is free for professionals who have received training and transitioned to patient-centered technologies in therapy.

Our next step was to expand professional dialogue. In 2024, the Company supported Russian specialists' participation in the conference of the European Academy of Childhood-onset Disabilities (EACD), which was held in Belgium. This is one of the largest international platforms that brings together doctors, rehabilitation specialists, scientists, patients and their families from all over the world.

With the support of Kaspersky, four Russian specialists and the foundation's director participated in the conference. This allowed the foundation to establish direct contacts with leading global experts, including the founder of the CanChild research center, which has developed practical solutions for helping special-needs children for many years.

One of the important outcomes was an agreement to create Russian translations of CanChild resources and classifications, which are intended for both doctors and parents.

In 2025, the Company again supported participation in the conference, this time helping seven Russian delegates attend. For the first time in the conference's 37 years, three Russian scientific papers were presented: one on setting rehabilitation goals for children after brain tumor treatment and the other on telerehabilitation for children in remote regions.

How we work with local communities

GRI 413-1

During the reporting period, Kaspersky stepped up its direct engagement with local communities. The main focus was on developing digital literacy, improving cybersecurity, and reducing digital inequality among schoolchildren and university students, parents and teachers, and employees of non-profit organizations and social institutions.

We implemented and supported educational and awareness-raising initiatives on the safe use of digital technologies, as well as inclusive projects in partnership with relevant organizations. The employees' participation in educational and social events played an important role in these efforts.

For more information, see the "Inclusivity in cyber space" (page 79) and "Digital awareness" (page 86) sections

How we involve employees in charitable work

We regularly organize events and activities that allow our employees to participate in charitable work. In 2024–2025, as usual, the Moscow office hosted two New Year's charity fairs in support of the Zhivi Foundation. The Company and its employees raised more than $30,100 (2.8 million rubles) through the 2024 fair, and the fair in 2025 raised more than $36,600 (3.4 million rubles). These funds were sent to regional pediatric oncohematology departments.

In 2024, the funds raised at the fair helped improve treatment conditions for children at the Tula Regional Children's Clinical Hospital and the E.P. Glinka Children's Clinical Hospital in Grozny. They were used to purchase high-tech medical equipment, modernize wards and common areas of departments, create leisure spaces and activities for children in the hospital, and add more treatment beds.

>$66,700

(>6.2 million rubles) raised at charity fairs for the Zhivi Foundation in 2024–2025

In December 2024, Kaspersky partnered with the Vera Hospice Foundation to release and sell its first collection of charity merch, including hoodies, T-shirts, and tote bags. Half of the proceeds amounting to over $5,400 (500,000 rubles) went to the needs of the foundation.

Together with the Nika Foundation, we also released a special collection of socks to sell at our corporate Children's Day. All proceeds from the sale went to support the foundation's beneficiaries. In the future, we plan to release other collections in collaboration with partner foundations.

In July 2025, the Company supported the Generous Bookstore event, organized by the Nizhny Novgorod Women's Crisis Center. We helped cover some of the organizational costs, got employees to volunteer, and provided books for sale and prizes for the raffle. The event raised more than $8,100 (750,000 rubles) for the center.

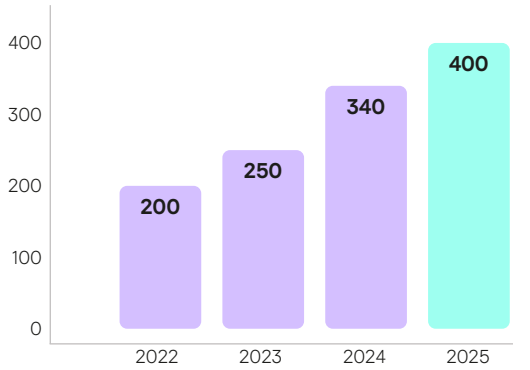
Our volunteer programs

Kaspersky's corporate volunteering grows rapidly every year. In 2024, 340 employees participated in volunteer programs, and in 2025, this number increased to about 400, which is twice as many as in 2022.

~400

corporate volunteers in 2025

Number of employees participating in the Company's volunteer programs



In 2024, Kaspersky joined the National Council for Corporate Volunteering in Russia.

In 2024, the Company's programs covered several areas: blood donations, charitable sporting events, support for orphanages, and free professional assistance. During the reporting period, we expanded our corporate volunteering program by adding new initiatives in partnership with the Dari Edu, Nika, and Second Wind foundations.

Donations

Donors make up the largest team of volunteers at the Company. Our employees donate blood twice a year. We hold this blood drive at Kaspersky's Moscow office in collaboration with the Blood Center at Russia's Federal Medical and Biological Agency (FMBA).

In 2024, 212 employees donated blood, and in 2025, 215 employees donated. About one third of them donated twice in the year. In 2024, the Russian Red Cross recognized Kaspersky in the "Best Corporate Volunteer Day" category at the All-Russian Corporate Donation Culture competition. In addition to donating blood, employees can be typed to join the bone marrow donor registry.

Sports volunteering

Sports volunteers make up the second largest volunteer group, currently comprising 139 employees (an increase of 26.4% compared to 2024). During the reporting period, Kaspersky sponsored 12 charitable sporting events in support of the Syndrome of Love, Vera, Foundation for Fighting Leukemia, and Bumazhnaya Ptitsa foundations. Our volunteers participated in runs, cycling marathons, and online triathlons.

We continue to expand this volunteering format because it is equally important for both our employees and partner foundations. Charitable sporting events attract a large number of like-minded individuals, and over the years they have built a vibrant community of sports enthusiasts within the Company. For charitable foundations, this is one way to talk about inclusivity and draw attention to social activities, which is also very important for the Company. For employees, this is an opportunity to support good causes and feel a sense of team unity while interacting with colleagues from different business units.

Community clean-up days

Another important area of volunteer work are community clean-up days and assisting hospices sponsored by the Vera Foundation. This is the company's third-largest volunteer group. It grew by 50% between 2024 and 2025, allowing us to take on more ambitious tasks.

Twice a year, volunteers visit Moscow hospices and palliative care centers to help with cleaning and landscaping. They tidy up the hospice premises, clean the surrounding areas, plant flowers, and take on housekeeping tasks—from purchasing food and water to acquiring necessary supplies.

Thanks to cleanup days, the outdoor spaces of the First Moscow Children's Hospice were ready for Children's Day and the summer season, and in the fall, the grounds of a hospice in Rostokino were spruced up for its 22nd anniversary.

In addition to helping with housekeeping tasks, our staff collects gifts for hospice patients and staff. In 2024–2025, more than 500 gifts were collected for International Women's Day in collaboration with the Vera Foundation.

Pro bono volunteering

Since 2022, Kaspersky has been expanding its pro bono volunteering—providing unpaid professional assistance to charitable foundations and non-profit organizations. This type of volunteering lets employees share their professional expertise and support partners in solving practical problems, making NPOs more sustainable and expanding their capabilities.

In 2024–2025, Kaspersky specialists from various business units participated in the following projects:

- **Strategic support for the Love Syndrome Foundation**: Our Russian marketing team conducted a workshop to analyze the foundation's promotional campaigns, tools and channels used, metrics, and KPIs, and offered practical recommendations for improving communications.
- **Mentoring for students with disabilities**: Kaspersky employees acted as mentors in Perspectiva's Try a Profession in Action program, which helps participants identify their professional interests and take the first steps in their careers.
- **Design support for the AIDS.Center**: Our design department helped create an interactive map powered by a database of verified HIV service organizations. Our team transformed vital but complex data into a user-friendly digital tool for finding nearby help centers and available services.
- **Cyber hygiene training for non-profit organizations**: Our information security experts conducted training sessions on basic cyber hygiene and provided lectures on modern digital threats for employees of non-profits, including the Perspectiva, Deti Nashi, and Vverkh foundations.
- **Career guidance events for teenagers**: A Kaspersky cybersecurity analyst spoke at an event organized by the SOS Children's Villages foundation, educating the young people in its care about career opportunities in cybersecurity.
- **Educational programs**: Leading Kaspersky specialists participated in the Leave Your Mark program organized by the Business Solutions and Technologies (DRT) company. They shared their knowledge about working safely with AI, protecting personal and corporate data, and recognizing common cyber fraud schemes.
- **Technologies for Good conference**: One of the Company's leading experts in information security threat research moderated a conference session entitled "From cyberattacks to social engineering — how non-profit organizations and businesses can effectively protect themselves and their audiences." He shared real statistics and examples of cyberattacks with the audience and spoke about effective security tools.

Support for children's institutions

Kaspersky employees continue to support the Udomlya Orphanage and Tverskaya School No. 4, a specialized boarding school for children with mental development challenges, autism spectrum disorders, and musculoskeletal disorders. We regularly volunteer at these institutions and take on some of their organizational and routine needs.

The Company's employees visit the Udomlya Orphanage four times a year and carefully prepare a program for the children each time. It includes educational lectures, sports and creative activities, games and master classes. Once a year, volunteers also organize a summer camping trip for the children—complete with a campfire, singing, and shared recreation. We have cooperated with the Udomlya Orphanage for over 15 years.

Before each visit, employees help buy everything necessary for the daily life and education of the children. Additionally, the Company makes repairs, buys equipment and household goods, and helps organize recreational trips for the children.

New activities

In 2025, we expanded our corporate volunteering program by testing new formats of collaboration with partner foundations. These activities allowed Kaspersky employees to help various target groups: teenagers, the elderly, and even abandoned pets.

- **Support for graduates in difficult life situations**: As the academic year came to an end, the Company's employees were volunteers and coordinators for the Second Wind Foundation's Support Day for graduates in difficult life situations. On this day, the volunteers helped graduates dress sharply for their upcoming prom parties.
- **Help for the elderly and people with disabilities**: Our employees served as couriers for the Dari Edu project, helping deliver hot meals to the elderly and people with disabilities.
- **Volunteering at an animal shelter**: The Company's employees made their first visit to the Nika Foundation's 'Wet Nose' shelter, where volunteers walked dogs and interacted with cats. These visits help socialize animals and increase their chances of finding a new home.
- **Participation in the Woof Festival**: We joined a large team of volunteers at the Woof Festival, organized by the Nika Foundation in support of abandoned pets. Kaspersky employees assisted with the charity market, managed social media and photography, filled out contracts, accompanied festival guests and participants, and collected and presented gifts.

In 2026–2027, we plan to expand our current initiatives and are considering the possibility of launching one or two joint educational projects with partner foundations.

Inclusivity in cyberspace

We strive to create an environment where people with disabilities can safely use digital services, develop skills, and build careers in IT.

For Kaspersky, inclusivity in cyberspace means, above all, equal access to knowledge, technology, and opportunities for professional development.

One of the key areas of our work is inclusive employment. Since 2022, Kaspersky has been a member of the Business Council on Disability Issues, organized by the Perspectiva Regional Public Organization of Disabled Persons. The Company participates in joint projects aimed at expanding opportunities for students and young professionals with disabilities.

Our employees regularly participate in job fairs and career guidance events, including the Career Path competition and job fairs for students and young professionals with disabilities. They also conduct tours, career guidance lectures, and meetings at our Moscow office. In 2025, we helped organize a business breakfast attended by over 30 representatives of companies that support inclusive employment.

We create inclusive internships

During the reporting period, we continued to expand inclusive employment. Kaspersky invited university students and recent graduates with disabilities to participate in internship programs in various departments of the Company.

In 2025, we conducted a study on ESG practices at Russian companies, which showed that most Russians (63%) felt positively about hiring an intern with a disability. About one third of respondents were neutral.

What was the result?

By the end of the reporting period, we had filled all vacancies for interns with disabilities at the Company. In 2026, we plan to expand our inclusive hiring program and open new positions.

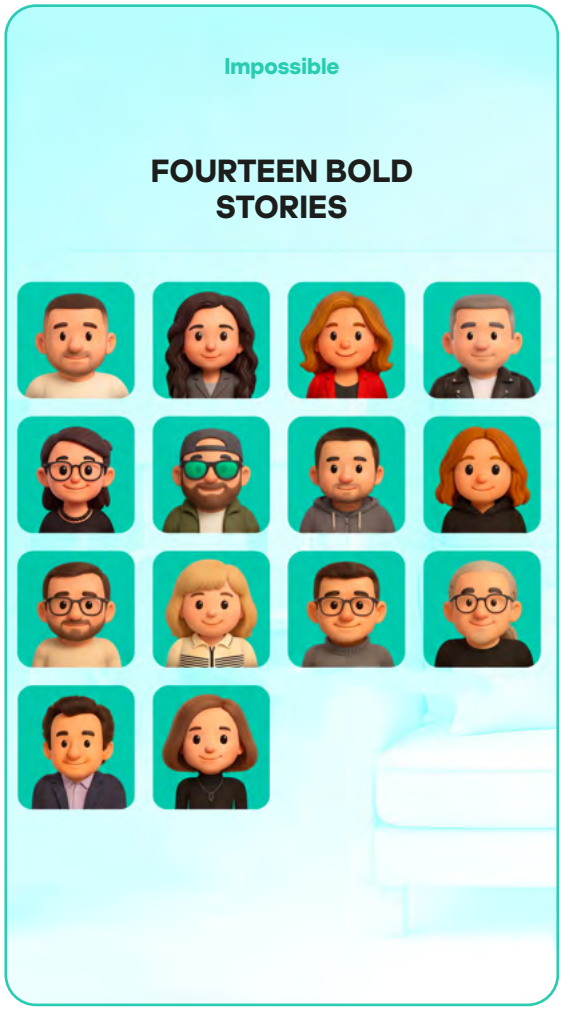
We also emphasize physical and digital accessibility in workspaces. In the fall of 2024, Perspectiva audited the Company's Moscow office to assess the accessibility of the broad environment and access to workstations for people with disabilities or limited mobility. The audit produced a detailed report with recommendations that we are using to further improve our office spaces.

An important part of our work remains the creation of a culture with more acceptance and less stigma. Since 2022, our Sustainabity team has published special websites for International Day of Persons with Disabilities, sharing the professional and personal experiences of employees with disabilities and of parents of children with disabilities.

In 2023, we launched the Impossible website to share their stories. It is updated annually with the addition of new stories. In 2025, we significantly expanded the project: website visitors can now tour the Company's virtual office, meet 3D characters, get information about various disabilities and illnesses, and donate to Perspective's inclusive employment programs.

We also address digital literacy for people with mental disabilities. In fall 2024, together with the Syndrome of Love Foundation, the Company unveiled Russia's first digital literacy manual for people with Down syndrome. In 2025, we expanded the project by partnering with the Kun Bala Foundation in Kazakhstan, donating computer equipment and educational materials. In the future, we plan to extend the project to other regions where Kaspersky has a presence.

In addition, in 2024, the Company once again joined the nationwide Dobroshrift campaign in Russia, dedicated to Cerebral Palsy Support Day, supporting the initiative to raise awareness about inclusion and accessible environments.



Accessibility of our products and services for people with disabilities

Over the past few years, the company has been systematically improving the accessibility of its corporate digital resources. Key corporate websites, including consumer-facing (B2C) pages, the shopping cart, checkout pages, and support services, have been adapted in line with accessibility requirements. Accessibility principles have also been integrated into the development and update processes for digital products.

During the reporting period, the company's work focused on building sustainable processes: automated accessibility tests were introduced, and accessibility requirements were embedded into development standards. This helps ensure that accessibility is considered at the stage of creating new features. Thanks to the component-based architecture, many improvements implemented for the B2C segment can also be scaled to B2B websites.

In addition, the company conducts user research involving people with disabilities. In particular, testing sessions were organized with a blind user, who completed purchase and support request scenarios. The results of such research are used to identify barriers and prioritize further improvements.

At the same time, not all corporate digital resources currently fully meet accessibility requirements. In particular, some smaller subsites, which are developed and maintained with limited resources, have not yet undergone full accessibility adaptation. The company recognizes these limitations and is considering opportunities to address them gradually as resources become available, with the aim of ensuring a consistent level of accessibility across all digital platforms.

Work to improve accessibility is continuous: the company regularly enhances its interfaces, including improvements to navigation elements such as display mode switches, and further develops internal processes and methodological materials aimed at maintaining and further improving the accessibility of its digital services.

Training personnel for the IT industry

GRI 3-3

We systematically cultivate human resources in IT and cybersecurity: we prepare specialists in advance, combine training with practical experience, and support professional growth at every stage.

52%

of companies believe they are at risk due to the careless actions of their own employees

46%

of incidents in 2024 were made possible by employees' ignorance

Our approach to teaching

One of the key problems facing the industry is a shortage of qualified IT and cybersecurity specialists. According to a 2024 Kaspersky study, most companies experienced at least one cyber incident related to the shortage of qualified specialists over the previous two years.

At the same time, 52% of organizations believe they face internal threats: employees' mistakes, careless actions, or lack of knowledge directly impact the security of business information[1].

In 46% of incidents in 2024, employee ignorance or negligence was a contributing factor in the attack.

We believe that personnel training is a continuous process. To ensure specialists are prepared for real challenges, systematic work is needed, from elementary school to advanced training programs for experienced professionals.

That's why Kaspersky is developing a range of educational initiatives that reach audiences ranging from schoolchildren to working IT and information security professionals. We create online courses, conduct hackathons[2] and competitions, support olympiads, and organize paid internships. We also implement joint educational projects with universities, government agencies, and local professional communities.

Kaspersky Academy and cooperation with universities

To scale up our training projects and make them universally accessible, in 2010 the Company launched Kaspersky Academy — a global platform for information security education.

Between 2022 and 2025, thousands of students from Russia, Europe, the Middle East, Africa, South and Southeast Asia, and Latin America received training on the platform.

Today, Kaspersky Academy offers courses, training sessions, and practical learning experiences for a wide range of audiences, from schoolchildren and university students to professionals and non-technical users. The lecturers and course authors are heads of departments and leading cybersecurity experts at Kaspersky.

During the reporting period, the Company focused on developing accessible and hands-on educational formats, including:

- As part of Kaspersky Academy, we launched the free online course Cyber Hygiene, which helps users learn the principles of safe use of gadgets and internet services. The course includes 16 video lessons lasting 15–20 minutes
- We launched the Introduction to Cybersecurity. Entry Level course for both IT specialists and non-technical users
- We created the Who Are You in IT? online course for high school and university students to help them understand professions in IT and information security, and identify a career development path. The program consists of 30 short video lessons up to 25 minutes long and covers more than 20 specializations—in both technical fields and the humanities.

We are also expanding our cooperation with universities. Today, the Company collaborates with more than 200 universities in 45 countries, including more than 70 educational institutions in Russia and CIS countries. We organize joint hackathons and competitions, create research labs and develop joint curricula, provide access to the Company's technologies and expertise, and offer students internships and the opportunity to participate in applied projects.

We cooperate with:

>200 universities

in 45 countries,

including:

>70 universities

in Russia and CIS countries

[1] According to a study conducted by Kaspersky and B2B International among more than 5,000 companies worldwide.

[2] A hackathon is an event where IT specialists work together to develop a solution to a given problem.

Kaspersky Academy Alliance

In 2023, Kaspersky launched Kaspersky Academy Alliance, a special partner program that lets universities integrate our courses, technologies, and practices into their educational process. The Kaspersky Academy Alliance has attracted interest from many educational institutions. By the end of 2025, we signed 50 agreements with universities in 16 countries.

In addition to universities, we actively collaborate with government and educational organizations, as well as with local professional communities in the Middle East, Africa, South and Southeast Asia, and Latin America.

For example, in 2025, Kaspersky signed cooperation agreements with the Jordan's Ministry of Digital Economy and Entrepreneurship (MoDEE) and Tuwaiq Academy, a national educational center in Saudi Arabia that teaches digital technology and programming.

~50 universities

in various countries have joined the Academy Alliance program in two years.

How we cultivate practical skills

Practice is essential when training cybersecurity specialists, which is why competitions, olympiads, and expert communities occupy an important place in our educational ecosystem.

International competitions for cybersecurity experts

We develop the professional community through hands-on training

Capture the Flag (CTF) is a cybersecurity competition format established in 1993 where participants search for "flags" (special files or data) hidden in vulnerable programs, websites, or hardware devices.

Kaspersky promotes this format through the **SAS CFT** competition, which consists of two stages: an online qualifying round and an in-person final, as well as Kaspersky{CTF}, an online competition whose winners also participate in the SAS CTF final.

The final stage is held as part of the Company's own Security Analyst Summit, an international conference that brings together the best experts from around the world.

What was the result?
CTF competitions give participants an opportunity to improve their skills and share experiences. For the Company, they are a way to cultivate an international community of researchers and help the industry train specialists who can act quickly, collaboratively, and creatively.

2024

SAS CTF 2024
Over 840 teams from more than 80 countries took part in the online qualifying round. This stage tested skills in reverse engineering, binary scanning, digital forensics, steganography, and programming.

Eight teams, including teams from Russia, China, and Japan, participated in the final, which was held as an Attack-Defense round. The final tested participants' skills at identifying vulnerabilities, fixing them to protect services from attacks by other teams, and developing exploits to attack opponents online.

The Russian Bushwhackers team won, receiving **$10,000** for first place. The total prize fund was $18,000.

2025

To give information security professionals and university students from around the world an opportunity to hone their skills, we introduced Kaspersky{CTF}, a competition held August 30–31, in which 1,100 academic teams and 490 corporate teams participated.

- **1,600 teams** from **90 countries** competed online.
- Teams tackled a series of challenges involving reverse engineering, cryptography, binary exploitation, web security, and digital forensics.
- All **25 tasks** were successfully solved.
- We identified **5 winners** from **5 regions**: Ganesh (Brazil), Pinely (Netherlands), SolidAll (Russia), PwnSec (UAE) and Odin (South Korea).
- These teams were invited to the **SAS CTF** finals in Khao Lak, Thailand.

The new competition reflects the Company's commitment to fostering the academic community's development through hands-on learning.

SAS CTF 2025
More than 900 teams from over 80 countries took part in the online qualifying round. This stage tested participants' ability to find vulnerabilities, solve cryptographic puzzles, and solve problems related to artificial intelligence.

A total of 13 teams (from Europe, the Middle East, the Asia-Pacific region, and Latin America) reached the finals: eight through SAS CTF and five through Kaspersky{CTF}. Participants simultaneously defended their own infrastructure and attacked the infrastructure of other teams. Each team got access to identical servers containing vulnerable services. Their task was to find the vulnerabilities, fix them on their own server, and exploit the same vulnerabilities on competitors' servers.

The teams competed for a $18,000 prize pool. The **C4T BuT S4D** team from Russia took first place and received $10,000.

In July 2025, Kaspersky collaborated with the Manipal Institute of Technology in Bangalore (MIT Bengaluru) to hold HackSky 2025. This event is a national, pan-Indian cybersecurity hackathon that brings together young developers and students from across India to solve real-world problems in data protection and IT security.

During the 48-hour hackathon, participants worked intensively, developing innovative solutions at the intersection of technology and security. Students on the MIT Tech Wizards team from MIT Bengaluru won by demonstrating the best skills and practical results. The event organizers provided prize money and opportunities for further project support and career development for young cybersecurity talent in India.

Kaspersky partnered with Kazan Digital Week 2025, an international forum where the Company's experts shared practical implementations using the KasperskyOS Cyber Immune architecture, as well as practical examples of using AI for telemetry analysis and incident detection. Our experts also demonstrated real-life scenarios for protecting digital infrastructure in transport and industry. This format—analyzing applied projects, demonstrating technologies, and engaging in professional discussions—helps promote practical skills among participants, including university students in relevant fields.

We work with gifted students

Another area of our work is support for gifted high school students. In 2024–2025, the Company helped prepare for and hold international cybersecurity olympiads. High school students received training from leading cybersecurity experts from Kaspersky and Central University.

The first International Cybersecurity Olympiad (ICO) was held in June 2025 in Singapore. The Russian team, which included eight 11th-grade students from Moscow and Kazan, competed against 128 talented students from 25 countries. In the end, the participants from Russia won eight medals, including three golds.

These olympiads cultivate practical skills and professional interest in future specialists. We plan to continue this work in 2026.

Kaspersky Academy expert community

To support not only high school students and university student, but also the academic community, we cultivate the expert community at Kaspersky Academy. We do this through a series of professional events for teachers, researchers, deans and heads of departments covering information security and related disciplines.

Once a quarter, we hold meetings for them, where our specialists share their expertise on hot topics. We also offer regular free two- or three-day training sessions for university faculty, led by our experts.

The Kaspersky Academy expert community has a broad geographic reach, encompassing virtually all of Russia and the CIS. We expanded this project to new countries during the reporting period.

- **Events in Russia**: In 2024–2025, we held seven community events (with an average of 30–35 participants), as well as four two-day trainings for faculty and specialists from universities in Russia and the CIS (with an average of about 35 participants).
- **International events**: In 2025, we held training sessions in Turkey for teachers from 20 universities, CyberDay in Jordan, which brought together representatives from more than 20 universities, educational events for the academic community in Hong Kong (six educational institutions, for example, two-day workshop for The Hong Kong Polytechnic University students) and Malaysia (nine universities, for example, signing a Memorandum of Understanding (MoU) with Universiti Tun Hussein Onn Malaysia (UTHM) to support the university's Information Security Programme). These formats bring together faculty and students, enable discussion of today's cybersecurity challenges, and introduce hands-on approaches into curricula.

Our plans for 2026–2027

- **Deepen cooperation with universities in Russia.** We plan to expand investments in educational programs, update our collaboration with universities in line with evolving IT training requirements, increase the number of partner universities, and launch joint projects.
- **Expand our international presence.** We will continue to develop educational initiatives and partnerships in the Middle East and Africa, South and Southeast Asia, and Latin America—both by collaborating with educational organizations and by working with local professional and student communities.

How we develop IT specialists

We help employees and students hone their cybersecurity skills: we teach them how to deal with real-world threats, share expertise from leading professionals, and help them get a solid start in an IT career.

We are developing the Kaspersky Expert Training portal

Technological advances and legislative changes continually impose new requirements on cybersecurity professionals. As a result, continuous learning is an integral part of the profession. To help specialists update their knowledge and master cutting-edge tools, we are developing a hands-on training system on the Kaspersky Expert Training platform.

These self-paced online courses are developed by leading Kaspersky experts who work daily with hundreds of thousands of malware samples and real-world incidents. In the training, theory is always reinforced by practice: in virtual labs, students complete assignments and analyze cases based on current threats and scenarios that specialists encounter in their work.

The course materials are designed for both individual cybersecurity specialists and companies that want to train their information security teams (SOC, CERT, etc.). Our courses can benefit research institutes, incident response centers and government organizations.

Skills that can be developed with Kaspersky Expert Training

- secure software development
- threat hunting and threat detection
- incident response and digital forensics

We offer basic courses for all skill levels, as well as advanced courses for experienced experts and professionals. We teach how to use Ghidra[1], Yara, Suricata, Frida and other security tools.

In 2024–2025, the portal gained three new online courses:

- **Windows digital forensics**. This course teaches methods for detecting and managing various types of digital evidence within a forensic examination, and offers practice using specialized tools for collecting evidence and analyzing artifacts in Windows.
- **Secure software development**. The course covers best practices for secure software development and teaches how to effectively integrate them into product development processes.
- **Large language models security**. A course on the fundamentals of security for large language models (LLMs), using real-world attacks, defense strategies, and security systems as examples.

>3,000
The Kaspersky Expert Training users in over 50 countries

>200
Employees received free access to Kaspersky Expert Training courses in 2024–2025

74.5 hours
students spent completing a course on Advanced malware analysis techniques

The Kaspersky Expert Training portfolio includes
13 online training courses

[1] Ghidra is an open-source software reverse engineering (SRE) framework created and maintained by the National Security Agency Research Directorate. Reference herein to any specific commerical product, process, or service by trade name, trademark, manufacturer, or otherwise, in this Software is used for informational purposes only and does not constitute any association or relationship with NSA or its products.

In addition to educational courses, we launched the Cyber Pathways website, which explores the wide range of roles available in cybersecurity. The website highlights the specifics of various roles, the required competencies, and possible career paths. Cyber heroes, each representing a key specialization, help users understand information security roles and acquire the necessary skills.

This project is integrated with the Kaspersky Expert Training platform and serves as a convenient starting point for professional development. After completing a career guidance test, visitors can receive personalized educational recommendations, including a selection of appropriate online courses or trainings. This lets visitors choose the right direction and identify a path for consistent growth.

In 2025, together with the Cybersecurity Service Center, we also launched new expert-product training for specialists working with Kaspersky solutions, such as KATA (Kaspersky Anti-Targeted Attack), KUMA (Kaspersky Unified Monitoring and Analysis Platform), and EDR (Kaspersky Endpoint Detection and Response). These programs help users gain a deeper understanding of the products' capabilities and learn how to effectively use them to detect threats and automate responses.

We emphasize providing localized training. In 2024, we launched the platform in Russia and published three training courses in Russian: "Windows incident response," "Advanced malware analysis techniques," and "Secure software development." A localized version of the "Suricata for incident response and threat hunting" program was also released at the end of 2025.

The Advanced malware analysis techniques course was the most time-consuming, taking an average of 74.5 hours to complete. In 2025, the most popular topics were information security monitoring and active threat hunting, as well as Windows incident response.

We also continue to provide free educational programs to international law enforcement organizations. In 2024, 32 INTERPOL officers completed training, and in 2025, training for around 40 AFRIPOL officers began in November and was completed in March 2026.

In 2026–2027, we plan to expand our portfolio of expert programs with training in machine learning and threat intelligence security. We will also partially update existing courses and continue to localize them into Russian.

We offer internship programs

Kaspersky operates **SafeBoard**, a paid internship program that helps Russian students immerse themselves in the field and work alongside industry experts.

Internships run twice a year, in spring and fall. The selection process includes tests of technical knowledge and practical assignments, and is designed to make the process as transparent and convenient as possible for the candidate. Students residing in Moscow and the Moscow Region must submit an application and complete an online selection process that includes a video interview, testing, and an assignment. Candidates who successfully complete the selection tasks may receive a job offer following interviews with expert teams who are hiring.

To bring candidates into the Company as quickly and conveniently as possible, in 2025 we moved the entire intern selection process into our recruitment system, unifying the hiring process. Now candidates receive all the required tasks at once, and the speed at which they complete the stages largely depends on them.

In the summer of 2025, we celebrated the 10th anniversary of the SafeBoard program. Our big celebration brought together nearly 500 people, including via an online broadcast: students, interns, and employees who began their careers at the Company through internships.

We constantly analyze feedback from interns and mentors to improve these efforts, and we continue to invest in onboarding new hires. All interns receive onboarding[1] materials and training recommendations to help them come up to speed and start working productively.

Results of the SafeBoard program after 10 years:

>800 interns
joined Kaspersky

>350 former interns
still work for the Company

>200 former interns
work for the Company in mid-level and higher positions

[1] Onboarding is the process of introducing a new employee/intern to a company and integrating them into the team.

Digital awareness

GRI 3-3

Kaspersky develops projects to improve society's digital literacy through accessible training and practical projects for various audiences.

How we educate users about cybersecurity basics

We believe that for technology to be beneficial, people need to understand how it works, what risks exist online, and how to protect themselves and their loved ones. That's why we develop educational initiatives that explain cybersecurity basics in simple, understandable language and foster a responsible attitude toward digital technology.

One of the key areas of our work is teaching digital security rules. We explain how to recognize telephone and online scams, protect personal data, and safely use connected devices and digital services. This knowledge helps people make informed decisions in digital environments and reduce risks in everyday life.

We speak about cybersecurity simply and clearly

Kaspersky has created several educational projects for people at every level of involvement in cybersecurity—from information security experts to ordinary internet users. The Change Your Password! and OBIBE podcasts discuss digital risks, cyber hygiene, and modern threats. They cover both universal topics that are relevant to every user and specialized issues of interest to professionals.

We offer the Kids' Cyber Resilience project for children and teenagers

In 2023, Kaspersky, together with international partners, launched the Cyber Resilience for Children program in the Asia-Pacific region. Over the years, it has expanded significantly and now covers Vietnam, Indonesia, Philippines, Malaysia, India, Egypt and the CIS countries.

The **Kids' Cyber Resilience** project hosts educational events for children, parents, and teachers, where everyone learns how to behave safely in digital environments. In 2024, we created a series of online training courses on the safe use of artificial intelligence in education. This training is designed specifically for educators and parents to help young people navigate new technologies.

In 2026–2027, we plan to launch the Kids' Cyber Resilience program in Russia and the CIS countries, as well as in several countries in the Middle East and Africa.

We build cyber resilience in society

Kaspersky is developing several projects aimed at fostering a responsible attitude towards technology through education and culture.

- IT Journalism is Russia's first educational course dedicated to information security for future journalists. Journalists play a key role in shaping public understanding of digital risks, cyber threats, the potential of new technologies, and principles that inform how to safely use them. To make future media professionals more competent in IT and cybersecurity, we launched the IT Journalism course at the HSE Institute of Media in 2025. Here, students study cybersecurity, the IT industry, and become familiar with specific aspects of working with technology topics in the media.

Case 404 online game

Teaching Gen-Z about cybersecurity through games

Problem

Many users, especially young people, underestimate digital threats, and traditional formats for cybersecurity training often prove to be difficult and uninteresting.

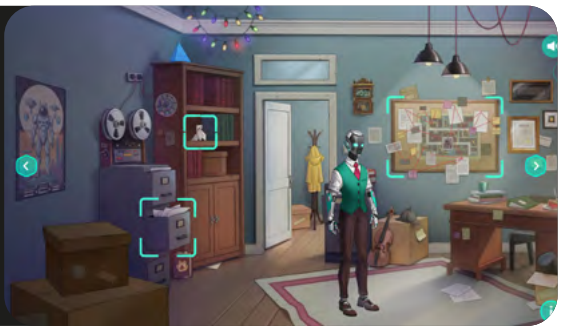
What we did

Kaspersky created Case 404, an interactive online game available in nine languages, that particularly targets Gen-Z users. In this game, players become cyber detectives who must solve exciting cyber crime cases. Users solve problems based on real-world cyberthreat scenarios: hacks, data leaks, online stalking, and social engineering.

To promote the project, the Company collaborated with NASR Esports and Reckoning Esports teams as well as Twitch Japan.

What was the result?

- **>30,000** players
- Better digital literacy in practice
- Accessible and easy-to-understand learning format
- More responsible behavior on the Internet



We develop educational programs for university students and schoolchildren

Comprehensive courses on the Kaspersky Academy platform

In 2025, we created a new learning platform for universities, providing access to our Introduction to Cybersecurity. Entry Level and Fundamentals of Cybersecurity courses, which we update in Russian and English. We also launched the Cyber Hygiene course, a universal basic course for anyone who wants to protect themselves online, and an online course on IT and information security for schoolchildren and university students.

Kaspersky Academy Alliance for Russian colleges

We know that secondary vocational education is an important stage in developing the skills of future specialists. That's why Kaspersky launched a program to collaborate with colleges to help their students get a cutting-edge cybersecurity education.

Partnerships and internships for students

In Indonesia, we entered into an agreement with PeaceGeneration Indonesia to increase digital awareness among young people. We also offer internship programs: in India, students are gaining practical experience in information security, and in Russia, the Technology Valley summer project held in 2024 gave schoolchildren and university students the opportunity to work on real Kaspersky projects.

We work with schools and teachers

Educational work in schools

Since 2018, Kaspersky has actively participated in educational work related to information security for students at Russian schools, their parents, and teachers.

For example, Kaspersky experts developed the Fundamentals of Information Security course for students in grades 7–11. Teachers can use the material in computer science lessons or as part of extracurricular activities. It is also available to parents of students. The curriculum is based on materials accumulated over years of work with computer science and mathematics teachers, as well as with Moscow schools in collaboration with the Moscow Department of Education and Science.

The course is regularly updated, thanks in part to the Company's collaboration with ten sponsored schools and a college, where offline classes are held regularly. Top managers from Kaspersky, including Eugene Kaspersky himself, give lectures to schoolchildren and teachers at the State Budgetary Educational Institution "Vorobyovy Gory".

Kaspersky experts teach classes at

10

sponsored schools

In addition, twice per academic year, the Company conducts online professional development courses for mathematics and computer science teachers in various regions of Russia.

All of Kaspersky's educational activities are carried out with the support and under the auspices of the Federal Institute for Digital Transformation in Education (FICTO) of the Russian Ministry of Education.

Digital Lesson

ЦИФРОВАЯ ЭКОНОМИКА
НАЦИОНАЛЬНЫЕ ПРОЕКТЫ РОССИИ

Personnel for the Digital Economy, a federal project

Digital Lesson, a nationwide Russian educational project

The project is being implemented by the Russian Ministry of Education, the Russian Ministry of Digital Development, and Autonomous Non-Profit Organization Digital Economy in partnership with leading Russian technology companies

Since 2018, Kaspersky has been a partner of Digital Lesson, a nationwide Russian educational initiative that is part of the Personnel for the Digital Economy federal project. Each year, we develop and release one focused lesson with an interactive simulator for students, parents, and teachers. These lessons are taught in Russian schools over the course of three weeks.

>22 million

Kaspersky's "Digital Lessons" have been completed more than 22 million times since 2018.

When creating new lessons, we try not to overload students with difficult information. Instead, we focus on what is essential. For us, it is important to present the material in an easy and accessible way, and to engage children with high-quality animations and interactivity.

Environment

ESG priority

PUE of 2
Kaspersky data centers' energy efficiency score

48%
of sales were in digital formats in 2025

52%
of collected clothing items donated to charity

How we manage environmental protection

Our commitment to security extends beyond the digital environment. It also informs our approach to environmental protection. Although Kaspersky does not have a direct impact on ecosystems, we monitor our resource use and promote responsible use of natural resources to support environmental security for future generations.

Our approach and key impacts

Kaspersky protects the environment through consistent, systematic efforts. We monitor the direct and indirect impacts of our activities on the environment and climate and strive to minimize them.

The Company's main environmental impacts are related to office activities and IT infrastructure. We consume water and electricity, generate waste (including packaging from physical products), and create a carbon footprint indirectly through air travel, servers and data centers, energy consumption at offices, corporate transportation, and the services required to develop and distribute our solutions.

To minimize these impacts, we optimize our business processes, strive to keep our offices and server infrastructure energy efficient, and reduce resource consumption and waste generated during the production of physical products.

Environmental protection issues fall within the area of responsibility of several department heads at Kaspersky. They develop and implement practical solutions that help reduce environmental impacts and support the Company's sustainable development.

Results for the reporting period

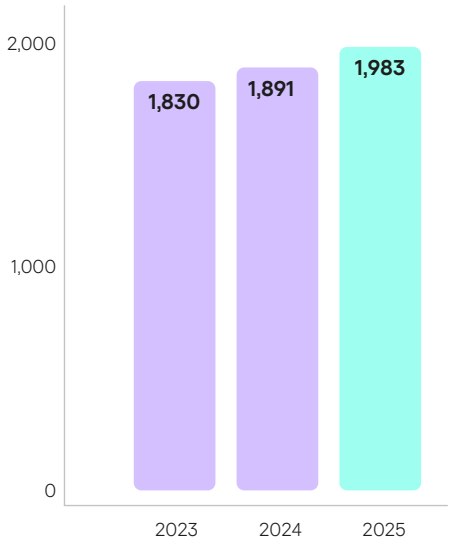
>43,000

US dollars

Kaspersky invested in environmental protection measures in 2024–2025.

We fully comply with environmental legislation. In 2024–2025, the Company did not receive any fines, non-financial sanctions or any complaints related to environmental violations.

Total environmental protection costs, thousands of rubles



We reduce our carbon footprint

Kaspersky recognizes the impact of climate change and consistently works to reduce the carbon footprint of its operations.

In 2024–2025, we continued to analyze the Company's climate impact and assess opportunities to reduce it. Our activities are aligned with the UN Sustainable Development Goals (SDGs), including SDG 13 "Climate Action."

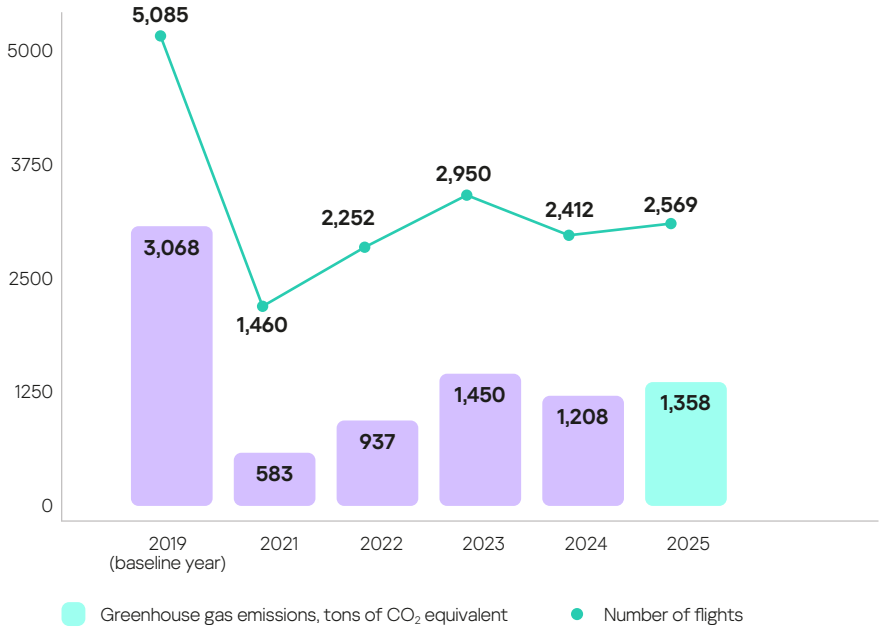
We are already taking practical steps to reduce emissions. In particular, we use energy-efficient equipment and technologies and strive to reduce the carbon footprint associated with all business-related travel.

How we manage transportation emissions

GRI 305-3, GRI 305-5

We understand that air and road transport significantly contribute to climate impacts, so we are committed to reducing emissions resulting from fuel consumption. In recent years, we have reduced our corporate fleet to three vehicles, which are used exclusively for urgent work trips.

Greenhouse gas emissions from air travel by Kaspersky employees[1]



We are also working to reduce the carbon footprint of our air travel. In 2024, the number of air trips taken by the Company's employees decreased by 18.2% compared to 2023, and in 2025 — by 12.9%. Moreover, in 2025 we managed to reduce our emissions by a factor of 2.3 compared to the baseline year of 2019.

[1] Air travel data for 2020 is not provided because air traffic was suspended in 2020 due to the COVID-19 pandemic.

We improve energy efficiency

We consistently work to reduce energy consumption in our offices and data centers by combining technological solutions and responsible infrastructure management.

Our approach to managing energy consumption

For Kaspersky, energy efficiency is an important part of sustainable development and reducing our environmental impact. We manage energy consumption in both office spaces and data centers by deploying cutting-edge technologies, upgrading equipment, and optimizing processes.

The Company's headquarters are located in the Olympia Park business center in Moscow, which has an A-class energy efficiency rating and is BREEAM[1] certified. Energy-efficient materials and technologies were incorporated during construction of the building.

In our office, we use LED lighting fixtures, motion sensors, and automatic lighting controls that account for the level of natural daylight. These solutions allow us to reduce energy consumption without compromising employee comfort. Similar LED lighting is also used in the business center's parking lot.

Current power consumption

GRI 302-1

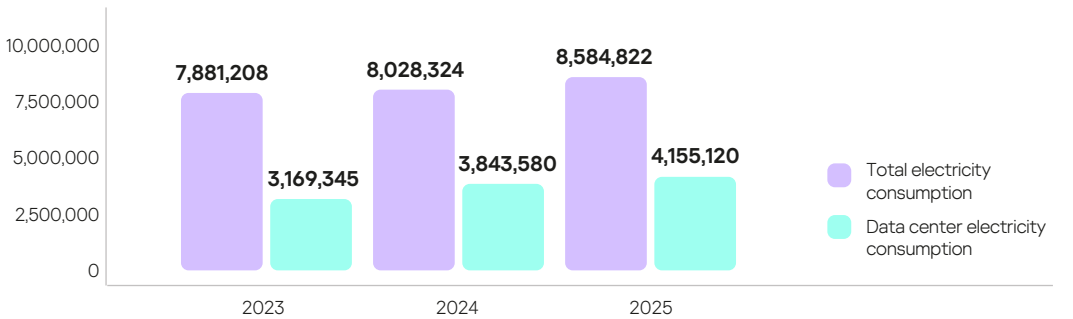
In 2024–2025, the Company's total electricity consumption increased slightly. This is due to natural business growth, expanded capacity at data centers, and the increased use of AI-based solutions for working with large volumes of data. Such technologies require significant computing resources and are therefore highly energy-intensive.

8,585 MWh
of total electricity consumption in 2025

At the same time, by consistently implementing energy efficiency programs, we have reduced electricity consumption at the Company's offices, despite the overall development and growth of our operations.

SASB TC-SI-130a.1

Energy consumption at Kaspersky[2], kWh



[1] The Building Research Establishment Environmental Assessment Method, developed by the British company BRE Global, is a standard or method for assessing the efficiency and environmental friendliness of buildings.
[2] This disclosure includes AO Kaspersky Lab's Moscow office, which includes the Company's data center. Information was not collected for the remaining offices during the reporting period.

Energy efficiency of data centers

GRI 302-4, SASB TC-SI-130a.3

PUE of 2

Kaspersky data centers' energy efficiency score

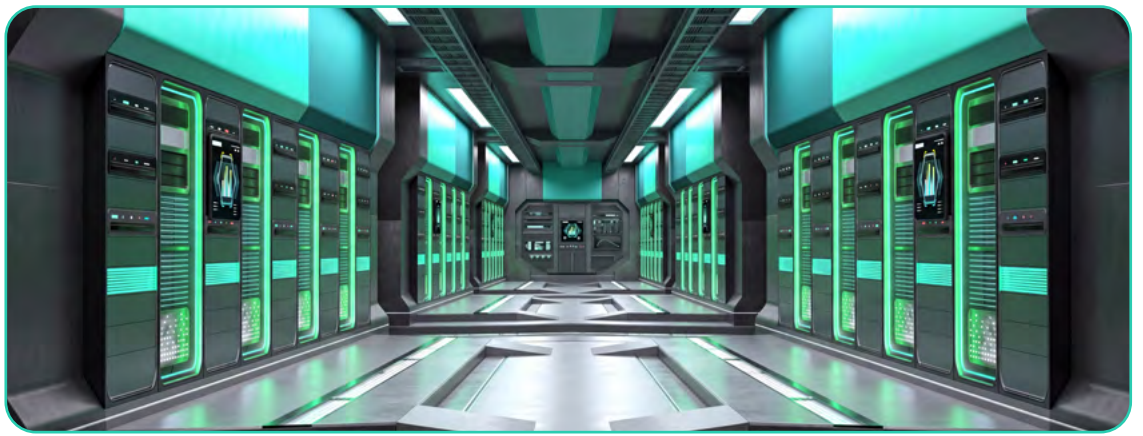
Data centers are one of the main sources of energy consumption in the IT industry. Energy is required for round-the-clock operation of numerous servers and the industrial air conditioners required to cool them. Kaspersky uses its own data center, which includes 33 server racks to support the user infrastructure and back office, as well as leased data centers for our development needs.

Our data center is connected to two independent substations. In the event of an emergency, a backup diesel generator allows the servers to continue operating for approximately 10 hours after all other power sources are disconnected. The batteries in uninterruptible power supplies (UPS systems) can keep servers running for 30 minutes, but their main purpose is to protect against short-term outages and seamlessly switch from city power to the diesel generator. The server room uses an environmentally friendly gaseous fire suppression system.

All electrical equipment is inspected regularly. The generator is started up for testing at idle speed once every two weeks and is started up under load once per quarter. The fuel in the generator is replaced annually. The uninterruptible power supply system is maintained quarterly and monthly. The construction of the data center involved energy-efficient technologies, including intelligent temperature controllers and occupancy sensors for lighting.

We also reduce energy consumption in data centers by upgrading computing equipment. We replace outdated equipment with new equipment that delivers greater performance per unit of power. We need fewer cables and racks by deploying servers with virtualization environments and solid-state drives (SSDs). We recycle old computer equipment and donate keyboards, laptops, monitors, and phones to charity.

We place high demands on data center infrastructure and employ energy-efficient solutions. In particular, during the cold season, we cool the data center naturally using outside air. We expand servers' permissible operating temperature range to 22–24°C and organize cold- and hot-air aisles. To prevent leaks of the refrigerants used in cooling systems, our staff checks the cooling equipment twice a day. If a leak is detected, the equipment is switched off, the refrigerant supply is shut off, and the gas is evacuated into a special cylinder.



To evaluate the efficiency of data centers, we use the Power Usage Effectiveness (PUE) metric, which is calculated as the ratio of the data center's total energy consumption to the energy consumption of the IT equipment.

In 2024–2025, our data centers had a PUE of 2, whereas the global average in 2024 was 1.56, according to the Uptime Institute, an international data center certification organization.

We optimize water use

We take a responsible approach to water use and strive to reduce consumption through technical and organizational measures.

Our approach to water use

GRI 303-1, GRI 303-2

At Kaspersky, water is used exclusively for the day-to-day office and data center operations. We get water only from municipal water supply systems and do not abstract water from natural sources.. Additionally, wastewater is not discharged into natural water bodies.

Our water management approach is based on preventing losses and ensuring that our engineering systems operate reliably. We pay special attention to the technical condition of our equipment and regularly upgrade our infrastructure to minimize the risk of accidents and inefficient water use.

Water consumption and measures to reduce it

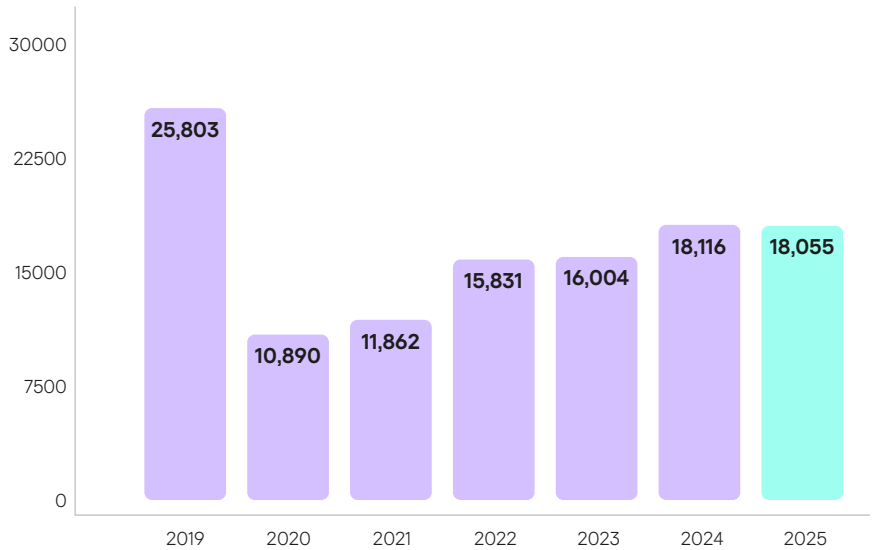
In 2024–2025, the Company's water consumption increased slightly compared to 2022–2023. This was due to a gradual change in format of work and an increase in how much time employees spend in the office instead of working remotely. That said, the current level of water consumption remains significantly lower than the 2019 baseline.

To reduce water consumption and prevent losses, we implement a range of technical measures, including:

- We regularly inspect the condition of shut-off and control valves.
- We periodically perform water analysis to monitor the condition of pipelines.
- We maintain the necessary stock of spare parts and equipment. This lets us promptly fix problems and minimize water loss in emergency situations.

GRI 303-5, SASB TC-SI-130a.2

Water consumption[1], cubic meters



In 2026–2027, we plan to explore the possibility of installing additional shut-off devices on main pipelines. This will let us find potential leaks more quickly and accurately, reduce the area affected by a shutdown, and decrease the volume of water that must be drained during repair work.

[1] This disclosure includes AO Kaspersky Lab's Moscow office, which includes the Company's data center (our main source of water consumption). Information was not collected for the remaining offices during the reporting period. In our business operations, water is used for ordinary purposes at the Company's offices. Accordingly, we report total water consumption. Our offices are not located in regions considered to be under water stress.

We manage waste generation

We aim to reduce and responsibly manage waste across all aspects of our operations, from our office work to our products.

Our approach to waste management

GRI 306-1, GRI 306-2

Waste management at Kaspersky combines waste reduction, separate collection of waste, and responsible disposal.

A significant percentage of the Company's waste is associated with day-to-day office activities and the production of physical products. These are the areas where we focus most of our efforts to reduce our environmental burden.

Types of waste and how they are handled

The Company's offices generate mainly household and office waste, as well as certain types of hazardous waste, such as batteries and electronic devices. We have implemented a separate collection system at our Moscow office: we set up containers for paper, plastic, glass, metal, and mixed waste, and in the printer rooms, we have separate containers for waste paper, plastic caps, batteries, rechargeable batteries, and e-cigarettes.

We entrust the collection, transportation, and transfer of waste for recycling or disposal to specialized companies. Additionally, all counterparties are checked for compliance with legal requirements. Waste of hazard classes I and III is subject to partial neutralization before being sent for disposal or burial.

GRI 306-3, 306-4, 306-5

Waste generation[1], tons

Indicators	2023	2024	2025
Total waste generation at the Company's facilities, including:	**225.6**	**353.7**	**410.8**
■ **Class I** (extremely hazardous, non-degradable waste: pesticides, asbestos, devices containing mercury)	0.1	0.3	0.3
■ **Class II** (highly hazardous waste that decomposes in more than 10 years: insecticides, fungicides, lead, arsenic, batteries, pyrotechnics)	0	0	0
■ **Class III** (moderately hazardous waste that decomposes in three to ten years: herbicides, paints and varnishes, detergents, shampoos, deodorants, mobile phones)	0.7	0.4	0.7
■ **Class IV** (low-hazard waste that decomposes within three years: nitrogen fertilizers, fiberboard, chipboard, polyethylene film, mirrors, rubber gloves and shoes, disposable tableware, household appliances)	219.4	353.0	409.9
■ **Class V** (practically harmless waste that decomposes within three years: food products, natural fabrics and products made from them, paper and cardboard products)	5.4	0	0
Sent for burial	225.1	352.9	409.9
Sent for recycling	0.2	0.4	0.7
Sent for neutralization	0.3	0.3	0.3

[1] This includes waste from the Moscow office, including the data center, as well as waste from business operations.

We work to generate less waste

Kaspersky consistently implements waste reduction practices.

To generate less waste at the Company, we:

- research and select suppliers that offer products in recyclable and environmentally friendly packaging
- refuse to use superfluous and functionally unjustified items in our operations
- use reusable tableware and high-quality materials with a long service life
- make our souvenir and advertising products more environmentally friendly by selecting sustainable materials and solutions

In particular, we consistently reduce the use of plastic in the production of souvenir products. Instead of plastic bags, we purchase bags made of durable materials as well as reusable canvas bags.

In 2026–2027, the Company plans to implement programs to improve employee environmental awareness and revise internal regulations to reduce the consumption of paper and disposable materials. We will also explore the possibility of using equipment with a longer service life and upgrading existing equipment to reduce the volume of discarded equipment.

We optimize packaging

A significant portion of waste in the world is generated by product packaging. To decrease the volume of this waste, we consistently reduce our production of physical products, reducing box thickness and pallet space. We provide information on packaging to facilitate recycling, reduce waste, and promote digital distribution. In 2025, the Company's share of boxed products in sales of solutions for home users remained at 8.8%.

We cannot yet completely stop releasing products on physical media: some customers still prefer CDs or DVDs, mainly out of habit. In some regions, including African countries, this preference is due to the lack of stable internet access. For these products, we use compact packaging with the minimal plastic content.

Kaspersky products on physical media formats

Boxes, leaflets and envelopes

cardboard boxes or thin envelopes containing a flyer with a product activation code and a CD with the product

DVD cases

plastic boxes that do not contain a disc; instead, they contain a leaflet with a code (in French-speaking African countries, the box also includes a disc)

Plastic cards

an activation code is hidden under a protective coating that is scratched off by the user for activation

POSA POR

A display card made of thin cardboard; the activation code is not located on the card but is printed on the receipt upon purchase.

POSA[1] cards

a cost-effective cardboard medium with a code (visible or hidden)

[1] Point-of-Sales Activation — A product that is activated at the point of sale.

We are increasing the share of digital sales

Overall, the share of digital licenses and digital formats trended upward in 2022–2025, at different rates in different regions. We are actively transitioning our existing clientele to digital licenses through various mechanisms. In Russia, Latin America and Northern Europe, 85–90% of licenses are already digital.

36% of revenue from sales of home solutions comes from renewals, i.e. one year after purchasing a new license, users return to our website to purchase another one. Between 2024 and 2025, 6% of home licenses became digital as customers made their purchase online one year after their initial purchase in a retail store.

We encourage our partners to transition to purchasing licenses online, and distributors to distribute licenses through their own websites, which also simplifies access to foreign markets.

We are introducing more environmentally friendly packaging

In 2024–2025, the Company overhauled its retail packaging to make it more environmentally friendly. The updated formats are more cost-effective. For example, the box is now 50% thinner and 20% lighter than the previous version, and the envelope is 80% more compact. We also completely eliminated the internal cardboard insert, which let us consume less cardboard and ink, reduce shipping volumes, and optimize storage at distributors.

52%

of sales were boxed solutions in 2025

48%

of sales were in digital formats in 2025

We use special labeling

In accordance with the Package and Packaging Waste Regulation **(PPWR)**, Kaspersky places information on packaging to help consumers properly sort and dispose of used materials, and also complies with Extended Producer Responsibility **(EPR[1])** requirements in all regions where it operates.

All Kaspersky packaging materials bear the required **PAP/PP symbols**. These are international labeling codes used to identify the composition of packaging and facilitate its sorting and recycling. **PAP** indicates paper and cardboard products, and **PP** means products made of polypropylene (plastic).

Our production is recorded in national **EPR** systems, and it is reported annually according to their rules. In France, we use the **Triman** logo, in Germany and Portugal the **Green Dot**, in Spain the colour-coded **Symbol for Recycling**, and in the Italian market **Disposal IT PRP** (Preparazione per il Riutilizzo e il Riciclo) labeling with detailed disposal recommendations.

In addition, since 2025, products supplied to the Italian market will be additionally labelled with Forest Stewardship Council **FSC[2]** certification, which confirms the use of packaging materials from responsibly managed forests.

We conserve paper by developing digital processes

We reduce the use of printed materials and recycle old banners, posters, and photo panels. To save paper, Kaspersky has actively used an electronic document management (EDM) system with external contractors since the end of 2022.

In 2024, 75% more documents were signed via our electronic document management (EDM) system than the previous year, and another 20% more were signed that way in 2025.

More than 50% of our counterparties already work with us digitally, which covers over 40% of our accounting documents.

In the future, we plan to implement an internal electronic document management system for human resources.

1 Extended Producer Responsibility is an approach to environmental regulation under which manufacturers and importers are responsible for the environmental aspects of their products throughout their entire life cycle, including the collection, recycling, and disposal of packaging and waste after use.

2 The Forest Stewardship Council (FSC) is an international non-profit, non-governmental organization that promotes responsible forest management worldwide.

We cultivate environmental awareness

We consistently develop eco-friendly habits among our employees and support initiatives that help care for the environment.

Kaspersky cultivates environmental awareness through systemwide programs and everyday practices. We educate employees about sustainable consumption principles, support their initiatives, and engage local communities in environmental projects.

Employees actively participate in the Company's environmental campaigns. Those who share a passion for eco-friendly living join the internal Green Like Midori community, where they can discuss various office improvement ideas. We regularly hold webinars and workshops dedicated to environmental protection, and we publish reports from these events on our intranet.

In 2024–2025, our main focus, besides environmental education within the Company, was on strengthening partnerships with the charitable foundations Second Wind and Nature and People.

We treat things purposefully

We have collaborated with Second Wind Foundation since 2022. We set up a container for collecting clothes and textiles in our office, and in 2024 we updated its design, making it more informative. The container now includes explanations about what items are accepted by the foundation and how they should be donated, as well as a visual map of an item's journey from the office to sorting, charity, recycling, or disposal. We also began sharing statistics regularly so employees could see the real impact of their actions.

These changes produced results. In 2024, our employees collected 1,535.8 kg of items (9.1% more than the previous year).

How collected clothing and textiles were handled in 2025, %

Helping people in difficult life situations	52
Repurposing	36
Recycling	10

In 2025, we collected 1,803.2 kg of items, 52% of which the charitable foundation was able to use to directly help people. The growth in this indicator is especially important to us, as it shows that employees are increasingly conscientious when donating items.

>3 tons

of items were collected by the Company's employees in 2024–2025

In collaboration with Second Wind, we also held eco-events for employees:

- a workshop on upcycling old clothing items — a foundation expert demonstrated how to give clothes a new look and extend their lifespan;
- workshops held during corporate children's days in 2024 and 2025, where participants created greeting cards and home décor items from recycled materials together with their children.

In 2025, we implemented another important project together with Second Wind: we recycled old Kaspersky merchandise. More than 1,500 T-shirts and sweaters with old logos were upcycled by the foundation's artisans into unique cosmetic bags and laptop sleeves. The collection was sold at the corporate Christmas charity fair in December 2025 in support of the Zhivi Foundation.

We conserve rare animal species

ПРИРОДА И ЛЮДИ

In partnership with Nature and People Foundation, we support projects to conserve rare animals and ecosystems.

In 2024, Kaspersky participated in the “Saving Sea Otters” project. In July, we supported a marine expedition to Urup Island and other islands of the Kuril chain to assess the status of sea otter populations and develop recommendations for their protection. Scientists covered 175 km of coastline and recorded more than 530 sea otters. The results confirmed the stability of the population and highlighted the importance of protecting these areas from human impact.

In 2024, we also organized an emergency fundraising campaign to support the foundation in purchasing food for blue Arctic foxes on Medny Island. That winter, the population of these animals was at risk of disappearing entirely due to a critical food shortage. Our employees raised more than $1,000 (100,000 rubles), the Company matched this amount, and then contributed an additional $3,260 (300,000 rubles) as part of the foundation’s New Year fundraising campaign.

In 2025, we again supported the “Saving Arctic Foxes on Medny Island” project. During expeditions to the islands in the Sea of Okhotsk, experts assessed population sizes, delivered 600 kg of feed to Medny Island, and set up two new feeding sites to help the animals survive the winter. Kaspersky also supported the foundation's New Year's fundraising for the Przewalski’s horse conservation project, donating over $2,000 (200,000 rubles).

The foundation also regularly shares the results of its work with the Company’s employees, including through lectures held as part of internal events, meetings of Kaspersky’s Travel Club, and other interest-based clubs.

420 kg

of electronic equipment was handed over for environmentally friendly recycling in 2024–2025

>1,300 books

collected and distributed to new readers

We make caring for the environment part of office life

We believe that environmental awareness is built through small but consistent actions, so we continue to create a work environment where making informed choices becomes second nature for our employees.

Every year we hold an Office Eco-week, where our employees collect their unwanted electronics, books, and clothing and donate them all to Kaspersky partners. In 2024, 170 kg of e-waste was donated to our partner Petromax for environmentally friendly recycling, and more than 400 books were donated to rural libraries as part of the Re:Books social and environmental project.

Then in 2025, employees collected 250 kg of electronics and 514 books. We also held a separate book drive for a charity festival in support of the Zhivi Foundation, which collected over 400 books.

In autumn 2025, we introduced a fast-charging station for electric vehicles at the office underground parking. This enabled more employees to use electric cars and charge them conveniently.

Responsible Business Conduct

$9.4 million
invested in the GTI's development over 7 years

13 transparency centers
around the world

155 patents
received by Kaspersky for its technologies in 2024–2025

Respect for human rights

Respect for the rights of employees, customers, local communities, and other stakeholders is a fundamental and integral principle of our operations and underpins Kaspersky's corporate culture and responsible business practices.

GRI 406-1

GRI 2-23 , GRI 2-24

Kaspersky is guided by the principles of the UN Global Compact, the UN General Assembly Resolution on Sustainable Development Goals, the Paris Agreement of December 12, 2015, the International Bill of Human Rights, including the Universal Declaration of Human Rights, the Convention for the Protection of Human Rights and Fundamental Freedoms, the UN-endorsed Guiding Principles on Business and Human Rights, and the relevant national and regional legislation of the countries where it operates.

Additionally, Kaspersky has signed the European Commission's Artificial Intelligence Pact to foster trustworthy AI use[1]. By signing the pact, the Company affirmed its commitment to promoting the rational and responsible use of AI technologies, thereby recognizing their importance in cybersecurity.

Upon signing the agreement, we assumed three main obligations:

- adopt an AI governance strategy to ensure that the Company implements AI in a way that complies with future AI regulations
- identify AI systems that may be classified as high risk under the AI Act
- raise the level of AI awareness among the Company's employees and other persons working with AI systems on behalf of the Company, accounting for their technical knowledge, experience, education and training, as well as the context in which the AI systems will be used.

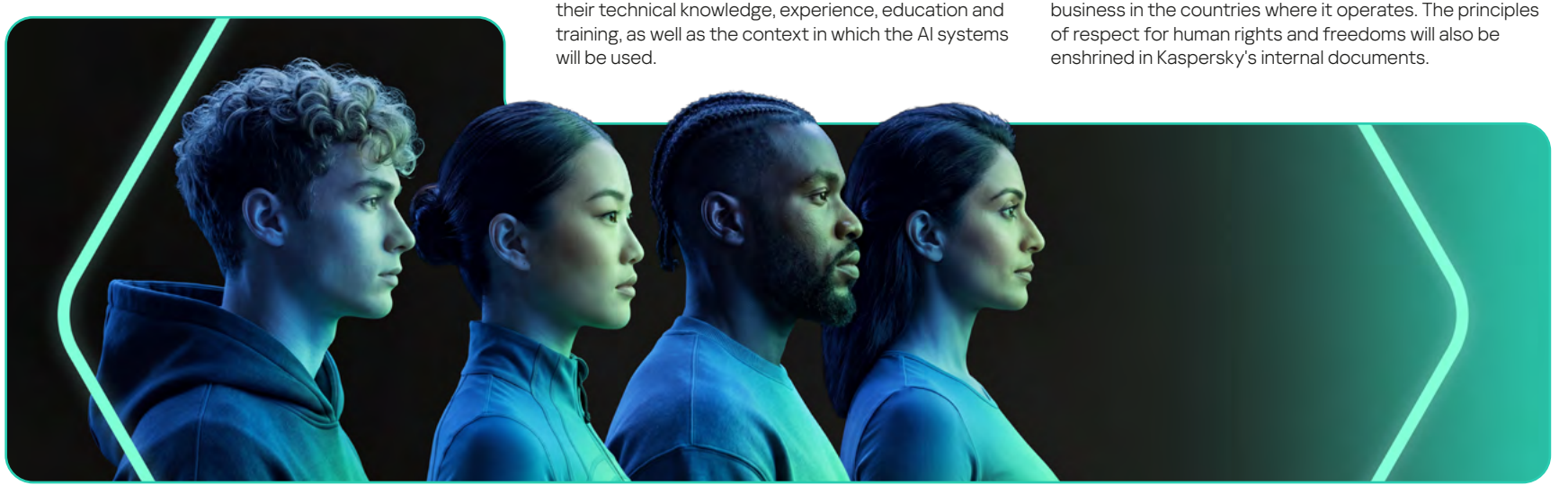
Kaspersky does not tolerate any form of discrimination or the use of child, slave, or forced labor, and expects similar commitments from its partners throughout its supply chain.

This position of the Company is enshrined in its internal policies, which reflect the guiding principles for conducting business in the countries where it operates. The principles of respect for human rights and freedoms will also be enshrined in Kaspersky's internal documents.

0

cases of discrimination at the Company during the reporting period

The Company strictly complies with international and local legislation, relying on the ISO 26000-2010 "Guidance on social responsibility" and the international standard AA1000 (AccountAbility Principles, Stakeholder Engagement Standard).



[1] The EU AI Act comes into force in mid-2026.

Respect for human rights in the Company's activities

Basic human rights	Documents that govern the Company's behavior	The Company's approach to respecting human rights	Stakeholder groups that the Company may affect in each area of human rights	Results for the reporting period
Right to life, liberty, privacy, and family life	■ Constitution of the Russian Federation, Articles 20, 22, 23 ■ Applicable laws in the countries where Kaspersky operates, including: – GDPR[1] – ISO/IEC 27001, an international standard for information security – Federal Law No. 152-FZ of July 27, 2006 "On Personal Data" – PIPL[2] – CCPA[3] – LGPD[4] – PDPD[5]	One of the Company's priorities is to ensure the protection of our clients' data worldwide through internal security systems and procedures. We do not use data for anything other than the purposes for which it was collected.	■ Users ■ Employees ■ Groups vulnerable to information security threats ■ Non-profit organizations	0 serious violations of personal data laws 0 significant data breaches
Right to work	■ Constitution of the Russian Federation, Article 37 ■ Labor Code of the Russian Federation ■ Internal labor regulations ■ Occupational Safety and Health Policy ■ Guidelines for Charitable Projects ■ Regulations on the Sustainable Development Committee ■ Applicable laws in the countries where Kaspersky operates	For Kaspersky, our employees are our most valuable asset. We are committed to ensuring that people at the Company feel comfortable and engaged, that they can work productively, feel protected, and that they can develop themselves and the Company. Kaspersky supports non-profit organizations that help people with disabilities with employment and social integration, as well as provide them with legal assistance.	■ Employees ■ Groups vulnerable to information security threats ■ Non-profit organizations	5.691 was the total headcount at the end of 2025 (+11.3% compared to the end of 2024). Employee turnover in 2025 was 10% (5 percentage points lower than in 2024). During the reporting period, the Company supported five non-profit organizations that help employ people with disabilities. The Company took part in ten inclusive employment events (business breakfasts, job fairs, and a mentoring program). The Company launched https://kasperskystories.com/, a website that shares the professional and personal journeys of our employees with disabilities and those raising children with disabilities

1 EU General Data Protection Regulation.
2 Personal Information Protection Law of the People's Republic of China.
3 California Consumer Privacy Act.
4 Brazilian General Data Protection Law (Lei Geral de Proteção de Dados).
5 Law of Vietnam on the Protection of Personal Data (Personal Data Protection Decree).

Basic human rights	Documents that govern the Company's behavior	The Company's approach to respecting human rights	Stakeholder groups that the Company may affect in each area of human rights	Results for the reporting period
Right to a healthy environment	■ Constitution of the Russian Federation, Article 42 ■ Federal Law No. 7-FZ of January 10, 2002 "On Environmental Protection" ■ Regulations on the Sustainable Development Committee ■ Guidelines for Charitable Projects ■ Applicable laws in the countries where Kaspersky operates	Responsible environmental stewardship is one of Kaspersky's core values. We reduce our environmental impact through efficient use of resources, well-organized business processes, and a responsible approach to energy sources for our data centers and offices.	■ Employees ■ Local communities ■ Users ■ Non-profit organizations	>50% of our counterparties are already connected to our EDMS[1] and work with us digitally. In 2024–2025, Company employees donated or recycled more than 3 tons of items. 420 kg of electrical equipment was recycled. >1.300 books were collected and distributed to libraries in small towns or villages over two years. >$4.000 was allocated to purchase food for blue Arctic foxes on Medny Island in 2024. $2.410 was donated to the Przewalski's horse conservation project in 2025. In 2024, the Company supported the implementation of the "Saving Sea Otters" project, initiated by the "Nature and People Foundation".
Right to education	■ Constitution of the Russian Federation, Article 43 ■ Federal Law No. 273-FZ of December 29, 2012 "On Education in the Russian Federation" (as amended on August 4, 2023) ■ Regulations on the Sustainable Development Committee ■ Guidelines for Charitable Projects ■ Applicable laws in the countries where Kaspersky operates	We encourage our employees to strive for new knowledge, constantly improving our internal educational programs and adding new ones. We implement joint educational projects with non-profit organizations that support people with disabilities, senior citizens, survivors of domestic violence, and others in vulnerable or difficult life situations. Kaspersky creates its own training programs designed to collaborate with educational institutions and audiences seeking additional education. We invest resources in the development of both school and university students, as well as experienced cybersecurity professionals who require further upskilling.	■ Employees ■ Users ■ Groups vulnerable to information security threats ■ Non-profit organizations	Kaspersky.Academy partners with ~200 universities in 45 countries. ~50 universities in various countries have joined the Academy Alliance program in two years. In 2024, together with the Love Syndrome Foundation, the Company unveiled Russia's first digital literacy manual for people with Down syndrome. Over the past 10 years, more than 800 interns have joined Kaspersky through the SafeBoard internship program >350 have become employees and still continue to work in at Kaspersky to this day. Kaspersky's "Digital Lessons" have been completed more than 22 million times since 2018. >3.000 users in over 50 countries use the Kaspersky Expert Training platform.

[1] Electronic document management system.

Basic human rights	Documents that govern the Company's behavior	The Company's approach to respecting human rights	Stakeholder groups that the Company may affect in each area of human rights	Results for the reporting period
Right to health protection and medical care	■ Constitution of the Russian Federation, Article 41 ■ Regulations on Compensatory and Incentive Payments ■ Applicable laws in the countries where Kaspersky operates	Caring for the health and well-being of employees is an important component of Kaspersky's social policy. The benefits package for Kaspersky's employees varies depending on the region where the Company operates. We also promote an active and healthy lifestyle among our employees.	Employees	0 employee injury cases in 2024–2025. 0 cases of occupational illness were identified among the Company's employees in 2024–2025. Webinars and Q&A sessions with an oncologist were held for Kaspersky HQ employees in 2024 and 2025 to cover common myths and misconceptions about cancer and the need for timely check-ups and testing.
Right to protection from discrimination	■ Constitution of the Russian Federation, Articles 19, 29 ■ Guiding Principles on Business and Human Rights ■ Kaspersky's internal policies, which reflect the guiding principles for conducting business in the countries where it operates	We do not tolerate discrimination of any kind in the Company's activities.	■ Employees ■ Users ■ Partners	0 cases of discrimination at the Company during the reporting period

Corporate governance

Our business is built on respect for the interests of our clients, partners, and the market as a whole. We encourage open communication, strive to improve the quality of information disclosure, and believe that trust and reputation are key assets of the Company and the foundation of sustainable development.

Key principles

- Ensure transparency in corporate governance
- Comply with anti-corruption policies by preventing violations
- Provide a high level of legal support to protect and defend intellectual property
- Reduce supply chain risks

Our approach to corporate governance

We value the Company's reputation and strive to build trust through responsible management, fair practices and high standards in all aspects of our activities.
The key principles and rules that shape our culture of business communication and professional conduct are set forth in Kaspersky's internal policies, as well as in the "Fundamentals of Corporate Ethics" online course, which is mandatory for all employees.

Board of Directors

GRI 2-10, GRI 2-11, GRI 2-13

The highest governing body of Kaspersky is the Board of Directors. It is responsible for key decisions and adopts global policies and strategies that are implemented in all companies within the group.
The current Board of Directors consists of two people. They each have been on a permanent contract for more than five years. The Board of Directors has no independent members, only executive ones.

Candidates to the Board of Directors are nominated by current board members.

Our Company does not have a permanent Chairperson of the Board of Directors. The chairperson is elected at each meeting of the board and has no special powers.

Responsibility for the economic, social, and environmental impacts of sustainable development has been delegated to Denis Zenkin, Head of Corporate Communications.

Management Board

The Management Board determines specific strategic and tactical steps for the Company's operations and the management structure of the group, and approves the appointments of top managers.

Eugene Kaspersky's management role as General Director is decisive, as he is simultaneously the holding company's largest shareholder and a member of the Board of Directors and the Management Board.

Collective knowledge of the highest governing body

GRI 2-17

To make the highest governing body more informed and competent in matters of sustainable development, members of the Board of Directors and the Management Board regularly participate in training events that external experts are invited to.

Evaluating the performance of the highest governing body

GRI 2-18

The performance of the Board of Directors and the Management Board is regularly assessed by the AGM of Kaspersky shareholders. This assessment is used to inform restructuring to improve the operational management of the Company. Criteria for assessing the governing bodies' oversight of the management of the Company's impacts on the economy, environment and social sphere were not adopted in the reporting period.

Business ethics and anti-corruption measures

Kaspersky complies with laws and regulatory requirements worldwide, consistently developing a culture of business ethics, transparency, and zero tolerance for corruption.

How we comply with anti-corruption policies

GRI 2-24

A fundamental principle of the Company's activities is that we do not accept any form of bribery or corruption, either directed towards us or on the part of the Company and its employees, and we do not participate in any form of unethical incentives or payments.

Kaspersky complies with applicable anti-corruption laws of the Russian Federation and the countries where it operates, as well as international anti-corruption laws, including the US Foreign Corrupt Practices Act (FCPA) and the UK Bribery Act 2010. Priority is given to the legislation of the Russian Federation at the Company's headquarters, whereas at foreign offices the local anti-corruption legislation is prioritized.

The basic principles of combating corruption are enshrined in our anti-corruption policy, which was adopted in 2012. It has been translated into 30 languages and is published on the Company's official website.

0

court decisions on violations of anti-corruption legislation in relation to the Company, employees, and partners

GRI 205-1, GRI 2-25, GRI 2-26

Kaspersky regularly assesses corruption-related risks.

The Company's management is responsible for compliance with the anti-corruption policy, but a compliance specialist coordinates and provides methodological support to bring internal regulations and procedures into compliance with the policy requirements.

Every employee and representative of the Company who becomes aware of actual or suspected violations of the anti-corruption policy and applicable anti-corruption legislation is obliged to report this. If desired, this can be done anonymously.

The Company provides several channels for reporting concerns:

- contacting your immediate supervisor or, if the concern relates to their actions, a higher-level manager;
- calling the Company's hotline at **+7 (800) 700-88-11**;
- sending information via email to nocorrupt@kaspersky.com;
- contacting a compliance officer or their representatives directly;
- reaching the Company's compliance officer at extension 3000 for employees in the Moscow office, or **+7 (495) 797-87-00** (ext. 3000) when calling from a landline.

Anti-corruption training and awareness raising

GRI 203-2, GRI 205-3

Every year, Kaspersky informs its employees about its anti-corruption policy and relevant procedures. When concluding contracts with counterparties, we integrate the anti-corruption policy into the contracts.

To train employees, the Company has developed a special online course dedicated to combating bribery and corruption. This course includes an introduction to the basic principles and key areas of the Company's anti-corruption policy, including:

- objectives of anti-corruption legislation;
- the importance of compliance with Russian and foreign laws on bribery and anti-corruption;
- patterns of behavior that lead to violations of anti-corruption laws;
- the need to exercise caution in business relations with third parties;
- internal control mechanisms that define employees' activities in accordance with the anti-corruption policy.

The anti-corruption training course is designed to take 30–40 minutes. The results of testing at the end of the course are recorded in an internal Kaspersky system. All Company employees, from senior management to junior specialists, completed the training during the reporting period.

In 2026, we plan to update our anti-corruption training materials and continue to implement anti-corruption best practices into the Company's activities.

100%

of employees and partners are aware of the anti-corruption policy

0

confirmed cases of corruption in the Company

How we prevent conflicts of interest

GRI 2-15

Kaspersky has a policy of disclosing the participation of employees and members of governing bodies in other companies as founders, participants, shareholders, or members of governing bodies. Such participation is permitted only if it is transparently disclosed and with the prior consent of the Board of Directors or Management Board.

Joint participation in the governing bodies or capital of other organizations without appropriate approval is considered an unacceptable conflict of interest and is prohibited by the corporate documents of the Company.

During the reporting period, there were no cases where members of the Company's highest governing bodies participated in other organizations without the consent of the Board of Directors or the Management Board.

Safeguarding users' trust

Kaspersky creates an environment in which users, customers, and partners can be confident in the security and reliability of the products and services provided by the Company.

Customer service

The trust of users and customers is the foundation of Kaspersky's long-term growth. The Company organizes all processes to ensure that interaction with the Company is convenient and clear at every stage: from choosing and using a product to communicating with customer support and getting a response. Our approach is based on respect for our clients, attention to their needs, and our desire to respond quickly and correctly in every situation.

Interaction with consumers

To effectively interact with consumers, clients, and suppliers, Kaspersky has a feedback form on the Company's official websites:

www.kaspersky.ru/about/contact — for Russian-speaking users

www.kaspersky.com/about/contact — for international users

For different types of inquiries—including product purchase questions, technical support, and partnership requests—dedicated channels and specialized teams are in place. This approach enables prompt handling of each case and ensures the most appropriate solution is provided.

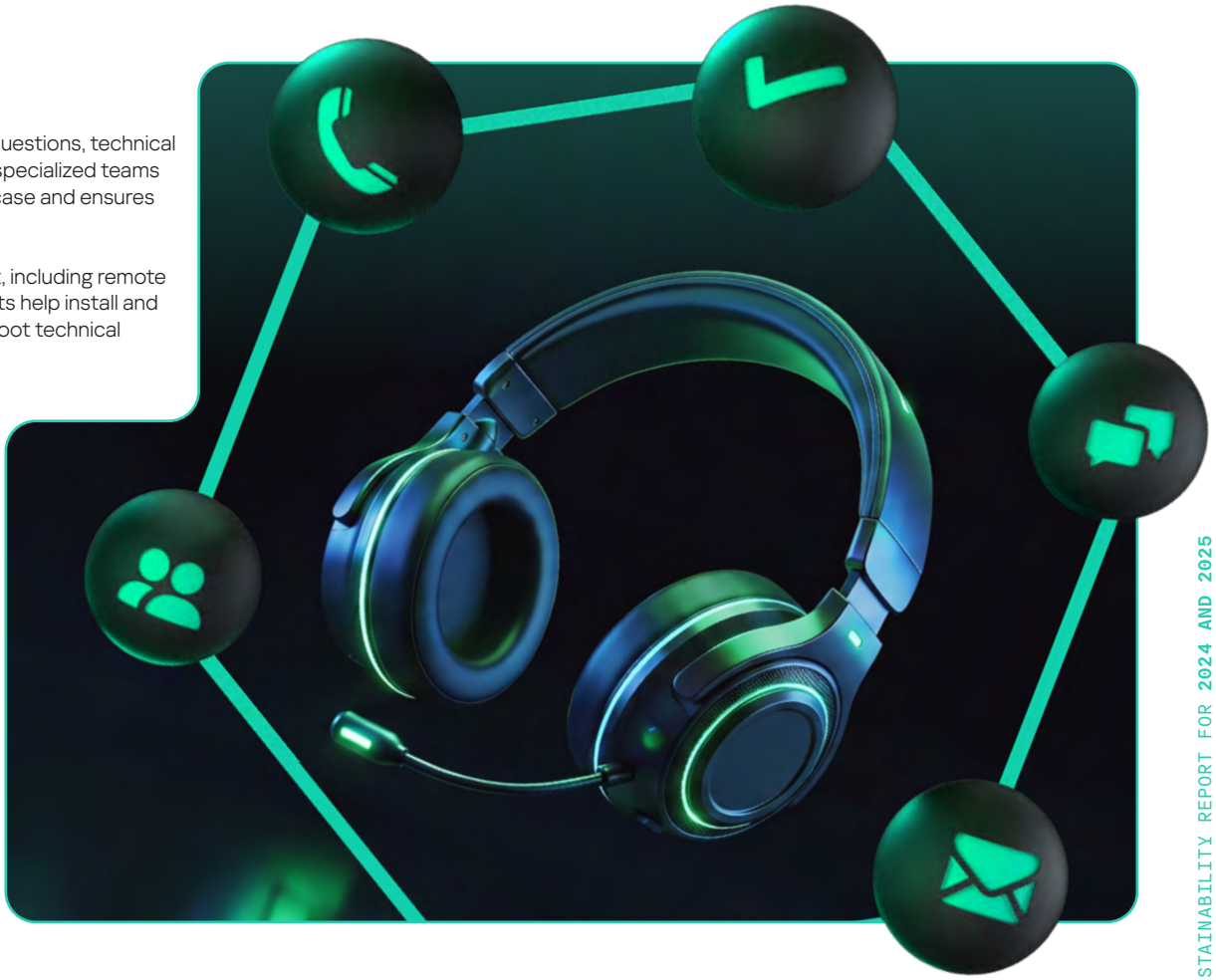
The Company's clients have access to 24/7 technical support, including remote assistance for users of our consumer products. Our specialists help install and configure solutions, scan systems for malware, and troubleshoot technical issues, ensuring stable and uninterrupted protection.

Handling complaints

GRI 2-25

If a client has questions, complaints, or suggestions, they can contact us using the form on the website, by email, phone, or other available channels. All communications are recorded and tracked, allowing us not only to respond promptly to each situation but also to identify recurring issues so they can be addressed systematically rather than on a case-by-case basis.

The team that handles complaints first seeks to understand the nature of the complaint and the reasons for the customer's concern, and then offers a clear, transparent and well-founded solution. The goal of this approach is not simply to formally close support tickets, but to restore trust and rebuild the client's confidence in the quality of the Company's services and products.



Data protection

GRI 3-3

We respect our clients' privacy rights and protect their data. Our goal is to prevent data leaks at Kaspersky and to help our customers combat them with our solutions.

>1.835

user data processing requests in 2024–2025

GRI 418-1

0

user data leaks during the reporting period

Key objectives

- Ensure the protection of customer data worldwide using information security best practices and taking into account local regulations
- Respond promptly to customers' requests regarding the processing and protection of their data
- Prevent unauthorized access to and leaks of user data

Data protection priorities in 2024–2025:

- Implement updated information security requirements in the Company's services
- Protect against supply chain threats
- Use AI to protect the Company's services
- Expand protection of critical services against DDoS attacks
- Launch a new bug bounty program[1]

Our approach to data protection

SASB TC-SI-230-a.2

Kaspersky is committed to protecting the data of its customers worldwide. In today's world, data is a valuable asset for companies, so data security and integrity are of paramount importance. We protect our customers' personal information[2] from unauthorized access and modification using best-in-class technologies and a comprehensive set of technical and organizational security measures.

The Company continuously monitors changes in legislation regarding the processing and protection of personal data in various jurisdictions and implements special projects aimed at bringing processes and systems into compliance with current requirements.

Most countries around the world use a risk-based approach when developing measures to protect personal data. However, in several states, a list of mandatory personal data protection measures is clearly established. The specified requirements are formalized and applied to the Company's services. In particular, these include the following technical measures:

- restriction of access to data;
- timely installation of updates and security patches;
- antivirus protection;
- registration and monitoring of events;
- network protection;
- data encryption;
- fault tolerance and backup copies.

We also implement organizational measures to protect data, including:

- limiting the amount of personal data collected;
- data anonymization;
- development of secure products and prompt elimination of identified vulnerabilities;
- use of digital certificates;
- separate storage of data on multiple servers.

How we protect data globally and prevent data leaks

SASB TC-SI-220a.1

We adhere to the key data processing principles set out in the European Data Protection Regulation (2016). This legislative act sets forth fundamental technical and organizational measures that are also recognized as standards in other jurisdictions. We also comply with international information security standard ISO/IEC 27001 as well as the privacy laws of various countries, including the PIPL, CCPA, LGPD, PDPD, Federal Law No. 152-FZ, and others.

Personal data is stored no longer than is necessary to achieve the purposes of processing that data, or for the periods established by applicable law. Up-to-date information on the countries where data is processing, data access procedures, and data storage periods is available in the current version of the Company's privacy policy.

[1] A program for reporting software bugs and vulnerabilities, typically announced by developers of applications and online platforms to identify security issues in their products. Typically, the program rewards enthusiasts for reporting exploitable bugs. The incentive may sometimes include access to a paid online service or recognition in the professional community.

[2] Personal data is any information related to an individual, including their full name, telephone numbers, physical address, IP address, email address, etc.

Five key principles of working with customer data:

- Ensure that data subjects' data is processed lawfully and transparently
- Ensure that data is processed for legitimate purposes
- Do not collect excessive data
- Comply with data retention time limits
- Ensure reliable data protection

We strive to prevent all information security incidents. During the reporting period, no violations of personal data legislation and no data leaks were recorded. These results were achieved through our systematic efforts to train employees, implement state-of-the-art information security technologies, and standardize data processing.

During the reporting period, we updated our data processing requirements and adapted them to the laws of various jurisdictions.

Up-to-date information, including the number of granted user requests, is provided in our Transparency Report. This document is publicly available, regularly updated and published every six months.

We teach rules for working with data

Kaspersky has an information security awareness program for employees who work directly with customer data. As of 2025, the program covers all current employees of the Company.

The training combines online and offline activities and aims to develop consistently safe behavior. As part of the program, employees learn the rules for working with personal data and trade secrets, the basics of safely using artificial intelligence services, and also undergo practical training on how to recognize and respond to phishing and fraudulent attacks.

Starting in 2025, the program also extends to new outsourcers and contractors that have access to Kaspersky information systems, ensuring a unified approach to information security across all participants in work processes.

We assess risks

We take a risk-based approach to protecting our users' data. Risk assessment is carried out at all key stages of work—when new systems are deployed, when solutions are developed, and during incident investigations. In each case, we first analyze the potential risks associated with processing customer data and then take measures to minimize those risks.

The requirements of the GDPR and regional legislation are based on an assessment of the risks that users may be exposed to. By using international standard ISO/IEC 27001, we further reduce reputational and financial risks for the Company.

We prevent customer data leaks

GRI 418-1 | SASB TC-SI-220-a.1 | SASB TC-SI-230-a.1 | SASB TC-SI-220-a.3

The Privacy Team is responsible for compliance with data security principles and procedures within the Company.

As part of complying with GDPR requirements, the Company established and operates a Privacy Team, which includes employees from the IT, R&D, Information Security, and Intellectual Property departments. In 2016, the Privacy Team brought all data processing into compliance with European regulations. Today, it provides data processing functions in areas such as consulting, organizational issues, and control.

Kaspersky regularly demonstrates the reliability and integrity of its engineering practices through independent audits. In 2025, Kaspersky reinforced its security credentials by re-certifying its information security management system (ISMS) against ISO/IEC 27001:2022, an international standard which outlines the best practices for establishing, implementing and continuously improving these systems. During the reporting period, the scope of information systems audits expanded significantly: ISO/IEC 27001 and SOC 2 Type 2 audits were conducted on a regular basis, and in 2025, an additional external audit was conducted for compliance with the requirements of the Cybersecurity Regulatory Framework (CRF) of the Kingdom of Saudi Arabia.

The certification covers Kaspersky's data processing for "Delivery of malicious and suspicious files and static activity data using Kaspersky Security Network (KSN) infrastructure, and their secure storage and access in the Kaspersky Distributed File System (KLDFS) and to the KSNBuffer database."

The certification applies to data processing services hosted in data centers located in Zurich, Frankfurt am Main, Glattburg, Toronto, Moscow, and Beijing.

0
serious violations of personal data laws and 0 significant leaks

0
losses resulting from litigation due to privacy breaches during the reporting period

46
internal information security audits were conducted in 2024–2025

We are developing a record-keeping system for data processing procedures

We continue to develop our record-keeping system for data processing procedures and services, which the Kaspersky development team created in 2023. The system makes it possible to track which services process customer data, which business processes use it, who acts as the data controller (operator) and data processor, what data is stored, on what legal grounds, in what volume, and for how long, and which countries the data is processed in.

During the reporting period, we updated personal data processing requirements, communicated them to services, and monitored compliance with these requirements.

Our plans for 2026

- Monitor changes in personal data legislation in various countries and align our processes with current requirements.
- Establish updated data processing and data protection requirements for all services that process customer data, and monitor compliance with these requirements.
- Consult with teams regarding updated requirements and data handling practices.
- Audit the effectiveness of services in relation to the processing and protection of user data.

Protection of intellectual property

We constantly develop and implement advanced cybersecurity solutions, and regularly patent our inventions and innovative technologies.

How we protect and defend intellectual property

One of the most important components of the growth and stability of our business is our intellectual property rights. We protect our innovations and also respect other companies' rights to their technologies and solutions.

Task

Protect and defend rights to products, solutions, and technologies

Solutions

We obtain patents in various jurisdictions

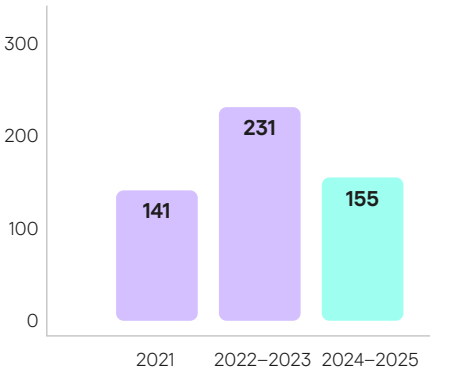
SASB TC-SI-520-a.1

Kaspersky consistently obtains state-protected exclusive rights to the results of its intellectual activity. If a violation occurs, we are prepared to defend our rights in court. This helps uphold the principles of fairness and legality in the business environment.

Between 2024 and 2025, the Company received 155 patents for its technologies in various jurisdictions. In recent years, the focus of patenting has shifted towards B2B products and KasperskyOS, and covers, among other things, machine learning technologies and the use of large language models (LLM) to solve information security problems. Additionally, during the reporting period, we increased the number of patent applications related to the design of our products, including user interfaces.

The protection and defense of intellectual property (IP) has been an integral part of Kaspersky's activities since 2005. In this time, we have established and optimized processes for obtaining legal protection for any results of intellectual activity. In a significant achievement, the Company has not lost any patent lawsuits brought against us by patent trolls[1].

Number of patents received for Kaspersky products



Kaspersky received

155

patents for its technologies in 2024–2025

[1] An individual or entity whose business consists solely of receiving royalties for the use of its patents, without attempting to put the patented inventions into practice.

Along with protecting our own innovations, we devote significant attention to preventing risks associated with the unauthorized use of third-party IP within the Company. This also applies to the use of third-party software code. Accordingly, we implement corresponding policies, thoroughly check licenses, and monitor compliance with all applicable requirements and regulations.

If necessary, we are always prepared to defend our rights in court. This is one of our key strategic positions. We protect our IP using all available legal mechanisms, without resorting to unreasonable settlement schemes. Our goal is a fair and legal dispute resolution that accounts for the interests of all parties.

For example, in April 2024, we concluded a two-year patent dispute in the United States with our direct competitor, the antivirus company Webroot. The dispute was settled on terms that were acceptable to both parties, which allowed us to avoid potential negative scenarios had the dispute continued.

We cultivate an intellectual property culture

Our accumulated experience and expertise allow us not only to effectively protect and defend our own innovations but also to cultivate an intellectual property culture within the Company.

An important part of this work is keeping employees trained and informed. Every new Kaspersky employee undergoes a special introductory training course that gives them a basic understanding of the principles of intellectual property and rules for working with it.

In January 2025, we also launched a specialized course on patents for employees in our technical departments. It helps employees understand the basics of patenting and how intellectual property protects innovations and promotes business growth. During the course, employees involved in new product development not only gain basic knowledge of patent law but also learn information about the Company's internal procedures related to intellectual property protection.

During the reporting period, our internal platform published significantly more content dedicated not only to patenting, but also to other objects of intellectual property.

In addition, we place strong emphasis on supporting employees who are pursuing higher education and wish to use Kaspersky's intellectual property in their academic research. Each of these employees receives the necessary expert support to carry out research initiatives while protecting critical information.

Our plans for 2026

- Expansion of the geographical scope of patent protection to additional jurisdictions, along with an increase in the total number of patent applications filed.
- Monitor changes in the legal landscape to promptly review local IP regulations and develop new documents to address current issues.
- Development of employee training and awareness programs, including the creation of resources and guidelines on intellectual property for employees who are students at higher education institutions. This will help ensure compliance with the Company's rules and policies.
- Increase the level of automation of internal processes related to intellectual property.

We maintain a high level of internal efficiency

As the range of tasks related to intellectual property expands each year, it becomes especially important to increase efficiency of processes and automate them. Several relevant initiatives were implemented in 2024–2025.

1 We continue to develop an automated system for analyzing software and other objects with open-source and free licenses. During the reporting period, we designed and implemented a separate module that efficiently identifies licensing terms and generates copyright information for open-source software used in the Company's products. This has significantly accelerated the legal review of our products and services and ensured compliance with global best practices for working with open-source software.

2 We revised the process for publishing open-source projects that give the developer community access to our technologies. We created well-structured and clear guidelines for development teams, which reduced the likelihood of errors when publishing code and also reduced excessive communication with the department responsible for intellectual property issues.

3 During the reporting period, we deployed an LLM assistant that helps speed up the analysis of patents from foreign jurisdictions and optimizes work in this area.

Global Transparency Initiative

Our goal is to provide the necessary tools and conditions for our corporate clients, partners, and regulators to verify the integrity and reliability of our products.

Proven.
Transparent.
Independent.

What is the Global Transparency Initiative?

The Global Transparency Initiative (GTI) is a system of measures aimed at increasing the transparency and reliability of Kaspersky's products, development processes, and business processes. GTI provides customers, partners, and regulators with access to information about product architecture, data management, and security procedures, including the ability to review source code at dedicated transparency centers. External experts provide feedback that helps us improve processes and ensure that our solutions maintain a high level of maturity.

How the GTI came to be and how it has evolved

The Global Transparency Initiative was launched in 2018 in response to requests from regulators and customers seeking greater insight into how our products work, including how data is processed and stored. Today, GTI is a comprehensive system that combines independent audits, source code analysis, educational initiatives, and the development of data processing infrastructure.

As part of the GTI, the Company:

- introduced independent analysis of source code, updates, and threat detection rules;
- introduced independent assessment of secure development and risk management in the supply chain;
- introduced independent assessment of secure development and risk management in the supply chain;
- improved the bug bounty program;
- moved part of the infrastructure for storing and processing suspicious files to data centers in Switzerland;
- began publishing reports on requests from law enforcement agencies and government agencies;
- developed programs to enhance competencies in IT infrastructure security, such as the Cyber Capacity Building Program.

In 2025, Kaspersky celebrated the seventh anniversary of the Global Transparency Initiative. Over its lifetime, the GTI has evolved into a full-fledged transparency system.

Seven years of results from the GTI

>$9.4 million
invested in the GTI's development over 7 years

2
data centers in Zurich

13
transparency centers around the world

67
visits to transparency centers

$97,770
paid for 77 bug reports as part of our bug bounty program

How does the GTI work?

Basic elements of the GTI

1. Source code access for clients and regulators

An important element of the system is independent verification of the source code of Kaspersky products. In addition, several stakeholders can receive information about the source code of the Company's main products and our data processing principles.

2. Cooperation with the expert community

We invite independent experts from around the world to test our systems and products, which creates even more confidence in their reliability.

3. Educational activities

The Company's educational initiatives under the GTI aim to raise awareness among users and partners about the importance of security in the digital world.

How we ensure that our products and business processes are transparent

13
transparency centers
around the world

Task

Strengthen public trust in the Company's products and activities

To build trust with our clients, partners, and regulators, we continually grow the GTI's infrastructure, disclose information about our processes, undergo audits, obtain certifications, and improve security standards.

2
independent SOC 2 and ISO 27001 compliance audits

We launched a GTI course for partners.

Key solutions

We are expanding our data processing infrastructure

In 2018, Kaspersky began moving the processing and storage of suspicious and malicious files to two data centers in Switzerland that operate under strict data protection regulations. As a result, data voluntarily shared by users from Europe, North and Latin America, the Middle East, as well as several countries in the Asia-Pacific region is now processed in Zurich within the Kaspersky Security Network cloud system.

We are expanding the network of transparency centers

Transparency centers allow our corporate clients, partners, and government regulators responsible for cybersecurity to examine the source code of the Company's products and learn more about its internal processes. The first center was opened in Zurich in 2018. In just seven years, we established 13 transparency centers in Brazil, Italy, Japan, Malaysia, the Netherlands, Rwanda, Saudi Arabia, Singapore, Spain, Switzerland, Turkey, Colombia and South Korea. Three of them were opened in 2024–2025.

The GTI's results for 2024–2025

3
new transparency centers were opened in Istanbul, Bogota and Seoul

7
The Company's products were reviewed 7 times at transparency centers

>$15.000
paid for 18 bug reports as part of our bug bounty program

We are assessed independently

Kaspersky regularly obtains independent assessments and proves that its internal processes are secure. Since 2019, the Company's data management systems have been certified as compliant with the ISO/IEC 27001:2022 standard and passed SOC 2 audits. In 2025, Kaspersky's information security management system was recertified as compliant with the ISO/IEC 27001:2022 standard, which confirms that it is secure.

In 2024 and 2025, the Company again successfully passed a SOC 2 Type 2 audit. The audit demonstrated that Kaspersky's internal controls, which ensure regular automatic updates of anti-virus databases, are working effectively, and that our process for developing and releasing anti-virus databases is protected from unauthorized interference.

In 2024 and 2025, we successfully passed two SOC 2 Type 2 audits.

We collect data on vulnerabilities through a bug bounty program.

Since March 2018, Kaspersky has received 77 reports of minor vulnerabilities through our bug bounty program, fixed them and, as of today, paid out bounties totaling $97.770 to independent researchers. The maximum reward for critical vulnerabilities is $100.000.

Since 2022, the Company has been running its public bug bounty program on the Yogosha platform. We also support Disclose.io, which provides a safe space for vulnerability researchers concerned about the potential legal repercussions of their disclosures.

77

bug reports received in 7 years

$97,770

paid for bug reports

We teach how to assess the cybersecurity level

Our educational Cyber Capacity Building Program helps employees of private and public companies, as well as universities, develop skills in assessing the security level of IT infrastructure. As part of the program, our specialists provide recommendations on code auditing, creating procedures for handling vulnerabilities, and code fuzzing techniques[1].

During the reporting period, representatives of several organizations, including the National Cyber Security Agency of Thailand and Boğaziçi University (Istanbul), completed the training.

In 2025, our Cyber Capacity Building Program was selected by the World Internet Conference (WIC) as an one of the Outstanding Cases of Jointly Building a Community with a Shared Future in Cyberspace.

We publish transparency reports

Our mission is to protect users from cyberthreats, which is why we support our partners, international organizations, and law enforcement agencies in the fight against cybercrime. We regularly process requests and, since 2020 we have published reports featuring information about the number of such requests by country, as well as how many we granted and rejected. Accordingly, the Company has a procedure for processing these requests, including, in particular, clear criteria for verifying their legality.

Every six months, Kaspersky discloses the number of law enforcement and government requests for user data, expertise, and threat intelligence data. However, we do not provide any third parties[2] with access to the Company's infrastructure, including the data processing infrastructure. We also regularly report on requests from our own users regarding their personal data, how we process it, where it is stored, and so on.

1 A software testing method where a program is given deliberately incorrect data, the response is analyzed, and any resulting bugs are detected.

2 Learn more about how we handle requests in our transparency reports.

Our contribution to promoting the ethical and safe use of AI in cybersecurity

Artificial intelligence allows new cyberthreats to be detected and neutralized more effectively, but its use carries risks for privacy, data security, and user rights. In 2024–2025, Kaspersky stepped up its efforts to develop and promote ethical standards for the use of AI in the digital world.

What we did

- We presented the Guidelines for Secure Development and Deployment of AI Systems at the UN Internet Governance Forum (IGF) 2024 in Riyadh. The purpose of the document is to help organizations avoid cyber risks associated with the use of AI technologies.
- We signed the European Commission's Artificial Intelligence Pact (AI Pact), confirming that we are prepared to build an AI governance strategy that is aligned with the logic of the future EU AI Act[1].
- We joined the Global Alliance on AI for Industry and Manufacturing, established in 2023 by the United Nations Industrial Development Organization (UNIDO), and the AI Alliance Russia (a-ai.ru), which unites leading Russian technology companies for the purpose of responsible AI development.
- We formulated clear relevant guidelines for stakeholders: from threat modeling and risk assessment to protection against AI attacks and compliance with international regulations, such as the GDPR.
- We committed to adopting an internal AI governance strategy and raising awareness among employees and others about interactions with AI.
- We reaffirmed our principles for the responsible use of AI in cybersecurity: transparency, safety, human control, the right to digital privacy, a commitment to cybersecurity objectives, and openness to dialogue.

Our achievements

- We strengthened Kaspersky's role as a leader in setting global standards for ethical AI in cybersecurity.
- We became an active participant in the pan-European discussion on AI regulation and prepared the Company to comply with the EU AI Act.
- We communicated to partners, clients, regulators, and the professional community how we ensure the reliability and security of AI systems and invited them to develop shared ethical principles for digital development.

GTI plans for 2026–2027

- Possibly expand the network of transparency centers (APAC)
- Diversify data centers, expand infrastructure for processing malicious and suspicious files
- Continue to invite stakeholders to transparency centers
- Recertify compliance with key standards
- Continue to publish reports on data requests

[1] The EU AI Act comes into force in mid-2026. This is a European Commission initiative aimed at creating a common regulatory framework for the use of AI.

Sustainable supply chain

Kaspersky's procurement activities are based on the principles of transparency, fair competition, and equal conditions for all potential counterparties.

All companies interested in cooperating with us receive equal access to participate in competitive procedures.

How we organize procurement

Procurement processes are governed by Kaspersky's internal documents, including our procurement policy and contract policy. In 2025, an updated procurement policy was adopted, aimed at making the procurement function more efficient and manageable. Key goals of the update included:

- simplify procedures — introduce clearer and more detailed rules, and simplify the procedure used for more than 20% of the total volume of purchases
- reduce key risks — strengthen control mechanisms and introduce annual planning
- increase employee awareness — develop training materials and workshops, and reduce the number of exceptions to standard procedures

The Company places particular emphasis on compliance with established rules both within the organization and among its suppliers. Sustainable procurement principles are communicated to counterparties through tender documents and contracts.

As part of the digitalization of its procurement function, Kaspersky is deploying an IT solution for procurement management that was developed by a Russian vendor.

The Company's procurement process is based on categories. Purchases are categorized according to similarities in technical and functional characteristics, areas of application, and business areas (marketing, professional services, IT, production costs, etc.). To ensure that procurement is managed effectively, thresholds have been established based on the cumulative annual procurement volume by category:

- purchases of up to $25.000 are carried out using a simplified procedure involving at least two competitive proposals
- purchases in the range from $25.000 to $100.000 require a minimum of three proposals or two proposals from trusted suppliers that were selected through tenders and have a successful track record of working with the Company
- purchases over $100.000 are carried out through a tender involving the procurement department, tender committee, and cross-functional teams

Depending on the budget, tender procedures also include additional levels of management. For example, Kaspersky's business director is involved in the procurement process for purchases worth around $1 million.

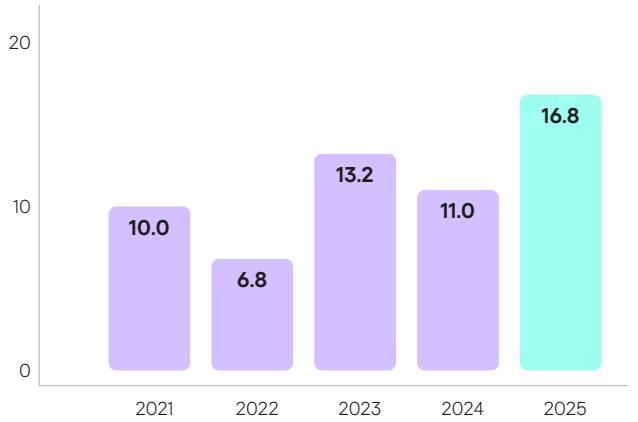
Before a partner is invited to participate in a tender, our security service scrutinizes it. Kaspersky cooperates only with counterparties with proven experience and a good business reputation: 99% of our suppliers have been operating in the market for at least three years. All contracts contain an anti-corruption clause.

GRI 2-6

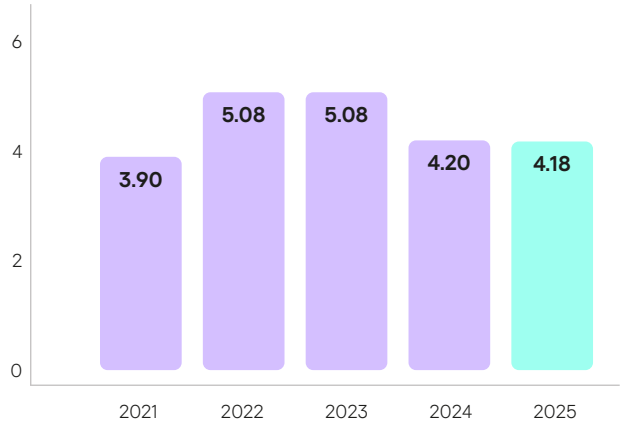
Purchases are made both directly from manufacturers (vendors) and through distributors and partner networks, depending on the supplier's business model and the specifics of the region.

In 2025, the Company will maintain approximately the same number of suppliers as in previous years. Cost savings achieved through competitive bidding procedures and cost optimization have stabilized, averaging around 7% of the total procurement spend covered by the procurement function.

The Company's savings resulting from tenders and cost reduction in the procurement of goods and services, $ million[1]



Number of the Company's suppliers at the end of the reporting period, in thousands



GRI 204-1

In 2024 and 2025, Russian suppliers accounted for about 50% of our total purchase volume. Additionally, the share of purchases from small and medium-sized businesses amounted to approximately 80% of the total purchase volume.

Plans for 2026

In 2026, we plan to further develop the procurement function as a business partner: procurement's active participation in planning and budgeting processes, as well as joint development and implementation of a procurement project roadmap with business units.

7%

Cost savings achieved through competitive bidding procedures and cost optimization have stabilized, averaging around 7% of the total procurement spend covered by the procurement function.

In 2024–2025, the Company worked with

>4,000 suppliers

[1] Excluding third-party costs.

Risk management

Our Company has implemented and consistently develops a proactive risk management system focused on responding promptly to internal and external challenges.

Kaspersky not only strives to minimize the consequences of risks, but also seeks to prevent them materialising at an early stage.

When developing our risk management principles, we accounted for the requirements of the legislation of the Russian Federation, the regulations of the Central Bank of the Russian Federation, as well as international risk management practices. In developing the system, we focus on state-of-the-art approaches and the best industry standards related to risk management.

Development of our risk management system

In 2024–2025, Kaspersky actively developed a risk management system (RMS) based on the Global Problem Management (GPM) process, which was created from the outset to manage technological risks. New business units and subsidiaries were involved in the process, and user-friendly dashboards were developed for routine monitoring of risks and incidents.

Goals and tasks of risk management

Operational risk management seeks to promptly identify risks and mitigate their impact, to ensure that the Company can operate and grow sustainably, and to maintain the high quality of its products and services amid a highly turbulent external environment.

As part of the GPM process, the Company manages technological risks by promptly identifying them and continuously working to mitigate them. This approach helps prevent incidents related to the quality of products and services, as well as the functioning of internal and external IT infrastructure.

Key tasks of risk management:

1. identify risks that could significantly impact the Company or users of its products and services
2. analyze and assess the identified risks
3. develop and implement risk mitigation plans
4. monitor and control both new and previously identified risks, including cases where they cannot be completely eliminated.

Principles of operational risk management

Create a risk-oriented environment

Risk management is an integral part of the Company's activities and is not limited to the functions of a single business unit. The GPM process facilitates risk management both within individual departments and at the intersection of the areas of responsibility of several business units. As the RMS evolves, new functions and teams are involved in the process.

Ensure that the risk management process is continuous and mandatory

Risk management is an ongoing process. Within the business units involved in GPM, staff are assigned to help identify, analyze, and assess risks and develop risk mitigation plans. New risks and incidents are synchronized at least once every two weeks, and the status of active risks is updated at least once per quarter.

Keep managers informed at every level of decision-making

The Company has a communications and reporting system that allows managers at all levels to be promptly informed about the current risk map (active, accepted, and closed risks) associated with decisions they are making. This creates the basis for risk-based decision making.

Ensure openness and uniform assessment methods

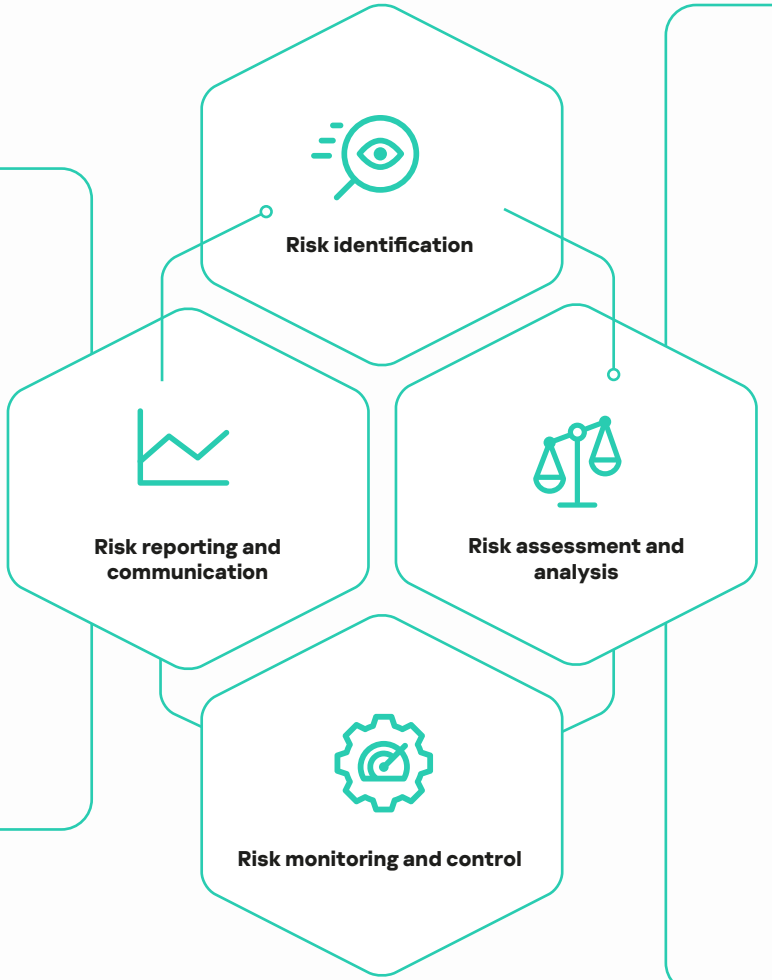
To analyze risks, the Company uses uniform classifications and assessment scales, which are set out in the GPM documentation and used by all participating business units. If disagreements arise or methodological shortcomings are identified, facilitated sessions are held and then the classifiers and assessment methods are refined.

Operational risk management process

Risk reporting and communication

To facilitate objective and effective management decision-making, the Company has implemented a multi-stage risk reporting system. Reports and dashboards reflect risk dynamics: changes in the significance of risks, and statistics on accepted and closed risks, and highlight the most critical risks in the current period.

Kaspersky's CEO receives an annual report on the most significant risks and incidents. Quarterly risk reports are presented to the Management Board. Additionally, the status of risks and incidents is regularly discussed with heads of departments and business units and their employees.



Risk identification (detection) is a multifaceted process that is distributed among various business units of the Company. Risks are identified based on the analysis of past incidents, modeling of potential incidents and analysis of business processes. The identified risks are analyzed and assessed according to developed classification scales that have been coordinated and approved by all departments involved.

Each identified risk is **analyzed and assessed** based on two key parameters: the likelihood it will be realized and the scale of actual or potential damage to the Company and its customers. For each risk, an owner, causes, and possible consequences are determined, a risk mitigation action plan is developed, and responsible persons are assigned.

The Company **monitors** actual and potential losses on a regular basis. All incidents are recorded, a mandatory damage assessment is carried out, and the sources and causes of risks are analyzed in detail.

Risk control in the Company is a continuous process and aims to:

- use risk information when making management decisions
- regularly monitor the status of active risks in accordance with the approved process
- promptly implement effective measures to reduce risks that could affect the Company's activities

ESG risk management

At Kaspersky, senior managers and department heads are responsible for managing sustainable development risks. During the reporting period, the Company identified two significant[1] ESG risks: changes in the political and economic environment across its regions of presence, including regulatory changes, and the risk of increasing cybercrime.

Key ESG risks

SASB TC-SI-550a.2

Risk of changes in the political and economic environment across its regions of presence

Why the risk matters

Potential legislative changes could significantly limit the Company's ability to conduct business in a country/region where it has a presence

Risk management measures in 2024 and 2025

- Continuously monitor legislative changes in the political and economic environment across its regions of presence in order to promptly identify potential risks
- Ensure the Company and individual employees belong to various industry organizations in order to communicate with regulatory authorities
- Participate in public consultations conducted by government authorities in countries/regions where the Company has a presence in relation to draft amendments to existing regulations or the introduction of new regulations in order to promote the Company's position
- Further develop the GTI to allow customers, partners, and regulators to verify the reliability of the Company and its products

Risk of increasing cybercrime

Why the risk matters

Currently, there has been a decline in the level of cooperation between law enforcement agencies and private companies in various countries. To prevent a surge in cybercrime, it is important to maintain cooperation and the exchange of expertise with the private sector.

Risk management measures in 2024 and 2025

The Company continued to actively cooperate with law enforcement agencies and international organizations during the reporting period:

- it contributed to several operations under the auspices of INTERPOL, including Synergia and Synergia II, Serengeti and Serengeti 2.0, Red Card and Secure
- it helped ensure the safety and security of major international sporting events such as the Paris 2024 Summer Olympics and the Formula 1 Singapore Grand Prix 2025
- it shared data for two editions of the INTERPOL African Cyberthreat Assessment Report (2024, 2025), which present the cyber threat and attack landscape on the African continent
- it participated in three meetings of expert working groups under the auspices of INTERPOL, held in Bangkok, Hanoi and Doha, sharing expertise in researching cyber threats with representatives of law enforcement agencies, cybersecurity agencies, other government organizations and private companies
- it participated in the formation of feedback and proposals for several documents developed under the auspices of the UN, including the Convention against Cybercrime and the Global Digital Compact
- it signed memorandums of understanding with AFRIPOL and several national cybersecurity regulators

Realized risks

SASB TC-SI-220a.5

During the reporting period, the following identified risks were realized amid geopolitical instability:

- termination of cooperation between individual counterparties and Kaspersky
- difficulties with paying for goods and services abroad

On June 20, 2024, the US Department of Commerce announced its decision to prohibit the sales and distribution of Kaspersky software in the United States. Following the release of the Final Determination, Kaspersky has stopped the sales of its cybersecurity products in the country and started to gradually wind down its U.S. operations and eliminate U.S.-based positions. Kaspersky maintains that the Department of Commerce made its decision based on the present geopolitical climate rather than on a comprehensive evaluation of the integrity of Kaspersky's products and services. The ban didn't cover Kaspersky's informational or educational products and services such as Kaspersky Threat Intelligence[2] and Kaspersky Cybersecurity Training, as well as Kaspersky consulting or advisory services (including SOC Consulting, Security Consulting, Ask the Analyst, and Incident Response), which continue to be available in the U.S. market.

Plans for 2026

In 2026, Kaspersky plans to focus on systematizing and aggregating its accumulated risk database, as well as further optimizing reporting formats and analytical tools.

[1] Significant risks are risks that, in the opinion of the Company's management, may have a material impact on operating results.

[2] Threat intelligence is the collection, analysis, and interpretation of data on existing and potential cyberattacks.

Additional Information

Appendix 1. About the report

GRI 2-1, GRI 2-2, GRI 2-3

In this report, Kaspersky discloses information in accordance with the requirements set forth by the following international sustainable development standards:

- Global Reporting Initiative Standards (GRI 2021)
- Industry-specific Standards of the Sustainability Accounting Standards Board (SASB Standards) for Software & IT Services

We present how the disclosed information complies with these standards in the GRI Standards Compliance Index and SASB Standards Compliance Index sections.

Unless otherwise stated, the information presented in this report covers the activities of AO Kaspersky Lab and other Kaspersky offices in countries of presence (regional offices).

The report covers the period from January 1, 2024 to December 31, 2025.

Kaspersky's forward-looking statements and plans in this report are tentative in nature. They may change under the influence of external and internal factors that could not be fully accounted for at the time the report was prepared. Accordingly, in subsequent reporting periods the results of sustainable development activities may differ from those presented in this report.

The report is available on the Kaspersky website in Russian and English.

Appendix 2. Determining material topics

GRI 3-1, GRI 3-2

To ensure that the content of our report best meets our stakeholders' interests and expectations, we conducted an online stakeholder survey to determine material topics for the document. The survey was conducted from October 9 to November 10, 2025, in Russian and English.

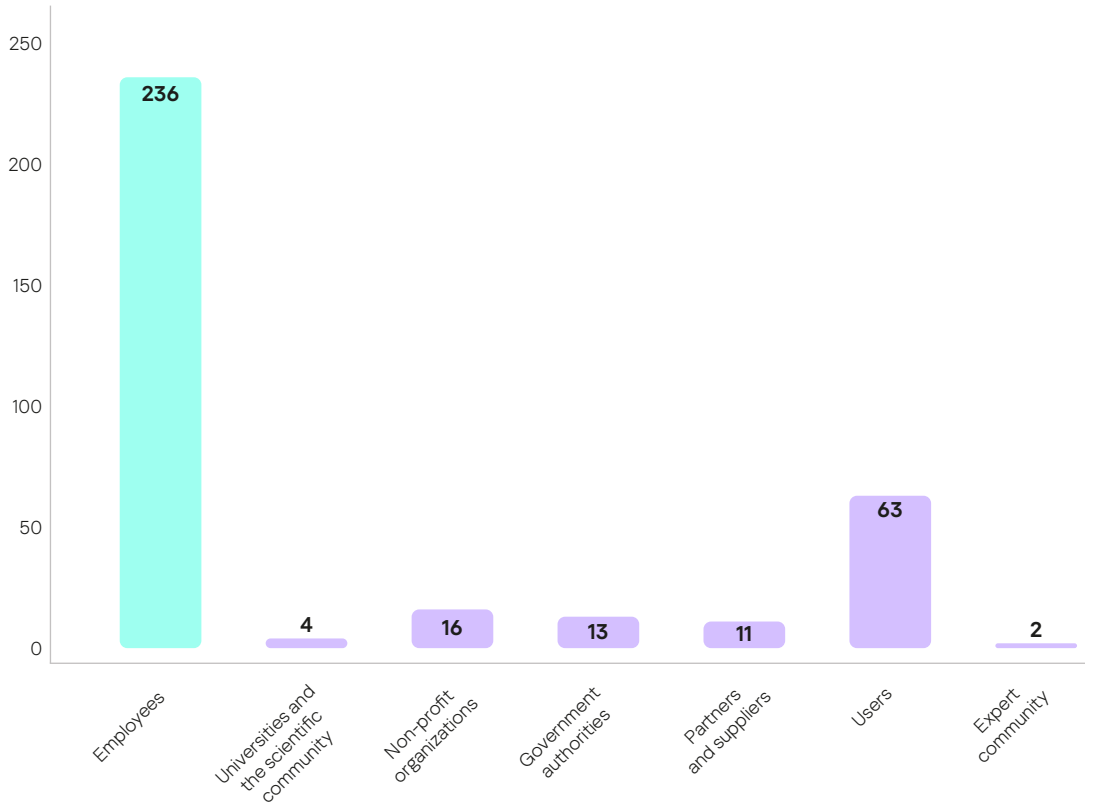
We compiled an initial list of report topics for stakeholders to rate based on the priority topic list generated by the previous reporting period's determination of material topics. An internal group of Kaspersky experts clarified the wording of three of the topics. It also augmented the lists of aspects reflected by each topic.

The list included 17 topics that reflect Kaspersky's impact on the economy, environment and society. Survey respondents were able to rate the importance of each suggested topic on a scale from 1 to 5, with 1 being least important and 5 being most important. The questionnaire also provided an opportunity to leave free-form comments: stakeholders could both comment on the suggested topics and propose new topics of their own. 345 stakeholders participated in the survey: 236 internal and 109 external stakeholders.

We adjusted the results using weighting factors to give equal weight to the opinions of each stakeholder group. Then, based on the averaged ratings received from stakeholders, we created a final list of topics in order of decreasing importance. Eight topics that received a total score of 4 points or more were considered material enough to include in the report. This allowed us to equally consider the opinions of both the internal and external stakeholders who participated in the survey.

Wording in the 2023 questionnaire	Wording in the 2025 questionnaire
Protecting users and user data	Data protection
Information security education	Digital awareness
Inclusive digital environment	Inclusion

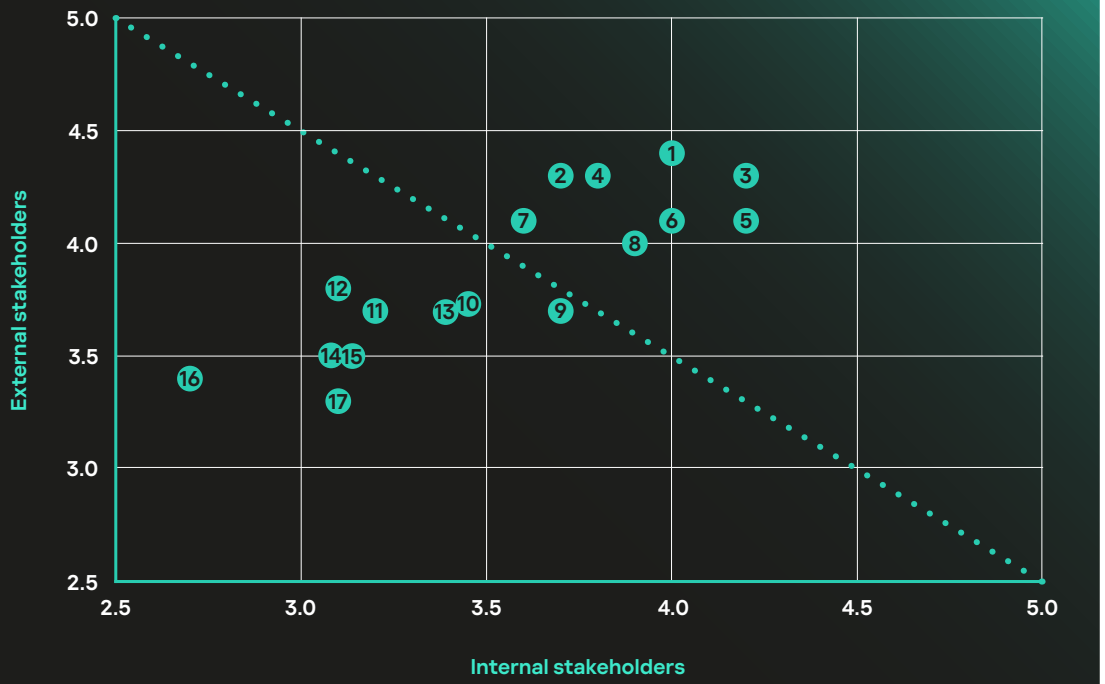
Survey participants by stakeholder category, number of people



List of material topics for Kaspersky's Sustainability Report for 2024-2025

Topic	Materiality score	Page
Data protection	4.3	108
Safe digital environment	4.2	44
Combating international cybercrime	4.2	25
Training personnel for the IT industry	4.2	81
Responsibility to employees	4.1	56
Ensuring software and digital resilience in a changing world	4.1	48
Digital awareness	4.1	86
Contribution to technology development	4.0	23

Materiality assessment by external and internal stakeholders



Number	Topic
1	Data protection
2	Safe digital environment
3	Combating international cybercrime
4	Training personnel for the IT industry
5	Responsibility to employees
6	Ensuring software and digital resilience in a changing world
7	Digital awareness
8	Contribution to technology development
9	Transparency in business and corporate governance
10	Business ethics
11	Sustainable supply chain
12	Inclusion

Number	Topic
13	Information and technological openness
14	Social projects, charity and volunteering
15	Women in STEM
16	Reducing climate and environmental footprint
17	Taxation

Appendix 3. Memberships in associations and unions

GRI 2-28

Kaspersky collaborates and participates in joint initiatives with the following organizations:

- INTERPOL
- AFRIPOL
- Working jointly with Europol for more than 9 years, the No More Ransom alliance has helped more than 6 million users recover their data without paying ransom
- Coalition Against Stalkerware
- Geneva Dialogue
- Paris Call for Trust and Security in Cyberspace
- Council of Europe
- World Internet Conference (member of the High-Level Expert Advisory Committee)
- International Telecommunication Union (ITU)
- International Organization for Standardization (ISO)
- Smart Africa Alliance

Appendix 4. To the "People at Kaspersky" section

Average number of Kaspersky employees by gender

2023[1]			2024			2025		
F	M	Total	F	M	Total	F	M	Total
1,301	3,727	5,028	1,290	3,794	5,084	1,329	4,025	5,354

Total number of employees by contract type and gender

GRI 2-7

2023				2024				2025			
Permanent		Temporary		Permanent		Temporary		Permanent		Temporary	
F	M	F	M	F	M	F	M	F	M	F	M
1,257	3,770	45	47	1,254	3,748	34	43	1,352	4,186	39	55

Total number of employees by employment type and gender

GRI 2-7

2023				2024				2025			
Full-time		Part-time		Full-time		Part-time		Full-time		Part-time	
F	M	F	M	F	M	F	M	F	M	F	M
1,265	3,796	37	21	1,253	3,764	35	27	1,365	4,215	26	26

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Total number of employees by age group

GRI 2–7

Employee age	2023		2024		2025	
	people	%	people	%	people	%
Under 30	1,161	23	1,100	22	1,298	23
30–50	3,635	71	3,617	71	3,926	70
50 and over	326	6	370	7	423	7

Total number of employees by region[1]

GRI 2–7

Region	2023	2024	2025
APAC	227	225	233
Latin America	134	144	176
Middle East, Turkey and Africa	135	166	187
Europe	341	283	235
CIS	4,250	4,290	4,858
■ including Russia	4,221	4,261	4,827

[1] From here on, regions with less than 1% of the total number of employees are excluded from the regional breakdowns, because the small base means this data is not representative.

Staff structure by employee function

GRI 405-1

Employee age	2023[1]		2024		2025		Change from 2024 to 2025, %
	people	%	people	%	people	%	
Managers	846	16	869	17	958	17	10
■ men	627	75	632	73	707	74	12
■ women	211	25	232	27	246	26	6
■ under 30	45	5	42	5	43	5	2
■ 30–50	698	83	717	83	789	83	10
■ over 50	96	11	105	12	117	12	11
Technical specialists	2,696	52	2,704	53	3,051	54	13
■ men	2,233	83	2,250	84	2,552	84	13
■ women	447	17	443	16	487	16	10
■ under 30	786	30	752	28	914	31	22
■ 30–50	1742	66	1,772	67	1,919	65	8
■ over 50	95	4	116	4	140	5	21
Other specialists	1,610	31	1,539	30	1,682	30	9
■ men	941	60	897	60	980	60	9
■ women	638	40	607	40	654	40	8
■ under 30	292	19	271	18	314	19	16
■ 30–50	1,140	73	1,068	72	1,148	71	7
■ over 50	134	9	145	10	158	10	9

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Number of employees hired

GRI 401-1

2023	2024	2025	Change from 2024 to 2025, %
944	563	961	71

Hired employees by age group

Employee age	2023[1]		2024		2025		Change from 2024 to 2025, %
	people	%	people	%	people	%	
Under 30	312	38	201	37	408	44	103
30–50	486	58	313	58	502	53	60
50 and over	34	4	27	5	28	3	8

Hired employees by gender

Employee gender	2023[1]		2024		2025		Change from 2024 to 2025, %
	people	%	people	%	people	%	
Men	703	76	390	71	732	77	86
Women	222	24	158	29	213	23	36

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Number of employees hired by region

Region	2023	2024	2025
APAC	33	39	53
Latin America	39	24	42
Middle East, Turkey and Africa	50	47	53
Europe	41	16	16
CIS	778	436	796
■ including Russia	769	432	790

Number of outgoing employees

Metric	2023[1]	2024	2025	Change from 2024 to 2025, %
Outgoing employees	779	750	533	–30

Outgoing workers by age group

Employee age	2023[1]		2024		2025		Change from 2024 to 2025, %
	people	%	people	%	people	%	
Under 30	246	32	173	24	131	26	–24
30–50	470	62	483	67	324	64	–33
50 and over	48	6	64	9	54	11	–16

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Outgoing employees by gender

Employee gender	2023[1]		2024		2025		Change from 2024 to 2025, %
	people	%	people	%	people	%	
Men	521	67	519	70	361	68	–30
Women	253	33	220	30	168	32	–24

Number of outgoing employees by region

Region	2023[1]	2024	2025
APAC	30	49	40
Latin America	13	16	16
Middle East, Turkey and Africa	20	19	36
Europe	54	78	57
CIS	655	527	382
■ including Russia	648	523	378

Staff turnover by gender and age group

GRI 401-1

Metric	2023	2024	2025	Change from 2024 to 2025, %
Overall turnover	15	15	10	–32
■ Male turnover	14	14	9	–38
■ Female turnover	20	17	12	–29
■ Turnover among employees under 30	22	16	10	–37
■ Turnover among employees aged 30 to 50	13	14	8	–38
■ Turnover among employees over 50	15	17	13	–26

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Staff turnover by region

Region	2023	2024	2025
APAC	13	21	17
Latin America	10	11	10
Middle East, Turkey and Africa	16	12	20
Europe	16	24	23
CIS	16	12	8
■ including Russia	16	12	8

Number of employees entitled to parental leave

GRI 401-3

Employee gender	2023		2024		2025		Change 2025/2024, %
	people	%	people	%	people	%	
Women	1,296	25	1,282	25	1,387	25	8
Men	3,801	75	3,779	75	4,239	75	12

Employees who took parental leave

Employee gender	2023		2024		2025		Change 2025/2024, %
	people	%	people	%	people	%	
Women	55	93	44	98	42	95	–5
Men	4	7	1	2	2	5	100

Employees who returned after parental leave

Employee gender	2023[1]		2024		2025		Change 2025/2024, %
	people	%	people	%	people	%	
Women	46	92	32	97	34	97	6
Men	4	8	1	3	1	3	0

Percentage of employees who returned to work

Year	Women	Men
2023[1]	98	100
2024	98	100
2025	100	100

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Employee retention rate, %

Year	Women	Men
2023[1]	73	50
2024	69	100
2025	67	100

Number of employees who completed advanced training and professional development programs

Employee function	2024	2025
Total number of employees who completed advanced training and professional development programs, including:	203	222
■ managers	40	39
■ technical specialists	95	137
■ other specialists	108	85
■ men	129	158
■ women	74	64

[1] The data for 2023 differs from the data provided in the Sustainability Report for the second half of 2022 and 2023 due to the transition to new accounting systems, changes in the employees' personal data and the adjustment of calculation methods not taken into account in the previous report.

Appendix 5. To the "Digital security" section

List of cybersecurity standards against which the KICS for Nodes and KICS for Network solutions, which are part of the KICS platform, are certified, as well as other international laws and industry standards whose requirements they address or help implement:

- ISO/IEC 27001 IEC 27002 (DIN 2008 in Germany) is a standard that establishes requirements for the creation, deployment, maintenance and continuous improvement of an information security management system within an organization;
- ISO/IEC 27019 (DIN 2011 in Germany) is a standard used to ensure information security in the energy sector;
- ISO/IEC 27032 is a standard that addresses internet security issues and provides recommendations for addressing the most common threats in this area (social engineering, zero-day attacks, spyware, etc.);
- ISO/IEC 15408, historically known as the "Common Criteria," represents the accumulated experience of various countries in the development and practical use of criteria for assessing the security of information technology;
- IEC 62443 (ANSI/ISA99) is a series of standards that contains requirements for the design of cybersecurity management systems for industrial control systems and SCADA;
- The NIST CSF is recommendations for ensuring the security of industrial control systems developed by the US National Institute of Standards and Technology (NIST), supported by, among others, ONG-C2M2, API-1164, TSA PSF, and CISA;
- NIST SP 800-82 is the US guide for securing industrial control systems (ICS), covering risk management, access control, incident response, security monitoring, and more;
- NERC CIP is a set of cybersecurity standards for critical infrastructure and power grid protection in the United States, which are also being adopted by some Latin American countries;
- NIS 2 Directive (EU) 2022/2555 is a new EU directive on cybersecurity;
- NIS/NIS2 is the first pan-European directive on cybersecurity, establishing a higher and more uniform level of security for network and information systems in the EU;
- IEC 62351 is standards for the security of power control systems and associated utility systems. It specifies requirements for security, protection measures, and communications networks in the power industry;
- IMO MSC.428(98) is a Maritime Safety Committee resolution that provides guidance on cyber risk management in the maritime industry as part of safety management systems;
- ICAO is a cybersecurity strategy for aviation[1];
- IAEA Nuclear Security Series No. 17-T (Rev. 1) is methods of ensuring computer security for nuclear facilities.

[1] FAA Advisory Circular 119-1 - Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP).

Appendix 6. GRI Standards Compliance Index

In this report, Kaspersky references GRI standards for the period from January 1, 2024 to December 31, 2025.

GRI 1.	Application of GRI 1: Principles 2021
Applicable GRI industry benchmarks	There are no applicable GRI industry benchmarks

Metric	Disclosure	Comment	Report section	Page
General disclosure				
GRI 2-1	Organizational details	The main legal entity in the Russian Federation is the AO Kaspersky Lab. The organization's headquarters are located at: 39A/2 Leningradskoe Shosse, Moscow, 125212, Russian Federation Legal information: https://www.kaspersky.com/legal.		7
GRI 2-2	Entities included in the organization's sustainability reporting		Appendix 1	122
			Appendix 9	145
GRI 2-3	Reporting period, frequency and contact point	Report publication date: June 23, 2026	Appendix 1	122
				145
GRI 2-4	Restatement of information	Some employee data for 2023 was recalculated due to the updating of employees' personal data, the transition to new accounting systems, and the adjustment of calculation methods. In each such instance, a corresponding note is included in the text.		
GRI 2-5	External assurance	The report has not been certified by an external entity.		
GRI 2-6	Activities, value chain and other business relationships		About the Company	8, 9
			Responsible business	116
GRI 2-7	Employees		People at Kaspersky	58
			Appendix 4	127
GRI 2-8	Workers who are not employees	All workers at Kaspersky the Company's employees.		

Metric	Disclosure	Comment	Report section	Page
GRI 2-9	Governance structure and composition		Managing sustainable development	17
			Responsible business	104
GRI 2-10	Nomination and selection of the highest governance body		Responsible business	104
GRI 2-11	Chair of the highest governance body		Responsible business	104
GRI 2-12	Role of the highest governance body in overseeing the management of impacts		Managing sustainable development	17
GRI 2-13	Delegation of responsibility for managing impacts		Responsible business	104
GRI 2-14	Role of the highest governance body in sustainability reporting	The information in the Sustainability Report is approved by representatives of the relevant departments, the legal department, and the public relations department.		
GRI 2-15	Conflicts of interest		Responsible business	106
GRI 2-16	Communication of critical concerns	The board of directors is notified of critical issues by representatives of relevant departments via email or during emergency face-to-face meetings.		
GRI 2-17	Collective knowledge of the highest governance body		Responsible business	104
GRI 2-18	Evaluation of the performance of the highest governance body		Responsible business	104
GRI 2-19	Remuneration policies	At the time this report was prepared, Kaspersky's remuneration policy did not account for the effectiveness of managing Kaspersky's impact on the economy, society and the environment.		
GRI 2-20	Process to determine remuneration	The information is not disclosed due to limitations imposed by Kaspersky's internal confidentiality policy.		
GRI 2-21	Annual total compensation ratio	The information is not disclosed due to limitations imposed by Kaspersky's internal confidentiality policy.		
GRI 2-22	Statement on sustainable development strategy		Statement from the CEO	3
GRI 2-23	Policy commitments		Managing sustainable development	17
			Responsible business	100
GRI 2-24	Embedding policy commitments		Managing sustainable development	17
			Responsible business	100, 105
GRI 2-25	Processes to remediate negative impacts		Managing sustainable development	18
			Responsible business	105, 107
GRI 2-26	Mechanisms for seeking advice and raising concerns		Responsible business	105

Metric	Disclosure	Comment	Report section	Page
GRI 2-27	Compliance with laws and regulations	During the reporting period, Kaspersky identified no instances of non-compliance with laws or regulations, and the Company did not incur any fines or other penalties for violations of the law.		
GRI 2-28	Membership associations		Appendix 3	125
GRI 2-29	Approach to stakeholder engagement		Managing sustainable development	20
GRI 2-30	Collective bargaining agreements	Kaspersky does not have a collective bargaining agreement.		
Material topics				
GRI 3-1	Process to determine material topics		Appendix 3	123
GRI 3-2	List of material topics		Appendix 3	124
Economic performance				
GRI 201-1	Direct economic value generated and distributed		About the Company	15
Market presence				
GRI 202-2	Proportion of senior management hired from the local community		The proportion of senior management hired from among the local population is 100%.	
Indirect economic impacts				
GRI 203-1	Infrastructure investments and services supported		Managing sustainable development	18
			Contribution to social development	73
GRI 203-2	Significant indirect economic impacts		Managing sustainable development	18
			Contribution to social development	73
Procurement practices				
GRI 204-1	Proportion of spending on local suppliers		Responsible business	117
Anti-corruption				
GRI 205-1	Operations assessed for risks related to corruption		Responsible business	105
GRI 205-2	Communication and training about anti-corruption policies and procedures		Responsible business	106
GRI 205-3	Confirmed incidents of corruption and actions taken		Responsible business	106
Energy				
GRI 302-1	Energy consumption within the organization		Environment	91
GRI 302-4	Reduction of energy consumption		Environment	92

Metric	Disclosure	Comment	Report section	Page
Water and effluents				
GRI 303-1	Interactions with water as a shared resource		Environment	93
GRI 303-2	Management of water discharge-related impacts	Kaspersky does not have approved wastewater quality standards, because it does not discharge water into natural water bodies.	Environment	93
GRI 303-3	Water withdrawal		Environment	93
Emissions				
GRI 305-1	Direct (Scope 1) GHG emissions	We are developing a methodology for collecting data and calculating the total amount of direct (Scope 1) greenhouse gas emissions for all Kaspersky facilities. This data will be presented in subsequent reports.		
GRI 305-2	Energy indirect (Scope 2) GHG emissions	We are developing a methodology for collecting data and calculating total indirect (Scope 2) greenhouse gas emissions from energy use. This data will be presented in subsequent reports.		
GRI 305-3	Other indirect (Scope 3) GHG emissions		Environment	90
GRI 305-5	Reduction of GHG emissions		Environment	90
GRI 305-6	Emissions of ozone-depleting substances (ODS)	Kaspersky does not emit ozone-depleting substances.		
GRI 305-7	Nitrogen oxides (NO_x), sulfur oxides (SO_x), and other significant air emissions	Kaspersky does not emit the specified pollutants into the atmosphere.		
Waste				
GRI 306-1	Waste generation and significant waste-related impacts		Environment	94
GRI 306-2	Management of significant waste-related impacts		Environment	94
GRI 306-3	Waste generated		Environment	94
GRI 306-4	Waste diverted from disposal		Environment	94
GRI 306-5	Waste directed to disposal		Environment	94
Employment				
GRI 401-1	New employee hires and employee turnover		People at Kaspersky	58
			Appendix 4	129

Metric	Disclosure	Comment	Report section	Page
GRI 401-2	Benefits provided to full-time employees that are not provided to temporary or part-time employees		People at Kaspersky	60
GRI 401-3	Parental leave		Appendix 4	132
Occupational health and safety				
GRI 403-1	Occupational health and safety management system	Within the scope of disclosure in this report, the occupational health and safety management system at all Kaspersky offices complies with the requirements of current labor legislation in the territories where Kaspersky operates. It includes regular employee training and regular special assessments of workplaces in all departments, a risk management and accident investigation system, and the organization of events to improve working conditions. The key performance indicator is the absence of workplace injuries.	People at Kaspersky	70
GRI 403-2	Hazard identification, risk assessment, and incident investigation		People at Kaspersky	70, 71
GRI 403-4	Worker participation, consultation, and communication on occupational health and safety		People at Kaspersky	71
GRI 403-5	Worker training on occupational health and safety		People at Kaspersky	70
GRI 403-6	Promotion of worker health		People at Kaspersky	71
GRI 403-8	Workers covered by an occupational health and safety management system	The occupational health and safety management system covers all Kaspersky employees.		
GRI 403-9	Work-related injuries		People at Kaspersky	70
GRI 403-10	Work-related ill health	During the reporting period, no cases of work-related illnesses were recorded at the Company.		
Training and education				
GRI 404-1	Average hours of training per year per employee		People at Kaspersky	67
GRI 404-2	Programs for upgrading employee skills and transition assistance programs		People at Kaspersky	68
GRI 404-3	Percentage of employees receiving regular performance and career development reviews		People at Kaspersky	69
Diversity and equal opportunity				
GRI 405-1	Diversity of governance bodies and employees		People at Kaspersky Appendix 4	63 128

Metric	Disclosure	Comment	Report section	Page
GRI 405-2	Ratio of basic salary and remuneration of women to men		People at Kaspersky	63
Non-discrimination				
GRI 406-1	Incidents of discrimination and corrective actions taken	No cases of discrimination were identified during the reporting period.	Responsible business	100
Child labor				
GRI 408-1	Operations and suppliers at significant risk for incidents of child labor	Kaspersky does not use child labor. Kaspersky also does not have any suppliers that are at risk of using child labor.		
Forced or compulsory labor				
GRI 409-1	Operations and suppliers at significant risk for incidents of forced or compulsory labor	The company does not use forced or compulsory labor. Kaspersky also does not have any suppliers at risk of using forced labor.		
Local communities				
GRI 413-1	Operations with local community engagement, impact assessments, and development programs	During the reporting period, Kaspersky implemented community engagement programs in Russia, Spain, Italy, Japan, India, South Africa, Singapore and Malaysia.	People at Kaspersky	76
Customer privacy				
GRI 418-1	Substantiated complaints concerning breaches of customer privacy and losses of customer data		Responsible business	108

Appendix 7. SASB Standards Compliance Index

This report was prepared in accordance with SASB Software and IT Services Industry Standard, Version 2018-10 (TC-SI). The table below presents the report's compliance.

Metric	Disclosure	Report section	Notes	Page
Environmental footprint of hardware infrastructure				
TC-SI-130-a.1	1) Total energy consumed, 2) percentage grid electricity, 3) percentage renewable	Environment		91
TC-SI-130-a.2	1) Total water withdrawn, 2) total water consumed; percentage of each in regions with high or extremely high baseline water stress	Environment	Water intake data is provided only for Kaspersky's HQ office in Moscow.	93
TC-SI-130-a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	Environment		92
Data privacy and freedom of expression				
TC-SI-220-a.1	Description of policies and practices relating to targeted advertising and user privacy	Responsible business		108, 109
TC-SI-220-a.2	Number of users whose information is used for secondary purposes		There are 0 (zero) such users.	
TC-SI-220-a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy	Responsible business		109
TC-SI-220-a.4	1) Number of law enforcement requests for user information, 2) number of users whose information was requested, 3) percentage resulting in disclosure		1) Detailed information on government requests can be found in Kaspersky's regular Law Enforcement & Government Requests Report here. The latest published report is for the second half of 2025. 2) The Company does not keep track of this statistic. We only track the number of requests to provide user data and non-personal technical information. 3) 0% — Kaspersky has not disclosed such data to government authorities.	
TC-SI-220-a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering, or censoring	Responsible business		120
Data security				
TC-SI-230-a.1	1) Number of data breaches, 2) percentage that are personal data breaches, 3) number of users affected	Responsible business		109
TC-SI-230-a.2	Description of approach to identifying and addressing data security risks, including use of third-party cybersecurity standards	Responsible business		108

Metric	Disclosure	Report section	Notes	Page
Recruiting and managing a global, diverse & skilled workforce				
TC-SI-330-a.1	Percentage of employees who 1) are foreign citizens, 2) work from abroad		1) As of December 31, 2025, 63 foreign citizens worked at AO Kaspersky Lab, which constitutes 1.3% of the total number of employees. Information was not collected from other regional offices during the reporting period. 2) Not applicable to AO Kaspersky Lab, since Russian labor legislation does not provide for work outside the Russian Federation. Information was not collected from offices outside Russia during the reporting period.	
TC-SI-330-a.2	Employee engagement	People at Kaspersky		69
TC-SI-330-a.3	Percentage of genders and racial/ethnic groups representation for 1) management, 2) technical employees, 3) all other employees	People at Kaspersky Appendix 4	Kaspersky does not keep statistics on the racial/ethnic groups of its employees.	63 128
Intellectual property protection & competitive behavior				
TC-SI-520-a.1	Total amount of monetary losses as a result of legal proceedings associated with anti-competitive behavior regulations	Responsible business		110
Managing systemic risks from technology disruptions				
TC-SI-550-a.1	Number of 1) performance issues, 2) service disruptions, 3) total customer downtime		The information is not disclosed due to limitations imposed by Kaspersky's internal confidentiality policy.	
TC-SI-550-a.2	Description of business continuity risks related to disruptions of operations	Responsible business		120
Activity metrics				
TC-SI-000.A	1) Number of licenses or subscriptions, 2) Percentage cloud-based		1) 813 2) 30%	
TC-SI-000.B	1) Data processing capacity, 2) Percentage outsourced		1) 292 units in the local network and 8,198 outsourced units 2) 96% outsourced (co-located)	
TC-SI-000.C	1) Amount of data storage, 2) Percentage outsourced		1) Not less than 100 PB 2) More than 93% outsourced (co-located)	

Appendix 8. Glossary

APTs	Advanced Persistent Threats — Technically sophisticated and covert cyberattacks on targeted entities or people that can remain undetected for a significant period of time and aimed usually at collecting confidential information or causing significant damage.
BEC	Business Email Compromise — A type of fraudulent attack in which an attacker impersonates a company employee, manager, or contractor in business correspondence in order to cause funds to be transferred, obtain data, or cause other actions detrimental to the company.
DDoS	Distributed Denial of Service — An attack in which multiple devices simultaneously flood a server, service, or network with requests in order to overload it and make it unavailable to users.
DLL hijacking	Dynamic Link Library (DLL) Hijacking — An attack technique in which an attacker replaces or places a malicious DLL library so that a legitimate program loads it instead of the regular one and executes malicious code.
DPI	Deep Packet Inspection — A network traffic analysis technology that makes it possible to examine not only packet headers but also their contents to identify threats, filter data, and control the transfer of information.
EDR	Endpoint Detection and Response — A class of information security solutions designed to monitor endpoints, identify suspicious activity, investigate incidents, and respond to them.
IoT	Internet of Things — A network of interconnected physical devices equipped with sensors, software, and communications tools to exchange data with each other, with cloud systems, and with other digital platforms.
LLM	Large Language Model (LLM) — An artificial intelligence model trained on large amounts of text data and capable of understanding and generating natural language and performing text-related tasks.
MDR	Managed Detection and Response (MDR) — A service or class of services in which an external team of experts uses specialized technologies and analytics to identify threats, investigate incidents, and help customers respond to them.
OCR	Optical Character Recognition (OCR) — A technology for converting text from images, scans, or photographs into a machine-readable format for further processing, storage, and retrieval.
OT	Operational Technology — The set of systems, hardware, and software that control physical processes in industry, energy, transport, and other critical infrastructure facilities.
PoSA	Point-of-Sale Activation - thin cardboard cards for electronic product delivery.
SOC	Security Operations Center — A dedicated function or department that continuously monitors information security events, identifies threats, and coordinates incident response.
TIP	Threat Intelligence Platform — A platform for collecting, enriching, analyzing, and using cyberthreat data, including indicators of compromise, attacker information, and attacker tactics.
V2X	Vehicle-to-Everything — A technology for exchanging information in real time between a vehicle and other entities: cars, road infrastructure, pedestrians, networks, and cloud systems.
XDR	Extended Detection and Response — A class of information security solutions that combine data from multiple sources (endpoints, networks, servers, clouds, and other systems) to detect sophisticated attacks and provide a centralized response.
ICS	Industrial Control System — A set of software and hardware designed to automate, monitor, and control industrial processes in production and industrial infrastructure.
Wipers	Malicious software designed to destroy, damage, or permanently erase data and disrupt the operation of information systems.
Vendor	Vendor (supplier, manufacturer) — A company that develops, produces and/or supplies products, solutions or services under its own brand.
Viruses, worms, Trojans	Common types of malware: viruses embed themselves in files and spread when they are executed, worms spread on their own, and Trojans disguise themselves as legitimate software.
Cyberstalking	Systematic stalking, intimidation, or control of an individual using digital technology, including instant messaging, email, social media, spyware, and other online tools.
Clicker games	A genre of digital games based on repeated simple user actions or automatic accumulation of game resources; also known as idle games.
Endpoints, end devices	Physical devices connected to a corporate or other network and capable of exchanging data with other systems: computers, laptops, smartphones, servers, virtual machines, and embedded devices.
Mining	The process of using computing resources to confirm transactions on a blockchain network and receive rewards in the form of digital assets.
Generation Z	The generation of people born between the mid-1990s and early 2010s who grew up in an environment when digital technology and the internet were widely used.
Reverse engineering	The process of analyzing software, code, a device, or a technology to understand its operating principles, internal structure, algorithms, and potential vulnerabilities.
Stealer	Malware designed to covertly collect and extract sensitive information, including passwords, cookies, banking information, and account credentials.
Hackathons	Competitions or intensive team events in which participants create prototypes of digital solutions, products, or services in a limited time period.
Exploit	Software code, a script, or a technique that takes advantage of a vulnerability in a system, application, or device to perform unauthorized actions.

Appendix 9. Contact information

GRI 2-3

For any questions related to this sustainability report, please contact
Maria Losyukova, Head of Sustainability:

CSR@kaspersky.com

Mailing address of central office:

39A/3 Leningradskoe Shosse, Moscow,
125212, Russian Federation,
Olympia Park Business Center

+7 495 797-87-00,
+7 495 737-34-12

Company website:
www.kaspersky.com

General inquiries:
info@kaspersky.com

Press contacts:
empr@kaspersky.com

Contact information:
https://www.kaspersky.com/about/contact