kaspersky

Contents

3 Statement from the CEO

4 About the Company
5 Mission and values
6 Geography
7 Value chain
8 Products
9 Brief Company history
10 Key achievements

12 Sustainable Development
13 ESG strategy
15 Managing sustainable development
17 Contribution to achieving UN Sustainable Development Goals
19 Material topics of the Report
21 Stakeholder engagement
23 Sustainable supply chain
24 Respect for human rights
27 Managing ESG risks

28 Safer Cyber World
29 Digital security
47 Combating cybercrime

55 Future Tech
56 Protection of industrial enterprises and critical infrastructure
57 What is critical infrastructure?
61 Industrial security ecosystem

72 Safer Planet
73 Managing our environmental impact
74 Reducing our carbon footprint
78 Water usage
79 Waste management
83 Developing environmental awareness among staff

84 People Empowerment
85 Talent management
89 Training and development
91 Social policy
92 Corporate culture and business ethics
95 Occupational safety and health protection
96 Engagement with local communities
102 Training staff for the IT industry. Our experience
112 Women in IT: Power of Equality

117 Ethics and Transparency
118 Global Transparency Initiative
125 Data protection
129 Intellectual property protection and defense
132 Corporate governance
135 Risk management

138 Additional Information
139 Appendix 1. About the Report
140 Appendix 2. Membership in associations and unions
141 Appendix 3. People Empowerment section
149 Appendix 4. Future Tech section
150 Appendix 5. GRI Standards Compliance Index
156 Appendix 6. SASB Standards Compliance Index
159 Appendix 7. Glossary
160 Appendix 8. Contact information

“Every day we take a step toward a safer and more sustainable digital world”

Eugene Kaspersky
CEO of Kaspersky

Dear Friends!

This is the second annual Kaspersky Sustainability Report prepared in accordance with the international GRI and SASB standards. It tells you all about what we have done to implement our ESG strategy for the second half of 2022 and the full year of 2023. While every day we face increasingly diverse cyberthreats, we remain convinced that it is only with Cyber Immunity in response that we can maximize security. Today, we will tell you how embedding sustainability into our business processes helps us in this challenging task.

For almost 27 years, Kaspersky has been making a significant contribution to the development of information-security technologies. Continuing to develop dynamically, we have successfully adapted to external changes, improved our technologies and products, and expanded our presence in the global market. Today our solutions are used on all continents and we protect users in more than 200 countries and territories across the world. We offer our customers a wide range of solutions – 36 products for home and business. We have regional offices in more than 30 countries on five continents. Our team employs more than 5 thousand highly-qualified specialists, while the number of our corporate customers has reached 220,000. Our solutions protect large industrial plants and critical infrastructure, as well as businesses of all sizes.

We are committed to our mission – creating a safe and sustainable world step by step where people are free to take advantage of the power of digital technologies to improve their lives. During the reporting period, Kaspersky actively developed all five key ESG areas: cyber-resilience, innovation and future technologies, environmental protection, care for employees and the people around them, and ethics and transparency.

In the area of cyber-resilience, we continued to develop advanced technological solutions that can effectively defend against the latest cyberthreats, implemented educational programs, conducted seminars and trainings, and assisted law enforcement organizations in countering malicious actors. Our team provided customers with robust tools for protection against cybercrime. In 2023, our solutions helped our customers repel more than 430 million attacks. Since inception Kaspersky has protected over a billion devices.

To protect critical infrastructure, Kaspersky has developed a unique ecosystem of modern IT technologies (KOTCS), which permits protecting all levels of an enterprise from a single console. We have accumulated years of expertise in combating cyberattacks on industrial facilities, and successfully continued to develop our Industrial CyberSecurity (KICS) solution, with sales growing 54% year-on-year in 2023.

Kaspersky has invested a great deal of time and effort into innovation. Together with our partners, we have created a hardware-and-software platform for neuromorphic machine learning, introduced our own cloud-based cybersecurity platform for connected vehicles, and developed a comprehensive plan for the cyberdefense of nuclear power plants during their early stages of design and construction.

In addition to technological advancement, we also aim to create sustainable and responsible business practices. In 2023, Kaspersky celebrated five years of its Global Transparency Initiative (GTI), which, as the name suggests, ensures the trasparency of the Company’s products and business processes. During the reporting period we increased the number of our Transparency Centers around the world to 11 with the opening of two more centers for the first time in the Middle East and Africa.

At Kaspersky, we not only achieve business success by developing the best technologies, but also contribute to environmental protection and the well-being of society as a whole. In this report, we describe our work on reducing our environmental footprint, what we do for the development and prosperity of our employees, and our social and charitable programs.

New challenges always bring new opportunities. In 2024, we will continue to move forward and achieve all our plans. On behalf of the Company, I would like to thank all our employees, partners and customers for their trust, support and commitment to our values. Together we can do more and create a truly secure – Cyber Immune – future for all.

About the Company

In the contemporary world, cybersecurity is a fundamental necessity for people, businesses and entire nations. Since 1997, Kaspersky has been working to build a future free of cyberthreats.

GRI 2-6

Kaspersky is an international company that develops information security and digital privacy products and solutions. We are committed to making cyberspace secure and building a safer world.

1 billion

Devices protected by Kaspersky to date*

* The figure is based on the data of Kaspersky Security Network (KSN) for automated malware analysis and includes records starting from 2011, when the system was rolled out.

220,000

corporate customers

>5,000

experts on the team

36

products for home and business

Mission and values

Kaspersky's mission is to build a safer, more sustainable digital world where people can use technology to improve life on the planet.

Implementing our mission involves making the digital space more resilient to threats by building Cyber Immunity and inherently protected systems. We also devote considerable attention to social projects and environmental protection.

For more about Cyber Immunity, please see p. 66

Our values

Be there for you

Even though we live and breathe the cyber world, people are at the heart of what we do.

We never lose sight of the people we build our solutions for. We are always aiming to meet the needs of our customers because we want to make them feel safer by providing the best solutions for all of their digital interactions.

We'll always be there for you, for our customers, partners, prospects and colleagues.

Be committed experts

Through our recognized technology expertise, we are committed to providing trust, safety and confidence.

We never give up on our mission to make the digital world a safer place and build a Cyber Immune future. And on this duty we always play fair. People who meet us understand that we are totally committed to the cause and will always be by our customers' side.

Be cleverly inventive

We're always switched on and in touch with what's happening in the industry and the wider world.

We're tirelessly looking for new smart solutions and architectural approaches as we constantly strive to reach new levels, evolve and identify the most effective and inventive ways to build a Cyber Immune future.

Be powered by challenges

Changing the world and industry has never been easy.

We constantly challenge ourselves to do what others can't. We deliver outstanding solutions to overcome obstacles of all kinds, and this is proven across our 25-year history. Independence and originality are in our blood. We follow our own path and develop our own approach to guide the next generation of cybersecurity.

Geography

GRI 2-1

Our customers use Kaspersky's products all around the world. Kaspersky companies operate in more than 30 countries on five continents.

Countries where Kaspersky companies operate:

Commonwealth of Independent States (CIS)

- Russia
- Belarus
- Kazakhstan

Middle East, Turkey and Africa

- Rwanda
- Saudi Arabia
- South Africa
- Turkey
- United Arab Emirates (UAE)

Latin America

- Brazil
- Mexico

Europe

- Czech Republic
- Germany
- Netherlands
- Romania
- Switzerland
- United Kingdom (UK)
- France
- Israel
- Italy
- Portugal
- Spain

Asia-Pacific region

- Australia
- Japan
- Greater China (China, Hong Kong)
- India
- South Korea
- Malaysia
- Singapore

North America

- Canada
- United States of America (U.S.A.)

Value chain

GRI 2-6

In its operations, Kaspersky is committed to adhering to the principles of socially responsible business at all stages of value creation.

	Materials and equipment	Operations and production	Distribution and sales	Product use	
Key stakeholders	■ Service contractors ■ Hardware and software suppliers ■ Partners ■ Government authorities ■ Regulators	■ Employees ■ IT community ■ Judicial and legislative authorities ■ Regulators ■ Non-profit organizations ■ Users	■ Employees ■ Distributors ■ Resellers ■ Enterprises ■ Users ■ Government authorities ■ IT community ■ Industry associations	■ Employees and their families ■ Non-profit organizations ■ Schoolchildren and university students ■ IT community ■ Partners ■ Contractors ■ Suppliers	■ Corporate customers ■ Private users ■ Government authorities ■ Regulators ■ Law enforcement agencies
Impact	■ Enhancing transparency of management and business sustainability.	■ Enhancing transparency of management and business sustainability. ■ Caring for the physical and mental health of our employees in their professional development. ■ Reducing environmental impact in all aspects of Kaspersky's operations.	■ Enhancing transparency of management and business sustainability. ■ Reducing environmental impact in all aspects of Kaspersky's operations.	■ Eliminating leaks of Kaspersky users' personal data. ■ Boosting the trust of users, customers and other stakeholders in Kaspersky. ■ Protecting users against cyberthreats with the Company's products and initiatives. ■ Protecting critical infrastructure through the creation of modern IT technologies and services.	■ Aiding national and international law enforcement organizations in cybercrime investigations. ■ Achieving gender equality in IT. ■ Training staff on cybersecurity and advancing the professional skills of IT specialists.

Products

Kaspersky's technologies protect our customers – both individuals and companies – against cyberthreats, regardless of the size of their business.

GRI 2-6

The Company's portfolio features 36 information security products for home and business[1]. In 2013–2023, Kaspersky's products took part in 927 independent tests and reviews, finishing first in 680 cases and among the top three in 779 of them.

The Kaspersky Endpoint Security Cloud solution proved to be highly effective in combating ransomware and outperformed products from 10 other vendors in AV-TEST testing. The Kaspersky EDR Expert solution demonstrated 100 percent effectiveness against targeted attacks in the SE Labs Enterprise Advanced Security (EDR) in 2022 and 2023 assessments and also twice received a high Strategic Leader rating based on the results of the AV-Comparatives Endpoint Prevention and Response 2022 and 2023 tests. Kaspersky Standard, the primary plan of the new Kaspersky Consumer Portfolio (launched in 2022), was honored with the "Product of the Year" award by AV-Comparatives for consistently delivering outstanding results throughout 2023.

36 products

in the Company's portfolio

680 times

our products were ranked first in independent tests from 2013 to 2023

779 times

our products were ranked in the top three between 2013 and 2023

Home products:

Kaspersky Standard
Kaspersky Plus
Kaspersky Premium

For more about home products

Business products (small, medium and enterprise):

Kaspersky Small Office Security
Kaspersky Endpoint Security
Kaspersky Container Security
Kaspersky EDR
Kaspersky XDR
Kaspersky Industrial CyberSecurity

For more about business products

KasperskyOS-based solutions:

KasperskyOS SDK for IoT controllers
Kaspersky Automotive Secure Gateway
Kaspersky IoT Secure Gateway
Kaspersky Thin Client

For more about solutions

[1] The list of products includes protected solutions on the kaspersky.ru and kaspersky.com websites. These products are offered based on numerous licenses that meet the needs of various customers (more than 1,500 positions in the Company's price list).

Brief Company history

During its more than 25 years of operation, Kaspersky has made a huge contribution to the development of information security technologies used by individuals, companies and government agencies in more than 200 countries around the world.

1989	Eugene Kaspersky discovers a virus called Cascade.1704 on his Olivetti M24 work computer and creates his first virus removal tool.

June 26, 1997

Kaspersky is established as a company

1999	The Company opens its first overseas office in the UK.
2001	Kaspersky Anti-Virus software developed by the Company for portable devices is supplied to Russia with Palm, Handspring and Sony pocket computers.
2003	Kaspersky opens offices in Japan, Germany, France, Spain, Italy and China.
2004	Kaspersky becomes the world's first antivirus software developer to update its antivirus databases every hour. The company opens its first office in the U.S.A.
2007	The Company presents the Kaspersky Open Space Security line of business products.
2008	The Global Research & Analysis Team (GReAT) is created.
2009	Kaspersky hosts the first conference for information security researchers and analysts from around the world – Security Analyst Summit.
2009	The Company sponsors an expedition to Antarctica and would go on to sponsor two more Antarctic expeditions and the 7 Volcanoes expedition.
2013	The Company begins cooperating with INTERPOL.
2016	Kaspersky, along with Europol and Intel Security, launches the No More Ransom initiative, which would soon be joined by dozens of countries and information security development companies.
2017	The Company releases its own secure KasperskyOS operating system, which provides protection against any threats, including unknown ones.
2018	Kaspersky launches the Global Transparency Initiative. The first Transparency Center opens in Zurich, Switzerland.
2019	The Company undergoes rebranding and states its mission as "Building a Safer World". Transparency Centers open in Spain, Malaysia and Brazil.
2020	During the pandemic, Kaspersky provides free licenses for key products to medical institutions around the world. Transparency Center opens in Canada.
2021	Kaspersky provides access to the Software Bill of Materials (SBOM), helping customers and partners understand what's inside its products and software. The Company finalizes a deal with Brain4Net and receives a new impetus for the development of its XDR platform. Kaspersky continues its strategy of business diversification and investment in promising IT businesses by increasing its stake in the capital of MyOffice and purchasing shares in ForPeople, which develops solutions to automate HR processes. The Company also acquires a 15 percent stake in Motiv NT, which it employed to continue working on the creation of Russia's first neuromorphic processor.
2022	The Kaspersky Cyber Immunity® trademark is registered in the European Union (EU).
2023	Transparency Centers open in the Saudi Arabia and Rwanda.

Key achievements

+8%

in global B2B sales[1] in 2022

+23%

in global enterprise sales in 2022

+54%

in global sales of Kaspersky industrial CyberSecurity in 2022

Milestones in the reporting period

Business expansion

- The Company has continued to open new Transparency Centers. In the second half of 2022, Kaspersky opened centers in Italy and the Netherlands. In 2023, it also opened its first Transparency Centers in the Middle East (Saudi Arabia) and Africa (Rwanda).
- Kaspersky acquired a 49 percent stake in ForPeople, a developer of solutions to automate HR processes, and a 49 percent stake in Ximi Pro, a developer of container security solutions.

Innovation

- Kaspersky and Motiv-NT presented Kaspersky Neuromorphic Platform (KNP), a software and hardware platform for neuromorphic machine learning. It is designed to train neural networks, conduct research in neuromorphic artificial intelligence, as well as to create and launch solutions based on next-generation AI systems.
- Kaspersky and Centerm, the world's leading thin client manufacturer, signed an original equipment manufacturer (OEM) agreement to begin global deliveries of KasperskyOS-based software products.
- Kaspersky, along with NAMI state research center and GLONASS, presented Russia's first cloud-based cybersecurity platform for connected vehicles.
- Atomenergoproekt and Kaspersky developed a comprehensive cybersecurity plan that considers the most stringent security requirements for nuclear facilities at the earliest stages of the construction of Generation III+ nuclear reactors.
- Kaspersky entered into a partnership with ASWANT to develop a Cyber Immunity ecosystem in Malaysia and Indonesia.
- Kaspersky and TSplus signed a partnership agreement to supply Cyber Immune solutions for remote workplaces.

Patents and standards

- Kaspersky registered the Kaspersky Cyber Immunity® trademark in the EU, which is valid throughout the entire EU.
- Starting in April 2023, two national standards took effect for systems with domain separation developed by Kaspersky and adopted by Technical Committee 194 "Cyber-Physical Systems", which define the basic concepts and architectural principles inherent in systems with domain separation, including KasperskyOS.

International cooperation

- Kaspersky aided to INTERPOL by providing cyberthreat intelligence as part of Operation Africa Cyber Surge II. This information led to the identification of compromised infrastructure and the arrest of 14 cybercrime suspects across the African region.
- The Qatar Olympic Committee uses Kaspersky products to ensure cybersecurity.
- The UAE Cyber Security Council and Kaspersky signed a memorandum of understanding to share information on identifying, investigating and responding to evolving cyberthreats in a timely manner.

[1] YOY growth in the SMB, enterprise and B2B digital segments. All segment and regional figures are in net sales bookings, not revenue, and are presented in fixed rates as of 2022. The 2022 growth is presented as compared with 2021.

Awards and recognition

Our developments receive high praise from independent experts and win awards at prestigious international competitions.

2022

In 2022, Kaspersky's products took part in 86 independent tests and reviews. They finished first 69 times and in the top three 73 times, while 85 percent of these products were among the top three in their category.

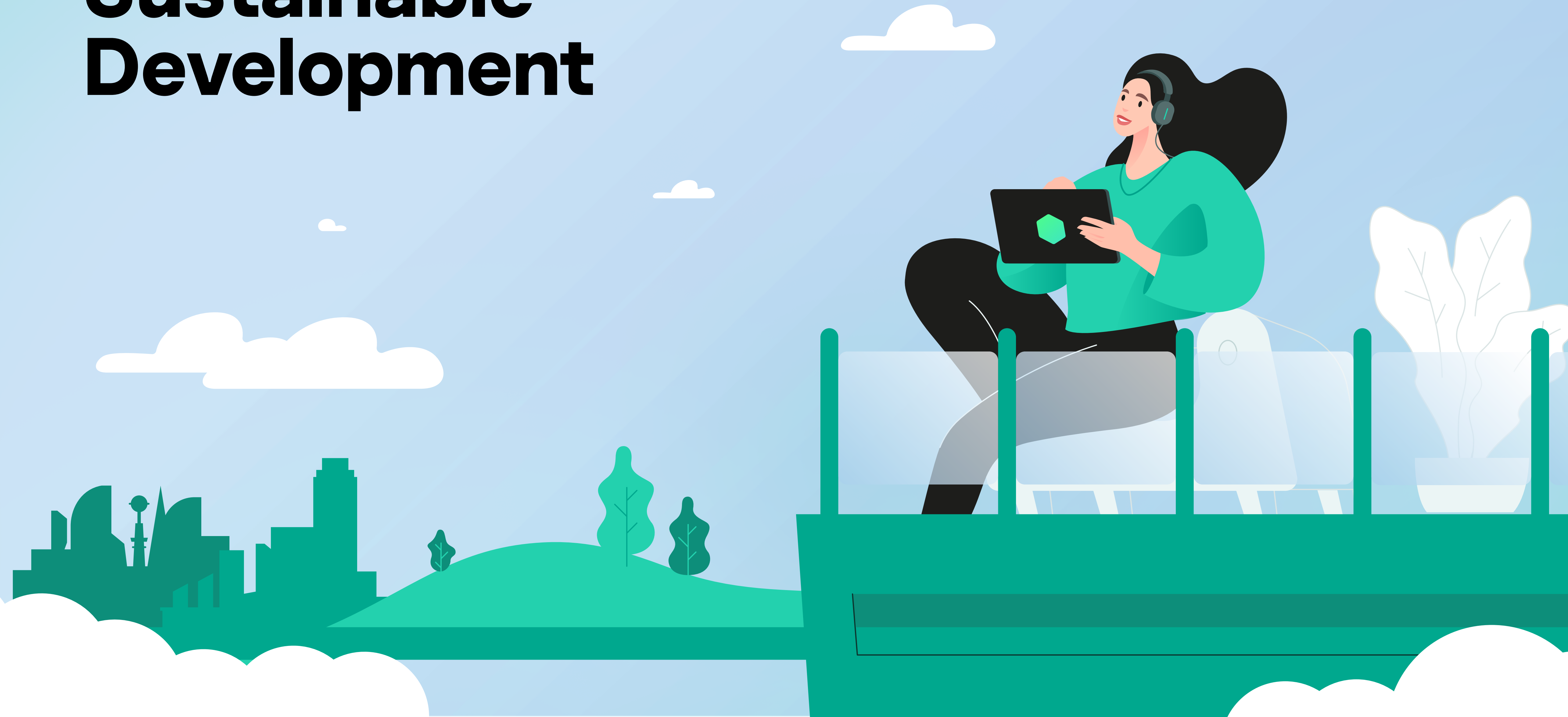
- Kaspersky is recognized as a leader in endpoint security per the G2 Crowd international platform.
- The Kaspersky EDR Expert solution repelled 100 percent of cyberattacks during the international SE Labs test.
- The Kaspersky Endpoint Detection and Response Expert solution was granted the status of a strategic leader as a result of comprehensive testing conducted by the Austrian company AV-Comparatives.
- Kaspersky became a leader in the global market for MDR solutions per the consulting company Quadrant Knowledge Solutions.
- Kaspersky Secure Remote Workspace solution received an award at the World Internet Conference in China.

2023

During 2023, Kaspersky participated in 100 independent tests and reviews, with its products being awarded 93 firsts and 94 TOP-3 finishes, achieving the highest result of all years.

- Kaspersky successfully underwent an audit by the Service and Organization Controls Type 2, a globally recognized reporting standard for cybersecurity risk management systems.
- Kaspersky Safe Kids received a quality certificate from the independent laboratory AV-TEST for the seventh time in a row.
- Kaspersky became a leader on the global managed services market per Quadrant Knowledge Solutions.
- Kaspersky Internet Security received an annual award from the AV-Comparatives independent laboratory for the 12th time in a row.
- International research company IDC named Kaspersky the vendor that defined 2022 in terms of endpoint protection.
- The solutions of Kaspersky Security for Business, Kaspersky Small Office Security and Kaspersky Internet Security demonstrated 100 percent protection against ransomware during testing by AV-TEST.
- Kaspersky solutions again repelled 100 percent of attacks during the international SE Labs test.
- The Kaspersky Security for Business solution demonstrated 100 percent effectiveness against unauthorized attempts to interfere with its work per the results of a test by AV-Comparatives.
- For the second year in a row, the Kaspersky EDR Expert solution received the maximum score in the Total Accuracy Rating based on the results of SE Labs Enterprise Advanced Security testing the Company's EDR-class solutions.
- The Kaspersky Security Awareness digital literacy training was named a leader in a report by the analytical company SoftwareReviews.
- The Kaspersky Automotive Secure Gateway solution received an award at the World Internet Conference in China.
- AV-Comparatives named the new Kaspersky Standard the "Product of the Year", the highest rating awarded by a reputable independent organization that specializes in testing security solutions.

Sustainable Development



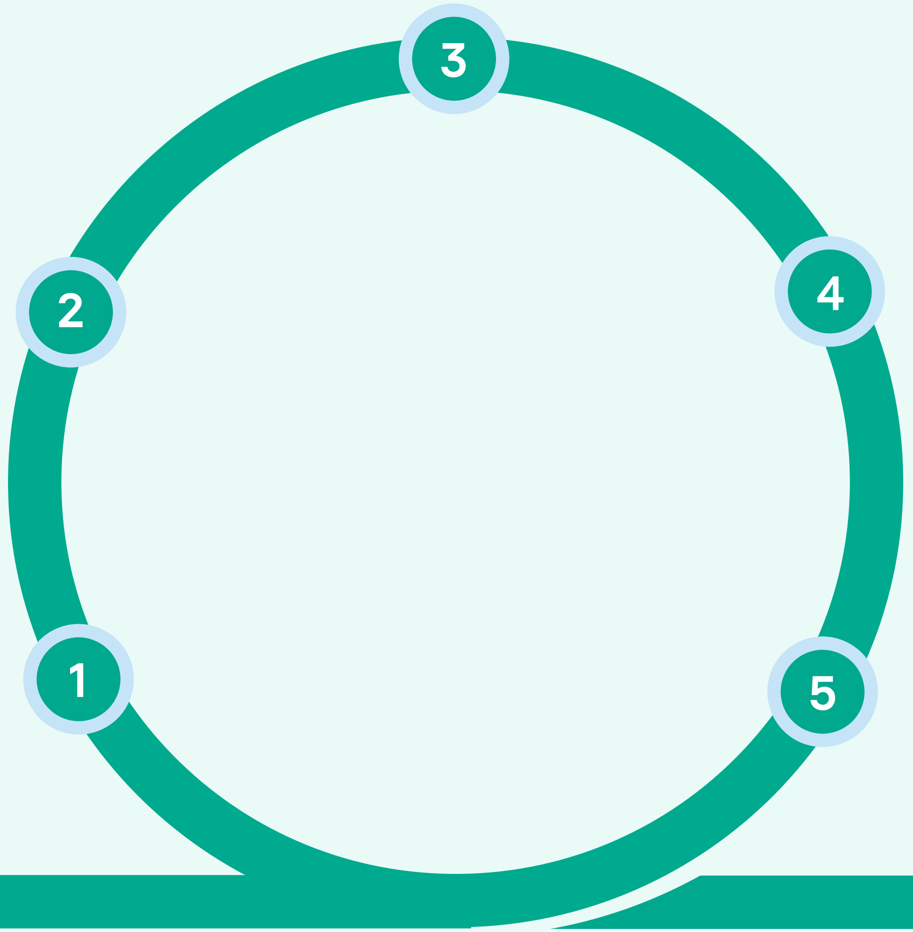
ESG strategy[1]

Kaspersky’s core principles and objectives are intertwined with ESG goals: we are building a sustainable digital world in which individuals, businesses and society can live and interact safely.

GRI 2-22

Kaspersky has identified five key sustainable development strategies. They provide guidance for the Company’s main ESG initiatives to ensure a safe digital environment as well as to address environmental and social issues.

Strategic priorities of sustainable development



Safer Cyber World

- Protecting critical infrastructure in a turbulent world
- Assisting in investigating cybercrimes around the world
- Protecting users against cyberthreats

Future Tech

- Cyber Immunity for new promising technologies

Safer Planet

- Reducing the environmental impact of our infrastructure, business activities and products

People Empowerment

- Caring for employees
- Women in STEM[2]
- Inclusivity and availability of technologies
- Talent development in IT

Ethics and Transparency

- Transparent source code and processes
- Data protection and privacy rights
- Transparent governance and business sustainability

[1] ESG-strategy stands for the Environmental, Social, Governance strategy.

[2] STEM stands for science, technology, engineering and mathematics.

# Goals

Safer Cyber World

- Protect users against cyberthreats using Kaspersky's products and initiatives.
- Protect industry and critical infrastructure using an ecosystem of modern IT technologies and services.
- Assist international and national law enforcement organizations in cybercrime investigations to ensure user safety.

Future Tech

- Involve new partners in implementing the Cyber Immunity strategy.

Safer Planet

- Reduce the environmental impact in all aspects of Kaspersky's operations.

People Empowerment

- Care for the physical and mental health of employees over the course of their professional development.
- Contribute to achieving gender equality in IT.
- Train cybersecurity personnel and raise the professional level of our IT specialists.
- Increase the accessibility of products, services and information security capabilities for people with disabilities.

Ethics and Transparency

- Enhance transparent governance and business sustainability.
- Comply with all personal data protection regulations, and to ensure the highest level of data security processing.
- Build users, customers and other stakeholders' trust in Kaspersky.

GRI 2-23

In terms of meeting its human rights obligations, Kaspersky is guided by the principles of the United Nations (UN) Global Compact, the UN General Assembly resolution on the Sustainable Development Goals adopted in 2015, the Paris Agreement dated 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, as well as the UN Guiding Principles on Business and Human Rights. The Company strictly complies with international and local legislation and relies on ISO 26000:2010 (Guidance on Social Responsibility) and the AA1000 international standard (Accountability Principles and the Stakeholder Engagement Standard).

Kaspersky also adheres to the precautionary principle (Principle No. 15) of the 1992 Rio Declaration on Environment and Development and constitutes an integral part of the Company's risk management system. The Company operates its data centers and develops its products and services taking into account its potential environmental impact.

GRI 2-28

Kaspersky works closely with numerous international associations and law enforcement agencies and participates in joint operations, cyberthreat investigations, cyber-diplomacy, and the promotion of an open and secure Internet.

→ For a full list of the Russian and international associations in which the Company is a member, please see Appendix 2 on p. 140

Managing sustainable development

GRI 2-9 GRI 2-12 GRI 2-13 GRI 2-16 GRI 2-24

Kaspersky employs a managerial system in which responsibilities are distributed among members of senior management and the heads of the relevant departments and units. The Sustainability Department and project team leaders coordinate the monitoring of results.

In early 2024, the Company established a sustainable development committee that reports to the board of directors. The committee's main goal is to develop recommendations for the board of directors on key sustainable development (ESG) issues, including:

- Minimizing the Company's environmental impact;
- Creating a productive work environment and developing human potential at the Company;
- Respecting and protecting human rights and providing an inclusive environment and equal access to the Company's products and services;
- Supporting local communities and non-profit organizations and promoting the Company's social development;
- Improving corporate governance, security and ESG risk management practices at the Company.

The committee will meet at least twice a year and actively collaborate with the Company's management bodies and teams that are involved in implementing sustainable development projects.

Teams responsible for achieving sustainable development goals in key areas

Safer Cyber World

- Government Relations
- KasperskyOS Business Unit
- Industrial Cybersecurity
- Threat Research
- Consumer Product Marketing

Ethics and Transparency

- Information Security
- Economic Security & Compliance
- Strategic IP Development & Research
- Internal Control
- Procurement

People Empowerment

- Talent Development
- Kaspersky Academy
- ESG & Sustainability

Safer Planet

- Consumer Channel
- Business Intelligence for Consumer Business
- Telecommunication IT Infrastructure
- Office Administration
- Finance
- Marketing Production
- Digital Business
- Business Travel

Future Tech

- KasperskyOS Business Unit
- Industrial Cybersecurity

Key documents

Anti-Corruption Policy[1]

Procurement Guideline

Contracts Approval Policy

[1] Adopted by Order No. 27 dated May 18, 2012.

Contribution to achieving UN Sustainable Development Goals

Kaspersky supports all 17 UN Sustainable Development Goals (UN SDGs) of the 2030 Agenda for Sustainable Development. The Company has identified six primary UN SDGs to which it contributes in the course of its day-to-day operations and the implementation of its key ESG initiatives.

4 Quality education

7 Affordable and clean energy

5 Gender equality

8 Decent work and economic growth

The Company's strategic priorities are also consistent with the focal UN SDGs.

9 Industry, innovation and infrastructure

12 Responsible consumption and production

10 Reduced inequalities

13 Climate action

The Company's strategic sustainable development focuses and their correlation with the UN SDGs

Ethics and Transparency

- Transparent source code and processes
- Data protection and privacy rights
- Transparent governance and business sustainability

8 DECENT WORK AND ECONOMIC GROWTH

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Safer Cyber World

- Protecting critical infrastructure in a turbulent world
- Assisting in investigating cybercrimes around the world
- Protecting users against cyberthreats

8 DECENT WORK AND ECONOMIC GROWTH

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Safer Planet

- Reducing the environmental impact of our infrastructure, business activities and products

7 AFFORDABLE AND CLEAN ENERGY

12 RESPONSIBLE CONSUMPTION AND PRODUCTION

13 CLIMATE ACTION

People Empowerment

- Caring for employees
- Women in STEM
- Inclusivity and availability of technologies
- Talent development in IT

4 QUALITY EDUCATION

5 GENDER EQUALITY

8 DECENT WORK AND ECONOMIC GROWTH

10 REDUCED INEQUALITIES

Future Tech

- Cyber Immunity for new promising technologies

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE

Material topics of the Report

GRI 3-1, 3-2

For the content of our Report to best meet our stakeholders' interests and expectations, we conducted a stakeholder survey in the form of an online questionnaire to determine the material topics of the Report.

We determined the initial list of topics for stakeholders to evaluate based on the list of sustainability priorities that were identified when determining materiality for the previous reporting period. It included 17 topics that reflect the Company's impact on the economy, environment and society.

Participants of the survey were asked to rate the importance of each of the proposed topics on a scale of one to five, with a rating of one assigned to the least important topics and a rating of five assigned to extremely important topics. The questionnaire also offered stakeholders an opportunity to leave their own comments on the proposed topics and suggest new ones. For the convenience of the participants, the questionnaire was prepared in Russian and English.

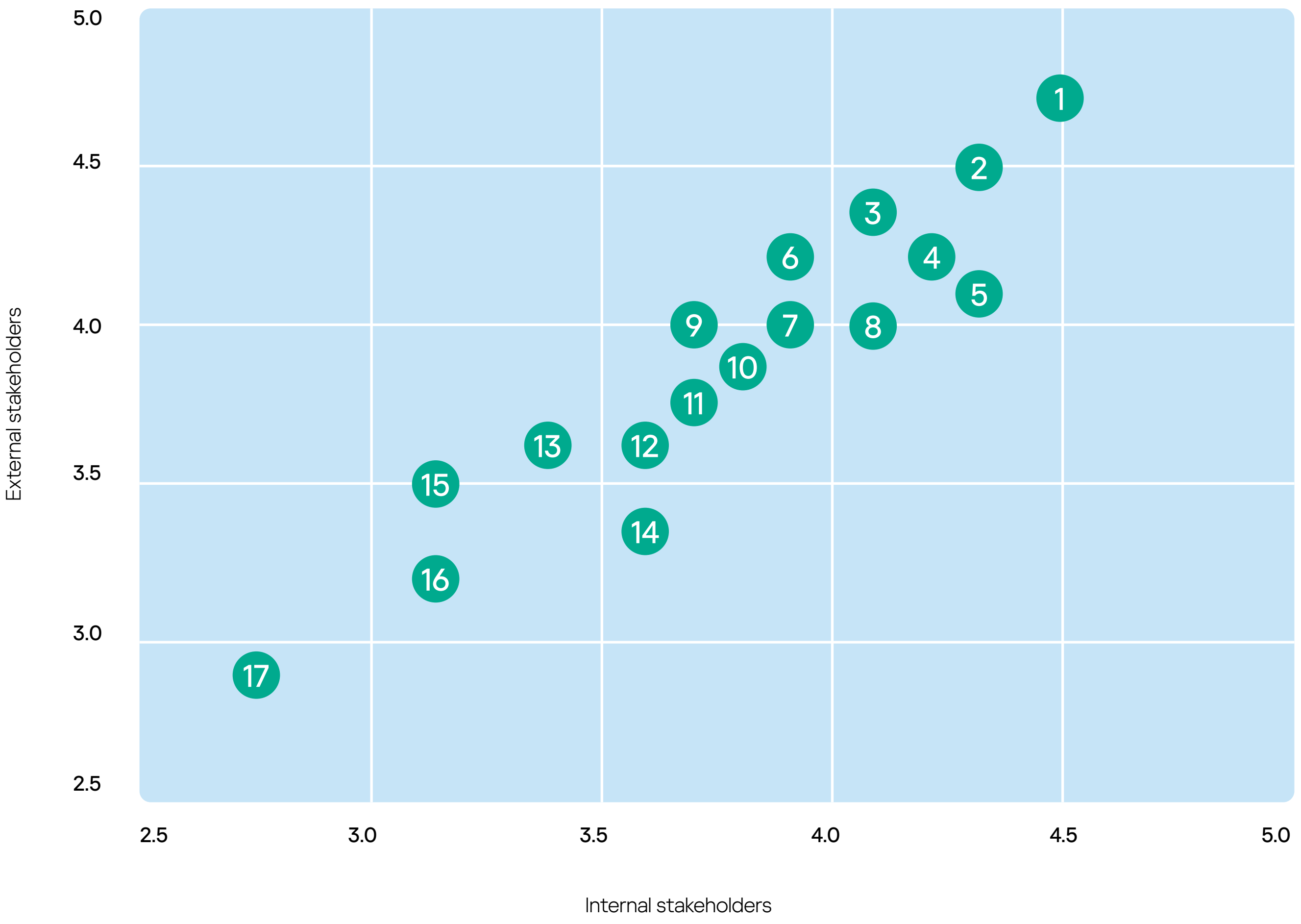
The survey was completed by 35 representatives of stakeholders, including 14 internal and 21 external stakeholders. The results were adjusted using weighting coefficients to give equal weight to the opinions of each stakeholder group. A final list of topics was then generated in descending order of importance based on the average ratings given by stakeholders.

A total of 15 topics with an overall score of 3.4 points or more were considered material for inclusion in the Report. This made it possible to equally consider the opinions of both the internal and external stakeholders who took part in the survey.

List of Kaspersky's material topics in the Sustainable Development Report for the second half of 2022 and for 2023

Topic	Materiality score	Page in the Report
Protecting users and user data	4.6	125
A safer digital environment	4.5	29
Ensuring software and digital resilience in a rapidly changing world	4.2	29
Educational activities in the cybersecurity field	4.2	38
Fighting international cybercrime	4.1	47
Contributing to technological developments	4.1	56
Training professionals for the industry	4	102
Responsibility toward employees	4	92
Inclusive digital environment	3.9	98
Business ethics	3.9	92, 134
Transparency of business and corporate management	3.7	132
Social projects, charity and volunteering	3.6	96
Women in STEM	3.6	112
Information and technological openness	3.4	118
Reducing the climate and ecological footprint	3.4	74

Materiality assessment by internal and external stakeholders



Topic number	Topic
1	Protecting users and user data
2	Safe digital environment
3	Ensuring software and digital sustainability in a changing world
4	Information security education
5	Combating international cybercrime
6	Contribution to technology development
7	Training professionals for the industry
8	Responsibility to employees
9	Inclusive digital environment
10	Business ethics
11	Transparency of business and corporate governance
12	Social projects, charity and volunteering
13	Women in STEM
14	Information and technological openness
15	Reducing the climate and ecological footprint
16	Sustainable supply chain
17	Taxation

Stakeholder engagement

Kaspersky's stakeholders include employees, users, partners, suppliers, government authorities, law enforcement agencies, local communities and groups that are vulnerable to information security issues (pensioners, children and their parents, as well as victims of cyberstalking). We are committed to interacting with them in a harmonious manner and fostering interactions based on the principles of mutual respect, transparency and responsibility.

GRI 2-29

Stakeholder group	Group's interests	Channels and methods of engagement	Results of engagement in the reporting period
Employees	■ Stable employment and career growth ■ Decent wages and social security ■ Comfortable and safe working conditions ■ Training and development ■ No discrimination	■ Internal corporate communications system ■ Meetings with Company managers ■ Joint conferences and educational and sporting events ■ Corporate website	Find out more about how the Company takes care of its employees in the "People Empowerment" section.
Users	■ Personal data protection ■ High quality products ■ High level of service ■ Reasonable prices for products	■ Feedback system and services ■ Press releases and advertising and promotional materials	Find out more about how the Company ensures privacy and protects users against cyberthreats worldwide in the "Safer Cyber World" and "Ethics and Transparency" sections.
Partners and suppliers	■ Transparency and openness of competitive procedures ■ Product quality control ■ Compliance with business ethics ■ Anti-corruption ■ Timely and proper fulfillment of contractual obligations	■ Conducting open competitive procurement procedures ■ Prompt handling of claims ■ Business meetings, conferences and exhibitions ■ Disclosure	Find out more about the Company's transparent policies and approach to procurement in the "Ethics and Transparency" section and the "Sustainable Supply Chain" subsection.

Stakeholder group	Group's interests	Channels and methods of engagement	Results of engagement in the reporting period
Government authorities and law enforcement agencies	■ Compliance with legal requirements and standards ■ Timely payment of all applicable taxes and fees ■ Investment in the development of regions of operation ■ Assistance in providing employment and supporting entrepreneurship ■ Ensuring the security of critical infrastructure facilities ■ Assistance in combating cybercrime	■ Consultations with law enforcement officials ■ Software development and licensing ■ Consultations on legislative issues	Find out more about the Company's interaction with the government authorities and law enforcement agencies in the "Combating Cybercrime" subsection.
Local communities	■ Creating jobs for local residents and developing human capital ■ Contributing to the development of social infrastructure ■ Development of local production and suppliers ■ Charitable projects and social investments ■ Minimizing the negative environmental impact in the regions of presence ■ Information openness and the transparency of activities	■ Hiring staff from local communities ■ Internships for students ■ Development and advanced training programs for staff ■ Training programs for a wide range of users ■ Procurements from local suppliers	Find out more about the Company's relevant policies and educational projects for employees and students in the "People Empowerment" subsection.
Groups vulnerable to information security issues	■ Ensuring Internet security	■ Conducting training events to improve digital literacy	Find out more about the Company's approach and educational projects for vulnerable groups (senior citizens, kids, people with disabilities) in the "People Empowerment" and "Safer Cyber World" subsections.
Non-profit organizations	■ Assistance in organizing and implementing environmental and social programs	■ Development, support and implementation of joint environmental and social projects	Find out more about the Company's approach and various projects with NPOs in the "People Empowerment" subsection.

Sustainable supply chain

Kaspersky's procurement activities are based on the principles of transparency and honesty. All companies that plan to become Kaspersky contractors are provided with equal conditions to take part in competitive procedures.

The Company's procurement procedures are regulated by the following internal documents:

- Procurement Guideline
- Contracts Approval Policy

All procurements are organized into distinct categories. Purchases are grouped based on similarities in technical and functional capabilities, as well as their relevance to various businesses, such as marketing, professional services, IT and production costs.

To manage procurements effectively, the Company has identified key thresholds based on the cumulative procurement amount per year for each category.

- Procurements up to US$25,000 have a simplified procedure: two competitive proposals are sufficient.
- Procurements ranging from US$25,000 to US$100,000 require a minimum of three proposals or two from trusted suppliers that were selected in the tender procedure and have successful experience working with our Company.
- Procurements valued at more than US$100,000 require a tender procedure, which involves several of the Company's units: procurement, the tender committee and cross-functional participants.

Tender-based procurements are subject to specific thresholds based on budgets. For instance, procurements exceeding US$1 million require the attendance of Kaspersky's business director during the tendering process.

Our security service verifies partners before they are invited to participate in a tender. We do not work with companies that do not have experience or a good reputation: 99 percent of our contractors have been working in the market for at least three years.

We plan to supplement the set of mandatory requirements for suppliers with a clause stating that the company must have an anti-corruption policy. During the reporting period, we already began including an anti-corruption clause in contracts with our contractors.

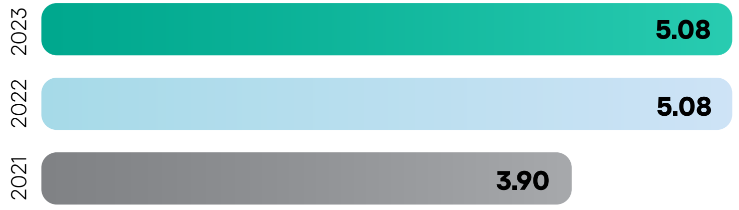
To ensure the confidentiality required by the specifics of the business and the competitive environment, and to avoid collusion among potential suppliers, we do not publish the numerical and qualitative results of tenders or the names of the parties involved.

In 2023, the number of suppliers remained at the same level as during the previous two years. The savings achieved through tender procedures and cost reductions in procurements more than doubled in 2023 compared with 2022 and amounted to US$13.2 million.

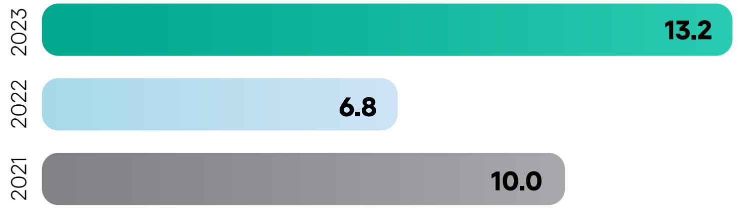
The Company worked with

5,080 **suppliers in 2023**

Number of Kaspersky suppliers at end of reporting period, thousand



Amount saved by the Company as a result of tenders and cost reductions during the procurement of goods and services, US$ million[1]



[1] Excluding costs for third parties.

Respect for human rights

GRI 2-22 GRI 406-1

Respect for human rights is a fundamental principle of Kaspersky's activities. The Company is committed to providing equal opportunities for employees around the world and supporting sociocultural diversity. The principles of respect for human rights and freedoms will be enshrined in Kaspersky's Code of Ethics, which is currently being developed.

Kaspersky does not tolerate any form of child, slave or forced labor and expects similar decisions from its contractors. This is outlined in Kaspersky's internal main principles and policies statement.

0 discrimination cases at the Company in the reporting period

Respect for human rights in the Company's activities

Fundamental human rights	Guiding documents for the Company	Company's approaches to respect for human rights	Stakeholders receiving special attention from the Company	Results of the reporting period
Right to life, liberty and privacy	■ Relevant regulations of countries of Kaspersky's presence. Amongst others: – EU General Data Protection Regulation (GDPR) – International information security standard ISO/IEC 27001 – Federal Law No. 152-FZ dated July 27, 2006 "On Personal Data" – China Personal Information Protection Law (PIPL) – California Consumer Privacy Act (CCPA) – Lei Geral de Proteção de Dados (General Data Protection Law (LGPD) in Brazil) – Vietnam's Personal Data Protection Decree (PDPD)	One of the Company's priorities is to ensure that the data of our users around the world is protected through internal security systems and procedures. We do not use data for purposes other than those for which it was collected.	■ Users ■ Employees ■ Groups vulnerable to information security issues ■ NPOs[1]	Zero serious violations of personal data legislation. Zero significant data breaches.

[1] Non-profit organizations.

Fundamental human rights	Guiding documents for the Company	Company's approaches to respect for human rights	Stakeholders receiving special attention from the Company	Results of the reporting period
Right to work	- Relevant regulations of countries of Kaspersky's presence as well as internal labor regulations and guidelines for compensation and workplace safety - Kaspersky Charity Policy - Sustainability Committee Regulation	Kaspersky's employees are our most valuable asset. We are committed to making it comfortable and interesting for people to work at the Company, so that they can work productively, feel protected, and be able to develop themselves as well as the Company. Kaspersky supports the activities of non-profit organizations that help people with disabilities with employment and socialization, as well as provide them with legal support.	- Employees - Groups vulnerable to information security issues - NPOs	5,152 people – total staff at the end of 2023 (+4.4% vs. the end of 2022). 15% staff turnover in 2023 (-8 p.p. vs. turnover in 2022). During the reporting period, the Company supported five NPOs that aim to employ people with disabilities. Kaspersky took part in four events on inclusive employment (business breakfasts, job fairs and a mentoring program). We also published an information project about the professional and personal path of employees with disabilities and those raising children with disabilities: https://kasperskyspecial.com/.
Right to a healthy environment	- Relevant regulations of countries of Kaspersky's presence - Kaspersky Charity Policy - Sustainability Committee Regulation	Environmentally responsible behavior is one of Kaspersky's most important values. We mitigate our adverse environmental impact through the economical consumption of resources, well-organized business processes and a responsible attitude to energy sources for data centers and offices.	- Employees - Local communities - Users - NPOs	285 contractors were connected to the electronic document management system from 2022 to 2023 and signed 7,126 documents. 1,407.9 kg of clothes and accessories were provided by the Company's employees for charity, recycling and disposal. 370 kg of electrical equipment were collected by employees for recycling during Ecoweek.

Fundamental human rights	Guiding documents for the Company	Company's approaches to respect for human rights	Stakeholders receiving special attention from the Company	Results of the reporting period
Right to education	■ Relevant regulations of countries of Kaspersky's presence ■ Kaspersky Charity Policy ■ Sustainability Committee Regulation	We encourage employees to acquire new knowledge and are constantly improving internal educational programs and adding new ones. We organize joint educational projects with non-profit organizations that help people with disabilities, pensioners, victims of domestic violence and other people who find themselves in difficult life situations. Kaspersky creates its own training programs that aim to collaborate with educational institutions and audiences that need additional education. We invest resources in the development of both schoolchildren and university students, as well as experienced cybersecurity specialists who need advanced training.	■ Employees ■ Users ■ Groups vulnerable to information security issues ■ NPOs	Kaspersky Academy has 200+ partner universities in 42 countries. During the reporting period, the Company received 13,549 applications to take part in the SafeBoard internship program. 134 students completed internships at Kaspersky during the reporting period. >6,000 students from all over the world have taken part in the Secur'IT Cup competition since 2018. The winners of the Secur'IT Cup receive grants worth US$10,000. 2,000+ users from more than 50 countries make up the expert training audience.
Right to health and medical care	■ Relevant regulations of countries of Kaspersky's presence ■ Kaspersky's regulation on compensation and incentive payments in countries of its presence	Caring for the health and well-being of employees is a key part of Kaspersky's social policy. The benefits package for Kaspersky's employees varies from region to region.	■ Employees	Zero injuries among employees in 2022 and 2023. Zero occupational diseases were identified among the Company's employees in 2023. A webinar and Q&A session with an oncologist was held for Kaspersky HQ employees in 2023 to cover common myths and misconceptions about cancer and the need for timely check-ups and testing.
Right to protection against discrimination	■ Relevant regulations of countries of Kaspersky's presence ■ Guiding Principles on Business and Human Rights	We do not tolerate or encourage any kind of discrimination in the Company's activities.	■ Employees ■ Users ■ Partners	Zero cases of discrimination at the Company during the reporting period.

Managing ESG risks

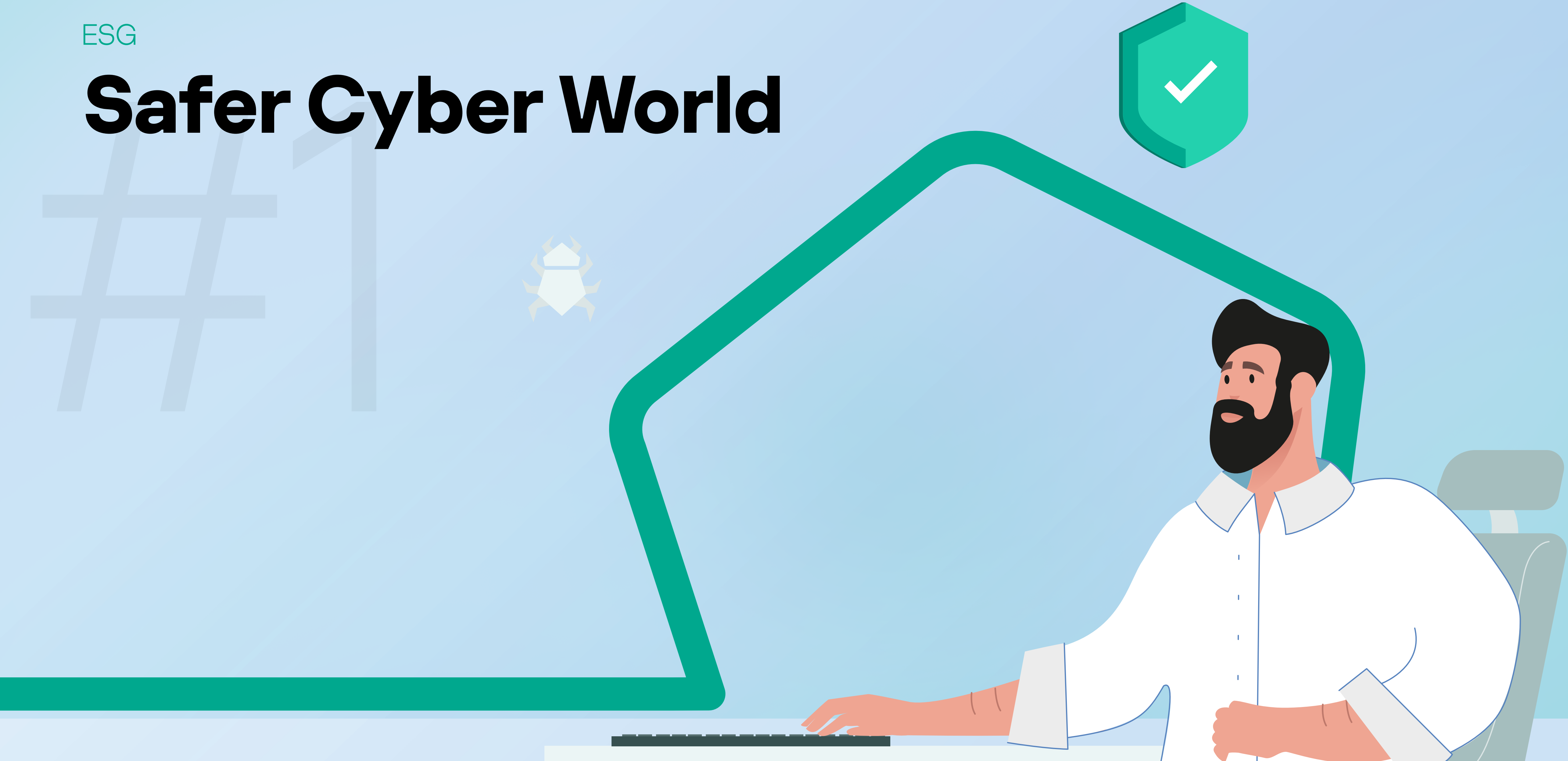
Kaspersky's senior executives and department heads are responsible for managing the Company's sustainability risks. During the reporting period, Kaspersky identified three key ESG risks: changes in the political and economic sphere as well as legislation in the regions of the Company's presence, rise in cybercrime and supply chain disruptions.

Key ESG risks

Risk	Why the risk is important	Risk management measures in 2022 and 2023
Changes in the political and economic sphere as well as legislation in the regions of the Company's presence	Possible changes in legislation could significantly limit the Company's ability to do business in the country/region of presence.	■ Regular monitoring of changes to legislation in the countries/regions where the Company operates in order to promptly identify potential risks. ■ Membership of the Company and its experts in various industry organizations to take part in communications with the regulatory authorities. ■ Participation in public consultations held by the government authorities in countries/regions where the Company operates on projects to amend existing regulations or introduce new ones in order to promote the Company's position. ■ Further development of the Global Transparency Initiative (GTI) in order to verify the reliability of the Company and its products for corporate customers, partners and regulators.
Rise in cybercrime	The level of cooperation between law enforcement agencies and private companies in different countries is diminishing in the current environment. To prevent a surge in cybercrime, it is crucial to maintain cooperation and exchange expertise with the private sector.	The Company continued to actively cooperate with law enforcement agencies and international organizations during the reporting period: ■ Assisted INTERPOL in conducting operations Africa Cyber Surge in November 2022 and Africa Cyber Surge II in August 2023, aimed at disrupting and combating cybercrime in African countries. ■ Organized training on incident response and malware analysis for more than 100 representatives of law enforcement agencies from various countries under the auspices of INTERPOL. ■ Took part in the INTERPOL International Cybersecurity Conference. ■ Participated in preparing feedback and proposals for the draft Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is currently being developed under the auspices of the UN. ■ Signed memorandums of understanding with several national regulators in the field of cybersecurity.
Supply chain disruptions	Geopolitical changes could cause disruptions in supply chains and have a negative impact on the Company's business and performance.	We ranked our services based on the level of their importance to business continuity and impact on results. Even though we assess the risk of supply chain disruptions as low, we have undertaken measures to mitigate this and switch to using new services and platforms, including: ■ Phasing out imports of software, systems, equipment and services. – Transition from CRM Sales Force to the Russian Bitrix platform. – Purchase of equipment from a Russian certified vendor. ■ Modifying logistics for the procurement of key components and replacing suppliers who were unable to provide equipment, software and services or were not willing to continue cooperation. ■ Transferring technical support and infrastructure services to other regions of the world.

ESG

Safer Cyber World



Digital security

Our goal is to protect users against cyberthreats with Kaspersky's products and initiatives.

In today's digital society, technology is ingrained in people's daily lives, with the number of cyberthreats constantly on the rise as a result. You may be exposed to danger while performing simple actions such as exchanging messages, downloading photos, or transferring money online. Threat actors are improving their attack methods as they invade people's personal lives. We are committed to protecting users' interests in the digital realm and making it a place where everyone feels safe.

Kaspersky solutions

>411,000
malicious files detected daily in 2023

33,790,599
malware, adware, and riskware attacks blocked in 2023

~125 million
malicious files found from January to October 2023

135,980,457
malicious email attachments blocked in 2023

>437 million
malware-class attacks blocked from November 2022 to October 2023

709,590,011
attempts to click on phishing links thwarted in 2023

How we protect users against cyberthreats

To counter cyberthreats, we create high-quality products and promote awareness by teaching users the basics of digital literacy and the fundamentals of cybersecurity for corporate clients.

TC-SI-230a.2

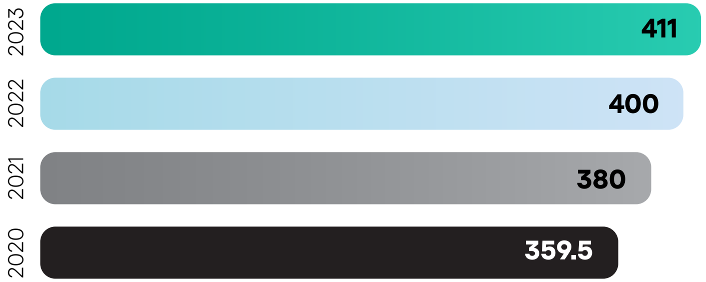
Our solutions protect users against a wide range of cyberthreats, from online fraud to data leaks and targeted cyberattacks. To gain control of computer systems, hackers use various types of malware:

- **Viruses.** Programs that infect files with malicious code. They replicate themselves to spread throughout a computer system.
- **Trojans.** Programs that perform actions that are unauthorized by the user: they destroy, block, modify or copy information, and disrupt the operation of computers or computer networks. One of the key differences between this type of malware is its inability to self-replicate. The first Trojans appeared in the late 1980s and fully lived up to their name, posing as legitimate software.
- **Spyware.** Programs that secretly monitor a user's actions and collect information that hackers can use for their own purposes.
- **Ransomware.** Software that encrypts files and data on a user's computer, after which hackers demand a ransom to restore access to information, claiming that otherwise the user will lose their data. Attackers may also threaten to make compromised data publicly available.
- **Adware.** Advertising-supported software that can create problems on a user's device.
- **Botnets.** Computer networks infected with malware that hackers use for their own purposes.

Users and companies can also fall victim to phishing, scams, phone fraud and DoS attacks.

The modern world has seen a significant increase in the number of cyberthreats as digital technology and the internet evolve. The number of malicious files is growing each year: whereas in 2020 we detected about 360,000 new malicious files per day, in 2023 this figure was already up to 411,000, a 3 percent increase from the year before.

Number of malicious files detected daily by Kaspersky, thousand



Combating cyberstalking

# Objective

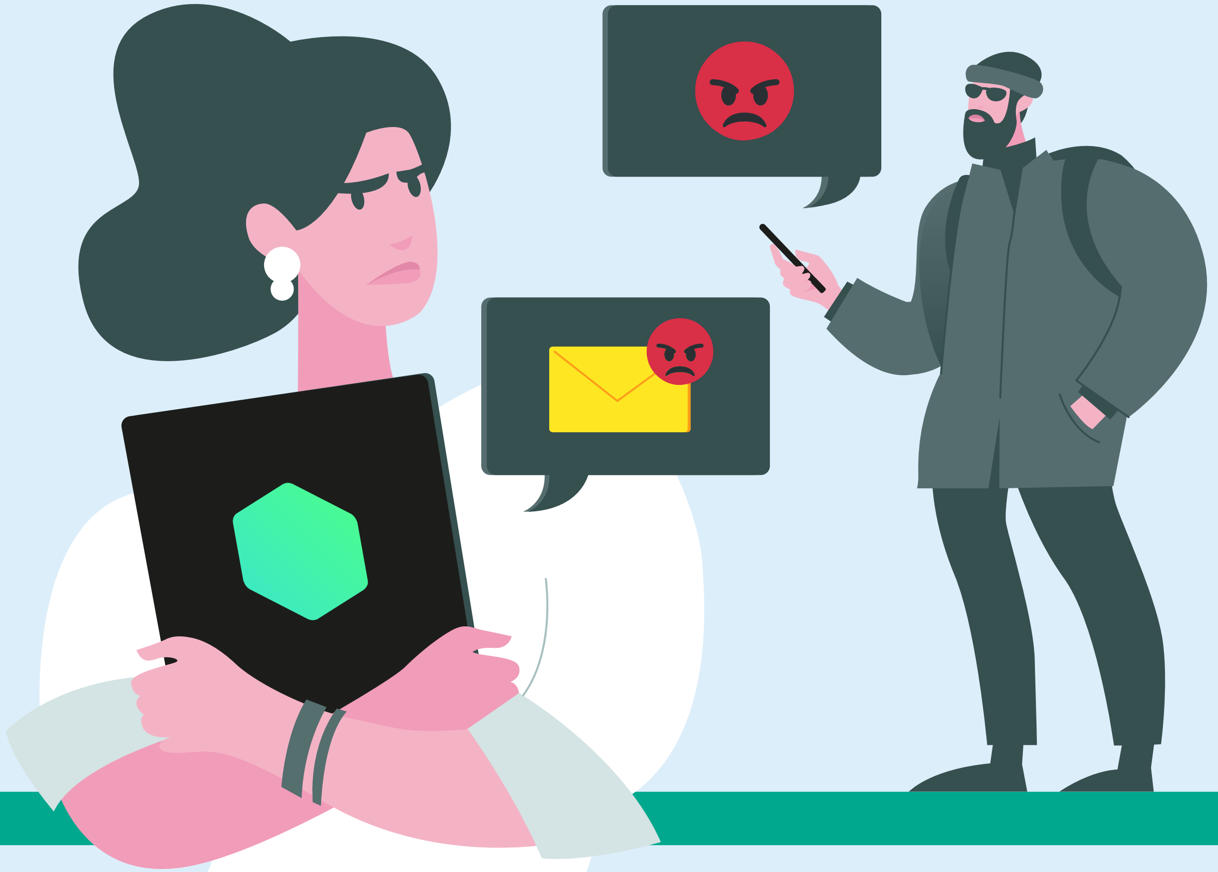
Protect users against digital harassment

Our research shows there has been a steady increase in the number of attacks using digital surveillance software, otherwise known as stalkerware. In 2023, the victims were most often residents of Russia, Brazil and India, but in general this phenomenon has spread throughout the world.

Stalkerware is commercially available software that can be discreetly installed on smartphone devices, enabling perpetrators to monitor an individual's private life without their knowledge. It isn't solely a technical issue; it's also a social problem requiring input from all parties involved in the digital realm to be effectively addressed. We notify users about this threat through our products, including Kaspersky for Android, which offers a solution to protect smartphone data and warn users about the detection of stalker applications on their device. We are also working to address the problem of cyberstalking by partnering with non-profit organizations, industry experts, research companies and government agencies worldwide to offer the TinyCheck digital surveillance tool.

>31,000

users worldwide experienced cyberstalking in 2023 (+5.9% vs. 2022)



# Solutions

GRI 203-1

Take part in projects to protect users against stalkerware

In 2019, Kaspersky co-founded the Coalition Against Stalkerware, an international working group featuring IT companies, non-profit organizations, research institutions and law enforcement agencies, which seek to combat stalkerware and domestic violence.

Today, the coalition includes more than 40 organizations that share their expertise in domestic violence survivor support and perpetrator work, digital rights advocacy, and cybersecurity to address the criminal behavior perpetrated by stalkerware. Users who suspect they are being spied on via a mobile device can seek help on the Coalition's website, which is available in seven languages.

>40

organizations have joined the international Coalition Against Stalkerware co-founded by Kaspersky

Kaspersky also works with the European Network for the Work with Perpetrators of Domestic Violence (WWP EN). In September 2022, we launched the global campaign #NoExcuse4Abuse, which aims to raise public awareness about how people in relationships abuse technology. We believe it is important to refute the myths surrounding this issue and help victims recognize the signs of possible digital abuse. The campaign resulted in the release of comics that show examples of inappropriate behavior in relationships disguised as "caring". The project's main goal is to challenge the arguments and justifications used by abusers in order to deter them from committing violence against their partners.

78,100

reach of the #NoExcuse4Abuse campaign

Organize research and educational projects against cyberstalking

Kaspersky together with various international companies, the academic community and non-profit organizations is taking part in the study on how to protect victims/survivors of Intimate Partner Violence (IPV) from the risks created by digital technologies together with various international companies, the academic community and non-profit organizations. To participate in this joint study, we have formed a partnership with the UK research and innovation agency UKRI.

The project was launched in 2023, and will continue until 2026. Kaspersky provides support with its expertise in combating cyber violence and stalking, and by participating in additional events.

Notify users about the threat of cyberstalking

Our Company was among the pioneers in the industry to alert users about its solutions for detecting stalkerware on their devices.

In June 2022, Kaspersky launched a portal about TinyCheck, a free and secure open-source tool for non-profit organizations and police departments that work with victims of digital stalking. This solution is installed on a separate external device – a Raspberry Pi microcomputer – instead of a smartphone. TinyCheck can view outgoing internet traffic, analyze it in real time and recognize connections to the control centers of stalkerware developers. At the same time, the solution does not allow the initiators of surveillance to learn about such checks.

In 2022, we expanded our privacy notification functions as part of the launch of a new line of solutions to protect users' digital lives. TinyCheck users now receive a warning not only regarding the presence of stalkerware on their device but also about the potential consequences if they choose to delete the application. This could potentially escalate the situation by alerting the individual who installed it. In addition, the stalking victim should be aware that by deleting the app, they risk deleting important data or evidence that could be used by law enforcement.

DeStalk

From 2021 to 2023, Kaspersky partnered with the DeStalk project, which was launched as part of the EU Rights, Equality and Citizenship program. The project brought together five partner organizations, cybersecurity experts and representatives from research institutions, public organizations and the government.

As part of the DeStalk project, we trained more than 350 professionals who provide assistance to female victims and deal with issues of violence, as well as government officials. They learned effective methods to combat cyberstalking and how to counter other forms of digital gender-based violence. We have also worked hard to provide a wider audience with information about digital violence and how to hinder it.

More than **350** practitioners

addressing gender-based violence were trained as part of the DeStalk project

DeStalk e-learning

As part of the DeStalk project, Kaspersky has developed an electronic training course called The DeStalk e-learning on how to recognize and combat cyber violence and stalkerware in five languages. The goal of the course was to train 80–100 professionals from 20–30 different organizations, including:

- Professionals working with victims/survivors of cyberviolence and stalkerware
- Professionals working with perpetrators of domestic violence
- Public officers working in the field of domestic abuse

The course consisted of four lessons, including theory and testing focused on gender-based cyber-violence, different forms of cyber violence, the topic of cyber-surveillance and stalkerware, working with victims and survivors of violence and/or perpetrators. The electronic course is available on the DeStalk website.

130 people

passed the DeStalk e-learning course

Protection against ransomware

# Objective

Combat ransomware

Our data shows that ransomware attacks are becoming more sophisticated and are causing extensive harm to both companies and users. Targeted (and more complex) attacks on businesses – both enterprises and small and medium-sized businesses – are particularly dangerous. Organizers of targeted attacks carefully select their targets – governments, specific organizations or individual groups of people within a particular enterprise.

Ransomware has remained one of the most pressing cyberthreats of recent years, with attacks becoming increasingly sophisticated. Between November 2022 and October 2023, ransomware Trojans attacked 193,662 unique users, including 52,999 corporate (enterprise) users and 6,351 users from small and medium-sized businesses.

In 2022, Kaspersky discovered two new ransomware cybergroups – RedAlert and Monster. Most recently, their main goal has been to damage as many systems as possible by simultaneously adapting their malicious code to multiple operating systems. In addition, from July to September 2022, we detected two waves of attacks that affected Albanian government e-services using ransomware and wiper malware. The hackers used stolen Nvidia and Kuwait Telecommunications certificates to sign their malware.

Kaspersky solutions

Detected over

74.2 million

attempted ransomware attacks (+20% vs. 2021)

Identified

23,364

ransomware modifications and detected 43 new families from November 2022 to October 2023[1]

Prevented ransomware attacks on the computers of

193,662

unique users from November 2022 to October 2023

[1] Source – https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/28102415/KSB_statistics_2023_en.pdf.

# Solutions

Develop products to protect against ransomware

Kaspersky has developed and published a set of recommendations for users who want to protect themselves and their business against ransomware attacks. Users benefit from our products, which have proven to be highly effective in protecting against ransomware in tests[1]. In particular, three Kaspersky solutions – Kaspersky Endpoint Security for Business, Kaspersky Small Office Security and Kaspersky Standard – successfully passed all the tests, earned 35 out of possible 35 points and earned "Advanced Approved Endpoint Protection" certificate for business security solutions and "Advanced Certified" for consumer product.

Provide the latest cyberthreat intelligence

Kaspersky offers awareness services about modern cyberthreats that will help any organization effectively counter them. Kaspersky Threat Intelligence provides up-to-date technical, tactical, operational and strategic threat intelligence from our world-class analysts and researchers. This has helped Kaspersky become a trusted partner of law enforcement and government organizations around the world, including INTERPOL and various CERT units.

You can request access to this service here.

158
global press releases on cyberthreats were issued by the Company during the reporting period

In addition, the Company regularly conducts special research and surveys, which helps to inform users about the cyberthreats that they may face in real life without even suspecting it. During the reporting period, we shared our findings on:

- Vulnerabilities in popular smart pet feeders, which enable hackers to turn the feeder into a surveillance tool and change the feeding schedule, thereby jeopardizing the pet's health.
- An online fraud scheme that targets pet owners who want to buy imported medications for their pets. Using Telegram channels, scammers defraud people of money and financial information.
- Tourist traps during the summer holidays. Travel experts and cybersecurity specialists warned users about three different scams involving tickets, accommodation and surveys.
- A new campaign to steal cryptocurrency through a fake Tor browser. Under the guise of the Tor browser, hackers distribute the CryptoClipper Trojan on third-party internet resources. When users log into the system, they register in autostart, which is disguised as the icon of a popular app, for example, uTorrent. As soon as the clipper malware finds an address in the clipboard that looks like a crypto wallet, it immediately changes it to an address that belongs to the hacker. More than 15,000 users in 52 countries were affected by the malware campaign.
- Technologies that create deep fake videos. Kaspersky experts discovered that the darknet offers services to create such videos for as much as US$20,000 per minute. Deepfakes can be generated for various purposes, including scams, political manipulation, revenge and cyberbullying.
- Operation Triangulation – a zero-click attack targeting Apple mobile devices via iMessage to run malware gaining complete control over the devices and user data. The final goal was to hiddenly spy on users.
- The latest spam and phishing attacks: statistics and pathways that threat actors exploited in 2023 in a new report.

In addition, we created educational videos to talk about crypto phishing, participated in a webinar on cryptocurrency threat landscape trends in this regard and also published our own research on this topic.

[1] The AV-TEST was conducted in August 2023.

How we uncovered Operation Triangulation

Working together against spyware

In early June 2023, Kaspersky researchers discovered a previously unknown mobile APT campaign targeting iOS devices, which was later named Operation Triangulation. The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data.

Experts found that the embedded spyware transfers information from the victim's device to remote servers without being noticed. The attackers were interested in the owner's microphone recordings, photos from instant messengers, geolocation and data about other actions.

"I have some big news about a cyber-incident we've uncovered. Our experts have discovered an extremely complex, professional targeted cyberattack that uses Apple's mobile devices," **Eugene Kaspersky** wrote in his blog.

If a user is blocked from updating iOS, this is an indirect sign that the Triangulation malware has infected a device, Kaspersky said.

Find out more about Operation Triangulation and how to check your iOS device on Securelist.

What was the result?

We published a comprehensive guide on how to manually check iOS device backups for possible indicators of compromise using the Mobile Verification Toolkit.

Kaspersky developed the free triangle_check utility for computers running Windows and Linux operating systems, which can be used to check if an iPhone is infected with Operation Triangulation malware. To check for the malware using this utility on Windows and Linux, just download the binary assembly, while on macOS you can install it as a Python package.

Apple acknowledged the problem and released updates that eliminate the vulnerabilities.

GRI 203-1

NO MORE RANSOM

To combat malicious actors Kaspersky together with Europol, the Dutch National Police initiated the creation of the No More Ransom initiative in 2016. The initiative provides decryption tools, educates the public about ransomware risks and promotes cybersecurity best practices to counteract this pervasive cyber threat.

Our contribution to the No More Ransom initiative

Working together against ransomware

360,000
downloads of Kaspersky's free decryption tools

39
ransomware families targeted

2 million
victims were able to decrypt their data

The international No More Ransom initiative, co-founded by Kaspersky, provides decryption tools, educates the public about ransomware risks, and promotes cybersecurity best practices to counteract this pervasive cyberthreat.

This initiative represents a unique partnership between governments, law enforcement agencies, antivirus companies and educational institutions.

In March 2023, Kaspersky released a new version of the decryption tool to help victims of ransomware modifications based on previously leaked Conti code.

What was the result?

Our joint efforts have made the digital environment safer, helping hundreds of thousands of users and reducing the overall threat level in the online world.

Kaspersky's free decryption tools, which are available as part of the No More Ransom initiative, have been downloaded more than 360,000 times in the last five years. They can be used to decrypt files locked by 39 ransomware families. These tools provided victims with the means to recover important data without having to comply with the cybercriminals' demands. No More Ransom recently celebrated an important milestone, as more than 2 million users were able to recover data thanks to the initiative.

Training users on the basics of cybersecurity

# Objective

Provide users with self-defense tools

Being able to ensure your own online security is becoming a fundamental skill for individuals in the modern world. By teaching our users the basics of cybersecurity, we are able not only help them recognize potential threats, but also provide them with the tools to protect themselves. In doing so, we are investing in a secure digital future for everyone.

# Solutions

Kaspersky Academy

>8,000

students studied at Kaspersky Academy in 2022–2023

Back in 2010, we launched Kaspersky Academy to scale educational initiatives and make them accessible to everyone. We planned to turn the portal into a global university, able to house all the educational materials related to information security, and managed to implement this project.

At present, Kaspersky Academy speakers include the Company's department heads, leading industry specialists and invited information security experts. In 2022–2023, more than 8,000 students from Russia, Europe, Saudi Arabia, Rwanda and other countries were trained at Kaspersky Academy.

Advantages of Kaspersky Academy:

- It is one of the ways to gain access to content from the Education.kaspersky.com platform.
- It is adapted to two product formats:
  1. Video lessons + tests + certificate.
  2. Video lessons + live broadcasts + tests + final test + certificate.
  3. Online workbook format with auto-check + certificate.
- It allows to track students' results – both intermediate and final.
- It notifies students about upcoming webinars.
- It can quickly customize the training format and collect analytics to suit the customer's needs and project.
- It can manage the duration of students' access to the platform.

Courses launched in 2023:

- "Cybersecurity. Entry level". An updated flagship course for the Russian-speaking audience, which examines all the main aspects of information security. The course targets both IT specialists and students, as well as private users.
- "Cybersecurity for Senior Executives". The course gives students an understanding of cybersecurity as a system and shows how cyber risks affect businesses and how they can be managed.

Key Academic Affairs projects for school and university students in 2023:

SafeBoard offers 15+ areas for IT internships (more than 500 students have enrolled in the program since 2016). Over the eight years this program has existed, more than half of its participants have joined the Company's staff and are now employed, including those at the middle, senior and lead levels

Secur'IT Cup – an annual international competition of student cybersecurity projects (30+ participating countries and more than 2,000 applications from students each year)

Technology Valley – a summer internship for school and college students in Russia (more than 1,200 people registered in 2023 and 45 participants completed in-office internships)

Cyber Generation – a training program for students and recent graduates of Saudi Arabia (91 participants)

Kaspersky Academy Alliance – a special program for universities that integrates cybersecurity expertise and the latest Kaspersky technologies into the student learning process

We work with:

~200 universities

in **42** countries

>60 educational institutions in Russia and the CIS.

Cybersecurity training for non-profit organizations

GRI 203-1

Cybersecurity is crucial for the effective operations of non-profit organizations (NPOs), which rely heavily on digital technologies. Kaspersky regularly conducts training for NPOs to improve their level of protection against constantly evolving online threats. These partnerships help create a safer and more sustainable digital future for everyone.

In 2022–2023, we organized the following training for NPOs:

- **Cyberstalking.** Our leading information security threat researchers conducted two training sessions on the problem of cyberstalking: for the 'Blagie Dela' (Good Deeds) Foundation from Kazan and the Nizhny Novgorod Women's Crisis Center, which provides free psychological and legal support to people dealing with violence and abuse. We also trained the Nizhny Novgorod Women's Crisis Center, on how to use the free open-source tool TinyCheck, which can detect surveillance software installed on a device without notifying the stalker.

- **Doxing**[1]. Together with the Singapore Council of Women's Organisations[2], we held a free seminar on combating doxing. Our experts explained how people can reduce the risks of their personal data being misused and protect their own and other people's personal data, introduced the participants to reliable security software and revealed the possible motives of hackers.

- **Cyber-hygiene.** In partnership with the todogood social change platform, we conducted an intensive online course about cyber hygiene as part of the "I Can" program for vulnerable social groups, including women in difficult life situations, people with disabilities and older people. The program's goal is to support individuals in professional retraining, adjusting to online learning and work, navigating socio-cultural shifts, and adopting new technologies. A total of 946 people took the recorded and online intensive course, passed the test and received certificates.

We have also created several cybersecurity projects in partnership with international organizations. In particular, in March 2023, we launched the Kids' Cyber Resilience Project, which aims to educate children on how to keep themselves safe online while helping them build resilience internally in the Asia-Pacific region. This project involves multiple stakeholders, including parents, educators, students, non-profit organizations and government representatives.

- Together with the Center For Cybersecurity, a Singapore-based cybersecurity training organization, and The HEAD Foundation, an international charitable organization that does philanthropic work in education, Kaspersky launched its global **Kids' Cyber Resilience Project** in Singapore with a panel discussion on how a collaborative and proactive approach to online security can benefit children in digital environment.

- **Online seminars on cyber-resilience** were held for educators in the Asia-Pacific (APAC) region in partnership with the Coalition Against Bullying for Children & Youth (CABCY). As part of a series of webinars, we examined the topic of bullying and cyberbullying in more detail. The CABCY helped participants learn more about this complex issue and understand the role of adults in supporting children.

- **Face-to-Face.** A cyber-resilience workshop on basic cyber hygiene for educators from 71 public schools in Valenzuela City was held in September 2023 in collaboration with the Philippine Department of Education Schools Division Office. The workshop aimed to provide teachers with knowledge to effectively help their students become cyber-resilient.

- **Cyber Resilience Day.** In collaboration with Majlis Bandaraya Petaling Jaya (MBPJ) in Malaysia, Kaspersky co-presented an introductory cybersecurity awareness and resilience training session for more than 250 PJ Secondary School learners from 10 public schools. The program aims to educate the participants on how to keep themselves safe online while helping them build resilience internally.

- **Cyber security workshop in India.** In partnership with the Information and Security Analysis Center (ISAC) Foundation, Kaspersky teamed up to deliver a workshop on cyber security hygiene, Indian cyber laws, and dealing with various forms of cybercrimes. Approximately 150 teachers from more than 30 schools participated in the event, which aimed to increase their confidence to share cyber resilience practices with their students as well as improve their capacity to support children to recover from setbacks.

[1] Doxing is the practice of publicly disclosing personal information about people on the internet without their consent.

[2] The Singapore Council of Women's Organisations (SCWO).

Our contribution to improving cyber-hygiene awareness

A podcast aimed at educating people on safeguarding themselves from digital threats

The podcast Change Your Password! is a talk show on various issues surrounding information security hosted by journalist and writer Alexey Andreyev, Kaspersky Chief Security Expert Sergey Golovanov and Kaspersky Chief Technology Expert Alexander Gostev.

The podcast has been airing since 2021 and has – so far – had three seasons. It can be found on every popular podcast platform including Apple Podcasts, Yandex Music, Google Podcasts, VK, Castbox, YouTube.

The hosts of the Change Your Password! podcast discuss key issues in the world of digital security and help listeners understand the impact of current cyberthreats on users and businesses.

- Where is personal data leaked?
- Why is the Internet of Things dangerous?
- Does artificial intelligence offer protection or pose a threat?

Hosts and guest experts from other industries (banking, e-commerce, communications, etc.) provide answers to these and many other questions.

In autumn of 2023, an open recording of the Change Your Password! podcast became the first face-to-face event of the Cryptography Museum Discussion Club. Experts discussed how Russian codes differ from foreign ones, what cryptographic protection modern people need, why quantum computers resemble “apple trees on Mars,” and also answered numerous questions from listeners.

What was the result?

The podcast was listened to

>400,000 times

over three seasons

Over three years, the podcast has evolved into a primary outlet for the most up-to-date information concerning digital threats. Today, Change Your Password! helps listeners create a safer online space for themselves and their businesses.

- The third season of the podcast had been listened to more than 100,000 times as of the end of 2023, and the podcast has been listened to over 400,000 times in total.
- Since 2022, Change Your Password! has regularly been among the top podcasts about technology on Apple Podcasts, as well as in thematic selections from leading media outlets.

Ensuring children's online safety

# Objective

Protect children in the digital world

For several years in a row, the Company has consistently conducted surveys on children's online safety to grasp the impact of the internet on kids, their interests and the potential challenges they may face online.

The 2022 survey conducted by Kaspersky in major Russian cities[1] showed that 77 percent of children aged seven to 10-years-old had been introduced to gadgets before starting school. A new survey conducted by the Company in 2023 revealed that the overwhelming number of primary school students (88%) now have their own phone or tablet. Almost every high school student has his/her own gadget. Starting from middle school, a significant percentage of children spend almost all their free time on gadgets. Parents are concerned about who their children interact with online, whether they encounter aggression and what sites they visit.

88%

of primary school students have their own phone or tablet

Over the past year

55%

of children have come across violent videos or videos with adult content online

29%

of parents do not know what information about their children is publicly available online

> "To safeguard children from a diverse range of online threats, a combination of both technical and non-technical protective measures is required. The technical measures include special settings, such as family accounts, parental control programs, antivirus programs and automatic caller ID. Non-technical measures include constant attention to digital awareness, including information security issues. It is crucial to teach children the basics of digital hygiene from a very young age. Over time, this will become more effective than parental restrictions alone."

Andrey Sidenko,
Lead web content analyst and expert on children's online safety, Kaspersky

[1] More than 1,000 pairs of parents and children took part in the survey.

# Solutions

Teach children the basics of cybersecurity

Creating a safe online environment for children is a top priority that will shape our future. Kaspersky is addressing this challenge both on its own and in partnership with relevant ministries, agencies and other international organizations.

To understand how the internet influences young users, what they are interested in and what troubles they may encounter online, Kaspersky has been conducting surveys and studies on children's online safety for several years in a row. Below are a few of them that were presented during the reporting period.

- **"Adults and Children on the internet"** is a series of surveys on children's online safety and a report with the same name. In 2022, Kaspersky commissioned a survey that was conducted by the Online Interviewer company in May–June 2022. The company arranged a total of 2,008 online interviews with 1,004 pairs of parents (or single parents) and children aged three to 18-years in major Russian cities. The survey topics were selected to reflect the situation in various areas of online life. The results, along with comments from a Kaspersky expert on children's online safety, helped adults better understand the interests of young users and showed what needs to be done to make the digital world safer for them.
- **A new survey on children's online safety**. In May–June 2023, Online Interviewer specialists conducted a new study for Kaspersky to find out the latest about children's online safety. They conducted 2,032 online interviews (with a total of 1,016 pairs of parents and children), which revealed the following statistics:
  - 29 percent of parents do not know what information about their children is publicly available on the internet;
  - More than half (55%) of children said they have seen violent videos or videos with adult content on the internet over the past year;
  - A third of parents want their children to work in IT when they grow up, while the share of children who would like to work in this industry in the future is even higher (41%);
  - 30 percent of parents surveyed in Russia are concerned about the problem of children's internet addiction, while more than half of parents (54%) believe that children nowadays are addicted to gadgets and the internet;
  - Most children spend more than an hour a day on the internet starting from the age of seven;
  - More than half of parents (53%) are confident that in 10–15 years touch screens and blackboards will replace the usual teaching tools in schools, 39 percent noted that tablets will replace textbooks and 37 percent believe that voice assistants will be used in teaching in the future.
- **Kids on the web 2023.** Kaspersky regularly conducts global research on children's online safety based on anonymized statistics collected by the Kaspersky Safe Kids solution. The report for 2023 examines the categories of websites that kids visit most often across various platforms, the apps they spend the most time on, and what specifically piqued their interest during the period from May 2022 to May 2023.

We also organized several educational events and projects on cybersecurity for schoolchildren, teachers and parents during the reporting period.

- **"Mom, I'm Going To Be a Blogger!"** In June 2022, Kaspersky launched its own online interactive mini-series called "Mom, I'm Going To Be a Blogger!", 10 two-three minute long video episodes released in 2022. The series, along with the main character Mila, taught children how to safely record vines, avoid scammers, how to distinguish a phishing site from a real one and why it is important to follow netiquette rules on the internet.
- **"Digital Lesson".** In 2022 and 2023, Kaspersky continued taking part in the project "Digital Lesson" conducted by the Digital Economy autonomous non-profit organization with the support of the Russian Ministry of Education and Ministry of Digital Development. In 2022, we also made a series of lessons dedicated to researching cyberattacks, while children were taught about the issues surrounding mobile security in 2023. The latter course was completed more than two million times by learners from grade one to 11. They learned what types of malware exist for mobile devices, how to protect their data on the internet and were also introduced to various cybersecurity professions.

→ For more about the project, please see p. 104

- **"Digital Outreach".** Kaspersky and the Digital Economy autonomous non-profit organization, with the support of the Russian Ministry of Education and Ministry of Digital Development, created a series of short cartoons for children about digital security and privacy. In 2023, this series was added to the useful materials supplement of the national educational project "Digital Outreach".
- **Cybersecurity course for schoolchildren.** In October 2023, Kaspersky gave access to the online course "Information Security Basics" for seventh grade children. The course for learners in grades 8–11 will be available in the near future. It is a practical course that can be used by teachers in computer science classes and as part of extracurricular activities, as well as by parents and learners themselves.
- **Educational events for school children and teachers in Russia and the CIS.** In 2022–2023, more than 150 online and offline events were held for school children and teachers at secondary schools, as well as for parents in 26 regions of Russia and the CIS.
- **Kaspersky Safe Family Spain.** Kaspersky conducted cybersecurity lessons via a special puppet theater play for more than 16,000 Spanish children through its Familia Segura program. It includes the "Kasper, Sky and the Green Bear" initiative, which also aims to improve the cyber awareness of teachers and parents.
- **#ShareAware Hub.** Kaspersky helps parents and children improve their online safety with various tips. The hub provides lots of useful materials, quizzes, research and advice on how to use multimedia on the internet and avoid digital threats.
- **Kids on the internet.** An online safety course developed by Kaspersky. It helps parents to safeguard their children online and build trust. Kids get acquainted with digital literacy and gain online communication skills. It is also intended for anyone who uses the internet and wants to protect themselves and loved ones from modern mobile threats.
- **Hacker:HUNTER.** The Company took part in the production of a series about real cyber incidents. A new season was released in 2023, showing how cybercriminals get children involved in their activities and turn them into hackers, and how law enforcement agencies are combating this issue.
- **Cybersecurity Alphabet.** To help improve the digital awareness of children and their parents, the Company's experts prepared a fun and informative book and poster for children and their parents on how to recognize fraudsters' tricks and learn the importance of staying safe online. The book uses an A to Z approach to introduce readers to new technologies, common cyber risks and tools to protect themselves against them. Cybersecurity Alphabet is available in English for anyone to download on the Company's website. The book and poster will also be available soon in Spanish, Italian, French and Russian.

Cooperate with IT companies and regulators to protect children online

We strive to make the online space for children as safe as possible. Kaspersky is one of founders of the Alliance for the Protection of Children in the Digital Environment, which was created by Russia's largest IT companies in September 2021.

In 2022, Kaspersky, Yandex and VK launched a pilot project as part of the Alliance to identify and block content related to the distribution of child pornography, as well as so-called sexualized content involving minors.

In October 2023, the Alliance held a road show in Kazan called "Your Route Is Ready: Online Safety Paths". At this event Kaspersky shared the results of a study showing that the majority of parents in Russia (87%) are taking measures to protect their children from dangers on the internet. However, it also showcased that only 48 percent of adults themselves follow all the prescribed rules, which reduces the effectiveness of these measures. Our experts reminded parents of the need to be a good example for their children and compiled a checklist with recommendations on what to look for when choosing an appropriate parental control solution.

In December 2023, the Alliance hosted a two-day educational marathon called "Safe Digital" in St. Petersburg, which focused on the guidelines for maintaining online safety. The event was mainly attended by children and teenagers, who had a chance to take part in an IT quiz, special training sessions, roundtables and seminars while parents and teachers discussed digital safety issues. A business program was also organized with IT experts and representatives of the government, business and public organizations. The marathon was attended by the Alliance's founders.

Kaspersky Safe Kids

We are dedicated to safeguarding children from online threats and creating an environment where they can use the internet as safely as possible. To achieve this, we offer our solution Kaspersky Safe Kids – a parental control application that protects children against age-inappropriate content and helps form good digital habits. There is also a free version of this solution available.

Main functions of Kaspersky Safe Kids

Search safely
The application works with search engines and blocks unwanted requests. Once a week, parents receive reports about what their child was searching for online.

Control usage of the application
The basic function blocks applications that are not suitable for children. Usage is also time controlled (you can set time intervals and assign days off).

Control screen time
The application can set the specific number of hours of screen time allowed per day and lock the device if the limit is reached. You can also turn off the device at specific times.

Set a secure perimeter
Thanks to the GPS option, the application sends a notification to parents if their child leaves a designated location (e.g., school).

Monitor potentially dangerous contacts on social media
Parents cannot read their child's messages, but the application notifies them about any correspondence and allows them to see the profile of the person with whom their child is messaging.

In 2023, we updated the Kaspersky Safe Kids solution twice. The new versions have an improved design and interface, new functions for managing screen time, videos with tips on raising children, an easy functional configuration and other useful information for parents. The application can be installed on desktops and mobile devices with all popular operating systems. Children can now request more time from their parents to use the device, and all parents have to do is approve or deny the request.

7 AV-TEST certificates

7 AV-Comparatives certificates

>1 million downloads worldwide

106 million harmful websites blocked

Kaspersky Safe Kids testing results

The report released by the independent laboratory AV-TEST in December 2022 indicates that Kaspersky Safe Kids blocked:

- 92% in Windows for potentially inappropriate websites (up from 90% in 2021);
- 87% in Android for for potentially inappropriate websites tested (85% in 2021);
- Almost 100% of the most undesirable category "Adult Content" content is blocked on Windows.

Our contribution to protecting children in cyberspace

Teaching cybersecurity with the “Kasper, Sky and the Green Bear” puppet show

The number of children who use digital technologies is constantly on the rise. At the same time, there are new forms of digital threats spreading throughout cyberspace that are especially dangerous for children due to their lack of experience and knowledge about the threats lurking there. Cyberbullying, sextortion and other types of harassment have become daily problems for children and teenagers, which is why Kaspersky has made it our mission to protect them in the online world.

As part of the Safe Family program, the Company launched the “Kasper, Sky and the Green Bear” initiative in Spain, an adaptation of Marlies Slegers’ book for children aged six to nine years, which introduces them to the digital world and teaches them how to use the internet safely. Kaspersky turned this book into a puppet show that not only educates children, but also seeks to inform teachers and parents that cyberthreats are much more than just a simple virus today.

Thanks to Kaspersky’s efforts, thousands of children, teachers and parents have learned how to use the internet safely. In addition, the “Kasper, Sky and the Green Bear” campaign received the following accolades at the Social Enterprise Awards 2019:

- Best responsibility project for the protection of children
- Best social responsibility project in the field of cybersecurity
- Best responsibility project in the fight against bullying

In addition, Gala Acción Social presented an award to Kaspersky with the distinction “Company with the Best Actions To Protect Children.”

What was the result?

Since its premiere in October 2018, the play has been performed in

106

Spanish schools,

with

146

performances

staged to

16,805

students

35

performances took place during the 22/23 school year,

reaching

3,684

students.

Our achievements

Kaspersky was recognized at the Social Enterprise 2023 awards for its work to combat digital gender-based cyberviolence exercised through stalkerware. The Company received awards in the following categories: “Best Corporate Social Responsibility in the Cybersecurity Sector”, “Best Initiative for the Prevention of Gender-based Violence in the Cybersecurity Sector” and “Best Internet Security Project in the Cybersecurity Sector”. In addition, the organizer of the Gala Acción Social awarded Kaspersky the “Special Prize for the Company with the Best Cybersecurity Initiatives” and “Platinum Company and Company of the Year”.

Our plans for 2024

- Develop partnerships to combat stalking with international law enforcement organizations, coalitions and non-profit organizations;
- Release a new report on the current state of stalkerware;
- Launch a course on cyber hygiene in two languages;
- Conduct the Kids Cyber Resilience project in the CIS and META[1] regions;
- Release an analytical report on children’s online safety with survey data for 2023;
- Publish the Cybersecurity Alphabet and poster in Russian, Spanish, Italian and French.

[1] Middle East, Turkey and Africa.

Combating cybercrime

Our goal is to protect the world against cybercrime. Effectively combating cybercrime requires the joint efforts of the entire community, so we cooperate with law enforcement agencies and help improve legislation in this regard.

Key documents

- Kaspersky's internal policy governing work with requests from law enforcement agencies[1] (approved in September 2021 by the Company's senior executives);
- Agreement with INTERPOL on jointly combating cybercrime;
- Memorandums of cooperation with various cybersecurity and law enforcement agencies.

How we work with law enforcement agencies

Threat actors or hackers most commonly commit cyberattacks for financial gain. However, their motives can also be personal or political. Cybercrimes are committed by individuals and organizations that use advanced methods and are technically savvy.

Cybercrimes have serious consequences for both companies and individuals. They primarily result in financial losses, as well as a loss of trust and reputational damage. Cybercrime knows no borders, and no country or organization can tackle it alone. This task requires a comprehensive approach and joint efforts.

Law enforcement agencies often seek advice from IT companies that have a high level of expertise in cybersecurity. Kaspersky actively assists in the investigation of cybercrimes. At the same time, we take the issue of transparency in our joint work very seriously: we have a clear procedure for working with requests from law enforcement agencies, which is regulated by our own internal policy, and criteria for the legal verification of each request. If a request does not meet our criteria, we may reject or challenge it. It is important to point out that we do not provide access to our infrastructure or data.

[1] Processing Law Enforcement and Government Requests for Disclosure of Data.

# Objective

Solutions

Assist in investigating cybercrimes

Cybercrime knows no borders, which is why Kaspersky regularly takes part in operations and investigations conducted jointly with the global IT security community and international organizations such as INTERPOL, law enforcement agencies and national Computer Emergency Response Teams (CERT). We provide our expertise and all the technical information needed to investigate cybercrimes. We also regularly conduct trainings.

Protect cyberspace together with INTERPOL

We began cooperating with INTERPOL in 2014 when we signed the first agreement to jointly combat cybercrime. In 2019, we concluded a new five-year agreement, which significantly expanded the scope of our interaction.

Our support for INTERPOL

- We share expert information with INTERPOL on the latest types of malware and cyberattack methods.
- We take part in joint operations around the world to identify and stop cybercrime.
- We conduct cybersecurity training programs and consult employees of INTERPOL and other law enforcement agencies.

How we assisted INTERPOL in 2022–2023:

- Our specialists assisted INTERPOL in the operations Africa Cyber Surge and Africa Cyber Surge II, which aimed to combat cybercrime in Africa.
- We organized training on “Incident Response” and “Malware Analysis” for more than 100 law enforcement representatives from different countries under the auspices of INTERPOL.
- Vitaly Kamlyuk, Head of Kaspersky’s Global Research & Analysis Team in the Asia-Pacific region, made a presentation at the INTERPOL Global Cybercrime Conference (IGCC) 2023, in which he provided an overview of the world’s largest computer worm epidemics, described the measures that have been taken to combat them, and explained what lessons the Company has learned from these events and how this experience will help us prepare for the next wave of vulnerabilities.
- Kaspersky took part in operation Synergia – spanning more than 50 INTERPOL member states – focused on the disruption of malicious infrastructure involved in phishing, malware, and ransomware attacks.

Support international cooperation

Kaspersky works closely with numerous international organizations and law enforcement agencies, takes part in joint operations, cyber threat investigations and cyber diplomacy, and promotes the development of an open and secure internet.

33
international and Russian cyberspace defense partners

>10
memorandums of understanding signed with international organizations and government agencies

>60
organizations involved in the exchange of new malware samples

For example, as part of the No More Ransom Project, created together with Europol and other partners, we are helping ransomware victims in 30 countries recover their encrypted data without paying ransom. Over its seven years of operation, this project has helped roughly 2 million users recover their data worldwide.

Our partners in combating cybercrime and promoting the sustainable development of the digital space

- INTERPOL
- No More Ransom initiative
- Coalition Against Stalkerware
- Geneva Dialogue
- Paris Call for Trust and Security in Cyberspace
- Council of Europe
- Cybermalveillance.gouv.fr (GIP ACYMA) (France)
- Renaissance Numérique (France)
- World internet Conference (as a member of the High-Level Advisory Committee)
- China Industrial Control System CERT (industry partner)
- Industry IoT Consortium (United States)
- International Telecommunication Union
- International Organization for Standardization (ISO)
- Alliance for the Protection of Children in the Digital Environment (Russia)
- ANO Digital Economy (Russia) and many others

We also readily share our cybersecurity expertise by speaking at major conferences and events such as the RSA Conference and Virus Bulletin, publishing information on our own blogs and hosting free webinars on cybersecurity. In addition, in 2023, we expanded the free service features on the Kaspersky Threat Intelligence portal, which helps find information about cyberthreats in real time.

In 2022–2023, Kaspersky expanded cooperation with international and national organizations as part of its efforts to combat cybercrime. The Company signed several important agreements, including cooperation agreements with national cybersecurity centers and memorandums of cooperation with Korea University, the UAE Cybersecurity Council and the Italian Ministry of Education.

At the 2022 World internet Conference in China, Kaspersky received the World Leading Technology award for developing the Kaspersky Automotive Secure Gateway solution, and CEO Eugene Kaspersky was awarded the title of Special Contributor for his services in promoting global cybersecurity cooperation.

In 2023, Kaspersky received an award from the Alliance of Public Private Cybercrime Stakeholders (founded under the auspices of the Singapore Police Force) for its contribution to creating a cyber-resilient world.

In addition, we have helped generate feedback and proposals for the draft Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is being developed under the auspices of the United Nations (UN). We also submitted our proposals as part of the UN Global Digital Compact initiative, with a focus on improving digital literacy.

In 2022–2023, our experts took part in numerous forums and conferences on cybersecurity, including:

- UN Open-Ended Working Group on ICT (as part of an informal dialogue under the auspices of the Working Group chair);
- Fifth intersessional consultation of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes;
- African internet Governance Forum;
- Session on digital security as part of the UN Global Digital Compact initiative;
- Working groups of the Geneva Dialogue;
- INTERPOL Global Cybercrime Conference;
- UN Internet Governance Forum;
- Business 20 (B20) format as part of the G20.

In addition, we work with more than 60 other IT companies around the world by exchanging malware samples.

# Objective

Improve the legislative framework

Today's technological challenges require a more flexible and adaptive legislation. Threat actors are constantly refining their techniques, so laws must be able to effectively respond to new threats. In addition, improved legislation helps standardize legal mechanisms worldwide, which allows for the more efficient exchange of information and extradition of criminals.

# Solutions

Improve legislation to combat cybercrime

Kaspersky regularly takes part in drafting legislation, policies and other documents that aim to ensure cybersecurity around the world. Our experts share their knowledge and experience in protecting critical infrastructure, combating cybercrime, protecting data and other related topics. As numerous countries tighten their cybersecurity regulation, we are receiving more and more requests from national, regional and international organizations to provide expert assistance. Some of this expert content is available on our cybersecurity policy blog.

We consistently provide stakeholders with information regarding cybersecurity and cybercrime matters at the United Nations level. Since 2020, we have been actively participating in the UN informal dialogue under the auspices of the chair of the Group on developments in the field of information and telecommunications (ICTs), where discussions are held about various cybersecurity issues, measures to boost trust in cyberspace and the development of expertise. During the reporting period, the Company took part in two meetings at which it presented its proposals on the use of AI with an emphasis on cybersecurity, as well as comments on the annual OEWG report.

Our contribution to combating international cybercrime

Participation in the Africa Cyber Surge operation

The information security sector in Africa is less advanced compared to other regions, rendering its countries more susceptible to cyberattacks. To help INTERPOL combat cybercrime in Africa, Kaspersky provided the international organization with threat intelligence during the Africa Cyber Surge operation.

The first part took place from July-November 2022, and included a series of measures to gather intelligence against the hackers, while the second – Africa Cyber Surge II – began in April 2023 and lasted four months, encompassing 25 African countries. Along with other INTERPOL partners, Kaspersky provided the agency with indicators of compromise (IoC), including information about malicious servers, phishing links and domains, and fraudulent IP addresses.

What was the result?

With Kaspersky's assistance, investigators managed to detect compromised infrastructure and apprehend threat actors suspected of committing cybercrimes in Africa. The operation resulted in the arrest of 14 individuals and revealed network infrastructure that was used to cause more than US$40 milllion in financial losses.

> "The Africa Cyber Surge II operation has led to the strengthening of cybercrime departments in member countries as well as the solidification of partnerships with crucial stakeholders, such as computer emergency response teams and internet service providers. This will further contribute to reducing the global impact of cybercrime and protecting communities in the region".
>
> **Jurgen Stock,**
> Secretary General of INTERPOL

# Objective

Protect users against ransomware

Ransomware programs are called encryptors because their malicious software gains access to a device, encrypts the entire operating system or individual files, and then the attackers demand a ransom from the victims. Combating ransomware is crucial because ransomware attacks cause serious damage to both individuals and the economy as a whole. They can result in substantial financial losses and also pose a threat to public security.

Solutions

We reveal attack patterns, analyze the hackers' tools and update our own decryption utilities as part of the No More Ransom initiative.

During the reporting period, Kaspersky:

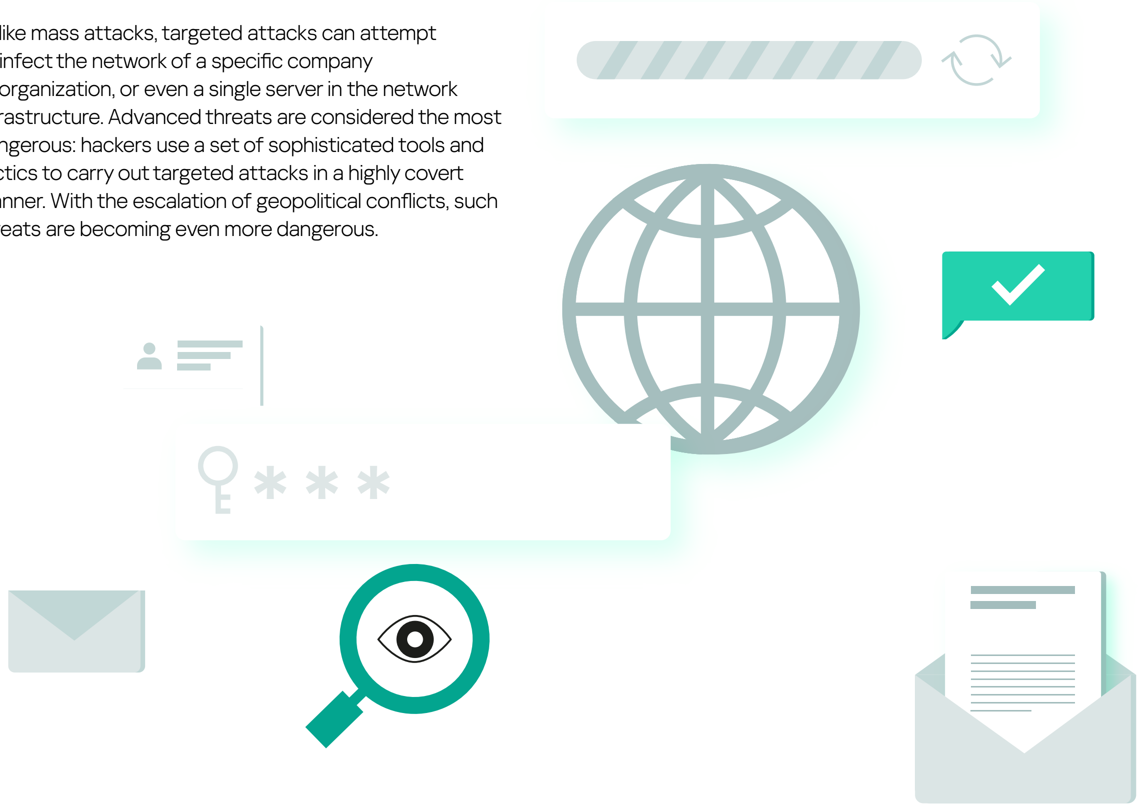
- Discovered an attack using zero-day vulnerability in the Microsoft Common Log File System (CLFS). Our Behavioral Detection Engine and Exploit Prevention components detected attempts to execute elevation-of-privilege exploits on Windows servers belonging to SMBs in the Middle East, North America and Asia.
- Updated decryption tool for victims of Conti ransomware. Kaspersky updated the publicly available decryption tool on the Noransom portal to a version that was used to attack commercial companies and government agencies.
- Analyzed the Lockbit 3 builder. Lockbit is one of the most common types of ransomware. It is distributed among partners using the RaaS[1] model, offering participants up to 80 percent of the ransom amount. In September 2022, the Lockbit 3 builder was leaked, allowing any user to construct their own version of the ransomware. Kaspersky's global cyber incident response team analyzed the builder to understand the ransomware design methodology and find opportunities for additional analysis. This tool allowed anyone to create their own version of ransomware.

[1] Ransomware-as-a-Service.

# Objective

Investigate targeted attacks and advanced threats

Unlike mass attacks, targeted attacks can attempt to infect the network of a specific company or organization, or even a single server in the network infrastructure. Advanced threats are considered the most dangerous: hackers use a set of sophisticated tools and tactics to carry out targeted attacks in a highly covert manner. With the escalation of geopolitical conflicts, such threats are becoming even more dangerous.



# Solutions

Experts from Kaspersky's Global Research & Analysis Team (GReAT) and the Kaspersky Cyber Threat Intelligence team closely monitor numerous advanced persistent threat groups, analyze current trends and predict how the cyberthreat landscape will further develop in order to stay one step ahead of hackers and ensure the security of Kaspersky customers.

Examples of cyber-groups that have been monitored and their attacks:

- **Analysis of threats from the Cuba Ransomware group.** In 2023, Kaspersky released the results of an investigation into a new cyber incident involving the Cuba group. This ransomware group has attacked numerous companies around the world, including retail, logistics, financial and government agencies and industrial enterprises in North America, Europe, Oceania and Asia. Our experts analyzed the infamous cyber-group's history, as well as its techniques, tactics and procedures.

- **Andariel's mistakes and a new malware family.** Kaspersky experts uncovered a new form of malware – a remote access Trojan called EarlyRat – in the arsenal of the Andariel cyber group, which is part of Lazarus. The malware can reach a device through a vulnerability found using the Log4j exploit, or via links in phishing documents.

- **A new APT group called GoldenJackal**. This group has been active since 2019 and usually attacks government and diplomatic organizations in the Middle East and South Asia. Kaspersky experts began monitoring the group in mid-2020. Its main distinction is a specific set of malicious implants that are distributed through removable drives and are used to control target computers, extract data, steal records, collect information about the victim's local system and online activities, and also create and send screenshots.

- **The cyber group ToddyCat is stepping up the complexity of its cyber espionage campaigns**. Kaspersky experts discovered a new set of malicious tools and programs used to steal and exfiltrate data, as well as the methods this active group uses to navigate infrastructure and conduct espionage operations.

Results of efforts to combat cybercrime

From November 2022 to October 2023[1], our Web Anti-Virus detected

112,922,612

unique malicious objects.

During this period, Kaspersky's solutions:

- Blocked 437,414,681 malware-class attacks launched from online resources across the globe;
- Found 106,357,530 unique malicious URLs;
- Prevented ransomware attacks on the computers of 193,662 unique users;
- Blocked miners from infecting 1,140,573 unique users;
- Prevented the launch of malware designed to steal money via online access to bank accounts on the devices of 325,225 users.

These results were achieved with contributions from four of our units: Anti-Malware Research (AMR), the Industrial Control Systems Cyber Emergency Response Team (ICS CERT), Special Cyber Forces and the Global Research & Analysis Team (GReAT).

Our plans for 2024

- Take part in creating a legal framework to combat cybercrime.
- Provide training and advanced training on cybersecurity for parties involved in cyberspace.
- Collaborate and partner with government agencies to share information on cyberthreats.
- Regularly update software and technology to ensure reliable protection against the latest threats.

[1] See Kaspersky's report https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/28102415/KSB_statistics_2023_en.pdf.

ESG

Future Tech

18

products and services included in the Kaspersky OT CyberSecurity (KOTS) industrial cybersecurity ecosystem

2

Russian information security standards developed by the Company

>1,000

major industrial customers worldwide protected by Kaspersky Industrial CyberSecurity (KICS) solutions

Protection of industrial enterprises and critical infrastructure

Our goal is to ensure the seamless operation of cyber-physical systems at critical infrastructure facilities and in industry using an ecosystem of modern technologies, knowledge and expertise.

Protected by Kaspersky solutions

12% of leading fertilizer producers

10% of the world's largest oil and gas companies

15% of nuclear reactors worldwide

What is critical infrastructure?

Critical infrastructure consists of systems that manage technological processes in industries that are of strategic importance for the global economy, government institutions and society.

Critical infrastructure in industry

Heavy industry

- Fuel extraction
- Electricity production and supply
- Mining industry
- Metallurgy
- Chemical industry
- Automotive production
- Mechanical engineering
- Production of construction materials
- Pulp and paper industry

Light industry and social infrastructure

- Logistics and transport
- Food industry
- Pharmaceuticals
- Housing and utility facilities

Critical manufacturing

- Defense industry
- Rocket and space industry
- Production of microchips and electronics

How we protect critical infrastructure and industrial enterprises

Ensuring industrial cybersecurity

# Objective

Eliminate cyber-incidents at our customers' industrial facilities

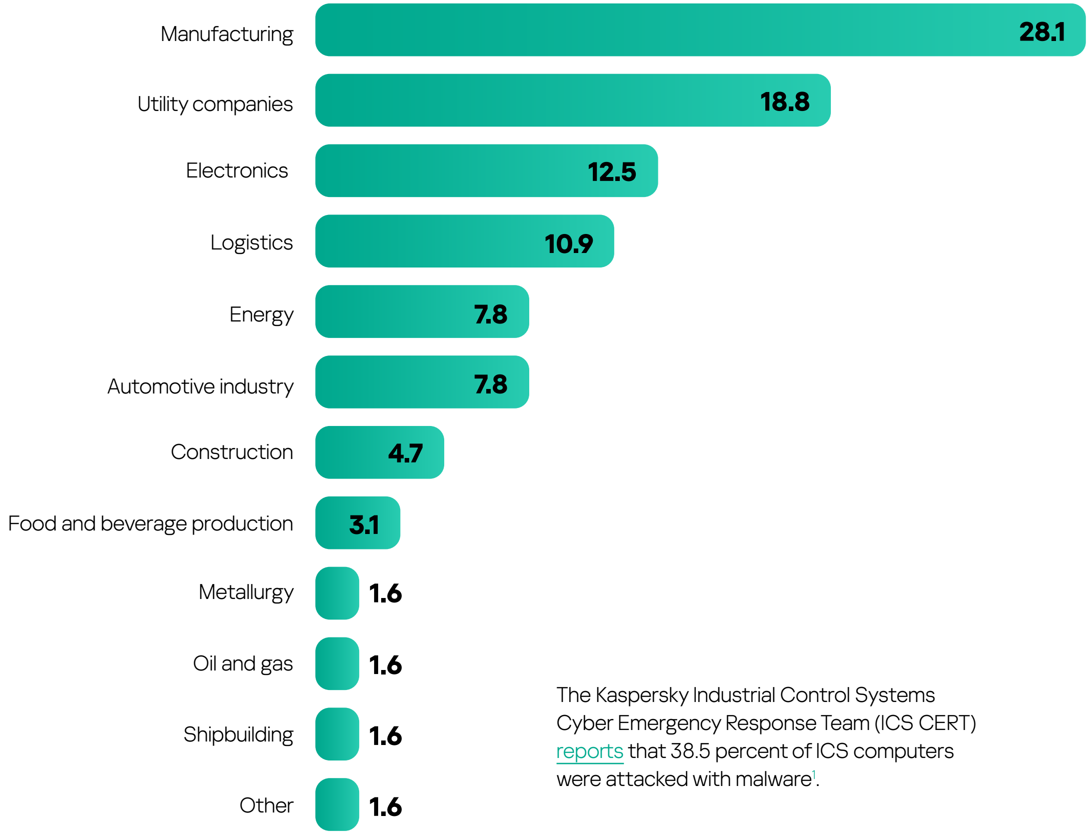
Today, industrial cybersecurity is a technology that promotes the sustainable development of enterprises. Our solutions can be used to protect companies from any industry and with any level of digitalization, whether they use conventional or cutting-edge computer equipment.

Our brief overview of main industrial cybersecurity incidents in the second half of 2023 showed companies in the manufacturing sector accounted for the vast majority of enterprises that came under attack.

Breaches of critical infrastructure in 2022–2023

- ThyssenKrupp had to suspend the production of automotive parts due to a cyberattack.
- Battery manufacturer Varta suspended production at all enterprises after its IT systems were hacked.
- Hackers took control of the IT system at a pumping station of the Municipal Water Authority of Aliquippa, which provides water supply services in the U.S. state of Pennsylvania.
- A cyberattack on the global container terminal operator DP World led to major disruptions at Australia's international ports.
- Nearly 2 million Texans experienced water outages due to a cyberattack on their water utility NTMWD.
- The hacktivist group SiegedSec hacked into and stole confidential data from the Idaho National Laboratory, a nuclear research center of the U.S. Department of Energy.

Industries most susceptible to cyberattacks in the second half of 2023



The Kaspersky Industrial Control Systems Cyber Emergency Response Team (ICS CERT) reports that 38.5 percent of ICS computers were attacked with malware[1].

Our contribution to minimizing risks and reducing damage from cyberattacks on manufacturing enterprises

We help customers save money with our solutions

Cyberattacks can lead to the disruption or complete shutdown of processes and services, which can diminish a company's economic performance. This can be avoided with the use of our products to protect critical infrastructure and industrial enterprises. In April 2021, Forrester conducted a study on how our industrial security solution, KICS for Networks, impacted the economic indicators of a major energy supplier and compared our customer's potential losses to the cost of a KICS license.

What was the result?

US$2.5 million

decrease in the risk of security breaches

US$338,000

reduction in possible equipment damage

US$1.6 million NPV[2]

135% ROI

The researchers concluded that the solution paid for itself in just eight months, and ROI was recorded as 135 percent net present value for an average customer over three years. In addition, introducing KICS helped the company correlate the real and documented network and created more transparency in terms of network assets and access points.

[1] All types of threats.

[2] Net Present Value is a financial indicator of the amount of cash an investor expects to receive from a project after cash inflows make up for its initial investment costs and the periodic cash outflows associated with the project.

# Solutions

Protect all levels of an industrial enterprise's systems and networks

Kaspersky OT CyberSecurity

We are committed to providing each and every customer with the value they need from the introduction of our cybersecurity systems, regardless of their industry, level of maturity or complexity of their request.

Our industrial cyber-physical security ecosystem, Kaspersky OT CyberSecurity (KOTCS), reduces the threat of cyberattacks and eliminates the risk of unacceptable events. It contains:

- **Technology:** a robust selection of tested, compliant, and approved industrial security solutions;
- **Knowledge:** reliable threat analytics and comprehensive industrial cybersecurity training;
- **Expertise:** a full range of professional services for comprehensive industrial cybersecurity.

The KOTCS ecosystem consists of 18 products and services for industrial enterprises that were developed by Kaspersky specialists with world-class expertise, including 15 years of experience in protecting industrial facilities and 10 years of work to develop the KICS. The most mature ecosystem on the cybersecurity market, it protects industrial enterprises at every level from a central location. It has advanced functionalities to protect against all cyber-physical threats (such as its own unique Antidrone system) and ensures safety at industrial facilities, including nuclear power plants, reliability of which is subject to the most stringent requirements by the regulatory authorities.

KOTCS – protection at every level

Level 3. Enterprise systems

- Convergence of IT and OT and correlation of data from all available sources
- Unified security processes and approaches using Hybrid XDR (Extended Detection and Response)
- Training programs, consulting and advanced threat analytics

Level 2. Monitoring and control

- IIoT[1], connectivity and perimeter supervisory control and data acquisition (SCADA)
- Access and usage control, audit and visibility of OT systems
- Expert on-site support

Level 1. Controllers and protection

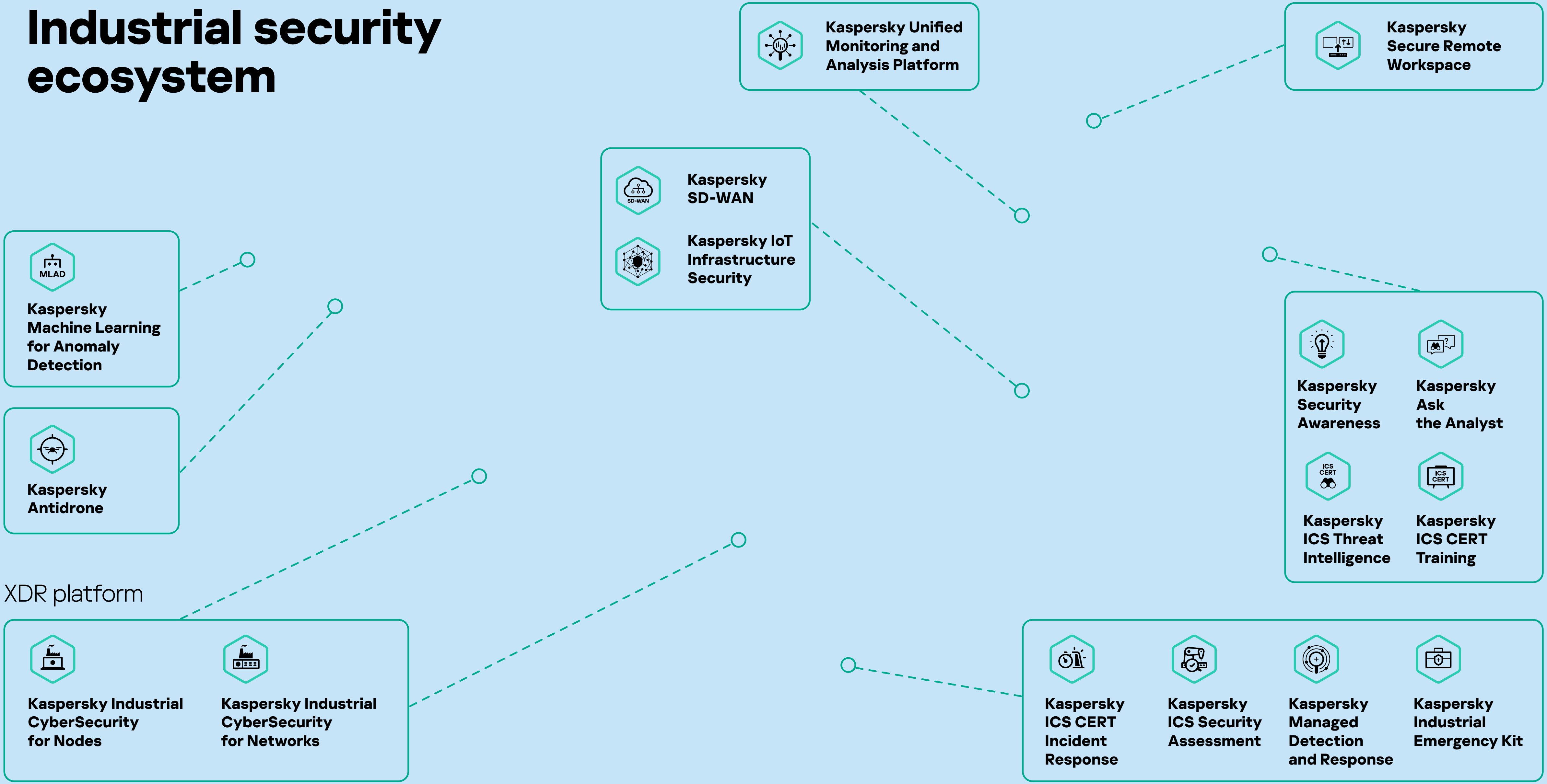
- Detection of intrusions, hacking and compromise attempts, as well as vulnerabilities in microprocessor technological equipment at the lower level of automation, such as controllers, security terminals and measuring centers
- Deep protocol inspection (DPI) and protection of embedded operating systems in industrial equipment against network threats and attempts to maliciously influence process settings (parameters)
- Detection of anomalies in technological processes with machine learning based on samples from databases or real-time data

Level 0. Technological process

Monitoring of airspace to protect essential equipment against cyber-physical threats and ensure the safety of connected vehicles

[1] The Industrial Internet of Things consists of a multi-tiered system that includes sensors and controllers installed on an industrial facility's components and assemblies, equipment to transmit and display data, powerful analytical tools to interpret information and numerous other components.

Industrial security ecosystem



Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Secure Remote Workspace

Kaspersky SD-WAN

Kaspersky IoT Infrastructure Security

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Antidrone

Kaspersky Security Awareness

Kaspersky Ask the Analyst

Kaspersky ICS Threat Intelligence

Kaspersky ICS CERT Training

XDR platform

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Kaspersky ICS CERT Incident Response

Kaspersky ICS Security Assessment

Kaspersky Managed Detection and Response

Kaspersky Industrial Emergency Kit

Kaspersky Industrial CyberSecurity

Key industries using the ecosystem

- Oil, gas and chemical industries
- Energy, including the nuclear sector
- Metallurgy and mining
- Industrial production

Future areas for the use of KOTCS

- Pharmaceuticals and medical equipment
- Transport and logistics
- Telecommunications

The key component of the KOTCS ecosystem is the Kaspersky Industrial CyberSecurity (KICS) platform, designed to protect industrial enterprises and critical infrastructure facilities without affecting the availability of systems or the uninterrupted operation of technological processes.

KICS

The native XDR platform KICS is a vital part of the automated process control system, conducts in-depth analysis of traffic and telemetry of components, actively responds to threats, or simply informs users about them. It helps protect modern digital and connected industrial automation systems against attacks of any complexity and also monitor the safe operation of software and hardware systems of previous generations.

KICS ensures the total visibility of what is happening at all levels of the technological process: physical devices, controllers, SCADA[1] servers and production management systems. The platform has been tested for compatibility with products from leading industrial automation system vendors, including Siemens, Honeywell, B&R (ABB Group), Yokogawa, Emerson, Schneider Electric, Baker Hughes, GE and others.

> The KICS platform is compatible with numerous process control systems from 50+ vendors

The platform features two closely interrelated and complementary components: KICS for Nodes to protect industrial operator panels, workstations and servers, and KICS for Networks to monitor industrial network security.

KICS today

~230,000
KICS for Nodes licenses sold

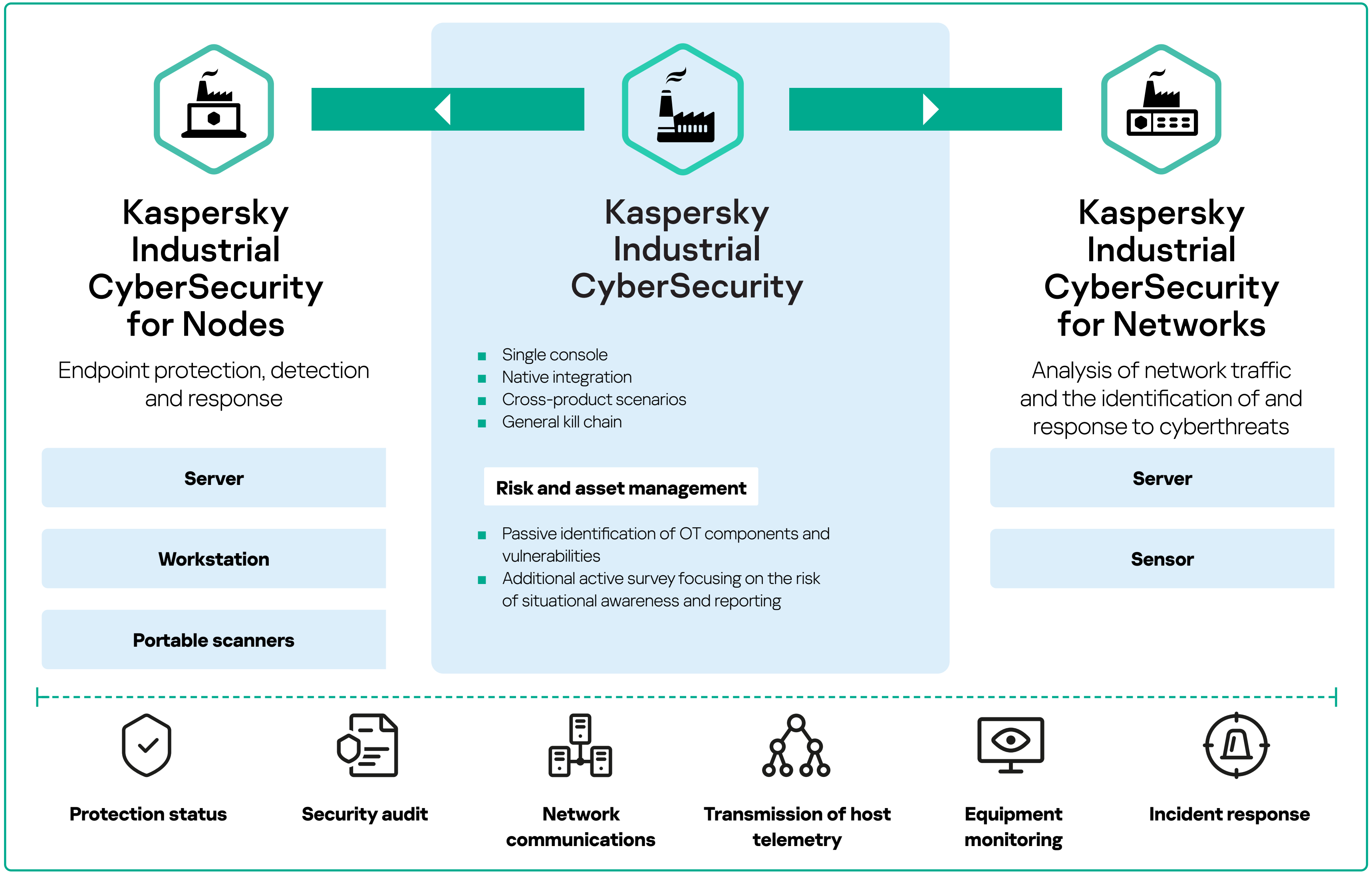
>1,000
industrial customers use KICS solutions

430
industrial networks of major customers protected worldwide

+20%
average income per customer

[1] Supervisory Control and Data Acquisition.

XDR platform for industry



Kaspersky Industrial CyberSecurity for Nodes

Endpoint protection, detection and response

Server

Workstation

Portable scanners

Kaspersky Industrial CyberSecurity

- Single console
- Native integration
- Cross-product scenarios
- General kill chain

Risk and asset management

- Passive identification of OT components and vulnerabilities
- Additional active survey focusing on the risk of situational awareness and reporting

Kaspersky Industrial CyberSecurity for Networks

Analysis of network traffic and the identification of and response to cyberthreats

Server

Sensor

Protection status

Security audit

Network communications

Transmission of host telemetry

Equipment monitoring

Incident response

KICS protects all automated process control systems that are currently in operation:

- Brown field (more than 90%) – systems created from 2005 to the 2020s, that generally consist of distributed control systems (DCS) with various types of microprocessor controllers (PLC[1], IED[2] and RPA[3]), computer human-machine interfaces (HMI) on old Windows OS and industrial Ethernet-based networks
- Promising projects and popular areas (5–10%) – various types of digitalization, connected sites, cloud technologies, the IIoT, digital twins, virtualization of industrial systems, AI/computer vision, DSS[4] and additive technologies

The KICS platform provides full visibility and control over what is happening in the control systems of an industrial enterprise's key technological processes. It detects and blocks network threats as well as traffic and process anomalies, prevents malware from infecting computer equipment and detects violations of safety policies by personnel. In addition, it helps conduct inventories of industrial assets, perform security audits, detect vulnerabilities and manage risks.

[1] Programmable logic controllers.
[2] Intelligent electronic devices.
[3] Relay protection and automation.
[4] Decision support systems.

Our contribution to the safe production of clean energy

We protect energy facilities with modern information and operational technologies and services

The Ust-Kamenogorsk and Shulbinskaya hydroelectric power plants are major strategic facilities that supply clean energy from renewable sources to residents and enterprises in Eastern Kazakhstan. The power plant managers were looking for the best solution to ensure their safe and seamless operation.

The project to protect hydroelectric power plant infrastructure was a complex one because the following key criteria had to be taken into account when selecting a suitable solution:

- Architectural requirements
- Requirements for compatibility with other solutions
- Requirements for automated process control systems

The KICS platform ultimately proved to be the most suitable solution for protecting the production processes of the hydroelectric power plants. It was incorporated into the technological systems of power plants that are located in different cities and only connected by a VPN channel.

What was the result?

Our KICS solution ensures the industrial infrastructure of the two hydroelectric power plants operates securely at all levels – from process control system servers and automated workstations to programmable logic controllers and network equipment – without disrupting the interaction of information systems and industrial equipment. KICS can effectively identify different types of threats at the hydroelectric power plants: human errors, disruption of communications between devices, employees performing work without approval, attacks and malware.

Creating Cyber Immunity

# Objective

Ensure the reliable and predictable operation of industrial systems and reduce the risk of incidents and related accidents

The number of internet-connected devices is growing with each passing day, which also entails an increase in cybercrime. Cyberthreats can cause substantial physical damage to industrial enterprises, energy facilities, cars and smart city systems, among other things. The information security industry is constantly creating new technologies and products, but they are often only just catching up with hackers. It is crucial to find a way to stay ahead of them and protect ourselves against cyberthreats.

Solutions

Prevent cyberattacks with KasperskyOS

Cyber Immunity makes it possible to create hardware and software IT systems with built-in protection against cyberattacks. It is a critical factor for the development of industrial automation, wearable industrial devices, the Internet of Things (IoT) and remote access to critical facilities. We already have access to such Cyber Immune devices as gateways for the Industrial IoT, thin clients, smart city controllers and gateways for cars.

As part of our Cyber Immune approach, we have developed our own operating system, KasperskyOS, a platform for creating products and solutions that are protected at the architectural level.

We achieve Cyber Immunity by splitting the system into isolated components and controlling interaction between them. With this approach, most attacks on the system will be futile, since it will continue to perform critical functions even in an aggressive environment and prevent hackers from pulling off successful attacks.

Two key features of KasperskyOS are its own microkernel and security monitor – the Kaspersky Security System subsystem – which provides a higher level of security and meets Cyber Immunity requirements right out of the box. Such solutions are virtually impossible to compromise, and the number of possible vulnerabilities in them is minimized.

Helping industrial companies implement their ESG strategies

# Objective

Monitor and analyze sustainability indicators

Major industrial companies operate on the principles of sustainable development and develop their own ESG strategies. They set climate change targets and plan to gradually minimize their carbon footprint. To track their progress in this regard, companies monitor and analyze greenhouse gas emissions and pollutants in real time and retrospectively. Companies with significant greenhouse gas emissions from their operations, including transport and mining companies, are particularly interested in such a reporting system.

Industrial and occupational safety is another key aspect of sustainability. Industrial companies are incorporating injury reduction goals into their ESG strategies. They collect and analyze data on working conditions and injuries to track their progress in achieving these goals, identify vulnerabilities, and take action to prevent workplace accidents. IT solutions are used for this purpose to automatically monitor compliance with safety regulations, record violations and transfer this data to the reporting system.

Solutions

Create products that can track ESG targets

In an effort to not only help our customers protect their cars against hacking, but also control fuel consumption, build optimal logistics routes and take into account emissions from vehicles, we created the Kaspersky Automotive Secure Gateway solution. It runs on the KasperskyOS, collects all the essential digital data about a vehicle's operation, makes such data visible, transparent and understandable, and sends it to servers for analysis with an assessment of how to improve performance in the future. Our solution enables customers to achieve their sustainability goals in reality, not just on paper. In addition, it securely updates the gateway, helps update other electronics in the vehicle, collects information about other internal network events in the vehicle and sends it to the security monitoring center, thereby ensuring that there is a single point of control and response, and minimizing maintenance costs.

Helping customers comply with requirements to protect critical infrastructure

# Objective

Ensure that users of our solutions comply with the laws of different countries

Industrial enterprises and operators of critical infrastructure must comply with local legal and industry requirements for risk management and reporting incidents. Kaspersky guarantees that its products comply with standards and legal requirements for industrial cybersecurity in different countries around the world.

→ For more about the legal and industry requirements we consider when developing our products and solutions, please see Appendix 4 on p. 149

# Solutions

Consider requirements and standards when developing products for industrial enterprises

KICS is the world's first XDR platform certified to IEC 62443–4-1

Both products of the KICS platform – KICS for Nodes and KICS for Network – are certified in accordance with major international cybersecurity standards and also consider or help meet the requirements of other international laws and the following industry standards:

- ISO/IEC 27 001 IEC 27 002 (DIN 2008 in Germany) – a standard that establishes the requirements for the creation, introduction, maintenance and continuous improvement of an information security management system at an organization
- ISO/IEC 27 019 (DIN 2011 in Germany) – a standard used to ensure information security in the energy sector
- ISO/IEC 27 032 – a standard adressing Internet security issues and contains recommendations for eliminating the most common threats in this regard (social engineering, zero-day attacks[1], spyware, etc.)
- ISO/IEC 15 408 – a standard with the historical name "Common Criteria" that describes the accumulated experience of various countries in the development and practical use of criteria for assessing the security of information technologies
- IEC 62 443 (ANSI/ISA99) – a series of these standards that contains requirements for the design of cybersecurity management systems for automated process control systems and SCADA
- IEC 62 351 – a standard that encompasses information security issues in energy systems
- NIST CSF – recommendations for ensuring the security of industrial control systems that were developed by the U.S. National Institute of Standards and Technology
- NERC CIP – a set of cybersecurity standards for critical infrastructure and the protection of the U.S. power grid that is also used by some Latin American countries
- NIS 2 Directive (EU) 2022/2555) – a new EU directive on cybersecurity[1]
- IMO MSC.428(98) – a Maritime Safety Committee resolution that regulates the management of cyber-risks in the maritime industry as part of safety management systems
- ICAO – a cybersecurity strategy in aviation[2]
- IAEA Nuclear Security Series No. 17-T (Rev. 1) – methods to ensure computer security for nuclear installations

Starting from February 8, 2022, the scope of certification extends to Kaspersky's data processing services (KSN). Many KICS customers enable KSN during installation. It is crucial for them that we use the best global practices at its data centers in Zurich, Frankfurt, Toronto, Moscow and Beijing. Find out more about this here.

Our KICS platform is fully certified by TUV Austria for compliance with the international standard for the software development life cycle to ensure the cybersecurity of industrial enterprises. The trust level is three out of four.

Kaspersky undergoes audits by Service Organization Controls (SOC 2). As part of Type 2 certification, the Company's solutions were tested for the effectiveness of controls used to protect the development and release of anti-virus databases against unauthorized intervention. The performance of Kaspersky's control mechanisms was not assessed on a specific date, as it is in the Type 1 audit, but over the course of six months.

[1] EU member states must adopt and publish the cybersecurity measures required to comply with the new directive by October 17, 2024.
[2] FAA Advisory Circular 119-1 – Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).

Our results

KICS

Sales of the KICS platform have increased significantly on all major industrial cybersecurity markets. In 2023, Kaspersky's industrial cybersecurity business demonstrated the following results:

- The KICS platform firmly moved into the top five of all the Company's B2B products in terms of revenue
- Industrial Cybersecurity once again had triple-digit revenue growth as a percentage compared with last year
- The sales plan was exceeded by 128%
- The gross EBITDA margin, operating EBITDA margin and EBITDA margin range from 20% to 40%

Main drivers in the development of the Kaspersky Industrial CyberSecurity platform

- Growing threats and emerging information security incidents that industrial companies increasingly encounter in their operations
- The need for a solution that is capable of protecting heterogeneous infrastructure that consists of technological processes that are simultaneously controlled by both legacy automation systems and modern solutions based on networks with advanced architecture, current operating systems and industrial software versions
- The active introduction of connected smart devices and devices of the Industrial Internet of Things as part of the digitalization process, as well as the widespread use of IT, software, hardware and network technology stacks at industrial facilities

We expect two-fold growth in this business segment over the next four years. To achieve this goal, we will continue to invest in the development of KICS technological capabilities and promote it in key regions.

KasperskyOS

During the reporting period, we started developing a regional business to protect virtual workplaces, which have become particularly important in the post-pandemic period, when many companies have switched to a hybrid workplace model.

In August 2023, we signed an agreement with Centerm, to deliver specialized workstations (thin client on KasperskyOS) based on orders from any country. We have already received the first orders from Switzerland and Malaysia.

In 2023, our specialists conducted an in-depth study on how to expand hardware platforms with unique solutions built on Cyber Immunity principles, and commenced expert work to obtain the required opinions and regulatory approvals.

Our plans for 2024

Industrial cybersecurity

We offer advanced and comprehensive protection

across every segment of our customers' infrastructure using the technology, knowledge and expertise within our OT ecosystem. We develop cross-product scenarios to use our natively-integrated technologies in response to new customer demands and also include our partners in our open ecosystem of solutions.

- Investments in Linux functions and the development of the KICS platform's technological capabilities
- Expansion of supported hardware platforms and industrial communication protocols, and development of an expert database of industrial devices
- Elaboration of scenarios for the use of wearable devices and secure data exchange, as well as creation of information security audit tools and routine checks even for isolated systems and networks

Expansion

to new vertical markets in which companies need to clearly monitor ESG indicators

- Collaboration with clients from such industries as transportation, logistics, semiconductors, as well as automotive and component manufacturing
- Partnerships with leaders in OT integration and creation of technology alliances with regional champions among vendors of industrial automation systems[1]

Geo-expansion

into regions where Kaspersky has a smaller presence. To accomplish this, we are adapting the ecosystem to the specific features of each region

- Continued investments in historical markets: Russia, the CIS and Europe
- Expanded cooperation with regional partners to protect critical infrastructure: Brazil, China, India, Indonesia, Saudi Arabia, UAE, Algeria and South Africa

KasperskyOS

Development

of the business community of partners, whose members use Cyber Immune products in vertical industry solutions

Launch

of pilot projects with key customers in various industries to develop a scenario with the effective use of Cyber Immune solutions

Analysis

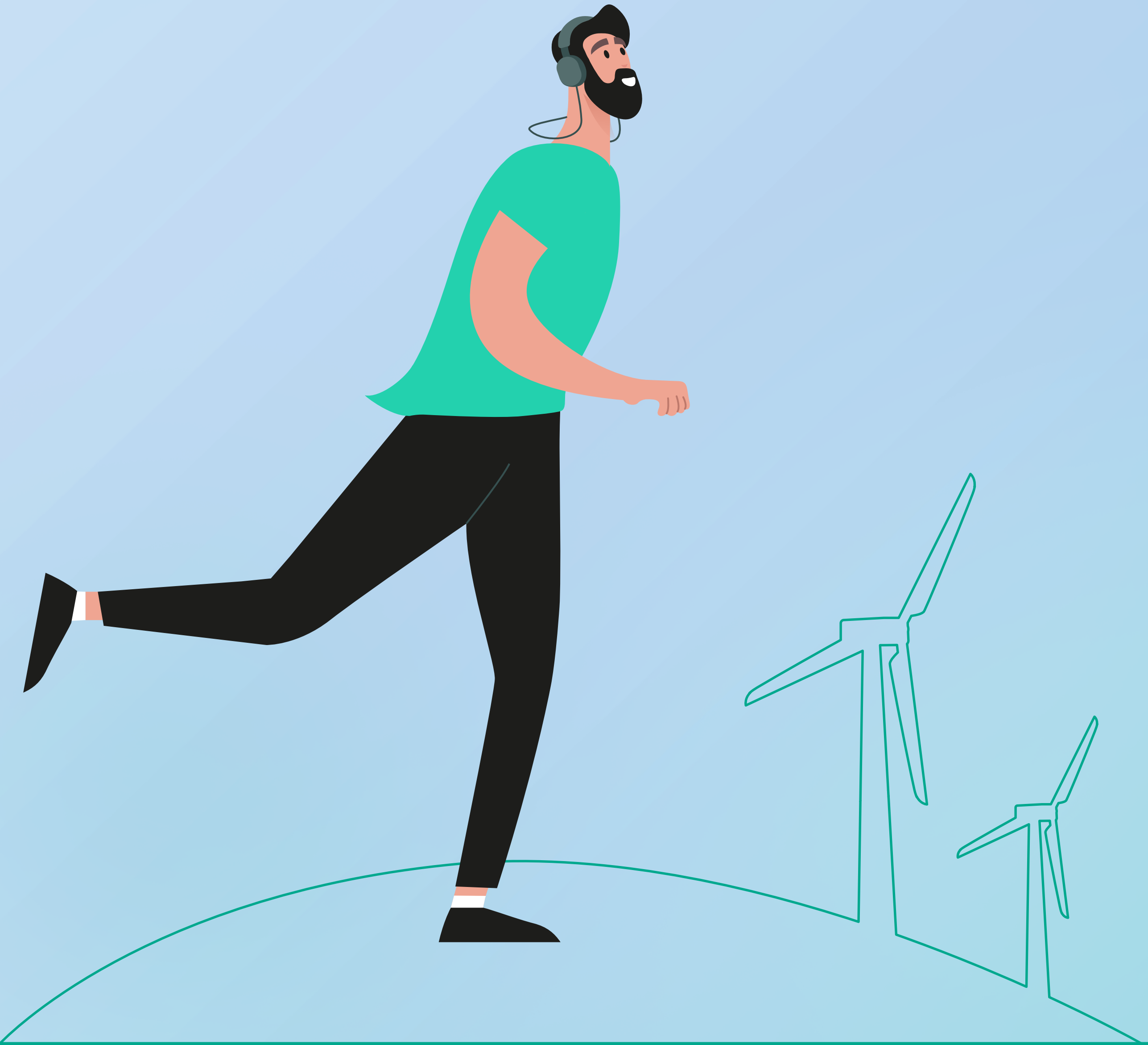
of regulatory requirements to create a description of a new class of devices with built-in (Cyber Immune) protection

[1] Regional leaders and manufacturers of industrial equipment and automation systems.

ESG

Safer Planet

#3



Managing our environmental impact

We monitor and strive to minimize any direct or indirect impacts our operations have on the environment and climate. To achieve this, we are optimizing business processes, reducing resource consumption and waste generation, to increasing energy efficiency of our office and data centers.

Key documents

In 2023, Kaspersky continued to draft its Unified Environmental Policy, the key document that will guide our environmental protection activities in the future. We plan to complete work on this policy by 2025.

Approach to our environmental management

GRI 307-1

Treating the environment responsibly is one of our key values.

Kaspersky consumes water and produces waste that is primarily generated from office activities and the packaging of tangible products.

Our carbon footprint results from indirect sources: air travel, server operation, energy consumption at the offices, corporate transportation as well as services used to create and distribute our products.

Protecting the environment is a responsibility shared among various department heads at Kaspersky. Our colleagues are implementing modern solutions, which the Company uses to reduce resource consumption and waste generation.

Reducing our carbon footprint

We recognize the significance of climate change and are committed to reducing the carbon footprint of our data centers and business operations.

We are committed to achieving SDG 13 "Climate action" and are constantly working to reduce our carbon footprint by using energy-efficient equipment and technologies, as well as minimizing the carbon footprint of our air and road travel.

13 CLIMATE ACTION

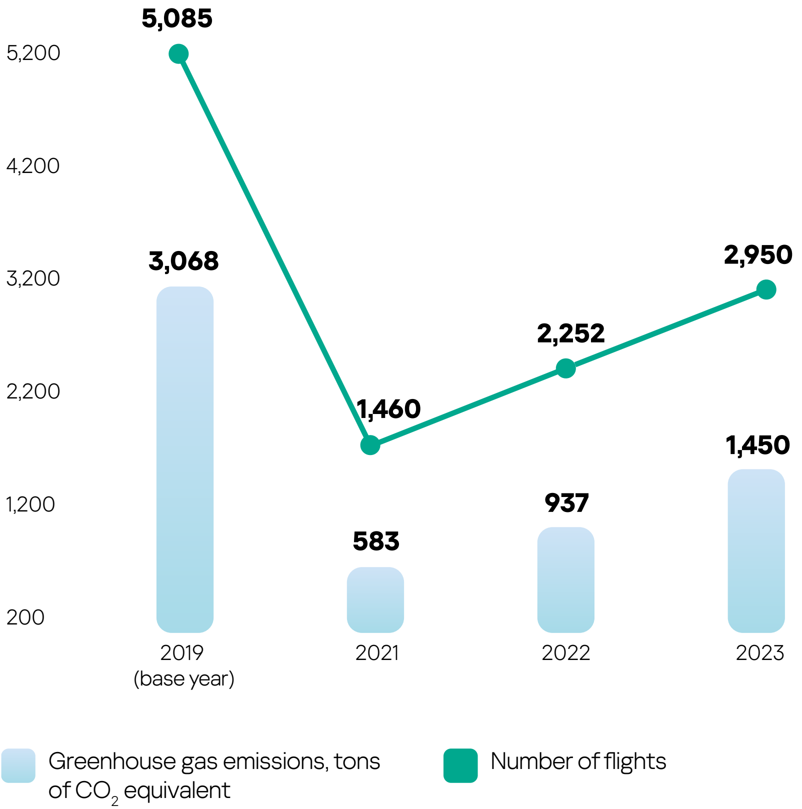
How we manage transport emissions

GRI 305–5

We understand that using air and road transport increases our environmental and climate impact, so we strive to reduce the amount of emissions from fuel combustion in transport. We have reduced our fleet to three vehicles and only use them for urgent travel.

We are committed to minimizing our carbon footprint from air travel. However, in 2022 and 2023, we expanded our business in Latin America, Africa, the Middle East and Turkey, which led to increased employee air travel compared with 2021. Nevertheless, in 2023, we managed to keep emissions at a level that was half of the 2019 base year (3,100 tons of CO_2 equivalent).

Greenhouse gas emissions from air travel by Company's employees[1]



Our contribution to reducing CO_2 emissions from crypto mining

In light of Earth Day 2023, Kaspersky revealed new data on the environmental impact of blocking crypto miners

Many of our users are victims of hidden crypto jacking, an illegal activity where cybercriminals secretly use the power of victims' computers to mint new tokens. Smartphones, personal computers, tablets, and even servers of unsuspecting individuals and institutions can be compromised and used for mining cryptocurrency. This can cause devices to work less efficiently, more slowly or even fail, and also lead to them being infiltrated by third-party viruses. Moreover, mining consumes a huge amount of electricity. The cryptocurrency industry's annual carbon footprint is comparable to that of a large city[2].

By protecting people from crypto jacking, we help reduce greenhouse gas emissions. In 2022, we developed and introduced a special methodology that allows consumers and businesses to assess the impact of illegal mining on the environment.

What was the result?

Our solutions prevented more than 200 million attempts to use other people's devices to mine cryptocurrencies[3] in 2022 and saved the possible energy equivalent of up to 3,000 tons of carbon dioxide emissions into the atmosphere comparable to the annual emissions of 652 cars.

[1] No air travel data provided for 2020 due to the suspension of air travel as a result of the COVID-19 pandemic.
[2] https://www.cell.com/joule/fulltext/S2542-4351(19)30255-7?_returnURL=https%3A%2F%2Flinkinghub.elsevier.com%2Fretrieve%2Fpii%2FS2542435119302557%3Fshowall%3Dtrue.
[3] Data based on anonymized statistics on the operation of Kaspersky solutions around the world in 2022.

How we manage energy consumption in the office

GRI 302-1 GRI 302-4 GRI 305–5 TC-SI-130-a.1

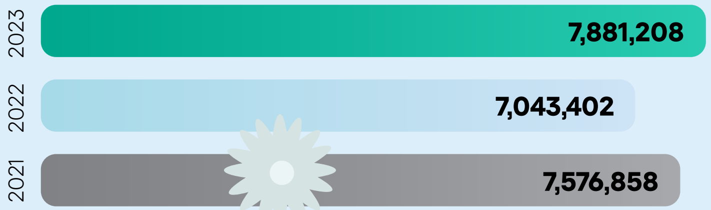
7,881,208 kWh
total electricity consumption in 2023

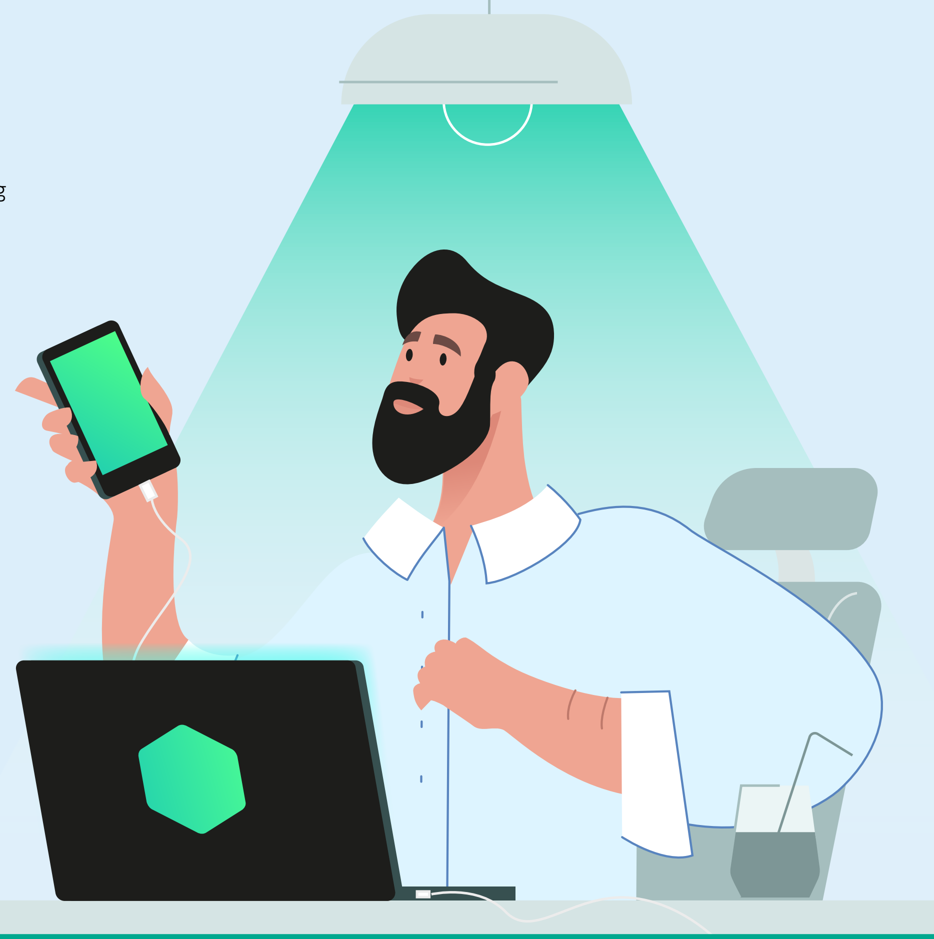
Kaspersky's headquarters in Moscow are located in the Olympia Park business center, which has a Class A energy efficiency rating. The building is certified according to the international environmental standard BREEAM, and energy-efficient technologies and materials were used in its construction.

At our main office, we employ modern solutions like LED lighting, motion sensors for light automation, and automatic lighting controls to optimize energy usage, especially during periods of reduced daylight. In 2020, we completely replaced fluorescent lamps in the business center parking lot with LED lamps, cutting our total lighting expenses by 30–45 percent.

We experienced a slight rise in electricity consumption in 2022 and 2023 compared to 2021, attributed to a shift in work formats for several employees from remote and hybrid arrangements prevalent in 2021 to in-office work. Additionally, in late 2023, the Company relocated employees from another office in Moscow to its headquarters, which led to increased energy consumption by computer equipment and lighting fixtures. Another contributing factor to the increased electricity consumption was the reopening of the on-site gym, cafeteria and restaurant following shutdowns due to COVID-19 restrictions.

Company's overall energy consumption[1], kWh





[1] Data provided for Kaspersky's Moscow office, which also includes the Company's data center. Information was not collected for other offices during the reporting period.

How we manage energy consumption at data processing centers

TC-SI-130-a.3

PUE 2

energy efficiency indicator at Kaspersky's data center

Data centers, or data processing centers (DPCs), are among the main factors that shape the carbon footprint of IT companies. Housing thousands of servers, these facilities operate continuously and require substantial energy consumption. In addition, the industrial air conditioners that provide DPCs with the necessary cooling consume large amounts of energy. Kaspersky uses its own DPC, which includes 33 racks of servers that support user infrastructure and the back office, as well as rented data centers for developmental needs.

The Company's DPC is powered by two independent substations, with a diesel generator on standby in the event of an emergency, and UPS batteries allow the servers to continue operating for roughly 30 minutes after all other power sources have been switched off. The server room is equipped with a clean agent fire extinguishing system that does not harm the environment.

Regular technical inspections are conducted on all electrical equipment within the Company. The generator undergoes a no-load test every two weeks and a loaded test once every quarter. The fuel in the generator is replaced annually. The UPS supply system undergoes maintenance once a quarter.

Throughout the construction of the DPCs, energy-efficient technologies and materials were used, including smart temperature controllers and occupancy sensors for lighting.

Utilizing the latest computing equipment helps us save power and reduce energy consumption. We are replacing outdated equipment with new equipment, which ensures better performance per unit of power, and are reducing the number of cables, racks and servers we use by utilizing virtualization environments and SSD drives. We also recycle old computer equipment and donate keyboards, laptops, screens, and phones to charity donating almost 240 pieces of equipment to seven various NPOs in 2023.

We maintain rigorous standards for DPC infrastructure and endeavor to utilize all available capabilities efficiently. For instance, during winter, we implement a free cooling system that utilizes outdoor air to cool the data center. We use energy-efficient cooling methods in the data center, such as expanding the temperature range of server operation to 22–24°C, as well as organizing cold and hot air corridors.

To prevent the leakage of gasses used to cool servers, our employees check the operation of cooling equipment twice a day. If a leak is detected, the equipment is shut down, the refrigerant supply is switched off and the gas is sent to a special cylinder.

To assess the energy efficiency of our data centers around the world, we use the power usage effectiveness (PUE) indicator, which is calculated as the ratio of a data center's total energy consumption versus the energy consumption of IT equipment. In 2023, our data centers had a PUE of two (compared with the global average of 1.55 in 2022, per the Uptime Institute).

Water usage

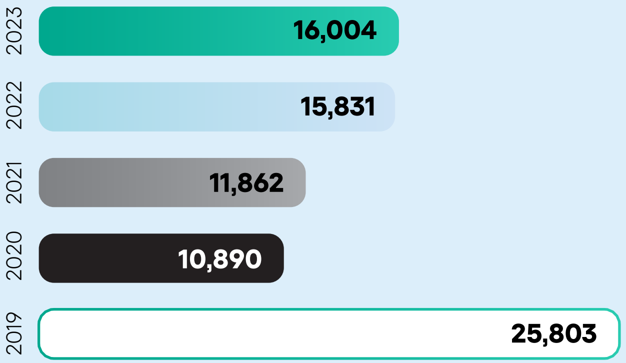
We are improving the water supply system in our offices in an effort to reduce water consumption.

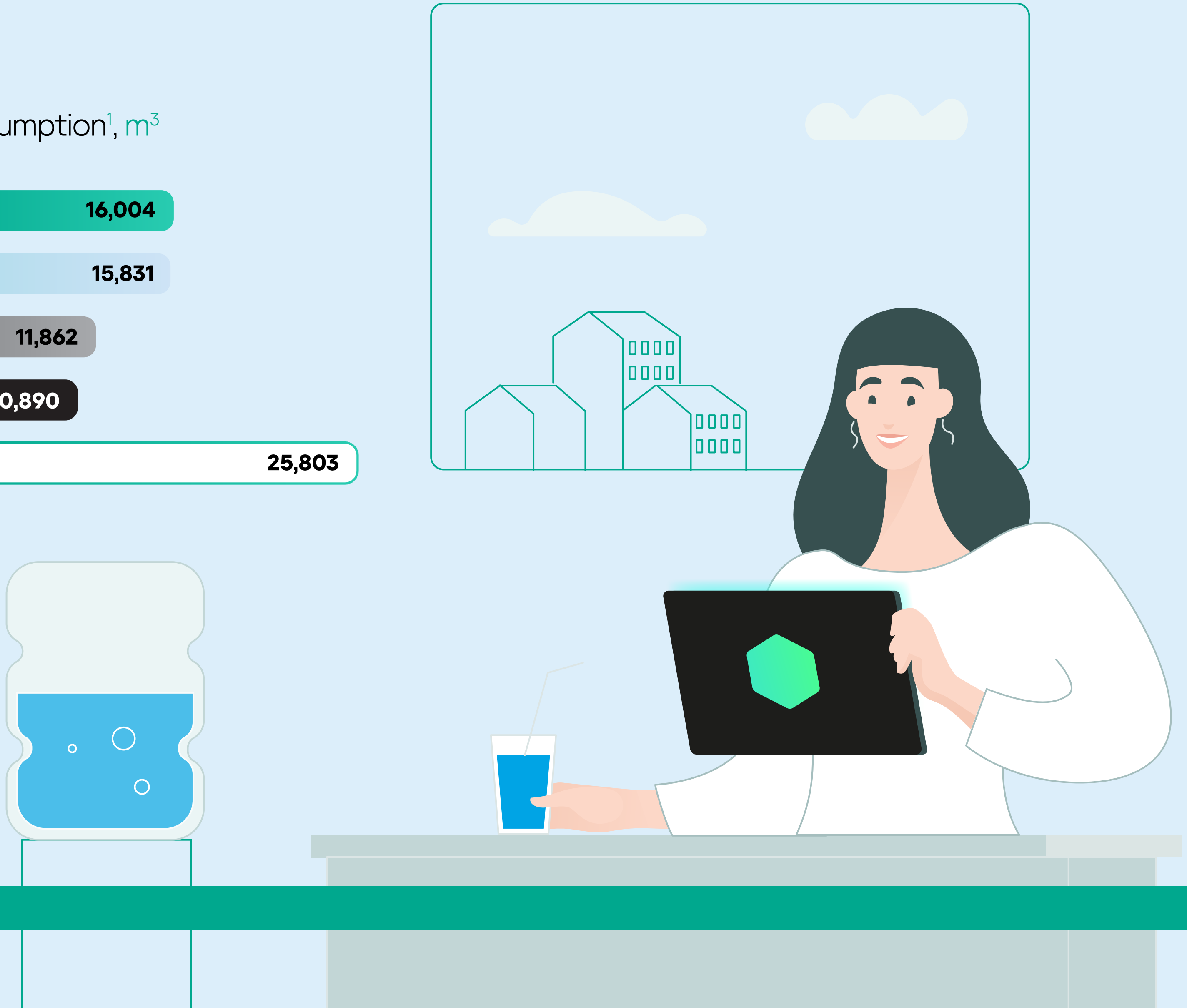
GRI 303–1 GRI 303–2 GRI 303–3 GRI 303–4 GRI 303–5 TC-SI-130-a.2

Kaspersky utilizes water only for office and data center support needs, and solely from municipal sources. The Company does not receive any water from natural sources or open water bodies and does not discharge water into any natural reservoirs.

In 2022 and 2023, the Company saw its water consumption increase compared with the previous two years. This increase can be attributed to the transition of employees from remote work mainly in 2020 and 2021 to a gradual return to the office in the subsequent two years, alongside the reopening of the office's cafeteria, gym, and restaurant facilities. All of these factors impacted the increase in water consumption. Water consumption levels for 2022 and 2023 were substantially lower than the 2019 baseline level, due to the installation of new water supply system sensors.

Water consumption[1], m^3

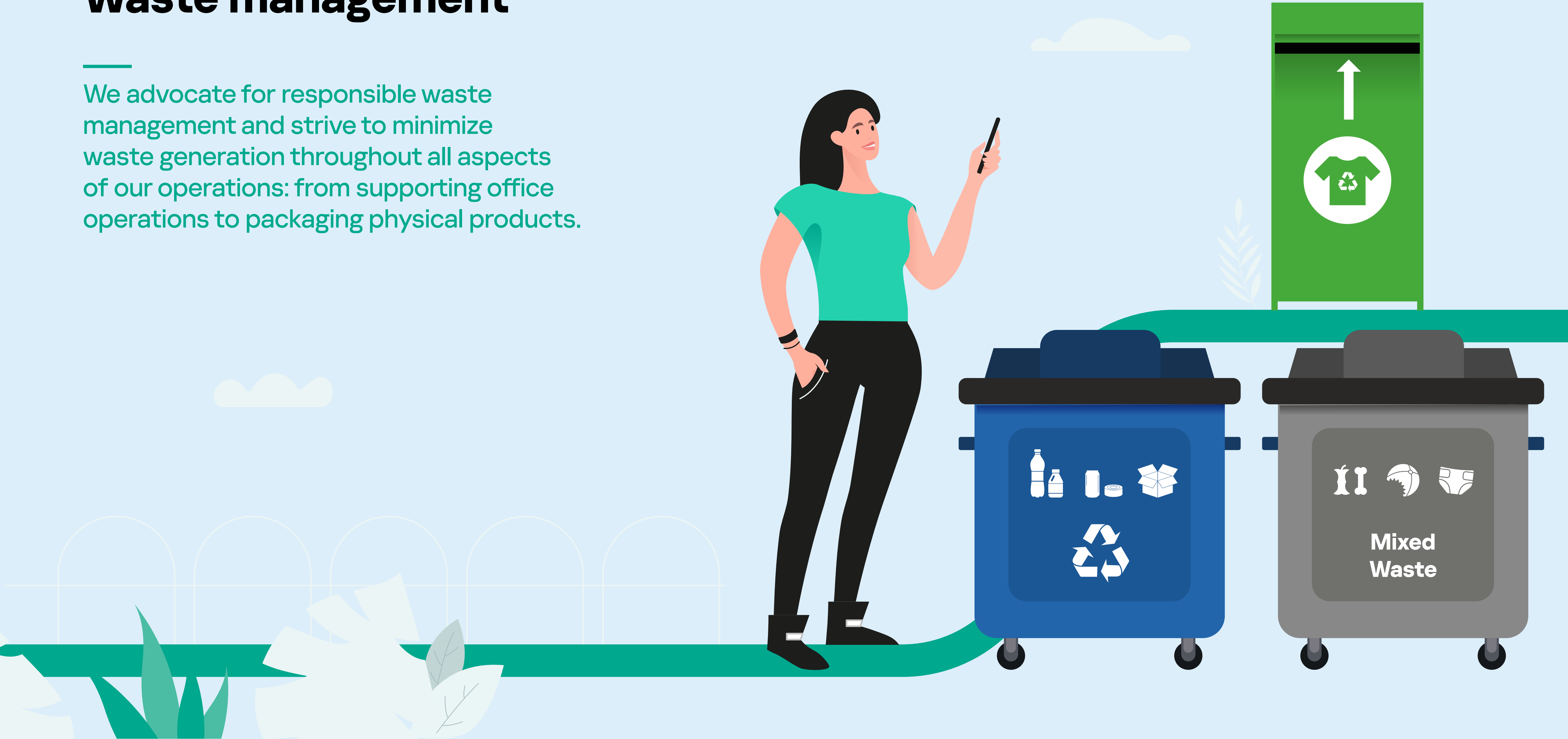




[1] Data provided for Kaspersky's Moscow office, which includes the Company's data center (its main source of water consumption). Information was not collected for other offices during the reporting period. In terms of business operations, the Company uses water for utility purposes at its offices and thus conducts general calculations of its water consumption. The sites where the Company's offices are located are not areas with water stress.

Waste management

We advocate for responsible waste management and strive to minimize waste generation throughout all aspects of our operations: from supporting office operations to packaging physical products.



How we mitigate the impact of product releases on physical media

GRI 306–1 GRI 306–2 GRI 306–3 GRI 306–6

Much of the world's waste comes from the packaging of actual goods. To minimize such waste, we are decreasing the number of products distributed on physical media and transitioning to online license sales. During the reporting period, the share of boxes in Kaspersky's B2C channel sales decreased (11% to 7%). The share of ESD (Electronic Software Distribution) and POSA[1] cards in global sales is approaching 40% and will continue to grow in the future. The best results in the sale of ESD have been seen in such regions as Russia and Latin America.

Kaspersky's products on physical media come in a variety of formats:

- **Boxes** (boxes with a CD containing the product)
- **Leaflets and check cards** (information materials intended for use directly at the store)
- **POSA cards** (thin cardboard cards for electronic product delivery)

Regrettably, we currently are unable to entirely discontinue the distribution of products on physical media, since some customers traditionally prefer to purchase CDs or DVDs, and in some regions, for example in African countries, due to a lack of stable access to the Internet. For such products, we have introduced compact packaging with the lowest possible plastic content. It is marked with international recycling codes to enable customers to dispose of it responsibly in their respective countries. Kaspersky complies with legal requirements related to the import and disposal of packaging in all its sales regions: it pays environmental fees, as well as collects and provides regulators with the necessary data on packaging and its disposal.

In addition, we are reducing the amount of plastic in the production of souvenirs and company merchandise and switching to the use of recyclable and eco-friendly materials.

The overall decline in the sale of physical goods and growth in digital distribution is a global trend, with pace varying depending on the region.

Reactivation, a process when users return to our retail store to purchase a new license a year later after buying it, accounts for 30% of B2C channel sales revenue. Each year the B2C digital retention from the B2C channel sales revenue amounts to 7%, as users make an online purchase a year after buying in our retail store.

In steering the Retail to Subscription project, we are of course consulting with all stakeholders, including our distributors, and working on incentive programs to bring success.

56%
Boxes

44%
ESD & POSA

Our contribution to reducing sales of physical goods

We encourage customers to buy digital products

During the reporting period, we launched the Retail to Subscription project. It encourages retail customers to create a My Kaspersky account and subscribe online to our new portfolio. Online subscriptions mean customers will buy fewer boxed versions of our products, and we will produce less packaging – greatly helping the environment.

What was the result?

Our customers can register on the My Kaspersky portal and receive an electronic subscription to the new product line through our website. We are currently focused on creating new and improved customer experiences to encourage users to choose the digital route. For example, we are upgrading our technology to make paying online easier, and introducing highly attractive pricing for digital-only customers.

[1] Point-of-Sales Activation.

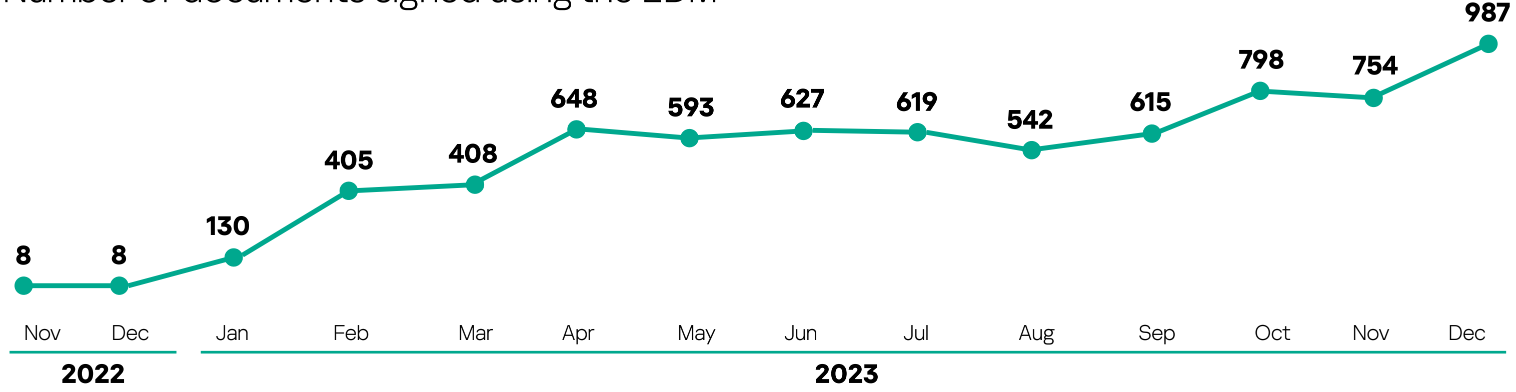
How we save paper

We are dedicated to minimizing the quantity of our printed informational and promotional materials, and we actively recycle outdated posters, signs, banners, and photo panels used for our internal events.

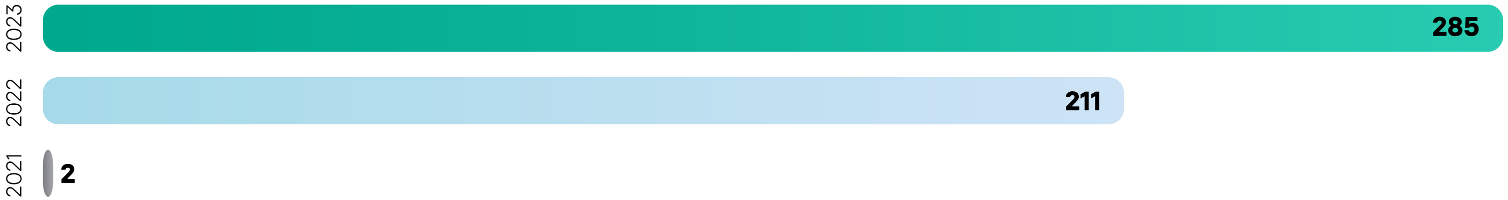
In November 2022, we implemented an electronic document management (EDM) system for our interactions with external contractors, allowing both us and our partners to substantially decrease paper usage. As of December 31, 2023, the number of counterparties using the electronic document exchange system with our Company was up to 498 (versus two in 2021).

In 2023, we conducted an audit of our infrastructure jointly with our vendors to increase its stability and speed, made changes to the interface of the EDM platform to make it easier to use, switched to interaction with third-party operators and began integrating the platform with the internal contract portal. This will help us further expand EDM and increase the number of partners using it in our joint work.

Number of documents signed using the EDM



New counterparties connected to the EDM



How we manage waste

Office operations account for a significant portion of the Company's waste. To reduce the amount of waste, we give preference to high-quality materials with a long service life.

Our Moscow office has posters with infographics about separate waste collection and has installed containers for the separate collection of paper, plastic, glass, metal and mixed waste. Additionally, new containers equipped with compartments for waste paper, plastic caps, batteries, rechargeable batteries and electronic cigarettes were installed in the printer rooms in 2023.

Kaspersky entrusts the daily removal, transportation, recycling and disposal of waste to specialized companies. All contractors, including waste disposal companies, are checked for compliance with legal requirements.

Hazard class I and III waste are partially decontaminated before being sent for burial or disposal.

Waste generation[1], tons

	Total waste generated			Waste sent for recycling, reuse or other forms of recovery			Waste sent for burial or disposal		
Waste class	**2021**	**2022**	**2023**	**2021**	**2022**	**2023**	**2021**	**2022**	**2023**
Class I									
extremely hazardous, non-degradable: pesticides, asbestos and devices containing mercury	0.068	0.072	0.098	0	0	0	0.068	0.072	0.098
Class II									
highly hazardous, takes over ten years to decompose: insecticides, fungicides, lead, arsenic, batteries and pyrotechnics	0	0	0	0	0	0	0	0	0
Class III									
moderately hazardous, takes three to ten years to decompose: herbicides, paints and varnishes, detergents, shampoos, deodorants, and mobile phones	0.926	0	0.728	0	0	0	0.926	0	0.728
Class IV									
low-hazard, takes up to three years to decompose: nitrogen fertilizers, fiberboard, chipboard, plastic film, mirrors, rubber gloves and shoes, disposable tableware and household appliances	172.4	224.7	219.4	8.14	0	0	164.26	224.7	219.4
Class V									
virtually non-hazardous, takes up to three years to decompose: food, natural fabrics and products made thereof, paper and cardboard products	3.1	4.8	5.4	0	0	0	3.1	4.8	5.4

[1] Includes waste from the Moscow office, including the data center, as well as waste from business operations.

Developing environmental awareness among staff

Kaspersky aims to cultivate an environmental culture among its employees, educating them about principles of sustainable consumption.

Our employees are actively involved in environmental initiatives. For people who want to lead an eco-friendly lifestyle, the Company has created the Green like Midori corporate community and invites all newcomers to join it. Moreover, we annually arrange online lectures on environmental protection for employees from sustainability experts.

In 2022, we launched the Trash Ninja online game for employees of the Moscow office. It introduces players to the types of waste generated in the office and at home, and lets players compete with their colleagues in sorting waste. Most of the Company's employees have already completed the Trash Ninja program and learned how to sort garbage.

Our contribution to promoting the idea of conscious consumption

We give clothes, bags and accessories a "second life"

In 2022, Kaspersky began collaborating with the Vtoroe Dykhanie Charitable Foundation, a major Russian non-profit organization (NPO) that collects, sorts, redistributes, and recycles unwanted clothing. We arranged a visit to the foundation's warehouse in Moscow, where our employees gained insights into the development of the NPO's infrastructure for collecting, processing, sorting, recycling, and donating used or unwanted clothing. Today in our Moscow office there is a container available for employees to donate their unwanted or old clothing, shoes and accessories. Every 2–3 weeks Vtoroe Dykhanie come to our office to collect what we have gathered. Subsequently, these items are distributed as humanitarian aid to various groups, including low-income and large families, homeless individuals, people with disabilities, refugees, and others. Items of high quality or of luxurious brands are sold in the NPO's charity shops, and acquired profits are used for statutory activities.

What was the result?

From October 2022 to December 2023, our employees donated 1,408 kg of items.

The foundation recycled 65% of these items.

The foundation donated 34% of these items as humanitarian aid or sent them to its charity shop and other second-hand stores to be sold.

Only 1% of the items were utilized and recycled.

The Company annually hosts events where employees can bring their non-functional home electronics and other appliances. All collected items are sent to our partner Petromax for eco-friendly disposal. Our employees can also dispose of lithium batteries at the office, which are later recycled by our waste management partners. In addition, since 2023, we have been working with the social eco-project Re:Books, which collects unwanted books and donates them to rural libraries.

370 kg

of electronic equipment collected for eco-friendly recycling in 2022–2023

350 kg

of batteries sent for recycling in 2023

ESG

People Empowerment

#4

Talent management

Key documents

- Local Labor Regulations
- Internal Labor Regulations
- Regulation on Compensation
- Regulation on Remuneration

Employees are the Kaspersky's most valuable asset. It is therefore important for us to make sure every person feels comfortable, taken care of, and engaged in what they are doing in order to be productive and can develop themselves and the Company further.

~ 5,100
people work at Kaspersky

+2,500
new jobs created in 2022–2023

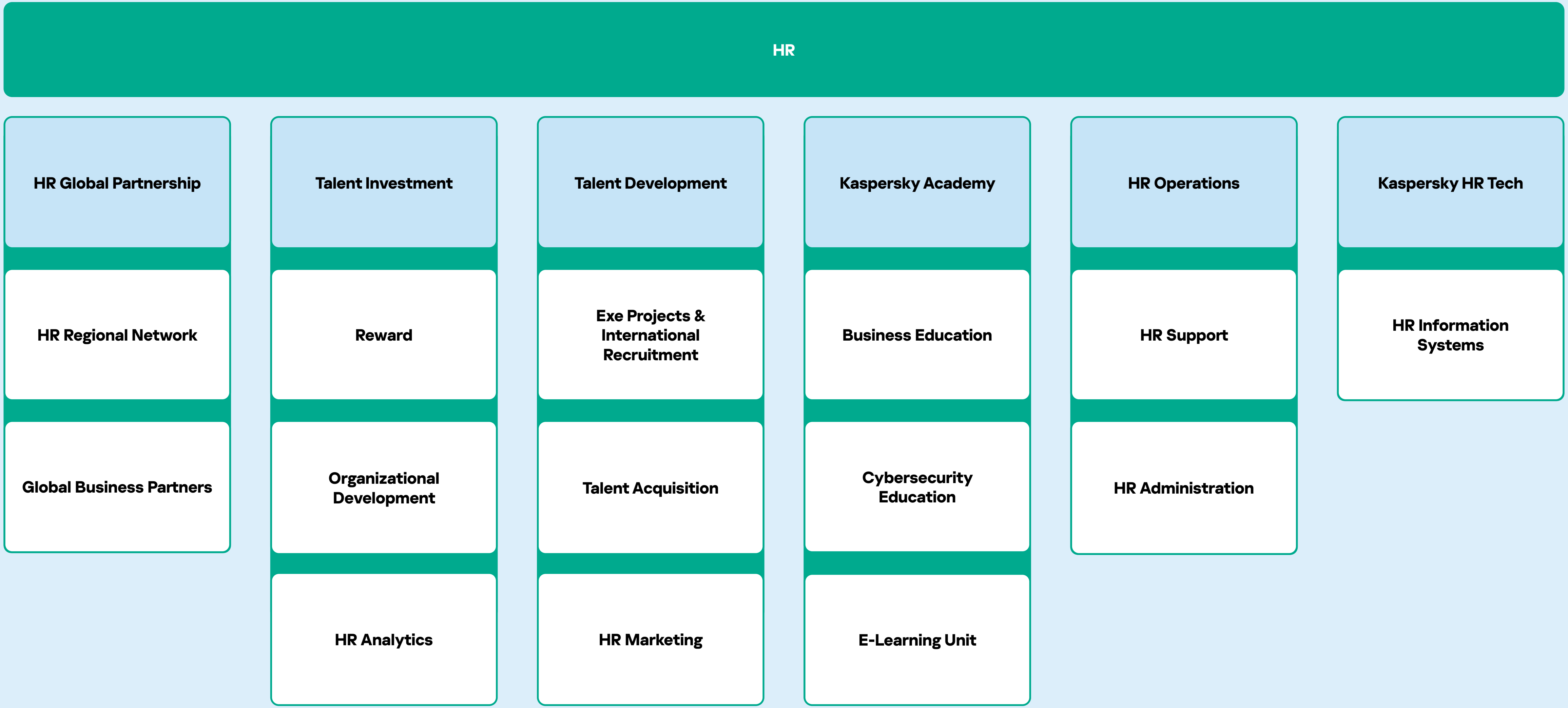
Approach to talent management

Relationships with our employees are based on trust and mutual respect. To guarantee a comfortable working environment for all employees, we thoroughly assess every aspect they encounter during their daily work routine, ranging from office conditions to performance evaluation procedures. We take note of everyone's needs and do everything we can to ensure Kaspersky's employees feel supported and taken care of in any situation. We create the conditions necessary for the development of individual employees, teams and the entire business as a whole.

Our key objectives:

- Provide suitable conditions for employees to work and develop, including competitive remuneration and an extensive benefits package
- Invest in the training and growth of employees through individual development plans, the introduction of new educational programs and an increase in the number of training hours per employee
- Develop the corporate volunteering program by increasing the number of participants and expanding cooperation with charitable foundations

HR management system



HR

- HR Global Partnership
  - HR Regional Network
  - Global Business Partners
- Talent Investment
  - Reward
  - Organizational Development
  - HR Analytics
- Talent Development
  - Exe Projects & International Recruitment
  - Talent Acquisition
  - HR Marketing
- Kaspersky Academy
  - Business Education
  - Cybersecurity Education
  - E-Learning Unit
- HR Operations
  - HR Support
  - HR Administration
- Kaspersky HR Tech
  - HR Information Systems

HR headcount and structure

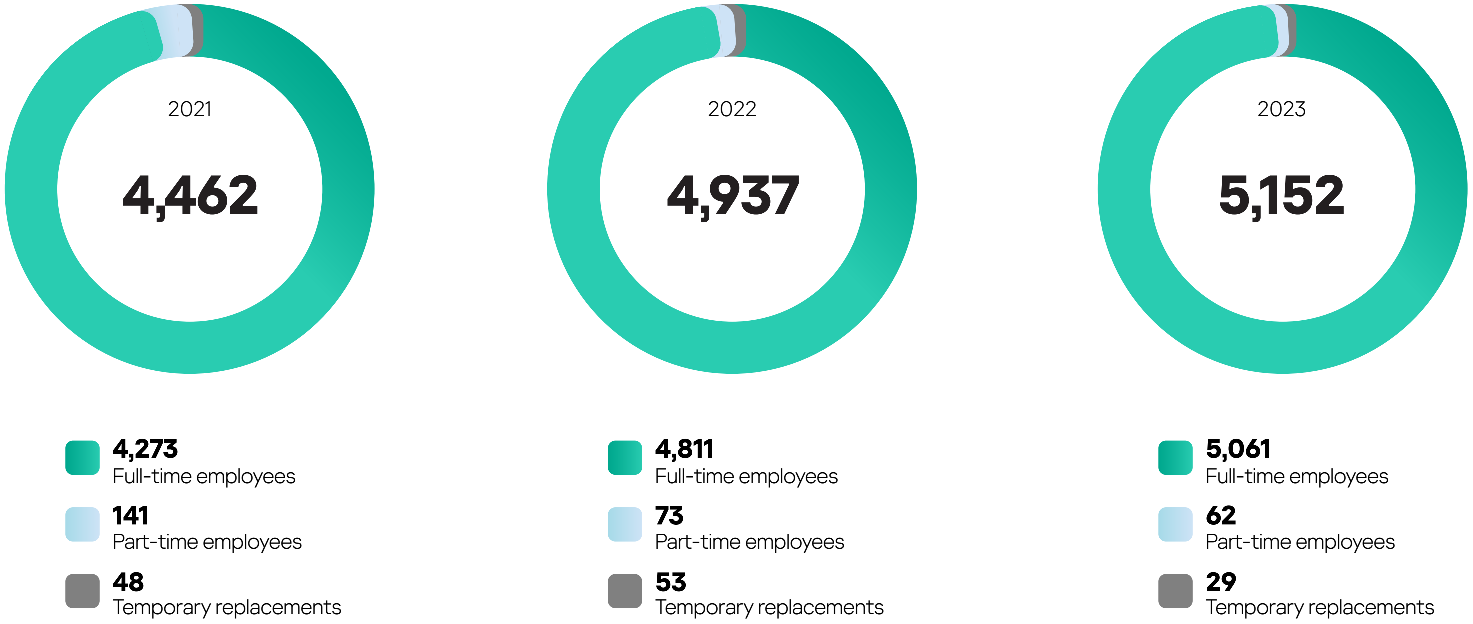
GRI 2-7 GRI 401-1

Kaspersky increased its staff size by 4.4 percent during the reporting period and had a total of 5,152 employees as of December 31, 2023. The increase in headcount is due to a decrease in overall resignations and the development of the Company's business in Latin America, Africa, the Middle East and Turkey.

+4.4%

growth in staff in 2023

Total number of employees, classified by type of contract



Staff turnover

Kaspersky brings together some of the world's best specialists and creates an environment in which each employee can showcase and develop their best qualities. This helps us solve complex problems quickly and efficiently.

When recruiting staff, we review candidates based on their professional expertise, and do not impose any limitations on hiring people based on age, gender, etc. For employees with disabilities, we create all the necessary conditions for them to fully realize their potential.

In 2023, staff turnover decreased in all the regions where Kaspersky operates and in all age groups due to changing trends in the labor market and the economic situation around the world.

33%

decrease in staff turnover compared with 2022

Career development programs

The Company strives to create the best possible conditions for employees to build their careers and to expand their professional experience or change their career path – moving positions vertically and horizontally within their team and/or transferring to another one. This provides an excellent opportunity to improve motivation and cross-functional interaction between units within a department. An individual development plan is created for each employee, which includes regular meetings with the Company's heads of departments, participation in cross-team projects and specialized training courses.

Kaspersky's employees are able to improve their professional and personal skills, learn foreign languages and take part in external training and educational events.

Since 2016, we have been investing in young talent and helping them build a career with Kaspersky. We also have a full-fledged paid internship program for Russian students – SafeBoard. Over the course of eight years since SafeBoard was introduced, more than half of the interns have joined our staff. They work in middle and senior level positions and some have become heads at various units.

For more about our SafeBoard program in the Training IT Staff subsection, please see p. 110

Financial incentives

We firmly believe that our skilled professionals should be rewarded for their contribution to Kaspersky's development. To this end, we maintain salaries at a competitive level and reward employees for their achievements.

To retain our talents and keep their salaries at a competitive level, we expanded our Compensations and Benefits team in late 2021. This helps us provide a faster and more in-depth analysis of market changes and trends, as well as financial assessments of employee benefits. In 2022, the Company doubled its investment in salaries and bonuses compared with 2021.

In 2022, salaries for Kaspersky's employees increased by an average of 20 percent in Russia and 18 percent worldwide. In 2023, remuneration for Kaspersky's employees grew by around 19 percent in Russia (17% worldwide).

Average salary increase for Kaspersky's employees worldwide:

18%
in 2022

17%
in 2023

Staff assessment

GRI 404-3

We regularly evaluate the performance of the Kaspersky's personnel with more than 90 percent of employees subjected to performance assessment process evaluations.

One of our key principles for compensation is "Remuneration for Results." The performance assessment results had a direct impact on the payment of bonuses, salary reviews and the promotions of our employees.

We plan to conduct employee performance reviews for 2023 in early 2024. The metrics used to evaluate the correlation between the assessment results and remuneration components remains unchanged.

Training and development

GRI 404-2

Kaspersky provides all its employees with opportunities for internal and external training. They can take online courses about our products, sign up for courses to develop their business, sales or personal skills, choose the most convenient way to learn a foreign language and also apply to participate in external training courses and events. We have both mandatory and optional corporate educational programs.

Compulsory courses

Information security

No matter what security measures we implement, ultimately, the human factor is the most vulnerable aspect in terms of information security. All Kaspersky's employees are trained in the basics of cybersecurity, even if they are not directly involved in the development or promotion of our solutions.

Kaspersky provides a series of information security courses to educate its employees on handling confidential information, secure password and account data storage practices, and recognizing phishing emails and websites.

Anti-corruption

At any modern company, employees need to understand and comply with anti-corruption laws. By following the rules learned in the anti-corruption course, our employees can help Kaspersky maintain its reputation and integrity, as well as avoid possible fines for the Company and personal liability.

Rules for addressing emergencies

Fire, smoke, sparks in electrical wiring and equipment, accidents and other incidents can cause harm to people's health and lives and lead to serious financial damage. Every Kaspersky's employees is required to learn safety rules so that they know how to take sufficient and coordinated actions in the event of an emergency.

Training on Company's products

Employees of the Sales and Presales teams are required to undergo mandatory training on Kaspersky's products. Depending on their position, employees must complete a course and pass an exam within 90–180 days to confirm their acquired knowledge about the Company's product line roadmap.

Optional courses and external training

- Massive open online courses (MOOCs)
- Face-to-face trainings and webinars on the Kaspersky.Academy internal portal
- Training programs as part of the Colab Tech project
- External courses to maintain and develop professional expertise
- Foreign language training

GRI 404-1

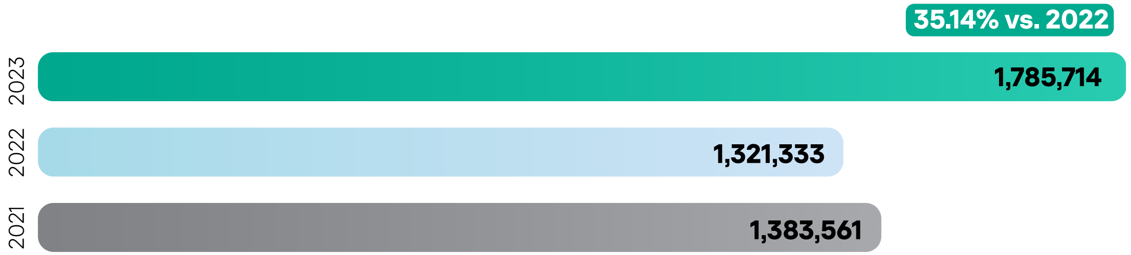
Training program results

Indicator	2021	2022	2023	Change 2023/2022, %
Average number of training hours (all types) per Company employee				
Total	**5.5**	**6.2**	**8.5**	**+37**
Total number of training hours per Company employee				
Women	7,903	8,909	**11,419**	+28
Men	15,555	21,002	**31,450**	+50
Technical specialists and managers	13,805	15,003	**21,806**	+45
Other specialists and managers	9,653	14,908	**21,063**	+41
Total	**23,458**	**29,911**	**42,869**	**+43**

In 2023, the average number of training hours per employee increased by 37 percent due to the fact that employees are choosing more comprehensive long-term external training programs over targeted short-term courses. Another reason is the significant growth in Kaspersky Academy's internal training portfolio and online courses available to employees on the portal.

We continue to improve our training programs and increase investment in employee education. In 2023, our training and development expenses grew by 13.5 percent compared with the previous year.

Investment in staff development and training, US$



In 2023, Kaspersky transitioned to a new learning management system with a more convenient interface and a variety of learning formats. The Company has immediate plans to further develop the platform, expand Kaspersky Academy's catalog of online courses, including training in foreign languages, and create educational journeys for the comprehensive development of employees both on specific topics (such as enterprise sales and communication skills) and for particular roles and positions.

Social policy

GRI 401-2

Kaspersky supports its employees throughout their entire career with us. We motivate them to lead a healthy lifestyle, provide access to professional medical care and offer financial support in difficult life situations.

Caring for people

We encourage our employees' commitment to a healthy lifestyle, offer them 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.

The Company believes it is crucial to know employees' opinions on various aspects of their work and have regular feedback sessions with them. We hold AMA sessions[1] and kick-off meetings with our management team several times a year to discuss results, plans and strategy.

The annual Kaspersky Awards ceremony equally recognizes the achievements of all departments for the year and rewards the most productive employees who made a major contribution to the Company's success over the past year.

Support for parenthood

GRI 401-3

We support all of our employees who have children: parents, adoptive parents and guardians alike. They are granted parental leave, and Kaspersky provides an additional corporate payment in the amount of their full salary on top of the government's maternity benefit for the entire maternity leave in Russia (usually 140 calendar days)[2].

The corporate voluntary health insurance program in Russia covers pregnancy and childbirth, as well as the following financial assistance after the birth of a child: US$1,600 for the first child and US$2,160 for the second and all subsequent children.

Kaspersky offers support programs for parents in every region where we operate, but specifics may vary depending on the laws of a given country.

[1] Ask Me Anything – an online event at which the Company's management answers questions from employees.

[2] For employees who have worked at the Company for at least a year.

Corporate culture and business ethics

Kaspersky is committed to following the best corporate practices, ensuring high-quality management and that we adhere to the ethical principles of business.

Key documents

- Local Labor Regulations
- UN Guiding Principles on Business and Human Rights

25%
of the Company's employees are women

95%
ratio of remuneration between men and women

Equal opportunities

Kaspersky does not tolerate discrimination in any form. This is one of the Company's key principles, which is consistent with the UN Guiding Principles on Business and Human Rights, as well as the UN Sustainable Development Goals (UN SDGs), including UN SDG targets 4.5, 5.1 and 8.5.

For more about the Company's contribution to the UN SDGs in the Sustainable Development section, please see pp. 17–18

We strictly comply with the law and do not restrict the hiring of people based on age, gender or other criteria. We also guarantee employment rights for individuals with disabilities at the Company. Kaspersky promotes the respectful relationships within teams and works to overcome industry stereotypes associated with working in IT.

Our contribution to breaking stereotypes about the IT industry

What is it really like to work in IT?

There are many assumptions about the IT industry that can scare off candidates with high potential, as well as prevent companies from recognizing the most valuable future employees. We have decided to debunk common myths based on the example of our employees who did not let stereotypes prevent them from building a career in IT.

Rapidly climb the corporate ladder and become a department head at 23? One can only dream...

You can't raise three children and have a successful career...

How can you be a valued non-technical specialist in a programming team? That is unimaginable...

There is no place for an extrovert in IT...

Can innovative and breakthrough products and solutions be created in Russia?..

We conducted a special research within our team and professional community and collected the top 20 stereotypes about the Russian IT industry. Then we invited our employees to refute them with their own examples to help us create the **People in Tech** project. Launched in late 2022 and involving 20 employees – from entry-level positions to Vice Presidents, who debunked industry myths and shared their professional journeys.

To make the project truly inspiring, we introduced an interactive component, giving users the chance to share their opinions about a certain stereotype. The results obtained were encouraging – up to 90% of respondents do not believe in the most common stereotypes even though the opinions on certain issues were divided almost equally.

What was the result?

Reach of the project

7+
million people

20,000
votes for or against a particular stereotype

People in Tech helped to strengthen Kaspersky's image as an open-minded employer that can find an unconventional way to present its teams and products to candidates. The project also helped dissolve outdated ideas about the Russian IT industry and inspired people to change their attitude towards it.

Find out more on the project's website careers.kaspersky.ru/peopleintech

Employee engagement

GRI 405-2

Kaspersky provides equal pay to all of its specialists based on their position and qualifications, regardless of age or gender. The market salary level is assessed for each position. To achieve this goal, the Company has strengthened the HR Department's team dedicated to compensation and benefits.

We are committed to attracting more women to the IT industry and collaborate with educational institutions around the world to achieve this goal, among others. Kaspersky holds educational events and master classes for young people in high schools and universities, and also organizes internships.

We have launched several online projects where women can share their knowledge and experience in IT, including the Women in CyberSecurity social media community, which has more than 30,000 members, and the Empower Women website, where the Company's employees share their educational and career journeys, provide guidance, and contribute to podcasts.

For more about the Company's contribution to solving the problem of gender imbalance in the IT industry, please see the Women in IT: Power of Equality subsection

GRI 405-1, TC-SI-330-a.3

Kaspersky provides support to applicants and employees with disabilities, as developing every person's true potential and achieving their personal goals matters most to us.

When selecting candidates, we exclusively evaluate their professional skills, experience and expertise. Many of our job openings offer remote work options, which can be especially beneficial for employees with disabilities.

All employees with disabilities are provided with the benefits in accordance with local law.

TC-SI-330-a.2

Each year, we evaluate employee satisfaction levels by conducting the confidential YourVoice survey. It enables Kaspersky to learn more about employees' views on changes at the Company, adjust its strategy and assess the extent to which employees are influenced by various drivers, such as pay, the benefits package, work-life balance, prospects for professional growth and the team atmosphere.

The key indicator we focus on is Employee Net Promoter Score (eNPS), which reflects the proportion of employees who are willing to recommend the Company as an employer.

The eNPS grew by 6.7 p.p. to 52.3 percent in 2022 and by 4.5 p.p. to a record 56.8 percent in 2023, which is higher than the average Russian market[1]. In 2023, the Company also broke a record for the number of survey participants, with almost 90 percent of employees taking part.

The survey results are available for analysis by all Kaspersky managers, including senior executives, with different breakdowns (by team, department, division, region, age group, position level and more). This makes it possible to objectively assess the situation both at the Company as a whole and within individual divisions, as well as identify strengths and areas for further development.

[1] According to Happy Inc, a Russian company in HR Tech and the market leader in solutions for engagement surveys.

Occupational safety and health protection

We make sure each work space at Kaspersky is comfortable and safe, and that all employees have access to professional medical care.

0

accidents involving occupational risks in 2022 and 2023

Key documents

- Labor Code of the Russian Federation
- Regulation on the Identification of Hazards and the Level of Occupational Risks
- Instructions on Fire Safety Measures
- Internal Labor Regulations
- Occupational Safety Policy

Occupational safety and health management

GRI 403-2 GRI 403-4 GRI 403-5

The HR Department and particularly HR Support team ensures occupational safety and the health of its employees at Kaspersky with the help of external consultants.

In addition, the Company has an occupational safety commission, which includes representatives of various departments. In spring 2023, a series of Safe Environment videos were created to remind our employees about the ways to maintain a comfortable and safe environment in the office: how to host parties, order office passes and park correctly.

GRI 403-9

Most Kaspersky's employees work in the office. Not a single case of injury was recorded among employees during the reporting period.

GRI 403-6

All of Kaspersky's Russian employees and their children under the age of 16 are covered by the corporate voluntary health insurance program, which also includes accident insurance (for Company's employees). If an employee has an accident, it can be reported to the insurance company through the HR Department.

The voluntary health insurance program enables employees to undergo cancer treatment, make use of hospital services, receive psychological help online and offline and get vaccinated against seasonal diseases. The Company's headquarters has a gym and a sauna, and employees can visit a therapist, psychologist, or massage therapist in-house. We also partly compensate employees' fees for membership at fitness centers as well as kids summer camps. We also regularly conduct employee surveys to assess the effectiveness of the occupational safety and health management system.

All the Company's units regularly conduct special assessments of working conditions.

Engagement with local communities

We consider the needs of those who require our support. Kaspersky works with federal and regional charitable foundations, helps people with serious illnesses and vulnerable population groups, and strives to involve its employees in such activities.

>US$845,300

in direct charity donations in 2022–2023

4,800

licenses for Kaspersky's products were donated to charitable foundations and private users with disabilities or people in difficult life situations to protect their devices

~300

units of technical equipment were donated to NPOs and educational institutions in the reporting period

In accordance with Kaspersky's internal charity policy, the ESG & Sustainability department determines:

- The main focuses of the Company's charitable activities
- The criteria and procedure for interaction with NPOs when developing, selecting and implementing charitable projects and events
- The procedures for the donation of product licenses for security solutions and IT equipment

In summer 2023, we created a dedicated CSR page on our intranet, which features all the relevant information about our sustainable development activities, a complete list of our partners (charitable foundations, NPOs and educational institutions), the amount of financial support provided and a list of volunteer projects that our employees can join.

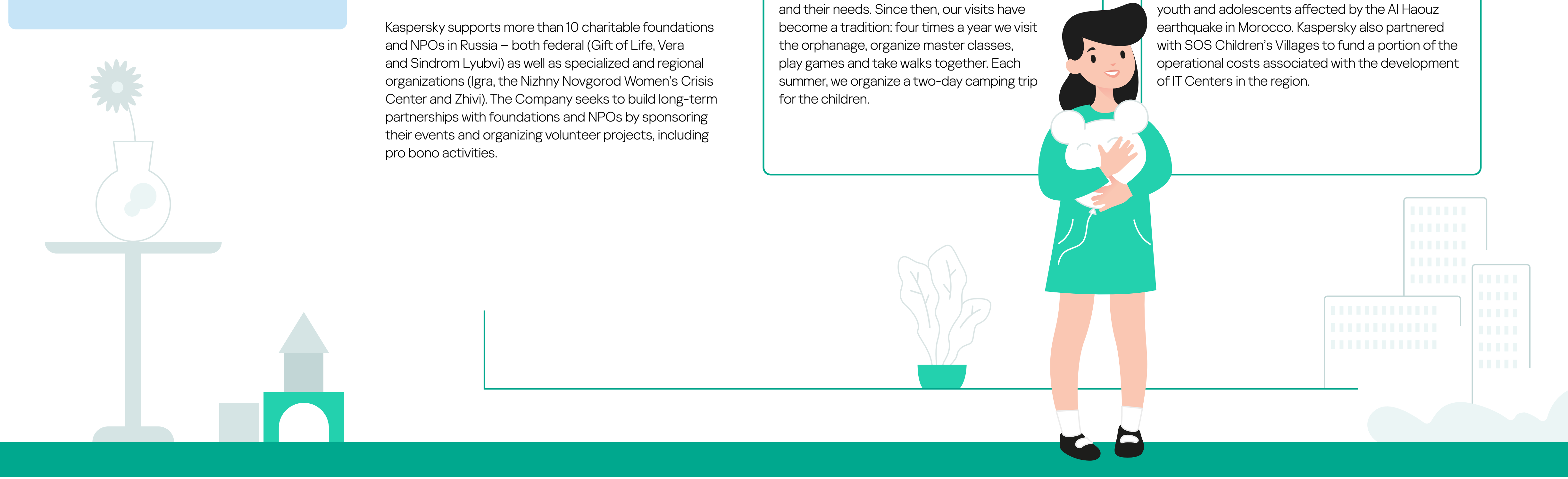
The Company also supports an orphanage and a school in Tver, educational institutions and NPOs that arrange care for orphans, help victims of violence (including digital violence) and people with disabilities and serious illnesses, as well as NPOs that protect the environment and raise awareness about blood donations, ecology and other sustainable development topics.

Kaspersky supports more than 10 charitable foundations and NPOs in Russia – both federal (Gift of Life, Vera and Sindrom Lyubvi) as well as specialized and regional organizations (Igra, the Nizhny Novgorod Women's Crisis Center and Zhivi). The Company seeks to build long-term partnerships with foundations and NPOs by sponsoring their events and organizing volunteer projects, including pro bono activities.

We also provide administrative and financial support to an orphanage in Udomlya and Tver School No. 4, a specialized school for children with psychological development impairments, autism spectrum disorders and musculoskeletal disorders. We assist these institutions with making repairs inside their buildings, purchasing of equipment, household appliances and chemicals, clothing, shoes and school supplies for foster children, as well as organize summer vacation trips for them. We help the Udomlya orphanage since 2014 after a group of Kaspersky volunteers along with their friends and relatives began traveling to Udomlya and got acquainted with the staff, children and their needs. Since then, our visits have become a tradition: four times a year we visit the orphanage, organize master classes, play games and take walks together. Each summer, we organize a two-day camping trip for the children.

In addition, the Company provides support to disaster victims, the elderly and people in difficult life situations.

In February 2023, Kaspersky allocated a budget of 390,000 Turkish lira for organizations helping earthquake victims: the Turkish Disaster and Emergency Management Presidency (AFAD), NPO Ahbap and the Turkish IT society Türkiye Bilişim Derneği (TBD). Our Turkey office colleagues sent a van of drinking water and power banks to the region affected by the earthquake. In September 2023, the Company allocated US$10,000 to support the well-being and quality education for youth and adolescents affected by the Al Haouz earthquake in Morocco. Kaspersky also partnered with SOS Children's Villages to fund a portion of the operational costs associated with the development of IT Centers in the region.



Social and charitable projects

GRI 203-1

Each year, we encourage fundraising efforts among our employees to support activities organized by our NPO partners and coordinate our own events around significant awareness dates or national holidays. From January 1, 2022 to December 31, 2023, our employees in Russia donated more than

US$28,000

for Zhivi, Igra, Gift of Life, Sindrom Lyubvi, Vera and Podarok Angelu foundations.

In early 2022, Kaspersky joined the Business Council on Disability Issues created by Perspektiva, a Regional Public Organization for People with Disabilities, and for the first time took part in a summer job fair for applicants with disabilities. The Company continued to support this event in 2023.

In autumn 2022, on International Day of Persons with Disabilities, the Company launched an internal special project aimed at destigmatizing the topic of inclusive employment “The Boundaries We Push”. We dedicated it to the professional and personal journeys of Kaspersky employees with disabilities. In 2023, we took the project further by creating a new online project Impossible, where this time both our employees with disabilities and those raising children with disabilities shared their personal stories. This marked the first time that the project became public, since we believe it is important to talk openly about complex and difficult subjects in order to remind people about the value of mutual support.

That same autumn, we began sharing updates about our charitable initiatives, as well as our social and volunteer projects on our social media accounts. The Kaspersky Daily telegram channel now has a dedicated CSR digest released every three months. In addition, Kaspersky supported the International Disability Film Festival Breaking Down Barriers organized by the Perspectiva Regional Public Organization. In winter 2022/2023, the Company together with the Gift of Life Foundation helped to open a playroom for young patients undergoing treatment at the radiation therapy department of the Morozov Hospital.

In May and December 2023, we helped organize business breakfast events for the Business Council on Disability Issues. The first event was devoted to the topic “First steps when hiring an employee with a disability: creating the right conditions within the company.” In December, the business breakfast participants discussed the topic “Employment of applicants with disabilities: communication and training of management and responsible employees.” Both events were attended by 30 representatives of companies, members of the council.

In November 2023, we began taking part in Technologies for Good, a federal project being implemented by Sovcombank and Skolkovo Fintech Hub to provide infrastructure support and ensure the digital development of NPOs and charitable foundations in Russia. The project provides socially oriented organizations with the products and services they need free of charge or on special terms. As part of the project, we provide complimentary licenses for Kaspersky’s products. Eleven NPOs received free licenses in 2023.

In 2024, we plan to issue special learning materials on the basics of computer literacy together with the Sindrom Lyubvi Foundation. These easy-to-read cards will make it easier for people with mental disabilities to get a better understanding of this important topic.

We strive to enhance the accessibility of our products and services for people with disabilities. To this end, we are working on updating our products to make them easier for people with disabilities to use.

In 2023, we made a number of improvements to our products. Kaspersky for Windows now supports high contrast mode. The update improved readability, element brightness and navigation, making the app experience more efficient and comfortable for color-blind users.

Kaspersky for Mac is now fully compatible with macOS Dark Mode and Display Settings, which make it possible to customize your experience to suit individual preferences. In addition, Kaspersky for Mac includes VoiceOver, which provides accessibility for users with visual impairments.

Our contribution to the career development of young professionals with disabilities

Helping young people realize their potential

- Participants from 22 Russian cities
- 8 mentors
- 6 weeks of online practice

In November 2023, along with other companies, Kaspersky took part in the “Try a real profession” program, which was organized by our partner “Perspektiva”, a regional NPO dedicated to enabling individuals with disabilities to access education and employment opportunities. The program aims to help students and graduates with disabilities realize their potential by immersing themselves in their future profession with a dedicated mentor.

Recent graduates and senior year students interested in the following field of work were invited to participate in the program:

- IT
- Economics/Finance
- Law
- Marketing
- HR

This was the first time that our Company took part in this program, with eight employees from various departments becoming mentors for participants with disabilities.

What was the result?

Students from 22 Russian cities took part in the program. Over the course of six weeks, they selected and worked on business cases with their mentors, and upon conclusion of the program, they presented their projects online. For example, one group of participants developed a browser solution, another came up with an application for editing ALT texts, while a third prepared a set of marketing assets for a fictional video game.

In doing so, the students and graduates had a chance to try their hand at different professions, apply their skills to solve real technical problems and also gained experience working in a team.

Volunteer programs

More than 200 Kaspersky's employees actively participate in the corporate volunteering program, which includes several initiatives: blood donation, charity sporting events, patronage of an orphanage and pro bono work.

Sports volunteering

In 2022–2023, the Company's employees participated in a number of charity sporting events to support its partner-NPOs Sindrom Lyubvi, Vera and Persperktiva: running and cycling marathons, online triathlons, biathlons and mini-football competitions. We continue to engage in this format for several reasons. First, sport is very popular among our employees. Over the past five years, our sports enthusiasts have established a full-fledged community. Second, sporting events help foundations and NPOs promote inclusion and doing good deeds, which is something that is very in line with the Company's mission. Third, sport activities are an excellent form of team building, uniting colleagues from different departments.

Patronage of the Udomlya Orphanage

Four times a year, our employees visit the Udomlya Orphanage. For each trip a special program of activities for the foster children is carefully planned, including educational lectures, sporting events and a summer camping trip with music and games. Prior to each trip, Kaspersky's employees help purchase medicine, hygiene products, clothing, shoes and school supplies for the kids.

Volunteering at hospices

Twice a year, our employees volunteer at Moscow hospices and palliative care centers under the patronage of the Vera Foundation. Teams gather to do spring cleaning of the facilities, plant flowers, gather leaves in the garden. For each visit, employees also help resolve housekeeping issues such as buying water, sweets, tea, milk, beauty and household supplies.

Blood donations

Roughly 150 employees from the Company donate blood twice a year to aid the beneficiaries of the Gift of Life Foundation. The event is held at Kaspersky's Moscow office together with the Russian Federal Medical-Biological Agency (FMBA) Blood Center. In 2023, we invited employees to become potential bone marrow and stem cell donors. We organized a lecture with a representative of the FMBA, who provided our donors with detailed information about the procedure for HLA (human leukocyte antigen) typing, how to prepare for the testing and what the recommendations are. At the following event in the autumn, 32 employees took part in HLA typing.

Pro bono volunteering

Starting in 2022, we launched a pro bono volunteering program.

Our experts helped to conduct online voting for the annual Charity Against Cancer award for the Gift of Life Foundation, organized two training sessions on the basics of cyber-hygiene for employees of SOS Children's Villages from different Russian regions and conducted two more sessions as part of the "I Can" educational project together with the Russian social change platform todogood.

In summer 2022, Kaspersky experts held a career guidance lecture for children with disabilities as part of a summer camp hosted by Perspectiva and served as mentors for people with disabilities as part of the Interregional Career Prospects educational project of the NPO.

In 2023, our design team helped Sindrom Lyubvi foundation update their annual online campaign dedicated to World Down Syndrome Day. The goal was to assess and update the promotional page visually, make it more attractive with new images, color combinations and logic (reduce the number of unnecessary clicks) and simplify the donor's journey. After analyzing similar promotions, our colleagues proposed a minimalist design with clear and simple visuals that would help emphasize the key message and gain the attention of an older audience. We are happy that we contributed to the improvement of the campaign and helped the foundation receive a record number of donations (more than US$10,000, which is twice as much as in 2022.

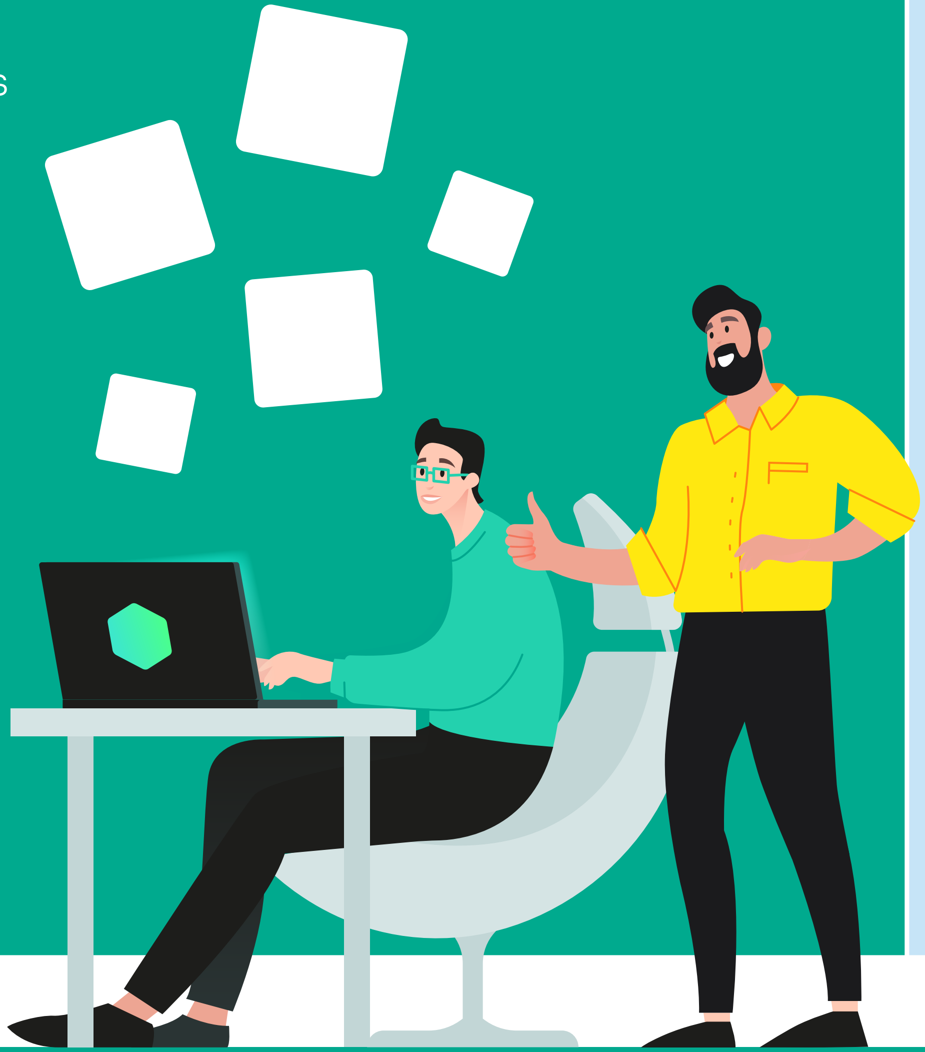
Our contribution to boosting employee motivation

Inspiring our colleagues to reach greater heights

In 2023, we added some new unique and useful features to the employee personal account on the corporate intranet. It now has sections where each employee can complete themselves. For example, they can specify their T-shirt size so that the internal communications and production team knows what kind of T-shirts are needed and exactly how many when ordering merchandise for the annual corporate event. These precise calculations helped us save more than US$5,000 last year.

In addition, employees are asked to indicate the projects they are involved in, their area of expertise and how they can be useful to other colleagues. All this data is loaded into their personal account in the form of tags, which makes it easier for our colleagues to not only find those responsible for a particular project, but also a friend with similar interests.

One of the most discussed innovations on the Kaspersky intranet in 2023 was the introduction of achievement icons in the employee's personal profile. The internal communications team calls these virtual awards (badges) that are presented for an employee's contribution to the Company. Achievements are awarded to employees who have worked for several years at Kaspersky, winners of corporate awards and competitions, athletes, volunteers, public speakers and authors of patented technologies. This tool enables employees to understand what kind of behavior is encouraged at the Company, while the competitiveness and playful style of the awards make them particularly attractive. Kaspersky's employees have a very busy life outside of work, so there are numerous reasons to reward achievements for various activities: musicians, artists, special achievements for memes and more.



What was the result?

In a little over a year since the award was introduced, the internal communications team has honored

43 achievements.

More than 1,700 people have already received

2,523 badges in total.

Training staff for the IT industry. Our experience

How we train specialists

- We give a jump-start to school students and train university students
- We upgrade the qualifications of information security specialists

As technology continues to rapidly develop, it is crucial for IT specialists to maintain their skill level and to constantly bring in new talent to the team. Kaspersky firmly believes the most reliable way to train the future workforce is to grow it ourselves. We are already implementing numerous educational and partnership projects that encompass an audience ranging from schoolchildren to IT specialists.

Our approach to education

With information technologies, it is important to think long-term: who will be working for Kaspersky tomorrow? In a year? In five to 10 years? Can we even imagine what these people are doing right now, whether they are specialists or school students who have just embarked on the path of studying information technologies? What will their knowledge and skills be like when they join our team? Will their knowledge level be consistent with how rapidly technology has developed?

Kaspersky conducted its own research "The portrait of modern Information Security professional" in order to evaluate the current state of the labor market and analyze the exact reasons for the cybersecurity skills shortage. Russia reported the largest cybersecurity staff shortage, followed by Latin America, APAC and META. A lack of in-house cybersecurity talent is one of the main reasons why companies turn to IT and security service providers, along with the increased efficiency of outsourcing and the need to comply with regulatory requirements.

41%

of the companies questioned describe their cybersecurity teams as "somewhat" or "significantly understaffed"[1]

We realize that training needs to be conducted early and continuously. This is why we have developed and are constantly expanding our range of educational projects. We work with school and university students and teachers, record cartoons and video lectures for the younger generation, hold hackathons[2], offer on-the-job training in summer and paid internships, and also implement numerous educational projects in partnership with key agencies and universities. Separately, we train specialists who also need to constantly refresh their knowledge and practical skills.

> "Education is one of the main drivers of the safe future that we seek to build, while paying special attention to social projects".

Kirill Shiryayev,
Head of Kaspersky Academy

[1] The research surveyed more than 1,000 InfoSec professionals from Asia-Pacific, Europe, the META region, North and Latin America.
[2] A hackathon is an event during which IT specialists jointly develop a solution to a given problem.

Educating school students

We believe it's important for children to acquaint themselves with the industry they will eventually work in. According to our survey[1], 41 percent of children in Russia want to work in IT. Kaspersky is constantly finding new formats to educate and train school children so they are familiar with, and can understand cybersecurity.

Kaspersky Math Vertical

One of our key educational projects is the Kaspersky Math Vertical, where we have crafted a specialized program focusing on information security. We take a comprehensive approach to this issue: engaging not only with school students but also with teachers in our program.

Kaspersky has been participating in the Moscow Math Vertical program under the auspices of the Moscow Department of Education since its launch in 2017. As part of the program, school students study mathematics and different aspects of natural sciences in depth. With the Company's support, a separate course called Kaspersky Math Vertical has been created with an emphasis on the Basics of Information Security, consisting of several key blocks such as programming basics, an introduction to cutting-edge technology, and advice on security in cyberspace. We have been implementing the course for three years at our partner schools in Moscow for students in grades 7–11.

15 schools
are taking part in the Kaspersky Math Vertical project

Today, Kaspersky has a presence at 15 schools in Moscow. Our experts teach special courses to students and host seminars. After finishing the tenth grade, students join us as interns, which not only simplifies their path to university for an IT major, but also provides them with an opportunity to remain at the Company and develop their skills.

In 2023, the first participants of the Math Vertical program graduated from school. Some of them won the National Technology Olympiad in Information Security.

School students take part in numerous online events organized by Kaspersky. In particular, we organized the Kaspersky IT Marathon at Moscow schools. In 2023, the marathon involved 34 schools with several thousand students participating.

More than 400 mathematics and computer science teachers in Moscow completed advanced training courses from Kaspersky in the 2022/2023 academic year.

We work closely with school teachers. This marks the third year in a row that our specialists conducted advanced training courses for Moscow teachers of mathematics and computer science together with the Moscow Department of Education and Science. The training takes place online, and on completion, teachers take tests to verify their knowledge. Some teachers take our course annually because they understand that the IT industry is developing rapidly and their knowledge needs to be refreshed.

34 schools
participate in the Kaspersky IT Marathon

Teachers who complete our courses receive a corresponding state-issued document, which is issued by the city's methodological center. In the first half of the 2023/2024 academic year, 250 teachers successfully completed these courses, and roughly the same number will complete them in the second half of the year. We are ready to extend our training programs to teachers in the regions.

> "A few years ago, we concluded a historic agreement with the Moscow Ministry of Education. The conditions were as follows: we start with one primary school, gradually expand our coverage, and publish online materials that could be useful to the whole city and eventually the whole country. We comply with these terms unconditionally".

Veniamin Ginodman,
Educational Projects Adviser

[1] The survey was commissioned by Kaspersky and conducted in spring 2023 among 2,000 parents and their school and preschool age children in Russia.

Digital Lesson

Since 2018, Kaspersky has been a partner of the Russian "Digital Lesson" educational project, which is part of the HR for the Digital Economy federal project. Each year, we develop and release a lesson focused on a specific topic with an interactive simulator for school students, their parents and teachers to use over a three-week period.

HR for the Digital Economy federal project

Russian educational project "Digital Lesson"

Implemented by the Ministry of Education, the Ministry of Digital Development and the Digital Economy autonomous non-profit organization in partnership with leading Russian tech companies

Since 2018, we have prepared six thematic lessons about cybersecurity, ways to protect yourself and your data, as well as the work of IT specialists and developers. We make efforts not to overload students with complex information and, on the contrary, only present the most important ideas in a simple and accessible way, while also using high-quality animation and interactivity to pique their interest.

The topic of one of the lessons for the 2022/2023 academic year was the protection of personal data and mobile devices: "What's Hiding in Your Smartphone: Exploring Mobile Threats." Every lessons since 2018 has been made available on the project's website and can be accessed at any time, so students can watch them at school, or at home with the whole family.

In early 2024, students time-traveled with us to the year 2050 and were able to try their hand at building a cybersecure future. Even in a fantasy world, these kids are solving a very real problem – how to protect a smart home and repel cyberattacks using the latest technologies. In addition, the children once again have a good reason to think about their future profession: in 2024, our lessons taught them who pentesters[1] and secure development specialists are.

The students pass through several stages in the learning process:

- Watch a video lecture with Kaspersky's mascot, Midori Kuma
- Practice on a simulator that is divided into three levels of difficulty depending on the student's grade. The simulator consists of an animated and interactive comic about the adventures of two kids, whom Midori and the students help resolve an IT problem
- Receive a certificate for completing the lesson and collect achievements

By recording cybersecurity lessons for children, we achieve the following goals:

- We tell children and adults about the virtual world and the threats it poses
- We teach them methods to protect their identity and personal data
- We introduce school students to new professions: a developer of security solutions for smartphones, an information security expert or a content and spam analyst
- We reveal some of the nuances of developing protection for mobile devices

Kaspersky's Digital Lesson has been completed

13.5 million

times since 2018

11–15%

of children have encountered at least one of the following threats: phone or online fraud, account hacking or infection of their devices with malware[2]

Digital Lesson completed

>2 million times

in 2023

[1] A pentester is a specialist who tests a program for deliberate penetration (hacker attack).

[2] According to a survey commissioned by Kaspersky Lab in Russia in 2022, featuring 2,008 people, including children and their parents.

Online course for school students

In October 2023, we published the first materials of the Basics of Information Security online course, which is designed for seventh grade students and available in the Moscow Electronic School (MES) system in Russian.

The course consists of three modules that gradually immerse students in the subject. It is based on materials Moscow schools accumulated when they were working on joint projects with the Moscow Department of Education and Science, and take into account the latest trends in the industry. School students study the topic in an interactive way by helping good guys fight evil.

What we teach middle and high school students:

- Programming in scripting languages[1]
- Secure information systems configurations
- Data encryption and decryption
- Secure application creation

In summer 2024, we plan to update our online course on information security. By October 1, we will prepare the exact same course for eighth grade students. It will not only target Muscovites, but all residents of Russia. Any student, teacher, or responsible parent from any corner of the country who is interested in the project and needs assistance can go to the website https://kids.kaspersky.ru and use our course materials.

Digital Outreach

We also use short cartoons to introduce the younger generation to Internet safety. In 2022, we joined the Russian “Digital Outreach” (“Tsifrovoy likbez”) educational project, which aims to improve digital awareness and cybersecurity literacy. The project is based on videos for children and adults created by leading IT companies.

In 2022–2023, together with the Digital Economy autonomous non-profit organization and with the support of the Ministry of Education and the Ministry of Digital Development, we released three cartoons for children over six years old. We recommend that adults watch them with their children to explain any words they do not understand and help them comprehend the information.

In just two quick minutes, we teach children about key cyberthreats. The story follows the adventures of the inhabitants of Ocean City. The main character, Lina, is an aspiring journalist who is interning at a major IT company Karasevsky, where she is writing a blog about how the town’s residents fall for cyber-fraudsters.

A written explanation of complex concepts and details accompanies the video, allowing adults to explain things that children might not understand, and further expand their own knowledge. Each video can be downloaded for educational purposes at any time, in a shareable format so they can been seen even when people do not have internet access.

We firmly believe that such programs increase the overall level of digital awareness, and also help us popularize the IT profession, ensuring that future specialists constantly maintain interest in it.

Technology Valley program

1,200

participants registered for Technology Valley program

44

finalists attended the final training session

While developing educational projects for school students, we decided to organize a real internship for them, just like we do for university students, to give them the opportunity to learn more about different IT professions and plunge into the world of cybersecurity. In 2023, we held our first open summer internship for grade 8–10 school students and first- and second-year university students. The three-week Technology Valley program consisted of webinars and offline classes at the Kaspersky’s headquarters. We invited students who excelled in the online training to participate in the in-person part of the on-the-job training.

A total of 1,200 participants registered for the project, and Kaspersky specialists introduced them to IT professions online. The Technology Valley participants then completed their homework, and based on their results, we selected 44 people (32 from Moscow and 12 from other regions) who came to our Moscow office. We took them on office tours, where our developers, testers and other experts spent three days telling the children about IT professions and helped them get an idea of what it is like to work at the Company. Team-building activities and quizzes were also organized for the students.

In 2024, the Company plans to repeat the program and scale it up, since we saw that the target audience has great interest in the Technology Valley project.

[1] Programming languages (e.g., JavaScript, Python).

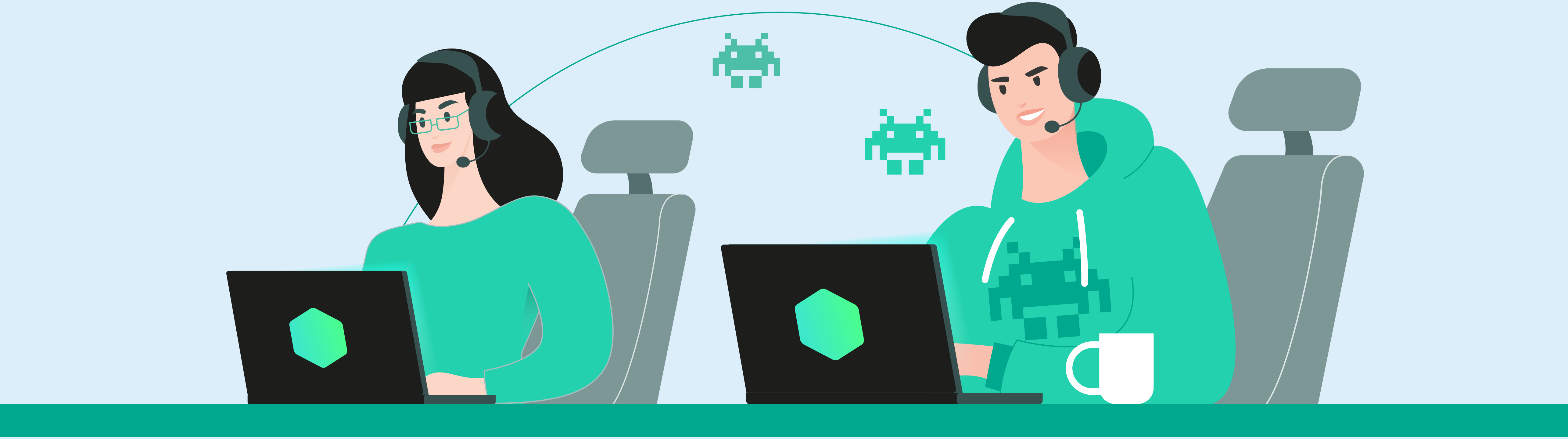
Development of e-sports for children and teenagers

Russia is the first country to officially recognize competitive programming as a sport. In June 2023, we concluded a strategic cooperation agreement with the Russian Sports Programming Federation. By helping athletes prepare for competitions, we hope to contribute to building up human resources in the IT sector. School and university students will have an opportunity to enhance their IT knowledge and skills and always stay up to date with the main events in our industry.

New projects for school students

We have received numerous inquiries from schools and colleges interested in our new courses. To meet their needs, Kaspersky plans to launch two new courses in 2024. One of them – Enter_IT – is dedicated to real professions at an IT company. This course will introduce students to the information security industry, outline various professions within this field, and provide guidance on how to pursue careers in this area. The new course will be available to students from any part of Russia and other Russian-speaking countries, since it will be released in video format.

We are also preparing a cyber-hygiene video course with a focus on the rules of online behavior which we plan to release in 2024 in Russian and English, and distribute internationally.



Kaspersky Academy

In an effort to bolster human resources in the IT sector, we are constantly expanding our collaboration with universities. Our goal is to provide the knowledge and hands-on experience required by students globally. Furthermore, we facilitate the connection of talented young individuals, fostering networking, knowledge sharing, and interactions with industry experts to enhance their readiness for the professional world.

To achieve this goal, we have established long-standing collaborations with universities across various initiatives: arranging hackathons and competitions, both domestically and internationally; providing internship opportunities for students; establishing joint laboratories and research centers equipped with state-of-the-art technology to enhance students' skills.

Academy Alliance

In autumn 2023, the Academy Alliance welcomed

~20 universities

from around the world

In 2023, we expanded the list of formats for cooperation with universities and students by developing the special Kaspersky Academy Alliance partner program, which we launched in September. It will enable us to use our cybersecurity technologies and experience in the educational process. We believe this will help strengthen existing programs and provide the industry with professionals who are best prepared to work in the real world. The program participants have access to online courses and global expertise, can attend lectures and trainings, and have access to Kaspersky's products.

The program offers two types of participation for universities:

- Associate Membership – for universities that annually graduate at least 400 bachelors and 50 masters in computer science, applied information science and computer science fields
- Advanced Membership – for universities that, in addition to the above, also graduate at least 50 students with degrees in information security

Numerous educational institutions spanning multiple countries are interested in the Kaspersky Academy Alliance program. We currently cooperate with around 20 universities and are in the process of signing agreements with several educational institutions. These include major universities in India, Spain, Kazakhstan, Uzbekistan and Peru. It is essentially an intercontinental partnership already. Over time, we anticipate that numerous European universities and educational institutions from Africa, Asia and Latin America will join the list of those that wish to participate in the program.

Eventually, Kaspersky plans for the Kaspersky Academy Alliance to formalize its collaboration with all universities previously engaged at the memorandum level and to further expand regional cooperation.

Cooperation with universities

Working with universities is a key component of Kaspersky's strategy to develop human capital and the Company's scientific and technical potential. We work with universities around the world.

200+ universities

42 countries

150 students

have undergone training based on KasperskyOS since the laboratory opened

For more about Cyber Immunity and KasperskyOS, please see the Safer Cyber World section

Robot semi-trailers and their Cyber Immunity

We follow trends in commerce, specifically how the popularity of automated logistics systems is on the rise. Boosting cyber-resilience is one of the key objectives for their further development. In November 2023, together with MAI, we held a hackathon to create a control system for Alphabot/RaspberryPi-based logistics robots that run on KasperskyOS. The system must be invulnerable to hacker attacks and successfully deliver cargo along a particular route.

Secur'IT Cup: spreading cybersecurity knowledge around the world

We believe it's important to provide students, universities, and people worldwide with opportunities to advance their ideas and pursue successful careers.

Since 2018, Kaspersky has been welcoming talented young individuals to demonstrate their innovative problem-solving skills in addressing critical information security challenges in our international Secur'IT Cup competition. As per the rules of the competition, we invite participants to develop projects individually or in teams in certain areas and compete for cash prizes and the opportunity to take our Kaspersky Expert Training online courses. The judges include experts from Kaspersky's Global Research & Analysis Team (GReAT), as well as representatives of foreign universities and winners of previous years' competitions.

In 2023, we focused on developing the gaming universe, ensuring data and financial security, as well as protecting seniors and pets. One key innovation in this year's competition is the opportunity to communicate live with Kaspersky experts during mentoring sessions in order to receive competent advice and perfect the project. Developers from Kenya, Mauritius, Nigeria, Russia, Saudi Arabia and Singapore reached the finals of the Secur'IT Cup 2023.

More than 6,000

people have taken part in the competition since 2018

US$10,000

top prize of the Secur'IT Cup 2023

KIPS Championship: training on information security skills

In autumn 2022, the Company held the Kaspersky Interactive Protection Simulation (KIPS) international championship among students. This gamified training session provides a realistic understanding of what happens during a cyberattack and allows contestants to gain gamified learning experience. The KIPS Championship helps young professionals learn to effectively respond to cyber-incidents in such areas as banking and public administration.

A total of 77 teams from 17 countries registered for the competition. The SPAM team from National Research Nuclear University MEPhI (Moscow Engineering Physics Institute) was declared the winner of the competition following the final event, which was held online on December 1, 2022. The final round of the competition was devoted to a technical attribution using a specially designed fictional environment that simulates cyberattacks on the United Nations. Players had to put together pieces of a puzzle with technical evidence of the attacks and make decisions using action cards to perform the most accurate technical analysis of the attack.

77 teams from 17 countries

registered for the KIPS Championship in 2022

Internships

We firmly believe demand for graduates depends on whether they have practical experience in the industry.

Kaspersky offers paid SafeBoard internships for students to work alongside industry experts. SafeBoard is a program where interns are guaranteed support and assistance, as well as a chance to get a job with an industry leader immediately after graduation. Internships are held twice a year – in fall and spring. To apply for an internship, students living in Moscow and the Moscow Region must submit an application and go through a three-stage selection process consisting of a technical knowledge test, practical task and a video interview.

As a socially responsible company, we monitor the salary level of SafeBoard program interns and increased it by 15 percent in 2023.

We ensure the internship does not interfere with the educational process: students can determine the number of hours they work per week on their own (from 20 to 35 hours when school is in session and up to 40 hours in the summer) and work format (entirely office or a hybrid format).

In 2023, we updated our onboarding process and now train interns on technical and business skills. They also have access to courses and meetups, as well as our online library. During the autumn selection process in Russia, 40 interns joined our team.

One key feature of our internship program is that students from any field of study, even non-technical ones, can participate in it. The main condition is that they are interested in the IT world.

>15

internship focuses, including C/C++, C#, Python, Go, JavaScript[1], as well as testing, threat analysis and DevOps[2]

13,500

applications for SafeBoard internships were received in the reporting period

Kaspersky Academy Expert Community

Kaspersky focuses not only on training school and university students, but also the teaching community. The Kaspersky Academy Expert Community offers a series of regular specialized events for teachers, researchers, deans and the heads of information security departments and related fields. It is also a community of like-minded people.

The events are held in several formats, including offline meetings and regular community meetings, which take place every two months at our office, where Company specialists share their experience on important issues. There is also the Training Lab, which provides free two- or three-day training sessions for university teaching staff with our experts. The training themes are highly diverse – starting from general areas of information security and ending with Kaspersky's products.

>50%

of interns joined the Company's staff within 8 years after completing the SafeBoard program

The geography of the Kaspersky Academy Expert Community is quite diverse and covers almost all of Russia and the CIS countries. We have had colleagues visit us from Chelyabinsk, Vladivostok, Almaty, Minsk and other cities. In 2023, we held teacher events in Dubai, Cairo, Bombay and Delhi, and we plan to repeat them in other cities and countries in the Middle East and Pacific regions in 2024. We are always glad to see new people in the Kaspersky Academy Expert Community – anyone who teaches information security at universities and is interested in developing their knowledge and communicating with like-minded individuals.

[1] Programming languages.
[2] DevOps is a methodology for interaction between developers and the integration of processes when creating a product.

Training IT specialists

The development of technology and legislation are among the main drivers of the emergence of new professions and expertise. This is why continuous training is one of the main requirements for cybersecurity professionals. To help them improve their skills, Kaspersky has developed a set of educational training courses on our own online learning portal, Kaspersky Expert Training.

The courses were written by leading Kaspersky specialists, who are familiar with more than 400,000 malware samples and know how to counter them. We supplemented the theoretical component with cases based on actual threats. It is not fundamental education, but practical training, in which specialists master techniques and tools that they can immediately use in their work.

The range of people who take the courses is broad and covers everyone in our industry – from cybersecurity professionals and SOC teams to research institutions, incident response centers and government organizations.

Skills that can be improved with Kaspersky Expert Training

- Reverse engineering
- Threat search and detection
- Incident response
- Product security analysis

The Company offers both basic courses that are designed for entry-level training, as well as advanced ones for experts and professionals. Some of the protection tools that we teach about include Ghidra, Yara, Suricata and Frida.

The portfolio of online training sessions for Kaspersky Expert Training experts includes 11 courses. In 2023, we expanded it with the following three online courses:

- **Advanced reverse engineering of malware using Ghidra**, which focuses on the process of analyzing malware using the Ghidra framework based on the real experience of its authors: experts from the computer incident investigation team and the Global Research & Analysis Team (GReAT)
- **Suricata for incident response and threat hunting**, which teaches users how to use Suricata to work with different data streams to detect and block even the most complex threats
- **Online cybersecurity training for managers** created by the Kaspersky Academy team for senior executives. It explains complex terms in simple language and aims to help understand the basic concepts of information security, as well as learn how to manage a company in the face of cyberthreats

2,000+ users

from more than 50 countries make up the expert training audience

~10 hours

the average time that Kaspersky Expert Training students dedicated to each program

20 hours

the average time Kaspersky Expert Training students spent in on their practical skills in our virtual laboratory

The most popular topics of 2023 were advanced malware analysis techniques with Yara. Students spent a total of 4,000 minutes on them.

The most practical courses are malware analysis and reverse engineering.

In 2024–2025, we plan to expand our portfolio with training courses on digital forensics and secure development. The Company is also translating existing training courses into Russian and has already selected a separate training platform for them. In 2024, Kaspersky plans to launch sales of Russian-language training courses.

In 2023, we continued to provide free training for INTERPOL employees from Russia, Europe, Latin America, Asia, Africa and the Middle East.

A total of 71 INTERPOL employees completed free Kaspersky Expert Training in 2023.

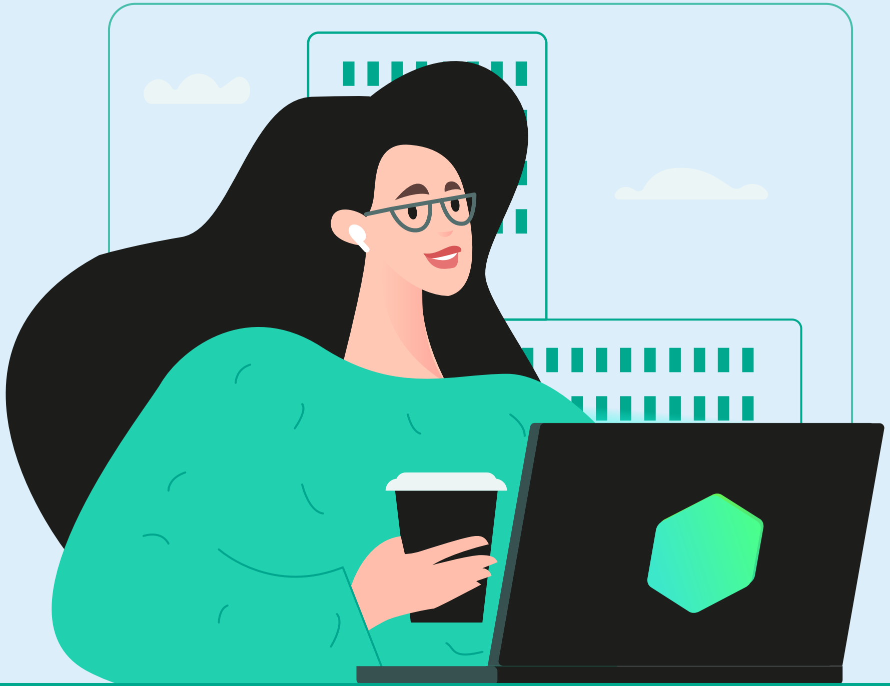
In addition, we provided 10 interns participating in the Suricata Outreach program with free access to training on how to use Suricata for incident response and threat hunting. The list of participants in the initiative was determined by the Suricata community. Our training courses were also used as prizes for the winners of the Secur'IT Cup international student competition.

158 Kaspersky's employees

took Kaspersky Expert Training courses for free

Women in IT: Power of Equality

IT was traditionally regarded as a field dominated by men, but today women are successfully leveraging their abilities in this sector, surpassing stereotypes and overcoming obstacles. Recruiting women to the IT industry and supporting them is part of our corporate culture.



Gender imbalance in the IT industry: causes and challenges

There is a major gender imbalance in the IT industry, which has considerably more male specialists than female ones. This phenomenon is due to a number of factors, ranging from cultural biases to social stereotypes. Computer technology was initially associated with male interests and hobbies, fostering a distinct culture that excluded women. Over time, this stereotype took hold and became part of the professional identity of the IT sector. In addition, this imbalance is exacerbated by the problem of inequality that women face in every industry, including IT. Not all companies provide the same conditions for their employees, and this hinders the attraction and retention of talented women. According to the Russian Ministry of Labor and Social Protection, there was a 28 percent disparity between the salaries of men and women in Russia at the beginning of 2023 in favor of the former, although this gap is narrowing each year. Women's careers advance at a slower pace than that of their male counterparts. One of the reasons for this is parental leave, which mothers usually prefer to take, although Kaspersky also provides such leave to fathers if they wish to take it.

Nevertheless, the number of women in the IT industry is gradually increasing. At the beginning of 2023, the share of women working in the tech industry worldwide was 25 percent, an increase of 6.9 p.p. over the past four years. At Kaspersky[1], women make up 25 percent of the workforce, including 16 percent of the Company's department heads and major managers, and 34 percent of technical specialists.

25%
female IT specialists worldwide in 2022

Women made up
25%
of Kaspersky's employees in 2023

[1] As of December 31, 2023.

Our approach to supporting women

In recent years, women have continued to make an active advance at the Company. They work on software development, project management and other areas of IT. Mixed teams with both men and women perform well due to the diversity of their experiences and perspectives.

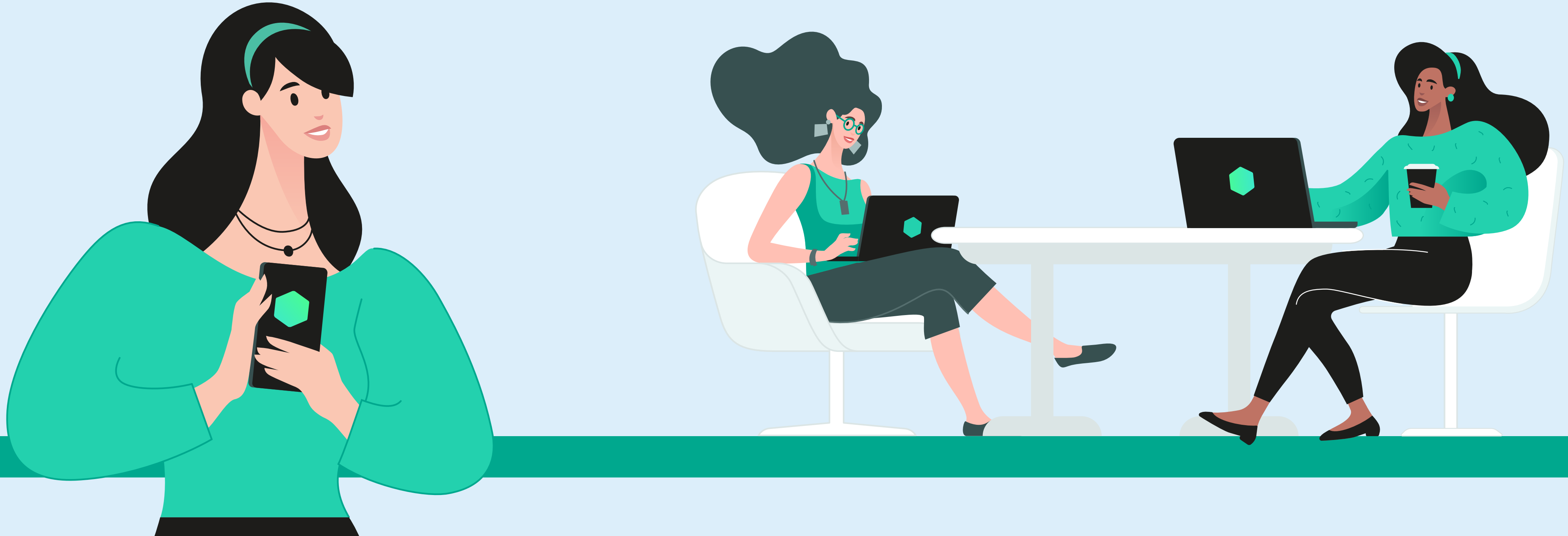
Kaspersky aims to address the issue of gender imbalance starting from schools and universities. We are committed to challenging gender stereotypes from an early age and making IT education accessible and open to everyone. We work with schools and universities to provide all students, regardless of gender, with information about IT education and the opportunity to unleash their potential in the tech sector.

We are also committed to ensuring equal pay for every Kaspersky employee. Our approach to remuneration considers each employee's position and qualifications, regardless of gender. To this end, we use an estimate of the market compensation level for each position. Based on this assessment, we decided to increase the salaries of Kaspersky's employees by an average of 20 percent in 2022 in Russia. The Company was able to invest twice as much in salaries and bonuses compared with 2021. In 2023, remuneration for Kaspersky's employees in Russia increased by around 19 percent.

We also provide our employees with additional support and benefits during maternity leave, as well as educational opportunities in their field of work, and help advance their careers through individual development plans.

We are also implementing various projects externally to attract more women to the IT industry. In particular, we cooperate with educational institutions around the world and organize educational events, master classes and internship programs. On social media, we have created the Women in CyberSecurity community – a space where women can seek support and mentorship on their path to success in the cybersecurity sector. This community already has more than 30,000 members.

To inspire as many girls as possible to pursue a career in IT and cybersecurity, Kaspersky has also launched another online project – the Empower Women website. Our Company's female employees share their personal journeys in cybersecurity and IT. They discuss their educational paths, career development, participate in podcasts, and provide valuable insights and advice.



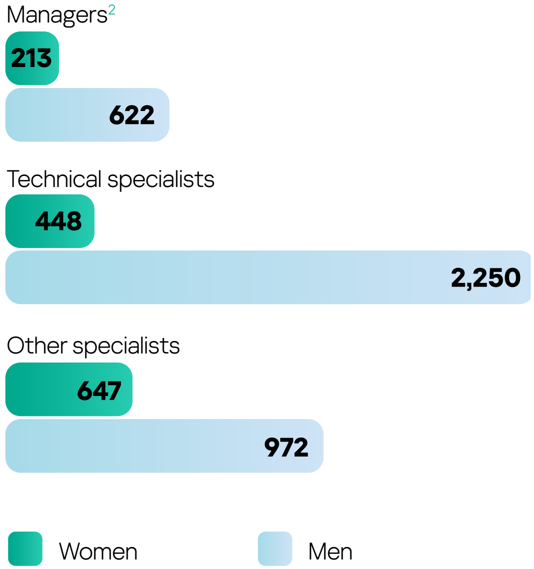
Increasing the number of women in IT development

Boosting women's involvement in the IT industry and supporting them is an integral part of Kaspersky's corporate culture, which is shaped by the board of directors and senior management. We strive to create an atmosphere of mutual understanding in all units, in which each woman can realize her potential and become successful in the IT sector. In addition, women who have already achieved success at various levels actively take part in support programs, communicate with their colleagues and subordinates, share their experience and inspire aspiring IT specialists with their example.

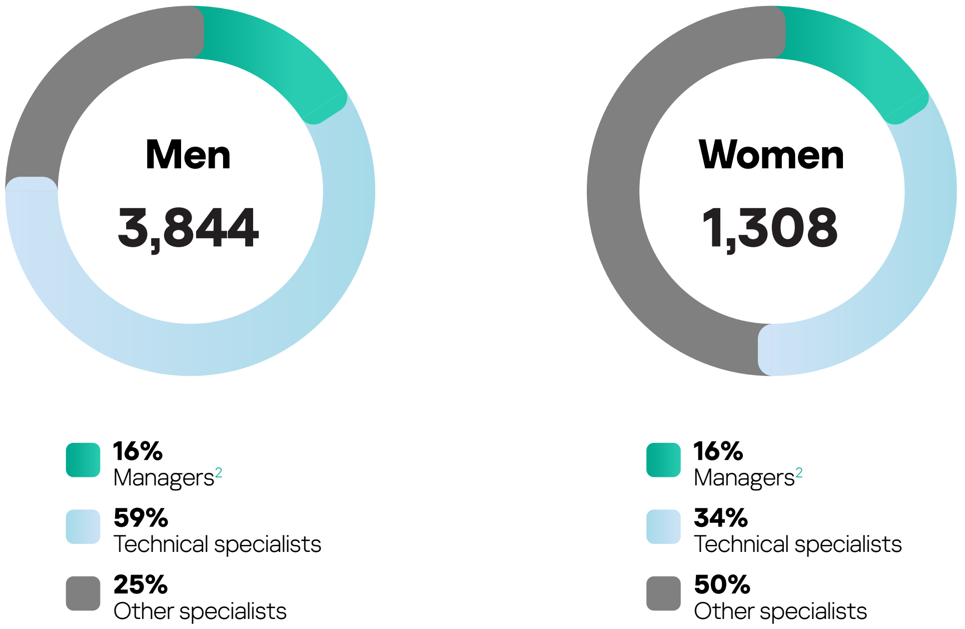
Kaspersky strives to be as honest and open as possible in order to prevent gender discrimination. When selecting new employees for our team, we only care about their abilities and skills, regardless of whether they are women or men. What's important is that whoever they are, they have the necessary expertise and the contribution they can make to our Company.

TC-SI-330-a.3

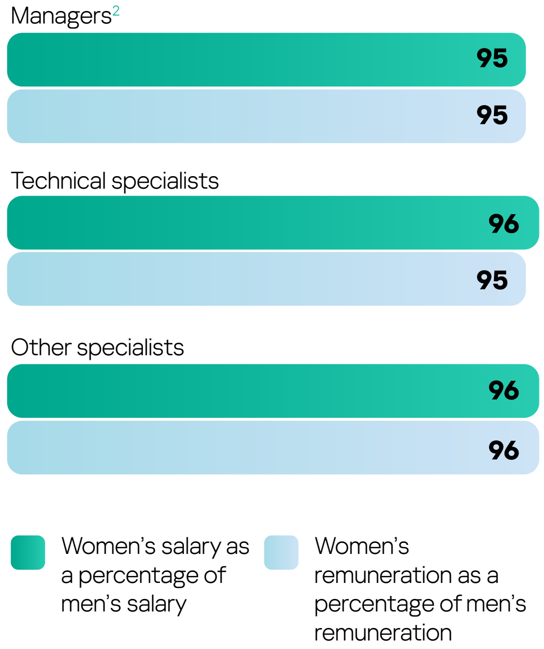
Total number of employees by gender and category in terms of gender balance[1]



Company employees by gender and category



Ratio of basic wages (salary) and remuneration[3] for women and men[4], %



[1] Data given as of December 31, 2023.
[2] Managers with at least one subordinate.
[3] Salary and benefits depending on category, length of employment and other factors.
[4] Data given as of December 31, 2023.

Social support for women and parenthood

In every country where we operate, we try to inspire employees along their career paths and support them in the most important moments of their lives. As an example, this is what we offer our employees in Russia who are getting a new addition to their family:

- Parental leave, which can be taken by any parent, regardless of whether the child is their own, adopted or under their care
- We match 100 percent of the government's maternity benefit, so that total remuneration is equal to a full salary for employees who have worked at the Company for at least one year
- A pregnancy and childbirth program as part of voluntary health insurance

Uniting women in online cybersecurity communities

The Company is currently implementing two major online projects for women in IT. We are committed to supporting women in the IT industry, helping them overcome barriers and achieving their goals. Our goal is to share information about career opportunities in the industry and inspire our members with stories of successful female professionals to create new role models.

In 2021, we launched the Empower Women project with a focus on women's activities in cybersecurity. The project includes research about women in the IT industry in various regions, interesting news, as well as the inspiring Women in IT podcast, where Kaspersky's employees share their professional and personal experiences. During the reporting period, 11 new stories about our colleagues from different regions of the world were posted on the website, where women share stories about their professional and personal development. We aim to showcase the wide range of career opportunities in the IT industry – many of our female employees do not have a technical education, but managed to achieve impressive results in their professional fields within an IT company, be it sales, educational projects or communications.

Another Kaspersky project that addresses female leadership in IT is the Fast Forward podcast. It features guests from all over the world who work at the forefront of our latest technologies. The first season of Fast Forward, which included episodes that focused on the supermarket of the future and the new space race, received the prestigious 2022 Webby Honoree Award for Best Branded Podcast and a Silver Award for Branded Podcast from the Content Marketing Association. In its second season, "Fast Forward" covers such issues as the metaverse, virtual fashion, technology in family life, digital health and so-called augmented humans. This season, the podcast focuses heavily on how women are changing the way they think about technology, and starting to lead the way. The two episodes focus on women and girls in gaming and career opportunities for women in STEM[1].

Our Women in CyberSecurity community, which we created on social media five years ago at the initiative of one of our employees, has also been a huge success. Today, it is an active and rapidly developing community that brings together cybersecurity professionals and other areas of the IT industry. Women use it every day to discuss topical issues, share their professional experiences and exchange advice on career growth, training and choosing a specialization in the field of cybersecurity. Women in CyberSecurity currently has more than 30,000 members, which makes it one of the largest and most popular online communities on this subject. More than 20 posts are published in the community each month.

In November 2023, Kaspersky sponsored the annual Female in IT (FIT) congress of the Vogel IT Academy in Germany. The congress brings together women who work in IT so that they can support each other in business, exchange experience and promote young talent. The slogan for 2023 was "Women, get ready for the next generation of business!". The Congress impressed its participants with a first-class program of interesting presentations, panel discussions and networking opportunities.

29,000

members of the Women in CyberSecurity community

Our plans for 2024

We will continue working on existing projects and developing new programs to attract women to the IT industry, participating in specialized conferences and forums, publishing the success stories of our colleagues, and talking about the professional development opportunities that are being created for women in the cybersecurity industry.

[1] STEM (science, technology, engineering and mathematics) is a broad term used to refer to technical disciplines.

How our female employees get to the top in IT and help other women

Introducing Genie Sugene Gan, who received the Excellent Woman ICT Leadership Award

Genie is responsible for developing trust-based relationships with government officials. She is a frequent speaker at international conferences and an opinion leader on issues related to government cybersecurity policy and the intersection of technology and policy.

Genie is a true ambassador for women's leadership in the IT world. She puts a lot of effort into supporting other women in the IT sector. Genie also helps them gain knowledge and also mentors and advises them. She creates special communities where women can share their experiences, knowledge and support. This approach helps them grow and develop, while overcoming stereotypes and obstacles on their path to success.

In 2023, Genie received several awards and acknowledgements for her work, including the following.

- Excellent Woman ICT Leadership Award: Genie received this award in Delhi as part of International Girls in ICT Day 2023, which is celebrated to draw attention to the need to increase the number of girls and women in the information and communications technology sector. The event was jointly organized by the Geneva-based United Nations International Telecommunication Union and the Telecom Equipment Manufacturers Association of India. Genie was the sole recipient in the cybersecurity sector.

> "As the only recipient of the award for the cybersecurity sector, this recognition isn't just a personal achievement, but an endorsement of Kaspersky, which has been nothing but enabling and supportive of my work endeavors, and is committed to creating a more diverse, more secure industry and championing women in cybersecurity."

Genie said in comments about her award.

- International Women Empowerment Forum (IWEF)

Genie was appointed vice-chairperson of the IWEF, which emphasizes the multidimensional development of women, including their social, economic, financial, and political empowerment. Genie is the only non-Indian to serve on the IWEF board of directors.

- Singapore's The Cybersecurity Awards

Genie was a finalist in Singapore's The Cybersecurity Awards (Professional Category). She received the award, which is organized by the Association of Information Security Professionals (AiSP) and supported by the Cyber Security Agency of Singapore, in recognition of the outstanding contributions of individuals and organizations to local and regional cybersecurity ecosystems.

- Top 25 Cybersecurity Star of the Year 2023

Genie was named one of the Top 25 Cybersecurity Stars of 2023, an award presented by DIGITALCONFEX for contributions to intellectual leadership on topics where public policy, technology and law intersect.

- Top 30 Women in Security ASEAN Region Awards 2023

Genie received the Top 30 Women in Security ASEAN Region Awards 2023, which is organized by the Association of Southeast Asian Nations (ASEAN) and is part of the global Women in Security & Resilience Alliance (WISECRA) campaign.

What was the result?

By actively promoting IT and supporting other women along this path, Genie has become an inspiring example, showing that anyone can achieve success in the world of technology, regardless of gender. Her story shows that hard work, education, and support can propel women to great results, even in traditionally male-dominated industries.

ESG

Ethics and Transparency

Global Transparency Initiative

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

Proven. Transparent. Independent.

What is the Global Transparency Initiative?

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

How the GTI emerged and has evolved

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

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

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

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

GTI results over five years

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

2
data centers in Zurich

11
Transparency Centers around the world

60 reviews
of the Company’s products at Transparency Centers

2
independent audits of SOC 2 and ISO 27001 annually

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

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

[2] ICT – information and communication technologies.

How the GTI works

GRI 3-3

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

Essential components of the GTI

1

Source code review for corporate and regulators

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

2

Collaboration with experts

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

3

Training and education

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

How we ensure the transparency of our products and business processes

# Objective

Strengthen public trust in the Kaspersky's products and activities

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

TC-SI-220-a.4

# Solutions

Transfer data to secure data centers

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

Open new Transparency Centers

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

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

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

11 Transparency Centers worldwide

RESULTS OF 2022–2023

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

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

34 visits to centers worldwide

Expanded list of products available for review at the Transparency Centers

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

Conduct independent audits

In 2023, we successfully passed a

SOC 2

Type 2 audit

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

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

Collect data on vulnerabilities via the bug bounty program

59 reports

on minor vulnerabilities received over five years

US$81,750

paid out for reports

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

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

Teach how to assess cybersecurity levels

2 organizations

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

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

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

Publish Transparency reports

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

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

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

GTI development plans for 2024

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

Our call for development and usage of AI in cybersecurity

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

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

Transparency

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

Safety

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

Human control

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

Privacy

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

Commitment to cybersecurity

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

Openness to dialogue

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

What was the result?

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

Data protection

We respect our users' right to privacy and protect their data. Our goal is to ensure data security of Kaspersky users.

~4,000 employees completed an internal course on working with user data

3,000+ requests for processing user data in 2023

GRI 418-1

Key objectives

- Ensure the data protection of all our users worldwide using the best information security practices and in compliance with local regulations.
- Promptly respond to privacy enquiries of our users regarding the processing and protection of their data.
- Prevent unauthorized access and risks to data processing.

GRI 3-3

Our approach to data protection

We are fully committed to protecting the data of our users worldwide. We protect our users' personal data[1] against possible unauthorized changes, compromise or loss. To this end, we use best-in-class technology and take the following security measures:

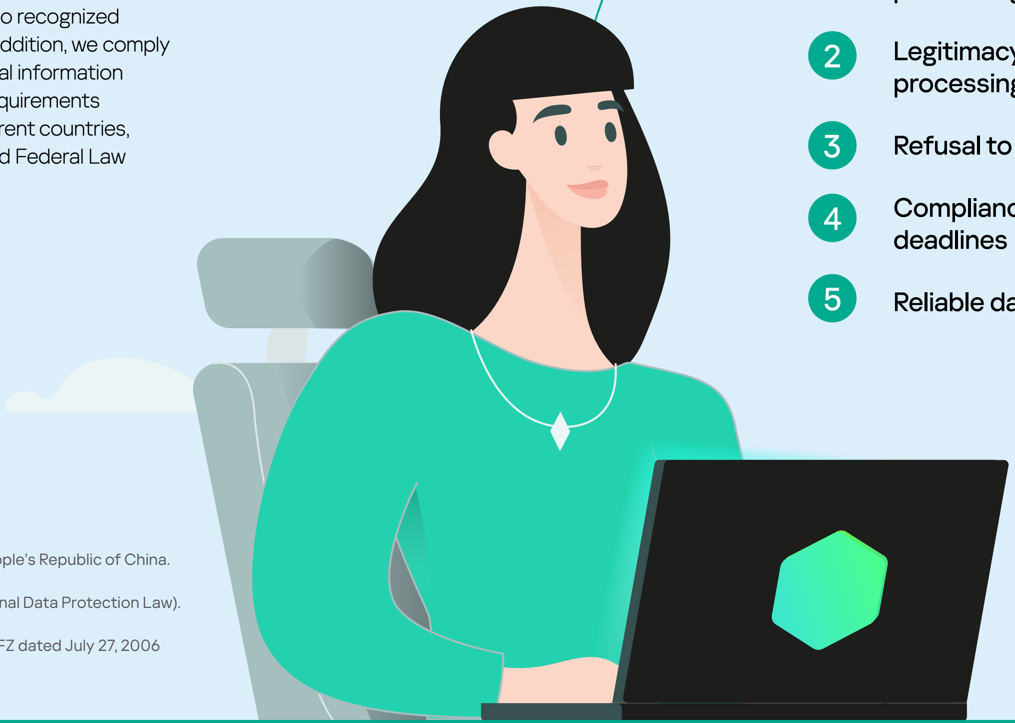
- The secure software development life cycle ensures the creation of secure products and the prompt correction of vulnerabilities.
- Reliable encryption ensures secure data exchanges between the user's device and the cloud.
- Digital certificates enable legitimate and secure server authentication and application updates.
- Data is stored separately on multiple servers with limited rights and strict access policies.
- Data is anonymized using various methods, including removing account data from transmitted URLs, obtaining the hashes of malicious files instead of the files themselves and hiding user IP addresses, etc.

[1] Personal data refers to any information relating to an individual, including his/her full name, telephone numbers, address, IP address or email address.

How we ensure data protection of our users worldwide

TC-SI-220-a.1 TC-SI-230-a.2

We are guided by the key data processing principles of the 2016 EU General Data Protection Regulation (GDPR). This legislative act prescribes the fundamental technical and organizational measures that are also recognized as benchmarks in other jurisdictions. In addition, we comply with the requirements of the international information security standard ISO/IEC 27001 and requirements of personal data protection laws in different countries, including PIPL[1], CCPA[2], LGPD[3], PDPD[4] and Federal Law No. 152-FZ[5].



Five key principles for working with user data:

1. Legality and transparency of data processing for data subjects
2. Legitimacy of the purposes of data processing
3. Refusal to collect redundant data
4. Compliance with data storage deadlines
5. Reliable data protection

We strive to reduce the number of incidents to zero. In the reporting period, we did not commit a single violation of laws on personal data or have any data leaks. This was possible due to regular employee training, the information security technologies that have been introduced, and standardization of data processing. During the reporting period, we updated our data processing requirements and also adapted them to be in line with the laws of different countries.

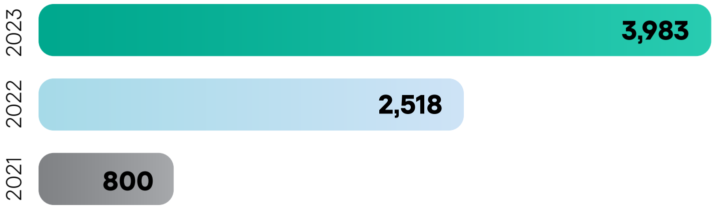
We compile the most current information, including the number of requests from our users that have been satisfied, in a transparency report. The document is publicly available, updated and published every six months.

[1] Personal Information Protection Law of the People's Republic of China.
[2] California Consumer Privacy Act.
[3] Lei Geral de Proteção de Dados (General Personal Data Protection Law).
[4] Personal Data Protection Decree of Vietnam.
[5] Federal Law of the Russian Federation No. 152-FZ dated July 27, 2006 "On Personal Data".

Ensuring responsible management of data

Kaspersky has an awareness course for employees who are directly involved in the processing of customer data. In 2023, 3,983 people completed this course, including all of the our European employees and workers worldwide who are involved in processing and protecting customer data, an increase of 58 percent from the previous year.

Number of employees who completed the awareness course



Risk assessment

We take a risk-based approach to the protection of our users' data. Risk assessments are conducted at all stages: when introducing new systems, developing new solutions and investigating incidents. In each case, we analyze in advance what risks may arise when processing customer data and minimize them.

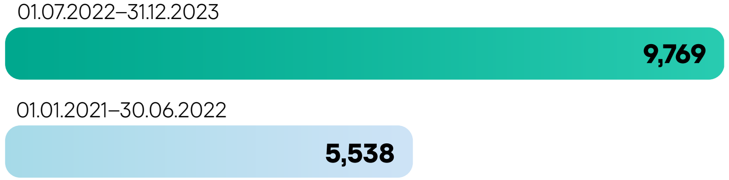
The requirements of the GDPR and regional legislation take into account the risks that users may be exposed to. The ISO/IEC 27001 standard helps us mitigate reputational and financial risks for the Company.

Prompt response to privacy enquiries from our users

TC-SI-220-a.1

Kaspersky receives thousands of requests for data processing from users each month, 90% of which are requests to remove their data from our databases.

Number of requests received from users over the reporting periods[1]



Users are also asked to upload their data, what information about them is stored and where it is stored. We successfully processed 9,769 requests during the reporting period (from July 1, 2022 to the end of 2023) and 5,538 requests in the period from January 1, 2021 to June 30, 2022. We are seeing the number of such requests increase both in Europe and around the world. This is happening for two reasons: growing user awareness about their rights and the adoption of new laws on personal data.

Our goal is to provide all the necessary information about data to users so that they can trust Kaspersky and its products. As part of our streamlined inquiry process, we create transparency reports that document the number and types of requests we receive from customers. We update and publish such reports every six months.

Like most companies, we work with user data and targeted advertising[2]. Per the GDPR, data obtained via cookies[3] is considered personal, which means that the relevant rules must be followed when collecting it. Brazil, the UK and Europe have uniform, strict policies to obtain consent for the collection of information on websites. In other countries, we collect minimal data to provide the relevant information to our potential customers.

To interact with consumers, customers and suppliers, Kaspersky has a feedback form on its official website:

www.kaspersky.ru/about/contact — for Russian users

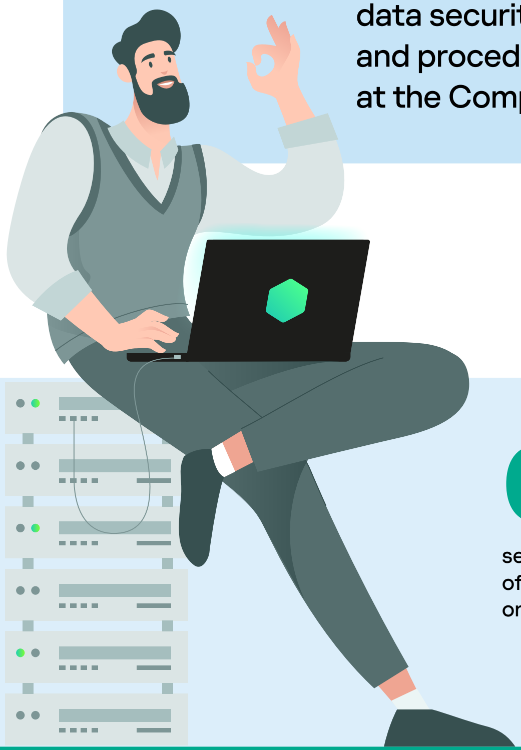
www.kaspersky.com/about/contact — for international users

[1] Per transparency reports.
[2] Targeted advertising is a key marketing tool that is used to collect users' personal data through various websites, applications and social networks in order to promote goods and services.
[3] Cookies are small files stored on computers and gadgets that websites use to remember information about user visits.

Preventing risks of user data processing

GRI-418-1 TC-SI-220-a.1 TC-SI-230-a.1 TC-SI-220-a.2 TC-SI-220-a.3

The Privacy Team is responsible for compliance with data security principles and procedures at the Company.



The Privacy Team, which includes employees from the IT, Research and development, information security and intellectual property departments, was formed in 2016, when GDPR requirements were being introduced. The team brought all the Company's processes into compliance with European regulations. It now performs data processing functions in areas such as consulting, organizational issues and control.

Since 2019, Kaspersky has annually certified its data processing systems for compliance with the requirements of the international standard ISO/IEC 27001, thereby verifying their high level of protection. The scope of the information systems audit was significantly expanded during the reporting period. We hired new staff and formed a new unit, which helped to complete 388 internal audits in 2023.

The scope of certification extends to Kaspersky's data processing function "Delivery of malicious and suspicious files and static activity data using the Kaspersky Security Network (KSN) infrastructure, the safe storage and access to the Kaspersky Lab Distributed File System (KLDFS) and the KSNBuffer database."

The certification is valid for data processing services located at data centers in Beijing, Frankfurt, Glattburg, Moscow, Toronto and Zurich.

Launch of a new tracking system

During the reporting period, we completed an ambitious project: the launch of a new system for tracking processes and data processing services, which was created by the Kaspersky development team. It tracks which services process customer data, which business processes they are used in, the controller (operator) and processor of the data, what data is stored in the system, for how long, on what basis, to what extent and in what countries, etc. The new system is ready for operation and 80 percent of the data has already been transferred to it.

0

serious violations of personal data legislation or major leaks

0

losses as a result of litigation due to violation of confidentiality during the reporting period

388
internal audits

for certification of compliance with ISO/IEC 27001 in 2023

Our plans for 2024

- Presentation of updated requirements for data processing and protection for all services that process customer data.
- Review of the updated requirements with responsible teams.
- Audits on the effectiveness of user data processing and protection services.

Intellectual property protection and defense

We work diligently to create and introduce long-term cybersecurity solutions and regularly patent our inventions and innovative technologies.

How we protect intellectual property

Intellectual property rights are among the most important components of our business's development and stability. We protect our developments and also respect the rights of other companies to their own technologies and solutions.

# Objective

Protect the rights of our products, solutions and technologies

231 patents

obtained by Kaspersky for its inventions in 2022–2023

# Solutions

Obtain patents in different jurisdictions

TC-SI-520-a.1

Kaspersky always strives to protect exclusive rights to the results of its intellectual activities and defends these rights in court when they are violated. This helps us maintain fairness and legality in the business environment.

During the reporting period, the Company obtained 231 patents for its technologies in different jurisdictions.

The focus of patents for key technologies has shifted towards B2B products and KasperskyOS in recent years. These include SIEM[1], Research Sandbox[2] and machine learning technologies that not only identify new malicious objects, but also anomalies (MLAD[3]), as well as anti-ransomware technologies.

The protection and defense of intellectual property has become an integral part of Kaspersky's activities since 2005. Since this time, we have managed to build and optimize the processes involved in obtaining legal protection for our intellectual property. In addition, over the years, our Company has achieved the impressive result of not losing a single court case involving patent-related lawsuits against us.

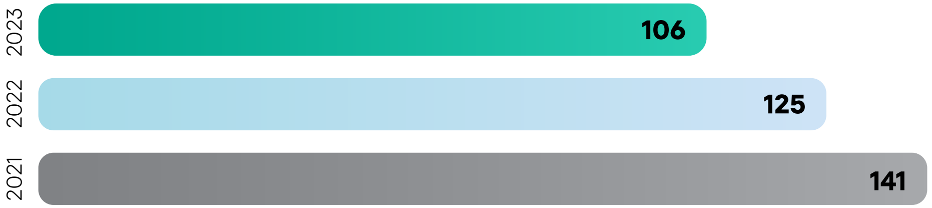
This experience and expertise not only helps us to successfully protect and defend our innovations, but also to promote the development of intellectual property as a whole.

In addition to improving our products, we are actively involved in the development of the open-source movement. In 2022–2023 alone, Kaspersky published 20 open-source projects that provide the entire developer community with access to our technologies.

We believe in the importance of such publications and their value for cooperation and the exchange of experience and knowledge.

We also attach great importance to the education and support of employees who study at higher education institutions and wish to use our intellectual property in their research. We are developing a process giving them an opportunity to fulfill their aspirations and protect critical information. For this purpose, regulations and instructions are being drafted on issues related to the use of intellectual property.

Patents obtained by Kaspersky for its inventions



20

open-source publications in 2022–2023

[1] Security Information and Event Management – a class of software products designed to collect and analyze information about security events.
[2] A sandbox for advanced threat research that can be deployed within a company's corporate infrastructure.
[3] Machine Learning for Anomaly Detection.

Strict compliance with the law on intellectual property

In addition to protecting our own achievements, we believe it is important to promptly respond to and eliminate the risks associated with the misuse of the intellectual property of other companies within our organization, including the use of third-party code. We are able to do this by introducing the appropriate policies, thoroughly verifying licenses and ensuring compliance with all the necessary rules and regulations.

Another crucial aspect of our work is the training and awareness of our employees. Each new employee undergoes special introductory training course, which provides a basic understanding of intellectual property.

In addition, in the second quarter of 2024, we plan to launch a specialized course on patents for employees of Kaspersky's technical units. As part of the course, our colleagues involved in the development of new products will receive information about internal procedures related to intellectual property protection issues.

If needed, we are always ready to defend our rights in court. This is one of our key strategic positions. Most litigation occurs in the United States, largely as a result of patent trolls[1]. In Russia, we have experience resolving disputes related to violations of antimonopoly legislation and have also successfully defended our interests.

We always strive to protect our rights by all available legal means, but are not willing to accept unreasonable settlement offers. Our goal is to ensure a fair and legal resolution to disputes that takes into account the positions of all parties involved.

During the reporting period, we resolved a patent dispute with a non-practicing entity Cybersoft, who claimed that our product Kaspersky Secure Mail Gateway violates a patent for a network security technology that can scan data transmitted over a network on a user's device. We estimate that the dispute could have resulted in approximately US$500,000 in damages in the worst-case scenario. However, we received a ruling in our favor in 2022. Cybersoft realized the futility of the case and moved for a settlement.

100%

success rate in defending patent claims filed against the Company over 18 years in the U.S.A.

In March 2022, Kaspersky had to take on a new challenge involving a patent dispute initiated by the antivirus company Webroot in the United States. This was a historical case, since it was the first time we had to deal with litigation with our direct competitor. In June 2022, we filed a countersuit against Webroot in response to the infringement of our patent rights. The actual court hearings in this case are not expected to take place until November 2024. We are determined to protect our rights and minimize the possible negative impact of this dispute on the Company's business and reputation.

Our plans for 2024

- Start receiving legal protection for inventions in new jurisdictions.
- Start patenting intellectual property associated with the design of our products (including the interface).
- Prepare and launch a patent course for employees.
- Revise certain in-house IP regulations in line with the changing legal landscape.
- Provide resources and guidance on intellectual property issues to employees studying at higher education institutions to ensure compliance with the Company's rules and policies.

[1] An individual or legal entity whose business consists solely of receiving royalties for the use of patents it owns without attempting to put the patented inventions into practice.

Corporate governance

GRI 2-9 GRI 2-10 GRI 2-11 GRI 2-13

Our business is based on the principles of transparency and honesty towards our customers, partners and competitors. We are dedicated to continually improving the transparency and openness of our company.

Approach to corporate governance

We value our Company’s reputation and are committed to enhancing the transparency of management in all aspects of our operations. We have developed key rules for business and corporate ethics. They will be enshrined in the Kaspersky Code of Ethics, which is currently being drafted.

Key principles

- Ensure the transparency of corporate governance.
- Comply with our anti-corruption policy by preventing violations thereof.
- Provide a high level of legal support for the protection of intellectual property.
- Reduce supply chain risks.

How our corporate governance system works

Kaspersky’s highest governing body is the board of directors, which is responsible for key decisions and adopts global policies and strategies that are implemented at all companies within the group. The current board of directors consists of four people, who have been employed permanently by the company for more than five years. There are no independent members on the board of directors, only executive ones.

Candidates for the board of directors are nominated by current board members.

Kaspersky does not have a permanent chairperson of the board of directors. The chairperson is elected at each board meeting, has no special powers and is also not the CEO.

Responsibility for the economic, social and environmental impacts of sustainable development has been delegated to Head of Corporate Communications Denis Zenkin.

Board of directors

Eugene Kaspersky

The sole executive body of JSC Kaspersky Lab and the LLC Kaspersky Group and a member of the holding company's board of directors and governing board.

Andrey Tikhonov

A member of the holding company's board of directors and governing board and the sole executive body of JSC Water Stadium Sport Invest.

Daniil Borschev

A member of the holding company's board of directors and governing board and a member of the board of directors of LLC New Cloud Technologies.

Svetlana Ivanova

A member of the holding company's board of directors.

Governing board

The governing board of LLC Kaspersky Group determines the specific strategic and tactical steps that are essential to the Company's operational development and the Group's management structure, and also approves the appointments of senior executives.

CEO Eugene Kaspersky plays the decisive role in the Company's management, since he is both the largest shareholder in the holding company and a member of the board of directors and the governing board.

Remuneration

GRI 2-20

The overall remuneration for members of Kaspersky's highest governing body and senior executives is regulated by the Company's general compensation policies and is comprised of the following elements:

- **Fixed component** (salary)
- **Bonus** (performance-based) – paid based on the results of achieving individual goals defined for each position for the fiscal year
- **Payments as part of a long-term incentive program** – made annually, but are tied to a three-year reporting cycle and depend on the Company's financial results as a whole (EBITDA and overall year-on-year sales growth are used as the basis for calculating such payments)

The total compensation package for senior executives is made up of all three components of the remuneration system in approximately equal shares. This remuneration system makes it possible to reward the Company's executives for individual successes and motivate them to achieve common corporate goals.

How we comply with anti-corruption policies

GRI 2-23 GRI 205-2

Kaspersky is an international company that complies with laws and regulatory requirements around the world.

0 **court decisions**

on violations of anti-corruption legislation by the Company or its employees or partners

Kaspersky's headquarters prioritize the laws of the Russian Federation, while its foreign offices adhere to local anti-corruption legislation.

The basic principles of anti-corruption are enshrined in the Company's anti-corruption policy, which was adopted in 2012. It is published on our official website and has been translated into 30 languages in the regions where Kaspersky operates. The main principle of the anti-corruption policy is that our Company does not tolerate any forms of bribery or corruption among individuals or government officials and does not take part in any forms of unethical incentives or payments.

The compliance officer and its representatives in the regions are responsible for complying with the anti-corruption policy. They investigate all potential violations, which any employee can report to their manager, compliance officer or its representatives, and also by calling the hotline 8–800–700–88–11 or sending an email to infosec@kaspersky.com. People can send a message or call anonymously if they wish.

GRI 205-1

Anti-corruption practices

Kaspersky regularly assesses corruption-related risks. We conducted such an assessment twice during the reporting period.

Throughout the reporting period, training was provided to all Kaspersky employees of the Company, ranging from senior management to junior specialists.

GRI 205-3

In addition, we annually inform employees about our anti-corruption policy and related procedures. We have prepared and integrated an anti-corruption policy into the contracts we sign with counterparties.

During the reporting period, we trained employees on anti-corruption policies and procedures through a special online course dedicated to combating bribery and corruption. This course includes an introduction to the basic principles and main focuses of the Company's anti-corruption policy, including:

- The goals of anti-corruption legislation;
- The importance of compliance with Russian and foreign laws on bribery and anti-corruption;
- Behavioral patterns that lead to violations of anti-corruption laws;
- The need to exercise caution in business relations with third parties;
- Internal control mechanisms that dictate employees' activities in accordance with the anti-corruption policy.

The anti-corruption course is 30–40 minutes long. The test results following the completion of the course are entered into the internal system.

100% **of employees and partners are informed about the anti-corruption policy**

0 **confirmed cases of corruption at the Company**

Plans to improve anti-corruption practices in 2024

In 2024, we plan to update the materials of the anti-corruption training course and also continue incorporating the best anti-corruption practices into the Company's activities.

Risk management

TC-SI-550-a.2

Kaspersky created and actively developed its risk management system (RMS), beginning in 2022, and is based on the Global Problem Management process for managing technological risks it previously operated. The RMS ensures the management of operational and technological risks, across individual company departments or units, and also in areas where various functional responsibilities overlap.

The company's fundamental risk management principles were developed based on Russian legislation, Russian Central Bank regulations, and international risk management practices.

Goals and objectives of risk management

The objectives of operational risk management are to identify, assess, aggregate and monitor the scope of Kaspersky's operational risks across all of its divisions. In addition, the company strives to maintain operational risks at an acceptable level, ensuring the sustainable operation and development of its business, implementation of its overall strategy, and the preservation of assets while maintaining the quality of its products and services.

Kaspersky manages technological risks by promptly and proactively identifying them. At the same time, we also act to prevent incidents that may impact the high quality of worldwide products and services, internal IT infrastructure and business continuity.

Objectives of the RMS:

- Ensure that Kaspersky management is aware of key operational and technological risks, including their nature and possible consequences, as well as the level of control of these risks.
- Timely identify and assess the Company's operational and technological risks in all its divisions, including all new businesses, processes, systems and assets, and reduce the probability and magnitude of losses to the Company's operations.
- Ensure the Company's uninterrupted operation.

Principles of operational risk management

- **Creation of a risk-oriented environment at the Company**

Operational risk management is not an isolated process within a specific unit. It is an integral part of the work of each and every Kaspersky employee.

- **Continuity and necessity of the operational risk management process**

Operational risk management procedures apply to business processes and operations that ensure the Company achieves its business goals performs its functions.

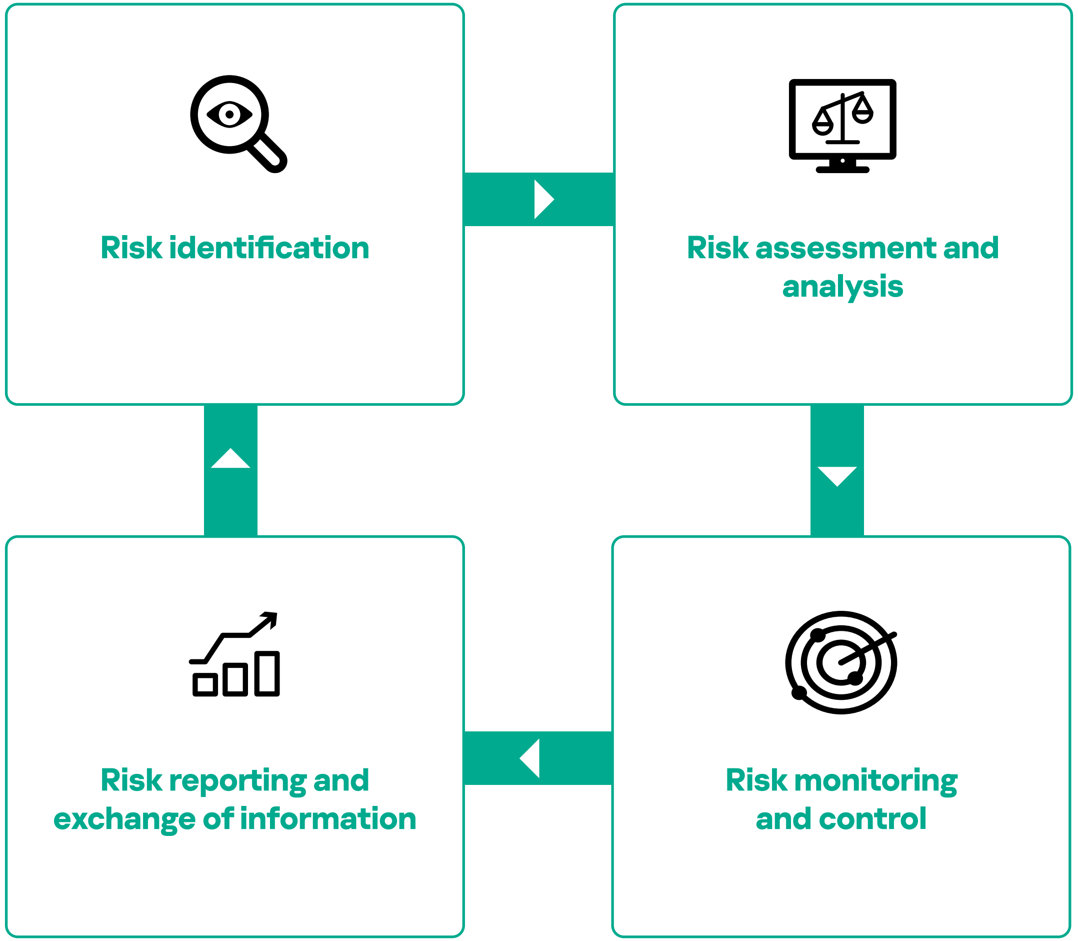
- **Awareness of operational risks for each level of decision-making at the Company**

The Company is creating a system to report on the level of operational risks and prioritizing risks so that decision makers have access to the most up-to-date information about the risks associated with the decisions they make. Thresholds are set for operational risk indicators, and when they are exceeded, higher-level managers are informed.

- **Openness and transparency of procedures and methods used to analyze operational risks**

The Company's risk analysis unit fully describes the approaches it takes to risk assessment in its internal regulatory documents and the procedure for analyzing operational risks. In the future, this will make it possible to assess the effectiveness of the operational risk management system.

Operational risk management process


Risk identification
Risk assessment and analysis
Risk monitoring and control
Risk reporting and exchange of information

Identifying risks involves defining and classifying risks that have been detected. A combination of various techniques and tools is used to identify risks. For each risk that is identified, the Company determines its owner, cause of the operational risk event; and assigns a person responsible for risk mitigation measures.

The significance of a risk is assessed and analyzed according to two parameters: an assessment of the Company's actual or potential losses in the event the risk materializes (impact) and the probability of an operational risk event occurring.

The Company regularly **monitors** actual and potential losses. This process involves identifying sources of risk, critical vulnerabilities in current business processes, compliance with the established risk level and violations of the acceptable risk level.

Kaspersky risk **control** is continuously conducted and primarily aims to:

- Comply with established procedures and powers when making and implementing management decisions that affect the interests of the Company and its customers.
- Manage operational risks that arise in the course of the Kaspersky's daily operations.
- Take timely and effective measures to help eliminate any shortcomings or violations that are found in the Company's activities.

Reporting and exchanging information about operational risks

Kaspersky has implemented a multi-level risk reporting system to facilitate the adoption of objective and effective management decisions. Such a reporting system contains information about actual or potential losses the Company could incur due to the materialization of operational risks, a breakdown of the categories of operational risks. This includes of operational risks as well as a quantitative analysis of events, map of operational risks and information about preventive and subsequent measures to minimize losses for the Company.

Kaspersky's CEO receives an annual report identifying the most significant risks and operational risk events. A quarterly report on operational risks is also presented to the governing board. In addition, the Company regularly discusses the status of incidents and risks with the department heads, managers and employees of its structural units.

Additional Information

Appendix 1. About the Report

GRI 2-2 GRI 2-3 GRI 2-14

In this Report, Kaspersky discloses information in accordance with the requirements of the following international sustainability standards:

- Global Reporting Initiative (GRI 2021)
- The industry-specific Standards of the Sustainability Accounting Standards Board (SASB Standards) for Software & IT Services

The compliance of this information with the requirements of these standards is presented in the sections GRI Standards Compliance Index and SASB Standards Compliance Index.

Unless expressly stated otherwise[1], the information published in this Report covers the activities of AO Kaspersky Lab, including the headquarters of AO Kaspersky Lab, and its affiliated companies in the countries of presence (regional offices), a list of which is given in the consolidated reporting of Kaspersky Lab Limited for 2021[2].

The Report covers the period from July 1, 2022 to December 31, 2023. Further sustainable development reports will be published annually.

Kaspersky's forward-looking statements and plans in this Report are of a preliminary nature and may vary depending on external and internal circumstances that were uncertain at the time of planning.

As such, the results of sustainable development activities in the succeeding reporting period may vary from those declared in this Report.

[1] The environmental impact information only covers Kaspersky's headquarters (Russian office).

[2] The reporting also includes the Company's office in Riyadh, Saudi Arabia, which opened in September 2023.

Appendix 2. Membership in associations and unions

GRI 2-28

Kaspersky cooperates with the following organizations:

- INTERPOL
- International Telecommunication Union
- International Organization for Standardization (ISO/IEC SC41). Active members of SC41 WG3 (Reference Architecture and Trustworthiness) and WG5 (Compatibility in IoT)
- No More Ransom Initiative
- Coalition Against Stalkerware
- Geneva Dialogue
- Paris Call for Trust and Security in Cyberspace
- Council of Europe
- IT- Sicherheitscluster e.V. (Germany)
- BVMW e.V. Der Mittelstand (Germany)
- Plattform Industrie 4.0 (Germany)
- Cybermalveillance.gouv.fr (GIP ACYMA) (France)
- Renaissance Numérique (France)
- World Internet Conference (member of the High-Level Expert Advisory Committee)
- China Industrial Control System CERT (industry partner)
- Operational Technology Information Sharing and Analysis Center (OT-ISAC, Singapore)
- SGTech
- Singapore Computer Society
- Malaysian Internet-of-Things Association (MyIoTA)
- Women in Technology movement
- Data Security Council of India
- Communication and Information System Security Research Center (Indonesia)
- Industry IoT Consortium (U.S.A.)
- Internet Association of Kazakhstan
- Domestic Soft Association of Developers
- Russian Union of Industrialists and Entrepreneurs
- Information & Computer Technologies Industry Association
- TK-MTK-22 Information Technologies
- Alliance for the Protection of Children in the Digital Environment
- Autonomous Nonprofit Organization Digital Economy

Appendix 3.
People Empowerment section

GRI 2-7 GRI 401-1 GRI 401-3 GRI 405-1 GRI 405-2

Total employees by type of employment contract and gender

2021						2022						2023					
Permanent		Fixed-term		Temporary replacement		Permanent		Fixed-term		Temporary replacement		Permanent		Fixed-term		Temporary replacement	
F	M	F	M	F	M	F	M	F	M	F	M	F	M	F	M	F	M
1,083	3,190	37	104	34	14	1,227	3,584	25	48	42	11	**1,263**	**3,798**	**23**	**39**	**22**	**7**

Total employees by type of employment and gender

2021				2022				2023			
Full-time		Part-time		Full-time		Part-time		Full-time		Part-time	
F	M	F	M	F	M	F	M	F	M	F	M
1,122	3,282	32	26	1,269	3,619	25	24	**1,271**	**3,823**	**37**	**21**

Percentage of total part-time employees, %

2021			2022			2023		
F	M	Total	F	M	Total	F	M	Total
3	1	1	2	1	1	**3**	**1**	**1**

Total employees by region

Region	2021	2022	2023	Change, 2023/2022, %
Asia-Pacific	242	222	**227**	2
Latin America	102	107	**134**	25
Middle East, Turkey and Africa	97	103	**136**	32
Europe	424	343	**340**	–1
North America	114	71	**65**	–8
CIS	3,483	4,091	**4,250**	4
including Russia	3,463	4,064	**4,221**	4

Staff structure by employee function

Category	As of December 31, 2021		As of December 31, 2022		As of December 31, 2023		Change, 2023/2022, p.p.
	people	%	people	%	people	%	
Managers[1]	**763**	**17**	**817**	**17**	**835**	**16**	**0**
including:							
men	577	76	621	76	**622**	**74**	–2
women	186	24	196	24	**213**	**26**	2
including:							
under 30	47	6	66	8	**65**	**8**	0
30–50	624	82	667	82	**685**	**82**	0
over 50	92	12	84	10	**85**	**10**	0
Technical specialists	**2,213**	**50**	**2,564**	**52**	**2,698**	**52**	**0**
including:							
men	1,822	82	2,107	82	**2,250**	**83**	1
women	391	18	457	18	**448**	**17**	–1
including:							
under 30	710	32	922	36	**940**	**35**	–1
30–50	1,448	65	1,575	61	**1,680**	**62**	1
over 50	55	2	67	3	**78**	**3**	0
Other specialists	**1,486**	**33**	**1,556**	**32**	**1,619**	**31**	**0**
including:							
men	909	61	915	59	**972**	**60**	1
women	577	39	641	41	**647**	**40**	–1
including:							
under 30	122	8	382	25	**356**	**22**	–3
30–50	1,184	80	1,079	69	**1,139**	**70**	1
over 50	180	12	95	6	**124**	**8**	2

[1] Managers with at least one subordinate.

Number of employees hired

Indicator	2021	2022	2023	Change, 2023/2022, %
Employees hired	1,039	1,445	**944**	–35

The number of employees hired in 2023 decreased by more than a third compared with 2022 due to a reduction in staff turnover and a corresponding decrease in the number of vacancies to fill.

Number of employees hired by age group

	2021		2022		2023		
Employee age	**people**	**%**	**people**	**%**	**people**	**%**	**Change, 2023/2022, %**
Under 30	351	34	557	39	**371**	**39**	–33
30–40	496	48	648	45	**407**	**43**	–37
40–50	142	14	200	14	**131**	**14**	–36
50 and over	50	5	40	3	**35**	**4**	–13

Number of employees hired by gender

	2021		2022		2023		
Employee gender	**people**	**%**	**people**	**%**	**people**	**%**	**Change, 2023/2022, %**
Men	762	73	1,075	74	**721**	**76**	–33
Women	277	27	370	26	**223**	**24**	–40

Number of employees hired by region

Region	2021	2022	2023	Change, 2023/2022, %
Asia-Pacific	47	37	**33**	–11
Latin America	22	25	**39**	56
Middle East, Turkey and Africa	19	24	**50**	108
Europe	53	45	**41**	–9
North America	14	7	**3**	–57
CIS	884	1,307	**778**	–40
including Russia	875	1,291	**769**	–40

Number of outgoing employees

Indicator	2021	2022	2023	Change, 2023/2022, %
Outgoing employees	826	1,101	**770**	–30

Number of outgoing employees by age group

	2021		2022		2023		
Employee age	people	%	people	%	people	%	Change, 2023/2022, %
Under 30	275	33	356	32	**265**	**34**	–26
30–40	361	44	477	43	**320**	**42**	–33
40–50	145	18	204	19	**142**	**18**	–30
50 and over	45	5	64	6	**43**	**6**	–33

The number of outgoing employees in 2023 decreased due to the general trend of lower staff turnover.

Number of outgoing employees by gender

	2021		2022		2023		
Employee gender	people	%	people	%	people	%	Change, 2023/2022, %
Men	521	63	812	74	**521**	**68**	–36
Women	305	37	289	26	**249**	**32**	–14

Number of outgoing employees and staff turnover by region

	Total outgoing employees			Staff turnover, %			
Region	**2021**	**2022**	**2023**	**2021**	**2022**	**2023**	**Change, 2023/2022, p.p.**
Asia-Pacific	54	59	**29**	22	26	**13**	–13
Latin America	9	21	**13**	9	20	**10**	–10
Middle East, Turkey and Africa	12	20	**19**	13	19	**15**	–4
Europe	77	127	**52**	18	34	**15**	–19
North America	39	44	**7**	31	49	**10**	–39
CIS	635	830	**650**	20	22	**16**	–6
including Russia	629	821	**644**	19	22	**16**	–6
Total	**826**	**1,101**	**770**	**19**	**23**	**15**	**–8**

Employees remaining with the Company after parental leave

	2021		2022		2023		
Employee gender	**people**	**%**	**people**	**%**	**people**	**%**	**Change, 2023/2022, %**
Women	28	72	38	76	**42**	**68**	11
Men	2	100	4	67	**2**	**67**	–50

Return to work rate after parental leave, %

Employee gender	2021	2022	2023
Women	98	96	**98**
Men	100	100	**100**

Employee retention rate, %

Employee gender	2021	2022	2023
Women	90	67	**71**
Men	50	38	**50**

Ratio of remuneration[1] of women and men[2], %

Indicator	2021	2022	2023
Managers			
Women's salary as a percentage of men's salary	96	95	**95**
Women's remuneration as a percentage of men's remuneration	98	95	**95**
Technical specialists			
Women's salary as a percentage of men's salary	97	98	**96**
Women's remuneration as a percentage of men's remuneration	97	98	**95**
Other specialists			
Women's salary as a percentage of men's salary	95	100	**96**
Women's remuneration as a percentage of men's remuneration	95	100	**96**

[1] Salary and benefits depending on category, length of service, etc.

[2] Data given for the Company's Moscow office.

Appendix 4. Future Tech section

List of laws, bylaws, orders or recommendations that the Company considers when developing products and solutions

Country	Regulator	Laws, bylaws, orders or recommendations
Russia	Russian Ministry of Digital Development, Communications and Mass Media Russian Federal Service for the Supervision of Communications, Information Technology and Mass Media Bank of Russia Russian Federal Service for Technical and Export Control Russian Federal Security Service	Federal Law No. 187-FZ dated July 26, 2017 On the Security of Critical Information Infrastructure of the Russian Federation Federal Law No. 149-FZ dated July 27, 2006 On Information, Information Technologies and Information Protection
Germany	UP KRITIS: BSI, BBK BMI; BDEW; BNetzA	IT Security ACT UP KRITIS; Namur 153; VDMA 66418; DIN2008; DIN2011
France	ANSSI	Critical Information Infrastructure Protection (CIIP) framework. CIIP law; Sécurité des activités d'importance vitale (SAIV); Décret 350, 351
UK	National Cyber Security Centre. National Protective Security Authority	OG86 — Cyber Security for industrial automation and control systems (IACS)
Spain	El Centro Nacional de Protección de Infraestructuras Críticas	El Plan Nacional de Protección de Infraestructuras Críticas
UAE	UAE Cybersecurity Council	NESA IAS
Saudi Arabia	National Cybersecurity Authority	OTCC Operational Technology Cybersecurity Controls
Turkey	Ministry of Transport Maritime affairs and communications	National Cybersecurity Strategy
India	NCIIP	Guidelines for the Protection of National Critical Information Infrastructure
Singapore	OTCCF. CII Cybersecurity ACT	Cybersecurity code of practice for Critical information infrastructure

Appendix 5. GRI Standards Compliance Index

Kaspersky presents its GRI Standards Report for the period from July 1, 2022 to December 31, 2023.

Indicator	Disclosure	Comments	Report section	Page
General Disclosures				
GRI 2–1	Organizational details	Parent company name: Holding Company Kaspersky Labs Limited (registered in the UK). The main legal entity in the Russian Federation is AO Kaspersky Lab. The organization is headquartered at 39A/2 Leningradskoe Shosse, Moscow, 125212, Russian Federation. Legal information: https://www.kaspersky.ru/legal.ru		6
GRI 2–2	Entities included in the organization’s sustainability reporting		Appendix 1	139
GRI 2–3	Reporting period, frequency and contact point	Kaspersky’s Sustainable Development Report covers the period from July 1, 2022 to December 31, 2023. Further sustainable development reports will be published annually, around the same time as the financial statement.		
GRI 2–4	Restatements of information	No information was restated.		
GRI 2–5	External assurance	This Report has not been externally certified.		
GRI 2–6	Activities, value chain and other business relationships		About the Company	4, 7, 8
GRI 2–7	Employees		People Empowerment Appendix 3	88 141
GRI 2–8	Workers who are not employees	All workers are Kaspersky’s employees.		
GRI 2–9	Governance structure and composition		Sustainable Development Ethics and Transparency	15 132–133
GRI 2–10	Nomination and selection of the highest governance body		Ethics and Transparency	132
GRI 2–11	Chair of the highest governance body		Ethics and Transparency	133
GRI 2–12	Role of the highest governance body in overseeing the management of impacts		Sustainable Development	15

Indicator	Disclosure	Comments	Report section	Page
GRI 2–13	Delegation of responsibility for managing impacts		Sustainable Development Ethics and Transparency	15–16 132
GRI 2–15	Conflicts of interests	The Company has adopted a declaration policy concerning its participation in any other companies in the capacity of founding members, shareholders or board members. Concurrent participation is not allowed without the consent of Kaspersky's board of directors or governing board. Members of the board of directors and the governing board only hold governing positions at companies owned by or affiliated with Kaspersky Labs Ltd. During the reporting period, there were no cases of members of the Company's senior management bodies concurrently participating in other organizations without the consent of the board of directors or governing board.	Sustainable Development	
GRI 2–16	Communication of critical concerns		Sustainable Development	15
GRI 2–17	Collective knowledge of the highest governance body	To improve the awareness and expertise of the highest management body in matters concerning sustainable development, representatives of the board of directors and the governing board regularly take part in training events with external experts.		
GRI 2–18	Evaluation of the performance of the highest governance body	The annual shareholder meeting conducts a regular performance assessment of the board of directors and the governing board. This evaluation serves as the basis for restructuring to improve the operational management of the Company. No assessment criteria were introduced during the reporting period to evaluate the management bodies' activities regarding the supervision of the Company's impact management on the economy, environment and social sphere.		
GRI 2–19	Remuneration policies	At the time of this Report, the Company's remuneration policy did not specifically take into account the effectiveness of managing the Company's impact on the economy, social sphere and environment.		
GRI 2–20	Process to determine remuneration		Ethics and Transparency	133
GRI 2–21	Annual total compensation ratio	This information is not disclosed due to limitations imposed by the Company's internal confidentiality policy.		
GRI 2–22	Statement on sustainable development strategy		Sustainable Development	13
GRI 2–23	Policy commitments		Sustainable Development	13
GRI 2–24	Embedding policy commitments		Sustainable Development Ethics and Transparency	14 134

Indicator	Disclosure	Comments	Report section	Page
GRI 2–25	Processes to remediate negative impacts		Ethics and Transparency	127, 134
GRI 2–26	Mechanisms for seeking advice and raising concerns		Ethics and Transparency	127, 134
GRI 2–27	Compliance with laws and regulations	During the reporting period, no incidents of Kaspersky failing to comply with legislation or any regulatory requirements were recorded; no fines or any other liabilities for violations of the law were imposed on the Company.		
GRI 2–28	Membership associations		Sustainable Development Appendix 2	14 140
GRI 2–29	Approach to stakeholder engagement		Sustainable Development	21
GRI 2–30	Collective bargaining agreements	Kaspersky has no practice of collective bargaining agreements due to a lack of demand for them among employees.		
Material Topics				
GRI 3–1	Process to determine material topics		Sustainable Development	19
GRI 3–2	List of material topics		Sustainable Development	20
Indirect Economic Impacts				
GRI 203–1	Infrastructure investments and services supported		Safer Cyber World People Empowerment	32–34, 37, 40 100–101
Anti-corruption				
GRI 205–1	Operations assessed for risks related to corruption		Ethics and Transparency	134
GRI 205–2	Communication and training about anti-corruption policies and procedures		Ethics and Transparency	
GRI 205–3	Confirmed incidents of corruption and actions taken		Ethics and Transparency	
Energy				
GRI 302–1	Energy consumption within the organization		Safer Planet	76
GRI 302–4	Reduction of energy consumption		Safer Planet	

Indicator	Disclosure	Comments	Report section	Page
Water and Effluents				
GRI 303–1	Interactions with water as a shared resource	The locations of the Company's offices are not qualified as water stress regions.	Safer Planet	78
GRI 303–2	Management of water discharge-related impacts		Safer Planet	
GRI 303–3	Water withdrawal		Safer Planet	
GRI 303–4	Water discharge		Safer Planet	
GRI 303–5	Water consumption		Safer Planet	
Emissions				
GRI 305–1	Direct (Scope 1) GHG emissions	The methodology of data collection and calculation of the total amount of direct greenhouse gas emissions across all of the Company's facilities (Scope 1) has yet to be developed and the data will be presented in subsequent reports.		
GRI 305–2	Energy indirect (Scope 2) GHG emissions	The methodology of data collection and calculation of the total amount of indirect greenhouse gas emissions (Scope 2) has yet to be developed and the data will be presented in subsequent reports.		
GRI 305–5	Reduction of GHG emissions		Safer Planet	75
GRI 305–6	Emissions of ozone-depleting substances (ODS)	Not applicable. The Company does not produce any ODS emissions.		
GRI 305–7	Nitrogen oxides (NOx), sulfur oxides (SOx) and other significant air emissions	Not applicable. The Company does not produce any emissions of these pollutants into the atmosphere.		
Waste				
GRI 306–1	Waste generation and significant waste-related impacts		Safer Planet	80–83
GRI 306–2	Management of significant waste-related impacts		Safer Planet	
GRI 306–3	Waste generated		Safer Planet	
GRI 306–5	Waste directed to disposal		Safer Planet	

Indicator	Disclosure	Comments	Report section	Page
Employment				
GRI 401–1	New employee hires and employee turnover		People Empowerment Appendix 3	87 141
GRI 401–2	Benefits provided to full-time employees that are not provided to temporary or part-time employees		People Empowerment	91
GRI 401–3	Parental leave		People Empowerment Appendix 3	91 147
Occupational Health and Safety				
GRI 403–1	Occupational health and safety management system	The occupational health and safety management system at all of Kaspersky's offices within the scope of disclosure in this Report complies with the requirements of applicable employment legislation in the Company's regions of presence. The system includes regular employee training and regular special workplace assessment in all divisions, as well as a risk management and accident investigation system and measures to improve working conditions. The main criterion for the system's effectiveness is zero on-the-job injuries.		
GRI 403–2	Hazard identification, risk assessment, and incident investigation	During the reporting period, no accidents related to occupational risks were recorded at the Company.	People Empowerment	95
GRI 403–4	Worker participation, consultation, and communication on occupational health and safety		People Empowerment	
GRI 403–5	Worker training on occupational health and safety		People Empowerment	
GRI 403–6	Promotion of worker health		People Empowerment	
GRI 403–8	Workers covered by an occupational health and safety management system		People Empowerment	
GRI 403–9	Work-related injuries		People Empowerment	
GRI 403–10	Work-related ill health	During the recording period, no incidents of work-related ill health were recorded at Kaspersky.		

Indicator	Disclosure	Comments	Report section	Page
Training and Education				
GRI 404–1	Average hours of training per year per employee		→ People Empowerment	90
GRI 404–2	Programs for upgrading employee skills and transition assistance programs		→ People Empowerment	89–90
GRI 404–3	Percentage of employees receiving regular performance and career development reviews		→ People Empowerment	88
Diversity and Equal Opportunity				
GRI 405–1	Diversity of governance bodies and employees		→ People Empowerment → Appendix 3	92 141–148
GRI 405–2	Ratio of basic salary and remuneration of women to men		→ Appendix 3	148
Non-discrimination				
GRI 406–1	Incidents of discrimination and corrective actions taken	During the reporting period, no incidents of discrimination were detected.		
Child labor				
GRI 408–1	Operations and suppliers at significant risk for incidents of child labor	The Company does not use child labor or employ employees under 18 years of age.		
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.		
Local Communities				
GRI 413–1	Operations with local community engagement, impact assessments, and development programs		→ People Empowerment	96–100
Customer Privacy				
GRI 418–1	Substantiated complaints concerning breaches of customer privacy and losses of customer data		→ Ethics and Transparency	125

Appendix 6. SASB Standards Compliance Index

Compliance of reporting elements with SASB Index Software & IT Services Standard, version 2018–10 (TC-SI)

Indicator	Disclosure	Report section	Comments	Page
Environmental Footprint of Hardware Infrastructure				
TC-SI-130-a.1	1. Total energy consumed 2. Percentage grid electricity 3. Percentage renewable	→ Safer Planet		76
TC-SI-130-a.2	1. Total water withdrawn 2. Total water consumed and percentage of each in regions with High or Extremely High Baseline Water Stress	→ Safer Planet		78
TC-SI-130-a.3	Discussion of the integration of environmental considerations into strategic planning for data center needs	→ Safer Planet		77
Data Privacy & Freedom of Expression				
TC-SI-220-a.1	Description of policies and practices relating to behavioral advertising and user privacy	→ Ethics and Transparency		125–128
TC-SI-220-a.2	Number of users whose information is used for secondary purposes		Number of such users is 0 (zero).	
TC-SI-220-a.3	Total amount of monetary losses as a result of legal proceedings associated with user privacy		No such incidents during the reporting period; the amount of monetary losses is 0 (zero).	

Indicator	Disclosure	Report section	Comments	Page
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	→ Ethics and Transparency	1. The policy is described in the corresponding section of the Report. The number of requests from government authorities can be found in Kaspersky's regular Law Enforcement & Government Requests Report. The most recent report covers the second half of 2023. 2. The Company does not keep track of this statistic; we only take into account the number of requests to provide user data and non-personal technical information. 3. 0% — Kaspersky has not yet disclosed such data to government authorities.	121–123
TC-SI-220-a.5	List of countries where core products or services are subject to government-required monitoring, blocking, content filtering or censoring		No such countries	
Data Security				
TC-SI-230-a.1	1. Number of data breaches 2. Percentage involving personally identifiable information (PII) 3. Number of users affected	→ Ethics and Transparency		128
TC-SI-230-a.2	Description of approach to identifying and addressing data security risks, including use of third-party cyber security standards	→ Ethics and Transparency		126–128
Recruiting & Managing a Global, Diverse & Skilled Workforce				
TC-SI-330-a.1	Percentage of employees that are 1. Foreign nationals, and 2. Located offshore		1. As of December 31, 2023, Kaspersky had 64 foreign citizens employed, which is 1.5% of the total headcount. No information concerning other regional offices was collected during the reporting period. 2. Not applicable to Kaspersky, since Russian labor legislation does not provide for working outside of the Russian Federation. No information concerning offices outside of Russia was collected during the reporting period.	
TC-SI-330-a.2	Employee engagement	→ People Empowerment		94
TC-SI-330-a.3	Percentage of gender and racial/ethnic group representation for 1. Management 2. Technical staff, and 3. All other employees	→ People Empowerment	The Company does not keep track of employee statistics by ethnic groups.	92, 114

Indicator	Disclosure	Report section	Comments	Page
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	Ethics and Transparency		130
Managing Systemic Risks from Technology Disruptions				
TC-SI-550-a.1	Number of 1. Performance issues and 2. Service disruptions 3. Total customer downtime		This information is not disclosed due to the limitations imposed by the Company's internal confidentiality policy.	
TC-SI-550-a.2	Description of business continuity risks related to disruptions of operations	Ethics and Transparency		135–137
Activity Metrics				
TC-SI-000.A	1. Number of licenses or subscriptions 2. Percentage cloud-based		1. 851 2. 33% cloud-based	
TC-SI-000.B	1. Data processing capacity 2. Percentage outsourced		1. 240 units in the local network and 7,372 outsourced 2. 97% outsourced (collocation)	
TC-SI-000.C	1. Amount of data storage 2. Percentage outsourced		1. Upwards of 100 petabytes 2. More than 91% outsourced (collocation)	

Appendix 7. Glossary

Alt Text	Brief description of an image to help with searching
APT	Advanced Persistent Threat
IoT	Internet of Things, a collective network of connected devices and technologies that facilitates communication between devices and the cloud and also between the devices themselves
Kill Chain	In cybersecurity, the term Kill Chain describes the sequence of steps that cybercriminals go through when attempting to carry out a successful cyberattack
LMS	Learning Management System
MOOC	Massive Open Online Courses, a modern form of distance education
ROI	Return on Investment ratio, which helps calculate the return on investment in a project
XDR	Extended Detection and Response, a class of information security systems for the extended detection and response to complex threats and targeted attacks
Additive technologies	A method of creating three-dimensional objects, parts, or things by adding material layer by layer
APCS	Automated process control system
Builder	A tool that can configure the parameters of malware before using it in a cyberattack

Endpoints and end devices	Physical devices that connect to and exchange data with a computer network (mobile devices, desktop computers, virtual machines, embedded hardware, or servers)
Neuromorphic processor	A processor whose functional principle and architecture are similar to the neural networks of living organisms
GG	Greenhouse gases and gaseous substances of natural or manmade origin that absorb and re-emit infrared radiation
Reverse engineering	Reverse engineering is the process of analyzing the machine code of a program in order to understand the principle of operation, restore the algorithm, discover undocumented program capabilities, etc.
MDR solutions	Managed Detection and Response solutions for the automatic detection and analysis of security incidents in infrastructure using telemetry and advanced machine learning technologies
Technical attribution	The process of determining or uncovering identification information that can identify or link a specific attacker, group of attackers or source country to a specific cyberattack or cyber incident
Unique user	A user who visited an Internet resource within a certain period of time (usually within 24 hours)
Data exfiltration	The process during which an attacker extracts sensitive data from another computer’s system and uses it for personal gain

Appendix 8. Contact information

GRI 2–3

For all questions related to this Sustainable Development Report, please contact **Maria Losyukova, Head of Sustainability:**

Maria.Losyukova@kaspersky.com

Headquarters mail address:

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

For general enquiries:

info@kaspersky.com

Contact information:

https://www.kaspersky.ru/about/contact

Press contacts:

empr@kaspersky.com