Kaspersky Corporate Kit

kaspersky

Our mission is simple — building a safer world.

We do that by becoming the global leader in cybersecurity. By securing technology we ensure that it stays free of cyberthreats – providing nothing but positive possibilities for everyone.

Bring on endless possibilities.
Bring on a safer tomorrow.

Eugene Kaspersky, CEO

Our key values that drive our work

Be there for you

We'll always be there for you, for our customers, partners, prospects & colleagues. We never lose sight of the people we build our solutions for.

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 on this duty we always play fair.

Be cleverly inventive

Focused and ready to act – we share cutting-edge information with customers, partners, colleagues and prospects to keep them ahead of the curve.

Be powered by challenges

We constantly challenge ourselves and the status quo to do what others can't. We deliver outstanding solutions to overcome obstacles of all kinds, and this is proven across our more than 25-year history.

Kaspersky at a glance

- Essentials
- Customers
- Geography
- Role in the global IT security community

Facts about us

Essentials

Founded in 1997
and led by Eugene Kaspersky

Present on five continents in more than 200 countries and territories

Provides innovative IT security solutions and services for businesses and consumers

Numbers

>10,5 million

consumer product activations per year

> 5,000

highly qualified specialists

US $721 million

global non-audited combined revenue in 2023

Customer reach

Our solutions and services are designed to meet the cybersecurity needs of a diverse range of customers, from individual users, small businesses and smart start-ups to large enterprises, critical infrastructure organizations and government institutions.

>200,000
Corporate clients worldwide choose our protection

1,000,000,000
Devices protected by Kaspersky to date*

Enterprises

Industrial facilities

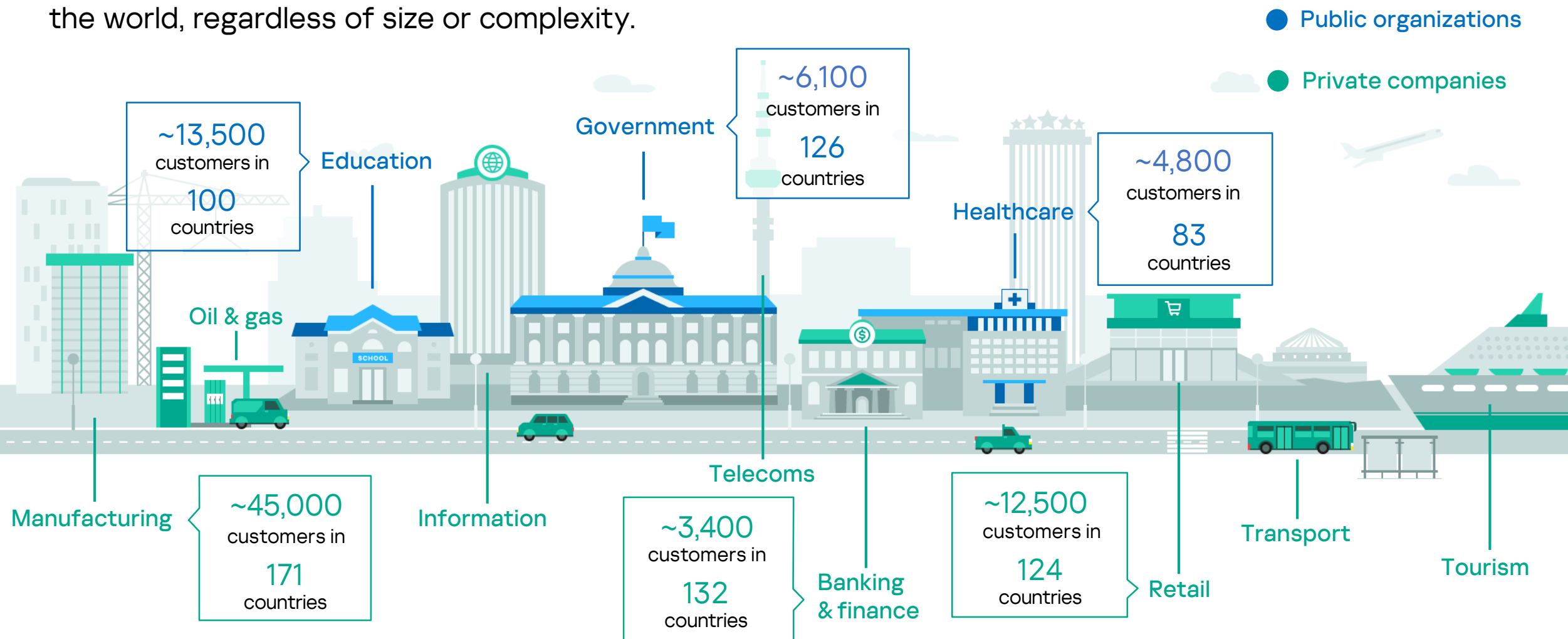Small and medium businesses

Very small businesses

Consumers

*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.

Our customers

We work in a wide range of industry sectors. Our solutions and services successfully protect over 200,000 clients around the world, regardless of size or complexity.

● Public organizations

● Private companies

Manufacturing
~45,000 customers in 171 countries

Oil & gas

Education
~13,500 customers in 100 countries

Information

Government

Telecoms
~6,100 customers in 126 countries

Banking & finance
~3,400 customers in 132 countries

Healthcare
~4,800 customers in 83 countries

Retail
~12,500 customers in 124 countries

Transport

Tourism

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | Education | Sponsorships & Partnerships

8

We are an international cybersecurity company

200 countries and territories where we operate

30+ representative regional offices

Africa
South Africa
Kenya
Rwanda

Asia
Greater China
(China, Hong
Kong)
India
Japan
Kazakhstan
Malaysia
Singapore
South Korea

Europe
Czech Republic
France
Germany
Israel
Italy
Netherlands
Portugal
Russia
Spain
Switzerland

Middle East
Saudi Arabia
Turkey
UAE

Latin America
Brazil
Mexico
Columbia

Transparency Centers

Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia
Kigali, Rwanda
Singapore
Bogotá, Colombia

Tokyo, Japan
Rome, Italy
Utrecht, the Netherlands
Riyadh, Saudi Arabia
Istanbul, Turkey
Seoul, South Korea

Our role in the global IT security community

We participate in joint operations and cybercrime investigations with the global IT security community, international organizations such as INTERPOL, law enforcement agencies and CERTs worldwide.

INTERPOL

Learn more

Coalition Against Stalkerware

Learn more

PARIS CALL
FOR TRUST AND SECURITY IN CYBERSPACE
11 · 12 · 2018

Learn more

industrial internet CONSORTIUM

Learn more

AFRIPOL

Learn more

Global Transparency Initiative

- Key transparency principles

- Global Transparency Initiative pillars

- Independent assessments and certifications

- Bug Bounty Program

Our key transparency principles

Data sent to Kaspersky is crucial for protecting users, it is robustly secured and is not attributed to a specific individual.

We detect and neutralize threats, regardless of their origin or purpose.

We work with international organizations to fight cybercrime.

We are committed to the trustworthy development of our technologies and solutions.

We cooperate with the IT security industry in joint cybercrime investigations.

Global Transparency Initiative pillars

Launched in 2017, Kaspersky's Global Transparency Initiative is aimed at engaging the broader information security community and other stakeholders in validating and verifying the trustworthiness of our products, internal processes, and business operations.

It includes a number of actionable and concrete measures:

Cyberthreat-related data infrastructure relocation to Switzerland.

Creation of a global network of Transparency Centers in some regions, where Kaspersky's trusted partners and government stakeholders can review the company's code, software updates and threat detection rules.

Third-party security assessments of Kaspersky's engineering and data management practices verify the security of the company's solutions.

Global Transparency Initiative pillars

It includes a number of actionable and concrete measures:

Vulnerability management program, under which security researchers can report vulnerabilities or bugs found in our systems for a designated reward.

Transparency reports, in which we publicly share information about the number of requests for user data and technical expertise.

Cyber Capacity Building Program – dedicated training to share security evaluation knowledge with the broader community.

Kaspersky Global Transparency Initiative

Cyberthreat-related user data storage and processing

Malicious and suspicious files received from users of Kaspersky products in Europe, North and Latin America, the Middle East, and also countries in Asia-Pacific region are processed and stored in Switzerland.

Transparency Centers

A facility for customers, partners and government stakeholders to review the company's code, software updates and threat detection rules, along with other activities.

Independent reviews

Regular third-party assessment of internal processes to confirm the security of Kaspersky's processes and systems, including:

- Regular SOC 2 audits
- ISO 27001 certifications for the company's data systems

Bug bounty program

Increased bug bounties up to $100k for the most critical vulnerabilities aim to engage security researchers to supplement the company's own work in ensuring the security of its solutions.

Transparency reports

Regular updates on how Kaspersky responds to requests from government and law enforcement agencies as well as to personal data-related requests from its own users.

Madrid, Spain
Transparency Center

Utrecht, the Netherlands
Transparency Center

Zurich, Switzerland
Transparency Center | Data Centers

Istanbul, Turkey
Transparency Center

Rome, Italy
Transparency Center

Seoul, South Korea
Transparency Center

Tokyo, Japan
Transparency Center

Riyadh, Saudi Arabia
Transparency Center

Kigali, Rwanda
Transparency Center

Singapore
Transparency Center

São Paulo, Brazil
Transparency Center

Kuala Lumpur, Malaysia
Transparency Center

Bogotá, Colombia
Transparency Center

kaspersky bring on the future

Proven.
Transparent.
Independent.

Kaspersky Transparency Centers

Review options:

Blue Piste (both remote & physical)

An overview of Kaspersky's transparency practices, products and services, as well as data management practices.

Red Piste

A review of the most critical parts of the source code, assisted by the company's experts.

Black Piste

The deepest review of the most critical parts of Kaspersky's source code, assisted by the company's experts.

Immerse yourself in the history of Global Transparency Initiative

Madrid, Spain
Transparency Center

Utrecht, the Netherlands
Transparency Center

Zurich, Switzerland
Transparency Center | Data Centers

Istanbul, Turkey
Transparency Center

Rome, Italy
Transparency Center

Seoul, South Korea
Transparency Center

Tokyo, Japan
Transparency Center

Riyadh, Saudi Arabia
Transparency Center

Kigali, Rwanda
Transparency Center

São Paulo, Brazil
Transparency Center

Singapore
Transparency Center

Bogotá, Colombia
Transparency Center

Kuala Lumpur, Malaysia
Transparency Center

kaspersky bring on the future

Proven. Transparent. Independent.

Kaspersky Global Transparency Initiative: our results in numbers

2 Additional data locations

in Switzerland: globally known as a neutral country, it contains strict data protection regulation.

Here we process and store cyberthreat-related user data from Europe, North and Latin America, the Middle East, and several countries in Asia-Pacific region.

13 Transparency Centers

in Brazil, Colombia, Italy, Japan, Malaysia, the Netherlands, Rwanda, Saudi Arabia, Singapore, South Korea, Spain, Switzerland, and Turkey.

2 Regular third-party independent assessments

confirming the trustworthiness of Kaspersky's engineering practices:

- SOC 2 audit
- ISO 27001 certification

$8.4 mln investment

Since 2018, Kaspersky has invested over $8.4 million in the program, which includes $5.6 million for equipment for the data centers in Zurich.

65 Transparency Center reviews

by public and private stakeholders

62 Bug Bounty report awarded

with total payments equal to $88,250

kaspersky bring on the future

Proven. Transparent. Independent.

Independent assessments and certifications

SOC

The Service Organization Controls (SOC) Reporting Framework, a globally recognized report for cybersecurity risk management controls, was developed by the American Institute of Certified Public Accountants (AICPA). Kaspersky successfully passed a comprehensive SOC 2 Type 2 audit in 2024.

Learn more

ISO/IEC 27001

The most widely used information security standard prepared and published by the International Organization for Standardization (ISO), the world's largest developer of voluntary international standards. Kaspersky's information security management system has been certified against ISO/IEC 27001:2013 international standard.

Learn more

Bug Bounty Program

Kaspersky is committed to the principles of [ethical vulnerability disclosure approach](#). To ensure the integrity of our products, Kaspersky has been running its public bug bounty program since 2016, and since 2022, it operates on the [Yogosha platform](#). The company also supports the Disclose.io framework, which provides a "Safe Harbor" for vulnerability researchers concerned about the negative legal consequences of their discoveries.

Rewards

$100,000
for the discovery and coordinated disclosure of severe vulnerabilities (high-quality reports with PoC).

$5,000 – $20,000
for the discovery of vulnerabilities allowing different and less severe types of remote code execution.

$1,000 – $5,000
for the discovery of bugs allowing local privilege escalation, or leading to sensitive data disclosure.

Learn more

Threat intelligence and research

- Expertise

- Threat research

- Current advanced persistent threat landscape

- Major discoveries and research

- Targeted attack research

- Enabling a privacy-minded world

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | Education | Sponsorships & Partnerships

20
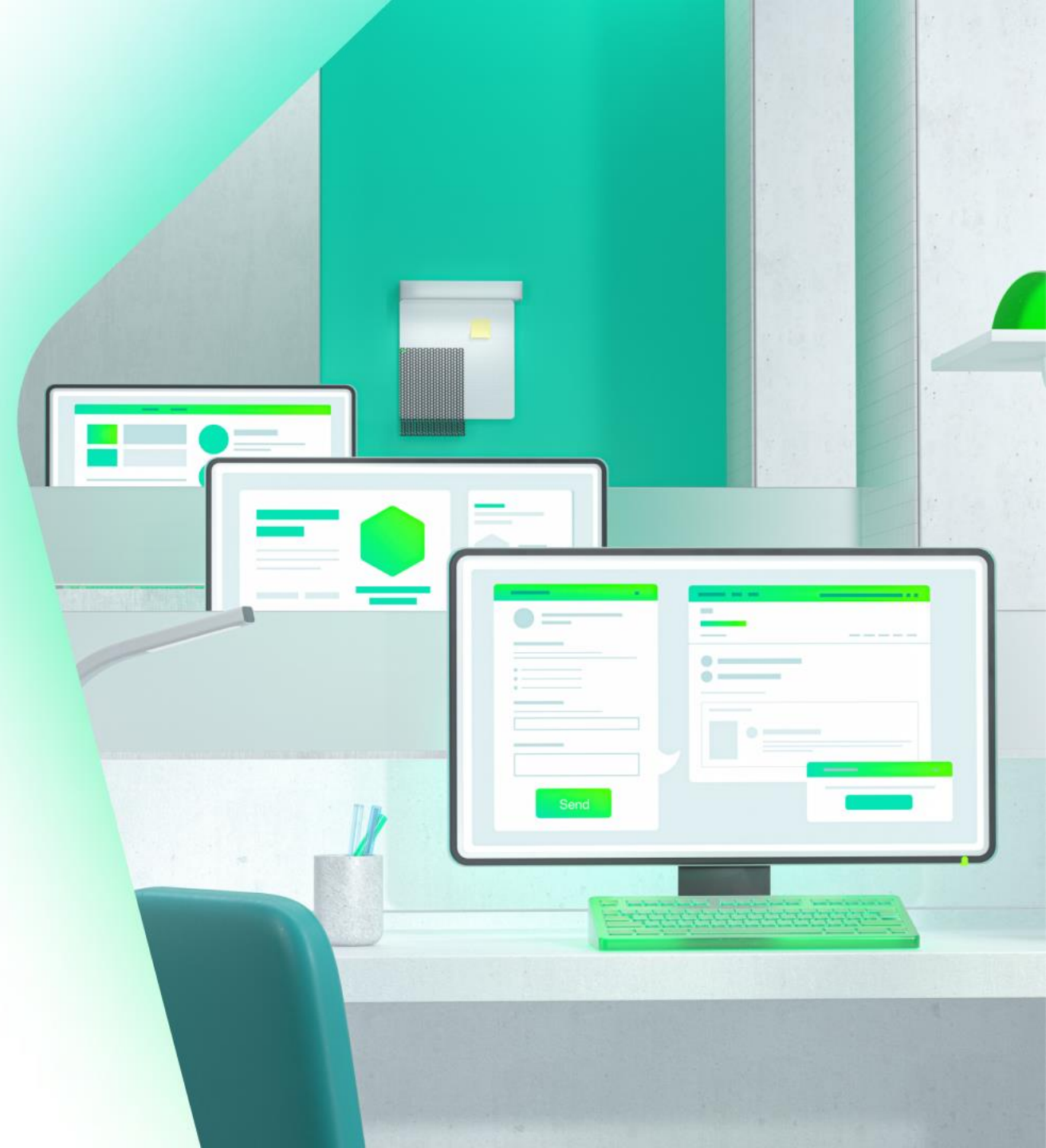
Expertise

Our unique team of security experts are at the forefront of protecting people around the world from the most sophisticated and dangerous cyberthreats. This expertise enriches our state-of-the-art protection technologies, making their quality unsurpassed.

>5,000 Highly-qualified specialists

50% of our employees are R&D specialists

35+ Members in our group of elite world-leading security experts - GReAT

Kaspersky Expertise Centers: international teams

Kaspersky Global Research and Analysis Team

GReAT

Research of the most complex threats: APT, cyber espionage campaigns, global cyber epidemics, etc.

Investigation of sophisticated financial cybercrime

Security of future-focused technologies

Kaspersky Threat Research

Threat Research

Anti-Malware Research

Content Filtering Research

SSDLC & Secure-by-Design Methodologies

Kaspersky AI Technology Research

AI Technology Research

AI-Powered Threat Detection / Solutions

AI Cybersecurity

GenAI Research

Every center contributes to Kaspersky's solutions and services

Expertise Centers

Kaspersky Security Services

Security Services

MDR

Incident Response

Security Assessment

SOC Consulting

Digital Footprint Intelligence

Kaspersky ICS CERT

ICS CERT

Critical Infrastructure Threat Analysis

Technology Associations, Analytics and Standards

ICS Vulnerability Research and Assessment
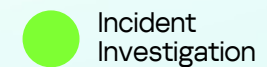
● Threat Research   ● Incident Investigation

Threat research

>1,900,000,000
cyberthreats

detected by Kaspersky since
the company's inception

4,900,000,000
cyberattacks

detected by Kaspersky in 2024

467,000
new malicious files

detected by Kaspersky every day

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | Education | Sponsorships & Partnerships

23
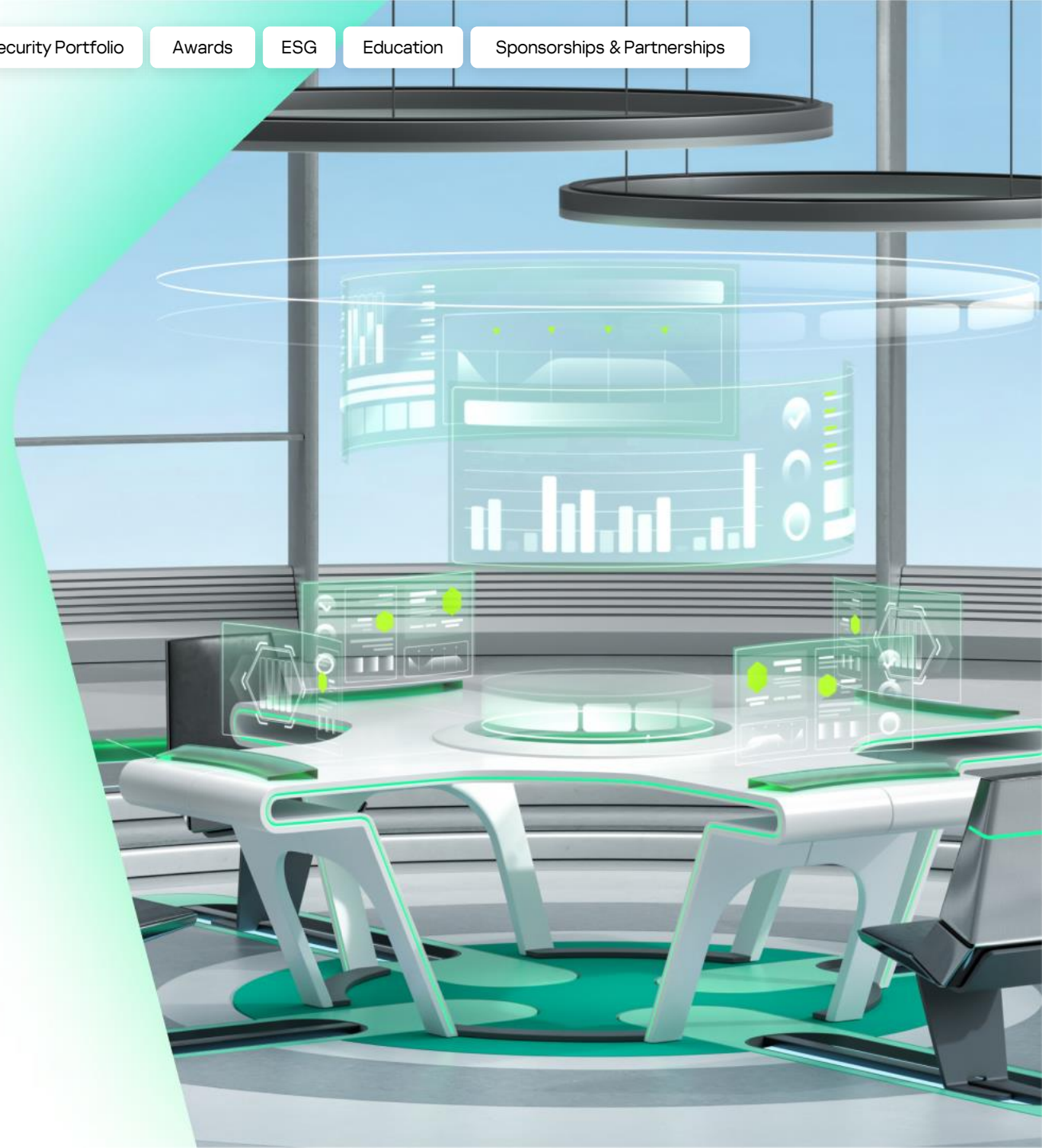
Advanced persistent threat landscape in 2023

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and analysis of the most advanced cyberthreats. According to their data, in 2023 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets

- Government
- Military
- Diplomatic
- IT companies
- Energy
- Telecommunications
- Cryptocurrency
- Industrial
- Manufacturing
- Technology Research

Top 10 significant threat actors

1. Lazarus
2. APT10
3. Kimsuky
4. ZexCone
5. Tomiris
6. Ghostwriter
7. DeathStalker
8. BitterAPT
9. SideCopy
10. Gelsemium

Top 12 targeted countries and territories

UAE · Egypt · Pakistan · Iran · Turkey · Afghanistan · Russia · India · China

Taiwan · Vietnam · Colombia

apt.securelist.com

Based on the data up to 31.12.2023

Kaspersky at a glance | Global Transparency Initiative | **Threat Intelligence and research** | Cybersecurity Portfolio | Awards | ESG | Education | Sponsorships & Partnerships

24

Our major discoveries and research

	Expetr/ Notpetya	Olympic destroyer	Shadow hammer	Tajmahal	Mosaicregressor	Ghostemperor	Moonbounce	Operation Triangulation
Detection	**2017**	**2018**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
Active since	**2017**	**2017**	**2018**	**2013**	**2017**	**2020**	**2021**	**2019**
Classification	Data wiping campaign	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	APT campaign
Description	A wiper pretending to be ransomware, using modified EternalBlue and EternalRomance exploits. Some observations point to a link between ExPetr and BlackEnergy APT	An advanced threat actor that hit organizers, suppliers and partners of the Winter Olympic Games in Pyeongchang, South Korea, with a destructive network worm. The deceptive behavior of this actor is an excessive use of various false flags	As a result of a sophisticated supply chain attack on the popular computer vendor's software update system, the malware disguised as a software update was distributed to about 1 million Windows computers and signed using a legitimate certificate	A technically sophisticated APT framework designed for extensive cyberespionage. Features around 80 malicious modules and includes functionality never before seen in an advanced persistent threat, such as the ability to steal information from printer queues and to grab previously seen files from a USB device the next time it reconnects	A multi-stage, modular framework aimed at espionage and data gathering. It is leveraging a UEFI bootkit based on Hacking Team's leaked source code for persistence. Capable of communicating and fetching payloads over multiple, covert channels.	A stealthy, sophisticated multi-stage malware framework incorporating Windows kernel mode rootkit. It's deployed via the ProxyLogon only days following the vulnerability disclosure.	A highly sophisticated, complex UEFI firmware rootkit we attributed to APT41, which allows the attackers to persistently execute a malware stager on the operating system via a malicious driver.	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. .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.
Targets	Spread around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. >50% of organizations attacked were industrial companies	Organizations related to Winter Olympic Games 2018; biological and chemical threat prevention organizations in the EU, financial institutions in Russia	Banking and financial industry, software, media, energy and utilities, insurance, industrial and construction, manufacturing, and other industries	Special instructions in malware code were aimed at targeting only 600 systems, identified by specific MAC addresses	Diplomatic entities with possible affiliation to DPRK	Government organizations and Telecommunication companies	Holding companies and industrial suppliers	iOS devices

Targeted attack research

2017	2018	2019	2020	2021	2022	2023
WannaCry	Zebrocy	Topinambour	Cycldek	Tomiris	ZexCone	PowerMagic
Shamoon 2.0	DarkTequila	ShadowHammer	SixLittleMonkeys (aka Microcin)	GhostEmperor	SilentMarten	CommonMagic
StoneDrill	MuddyWater	SneakyPastes	CactusPete	ExCone	MoonBounce	Trila
BlueNoroff	Skygofree	FinSpy	DeathStalker	BlackShadow	ToddyCat	LoneZerda
ExPetr/NotPetya	Olympic Destroyer	DarkUniverse	MATA	BountyGlad	MagicKarakurt	CloudWizard
Moonlight Maze	ZooPark	COMpfun	TransparentTribe	EdwardsPhesant	CosmicStrand	Operation Triangulation
ShadowPad	Hades	Titanium	WellMess	HotCousin	SBZ	BlindEagle
BlackOasis	Octopus		TwoSail Junk	GoldenJackal	StripedFly	Mysterious Elephant
Silence	AppleJeus		MontysThree	FerociousKitten	DiceyF	BadRory
WhiteBear			MosaicRegressor	ReconHellcat	MurenShark	Dark Caracal
			VHD Ransomware	CoughingDown		HrServ
			WildPressure	MysterySnail		
			PhantomLance	CraneLand		

Enabling a privacy-minded world

Privacy has become a valuable commodity as more and more users understand its importance and the need to change their habits to protect their digital presence. Being not just a cybersecurity firm, but a privacy company, Kaspersky invests in features that enable users to protect their data and digital privacy through educational assets and hands-on tools.

Anti-doxing course

Learn what the basic dangers of doxing are and how to protect yourself from it

Learn more

Anti-stalking Awareness Guide

Engaging psychologists and surveillance victims to combat stalking, this guide helps users identify signs of stalking and take protective measures.

Learn more

Stalkerware protection

Kaspersky's consumer security solution offers users best-in-class protection and detection of software used to secretly spy on people

Learn more

Privacy Checker

Instructions on how to set social media accounts and OS privacy levels

Learn more

Kaspersky Cybersecurity Portfolio

- Corporate Cybersecurity
- Industrial Cybersecurity
- Threat Intelligence
- MSSP/MSP Offering
- Cyber Immunity approach
- Consumer Cybersecurity

Kaspersky proposal for IT environment

Kaspersky Expert Security | Expert approach to protecting the corporate business segment

Corporate cybersecurity

1 Solutions
2 Threat Intelligence & Training
3 Expert Services

1 XDR Corporate — **Kaspersky Next XDR Expert**

Highest tier expert solutions

- Kaspersky Anti Targeted Attack
- Kaspersky Next EDR Expert
- Kaspersky Unified Monitoring and Analysis Platform

Targeted solutions

- Kaspersky Container Security
- Kaspersky SD-WAN
- Kaspersky Fraud Prevention
- Kaspersky Scan Engine

2

Awareness
- Kaspersky Security Awareness

Threat Intelligence
- Kaspersky Threat Intelligence

Trainings
- Kaspersky Cybersecurity Training

3

Assessment
- Kaspersky Security Assessment

Managed security
- Kaspersky Managed Detection and Response

Response
- Kaspersky Incident Response

Compromise assessment
- Kaspersky Compromise Assessment

Convergence of IT and OT environments | Environments boundary

Industrial cybersecurity

XDR Industrial — **Kaspersky Industrial Cybersecurity** — for Nodes / for Networks

Open Single Management Platform

Kaspersky proposal for OT environment

Corporate cybersecurity

XDR Corporate

k Kaspersky Next XDR Expert

Open Single Management Platform

Convergence of IT and OT environments

Environments boundary

Industrial cybersecurity

Kaspersky OT Cybersecurity | Kaspersky's complete industrial cybersecurity ecosystem

1 Solutions

2 Threat Intelligence & Training

3 Expert Services

1 XDR Industrial

Kaspersky Industrial Cybersecurity
- for Nodes
- for Networks

Specialized solutions

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection (MLAD)
- Kaspersky SD-WAN

Cyber Immune solutions

- Kaspersky IoT Secure Gateway
- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

2

Awareness
- Kaspersky Security Awareness

Threat Intelligence
- Kaspersky ICS Threat Intelligence (ICS CERT)

Trainings
- Kaspersky ICS CERT Training (ICS CERT)

3

Assessment
- Kaspersky ICS Security Assessment

Managed security
- Kaspersky ICS MDR

Response
- Kaspersky ICS CERT Incident Response

Kaspersky Threat Intelligence

Machine-readable Threat Intelligence

Kaspersky Threat Data Feeds ●

Kaspersky CyberTrace ● ●

Threat Intelligence expert support

Kaspersky Takedown Service ●

Kaspersky Ask the Analyst ● ●

Human-readable Threat Intelligence

● ● ○
Kaspersky Threat Lookup

● ● ○
Kaspersky Threat Infrastructure Tracking

● ○
Kaspersky Threat Analysis

Sandbox | Attribution | Similarity
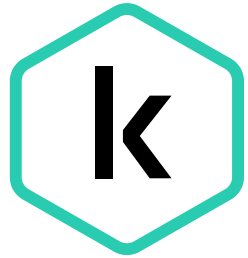
● ● ● ○
Kaspersky Intelligence Reporting

APT | Crimeware | ICS

● ● ○
Kaspersky Digital Footprint Intelligence

Kaspersky Threat Intelligence

● Tactical
● Operational
● Strategic

○ Available via

Kaspersky Threat Intelligence Portal

Kaspersky Next: B2B flagship product line

Kaspersky Next

Take your security to the next level

Build up your cybersecurity with leading-edge EDR and XDR that stops attacks in their tracks, supported by strong, proven protection technologies.

Kaspersky Next EDR Optimum

Optimum defense against advanced threats

EPP & EDR for small cybersecurity teams

- Strong endpoint protection
- Advanced system hardening controls
- Enhanced EDR capabilities
- Expanded cloud security
- Cybersecurity training for IT administrators

Kaspersky Next XDR Expert

Expert defense against sophisticated threats

Ultimate XDR instrument for large cybersecurity or SOC teams

- Strong endpoint protection
- Advanced system hardening controls
- Powerful EDR capabilities
- Advanced threat detection and response across the infrastructure
- Investigation graph, case management, playbooks
- Seamless third-party integration

Kaspersky Next EDR Foundations

Fundamental protection against mass threats

The best, most comprehensive endpoint protection for businesses with small IT teams

- Strong endpoint protection
- Basic system hardening controls
- Basic EDR capabilities
- Maximum automation

Comprehensive MSP and MSSP offering to build security services

MSP

MSSP

- MSP beginners
- Growing partners
- Expert advisors
- Commercial SOCs

Automation and integration

- RMM and PSA Integrations
- Subscription-based model and LMP

Knowledge and Support

- Kaspersky Cybersecurity Training
- Kaspersky Premium Support and Professional Services

#1 Managed Protection Services

- Kaspersky Next EDR Foundations
- Kaspersky Next EDR Optimum
- Kaspersky Hybrid Cloud Security
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security for Mail Server
- Kaspersky Security for Web Gateway

#2 Managed Detection & Response Services

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack
- Kaspersky Next EDR Expert

#3 Managed Threat Intelligence Services

- Kaspersky Threat Lookup
- Kaspersky Cloud Sandbox
- Kaspersky Digital Footprint Intelligence
- Kaspersky Threat Data Feeds
- Kaspersky Intelligence Reporting

#4 SOC as a Services

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky CyberTrace
- Kaspersky Threat Data Feeds

Build services:

- Endpoint Protection and hardening
- Vulnerability and Patch Management
- Office365 Protection
- Security Awareness
- Managed Mail & Web Protection

- Network Threat Detection & Response
- Endpoint Threat Detection & Response

- Brand protection service
- Detection context enrichment
- Threat reporting service

- 24/7 Security Monitoring
- Incident Response
- Proactive Threat Hunting

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | **Cybersecurity Portfolio** | Awards | ESG | Education | Sponsorships & Partnerships

33

Kaspersky Cyber Immunity

KasperskyOS-based Cyber Immune solutions have an "innate" protection against the consequences of the intrusion of malicious code and hacker attacks.

Kaspersky-OS grants a platform for creating secure-by-design solutions

IoT & Industrial IoT

Transportation

Smart cities

Professional mobile devices

Thin client infrastructure

Creates an environment that does not allow apps to execute undeclared functions and prevents the exploitation of vulnerabilities

Provides full transparency, flexible configuration of security policies and control over interactions across the whole system

The system requires minimal updates, effectively resists unknown threats, helping to reduce financial and image losses.

KasperskyOS-based product portfolio

Kaspersky IoT Infrastructure Security

A solution for cybersecure data transfer to digital and cloud business platforms, as well as for infrastructure protection and transparency

Kaspersky IoT Secure Gateway
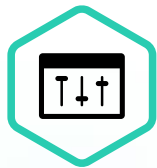
Kaspersky Security Center

Kaspersky Thin Client

A solution for building a Cyber Immune, functional, and manageable thin client infrastructure with convenient, centralized management
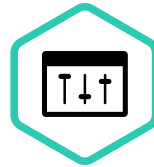
Kaspersky Security Center
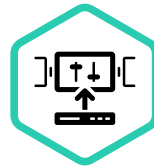
Kaspersky Security Management Suite

Kaspersky Appicenter

Digital application distribution platform for KasperskyOS-based devices, connecting end users, developers and global vendors.

Kaspersky Automotive Secure Gateway

Building reliable IT systems for smart road vehicles

Kaspersky Automotive Adaptive Platform

Kaspersky Automotive Secure Broker Framework

Kaspersky OTA Agent

Kaspersky Vehicle SOC Agent

Kaspersky Remote Diagnostic Agent

POWERED BY KasperskyOS

B2C Solutions: Core product portfolio

Our comprehensive plans cover the full range of customer needs

Complete protection for your digital life

🎧 Premium services

🪪 Identity

🏠 Smart home

👤 Privacy

📊 Performance

🛡 Security

Kaspersky Standard

Kaspersky Plus

Kaspersky Premium

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | **Cybersecurity Portfolio** | Awards | ESG | Education | Sponsorships & Partnerships

36

Complete protection for consumers' digital lives

With our diverse collection of security products, we inspire customers to embrace new technologies – because they know we're guarding them and their families.

Kaspersky B2C Solutions

Kaspersky Standard
Win | Android | Mac | iOS

Kaspersky Plus
Win | Android | Mac | iOS

Kaspersky Premium
Win | Android | Mac | iOS

Kaspersky VPN Secure Connection
Win | Android | Mac | iOS

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

Kaspersky Who Calls*
Android | iOS
*Only available in Russia, Kazakhstan and Indonesia

CBA-specific solutions*

Kaspersky Safe Web
Web-based

Kaspersky Smart Home
Router-based

*CBA (Consumer Business Alliance) includes partnerships with service providers and resellers for distributing tangible or electronic Kaspersky licenses.

Kaspersky awards

- Overview
- Top 3 metrics
- Recognitions

More than 600 awards*

Kaspersky Standard was honored with the **Product of the Year 2023** annual award by independent test lab AV-Comparatives**.

Kaspersky EDR Expert continually delivers top results: Total Accuracy Rating of 100% in Advanced Security EDR tests of 2022&2023 by SE Labs***; 100% protection from targeted attacks, and **Strategic Leader** status from AV-Comparatives****, and got approved by AV-Test*****.

Learn more

*The number includes independent test results of corporate and consumer products during 2013-2023.

** Kaspersky's flagship home user security solution – Kaspersky Standard – was honored with the annual Product of the Year 2023 award for high results in 8 Real-World tests, 2 Malware Protection tests, 2 Performance tests, and Enhanced Real-World test of 2023.

*** Enterprise Advanced Security EDR test reports of 2022 and 2023

**** Endpoint Detection and Response tests of 2022 and 2023

***** Advanced EDR Test 2023

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | **Awards** | ESG | Education | Sponsorships & Partnerships

39

Awards

Most Tested
Most Awarded*
Kaspersky Protection

*Kaspersky.com/top3

100

Tests/Reviews

93

First Places

94%

Top 3

As cybersecurity becomes vital to every individual and entity, trust in providers is essential. We protect home users and corporate clients worldwide, and market recognition is very important for us. In 2023, Kaspersky products participated in 100 independent tests and reviews. Our products were awarded 93 firsts and received 94 top-three finishes.

* 100 independent tests and reviews were completed by Kaspersky products in 2023 along other participating vendor products. More than 90 vendors took part in the test in 2023, but only 10 participated in 35% or more of the tests, and were represented in the chart. Additionally, we considered valuable to have another 5 vendors' results represented in the chart.

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | Education | Sponsorships & Partnerships

40

Recognitions

One of the five biggest endpoint security vendors.* **

Kaspersky products are regularly assessed by global research firms, and our cyber protection expertise is proven by the number of recognitions by key industrial analysts and peer review companies.

Among those are IDC, Canalys, ISG, Quadrant Knowledge Solutions, Info-Tech, and many others.

In 2023, Kaspersky was noted as the vendor "who shaped the year" in IDC's Worldwide Modern Endpoint Security Market Shares report.***

Kaspersky was named a Major Player in the 2024 IDC MarketScape: Modern Endpoint Security vendor assessments for Enterprises, Midsize Businesses, and Small Businesses.

*IDC Worldwide Modern Endpoint Security Market Shares 2023 (January 2024)
** IDC Worldwide Consumer Digital Life Protection Market Shares 2023 (June 2024)
***IDC's Worldwide Modern Endpoint Security Market Shares, July 2021–June 2022: Currency Exchange Rates Slightly Trimmed Accelerating Growth (Jan 18, 2023)

ESG

Our company's mission is to build a safe and sustainable digital world so that people can use technological solutions to improve not only their daily lives but also life on the planet as a whole.

We fulfill this mission by increasing the resilience of the digital space against threats through the creation of Cyber Immunity while paying special attention to social projects and environmental awareness.

Read our latest Sustainability (ESG) report covering results for the second half of 2022 and 2023 as well as key objectives for 2024 here.

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | Education | Sponsorships & Partnerships

42

ESG strategic development

Kaspersky's sustainable development is grounded in five key areas

1

Ethics and transparency

- Source code and process transparency
- Data protection and the right to privacy
- Management transparency and business resilience

2

Safer cyberworld

- Critical infrastructure protection
- Assistance in the investigation of cybercrimes on a global level
- Protection of users against cyberthreats

3

Safer planet

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

4

People empowerment

- Employee care
- Women in STEM
- Inclusivity and availability of technologies
- Talent development in IT

5

Future tech

- Cyber Immunity for new technologies

Learn more about our main accomplishments here.

Education

Despite the rapid development of technology, the human factor still plays a significant role in building a safer digital world. This is why Kaspersky aims to educate people of all ages and professions all around the world about cybersecurity, and create a life-long learning journey for passionate cybersecurity experts.

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | **Education** | Sponsorships & Partnerships

44

Education: Cybersecurity is for life-long learning

School: Primary

Kaspersky intends to educate young Internet users about being safe online by creating projects such as children's books on cybersecurity and partnering with schools.

- Kids Cyber Resilience
- Kids book
- Cybersecurity Alphabet

School: Secondary

Kaspersky is keen to help young talents to explore the field of cybersecurity and make their future professional journey to IT more vivid.

- Tech Valley

University

As part of our international educational project **Kaspersky Academy**, we promote knowledge of cybersecurity among students and professors worldwide.

- Kaspersky Academy Alliance
- SafeBoard

Professional

Kaspersky provides a wide range of knowledge on information security for IT professionals, business leaders, top managers and senior executives.

- xTraining
- Cybersecurity for Executives Online

Sponsorships
& Partnerships

As an innovative global company, Kaspersky cares about future by providing cybersecurity to different industries and by supporting promising talent in various countries.

We contribute to the development of science and contemporary art, help to preserve the world, and provide athletes with the opportunity to reach their full potential.

Kaspersky at a glance | Global Transparency Initiative | Threat Intelligence and research | Cybersecurity Portfolio | Awards | ESG | Education | **Sponsorships & Partnerships**

46

Sponsorships & Partnerships

Sport

As fans of team sports, we're proud to be the Official Cybersecurity Partner of the Mumbai Indians, a five-time champion of India's cricket league and one of the most successful and valuable cricket teams.

Learn more

Art

Kaspersky has partnered with the Moniker International Art Fair in London, supporting artists like Ben Eine, Shok-1, D*Face, Felipe Pantone, exploring with them new ways to explain innovative ideas through artistic expression.

Learn more

Gaming

Kaspersky partners with multiple eSports teams worldwide, including Nasr (UAE), Reckoning (India), and Red Canids (Brazil), to enhance the gaming experience of eSports enthusiasts by providing advanced cybersecurity measures.

Learn more

Bring on the future