

Kaspersky Corporate Kit

kaspersky

Updated: December 2025



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 nearly 30-year history.

Kaspersky at a glance

Essentials

Customers

Geography

Role in the global IT security community

01



Facts about us

Essentials

k

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

> 9 million

consumer product activations per year

> 5,500

highly qualified specialists

US \$822 million

global non-audited combined revenue in 2024

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.

1,000,000,000

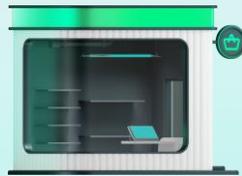
Devices protected by Kaspersky to date*

~200,000

Corporate clients worldwide choose our protection



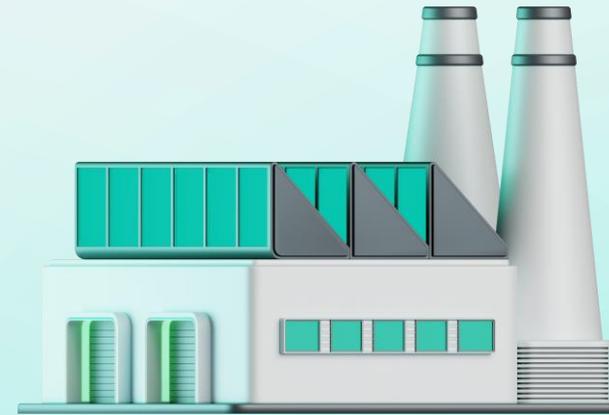
Consumers



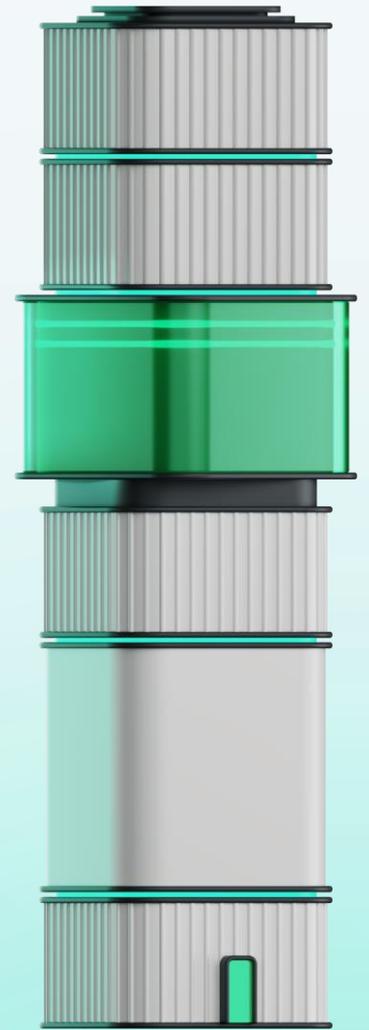
Very small businesses



Small and medium businesses



Industrial facilities



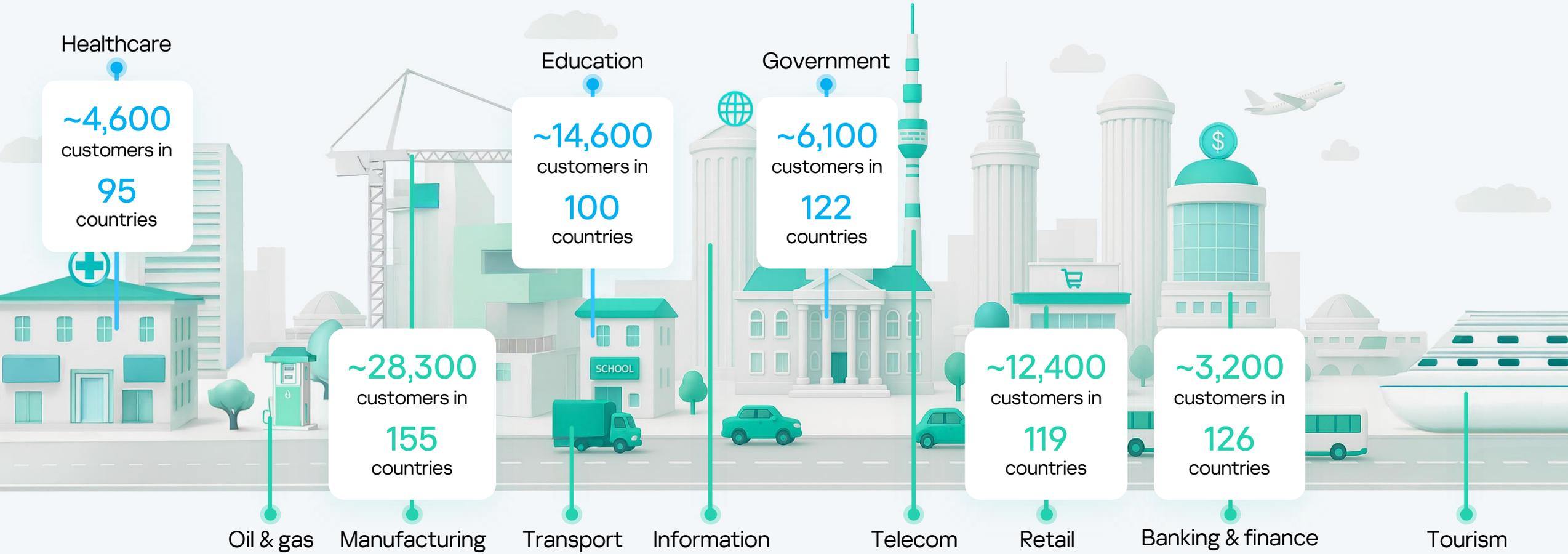
Enterprises

*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 nearly 200,000 clients around the world, regardless of size or complexity.

- Public organizations
- Private companies



We are an international cybersecurity company

200 countries and territories where we operate

30+ representative regional offices



Africa

South Africa
Kenya
Rwanda

Europe

Belarus
Czech Republic
France
Germany
Israel
Italy
Netherlands
Russia
Spain
Switzerland

Middle East

Saudi Arabia
Turkey
UAE

Asia

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

Latin America

Brazil
Mexico
Colombia

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](#)



[Learn more](#)



[Learn more](#)



[Learn more](#)



[Learn more](#)

Kaspersky and AI regulation

Kaspersky actively contributes to shaping global AI governance by joining key international alliances, promoting ethical standards, and providing expert input into regulatory discussions.

Strategic Alliances & Commitments

EU AI Pact (2024)

Kaspersky's pledge was accepted by the European Commission as part of the AI Pact, a preparatory step toward the AI Act – the world's first comprehensive legal framework for AI regulation.

UNIDO AIM Global Alliance

Kaspersky is a member of the Global Alliance on Artificial Intelligence for Industry and Manufacturing, launched by UNIDO, promoting responsible and inclusive AI in industrial contexts.

Standards & Guidelines

Ethical Principles for AI in Cybersecurity

Developed by Kaspersky and presented at UN IGF 2023, these principles called on the cybersecurity industry to adopt shared ethical standards for AI use.

Guidelines for Secure AI Development & Deployment

During IGF 2024, Kaspersky presented practical recommendations to help developers and security teams build AI systems responsibly.

Global Transparency Initiative

02



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



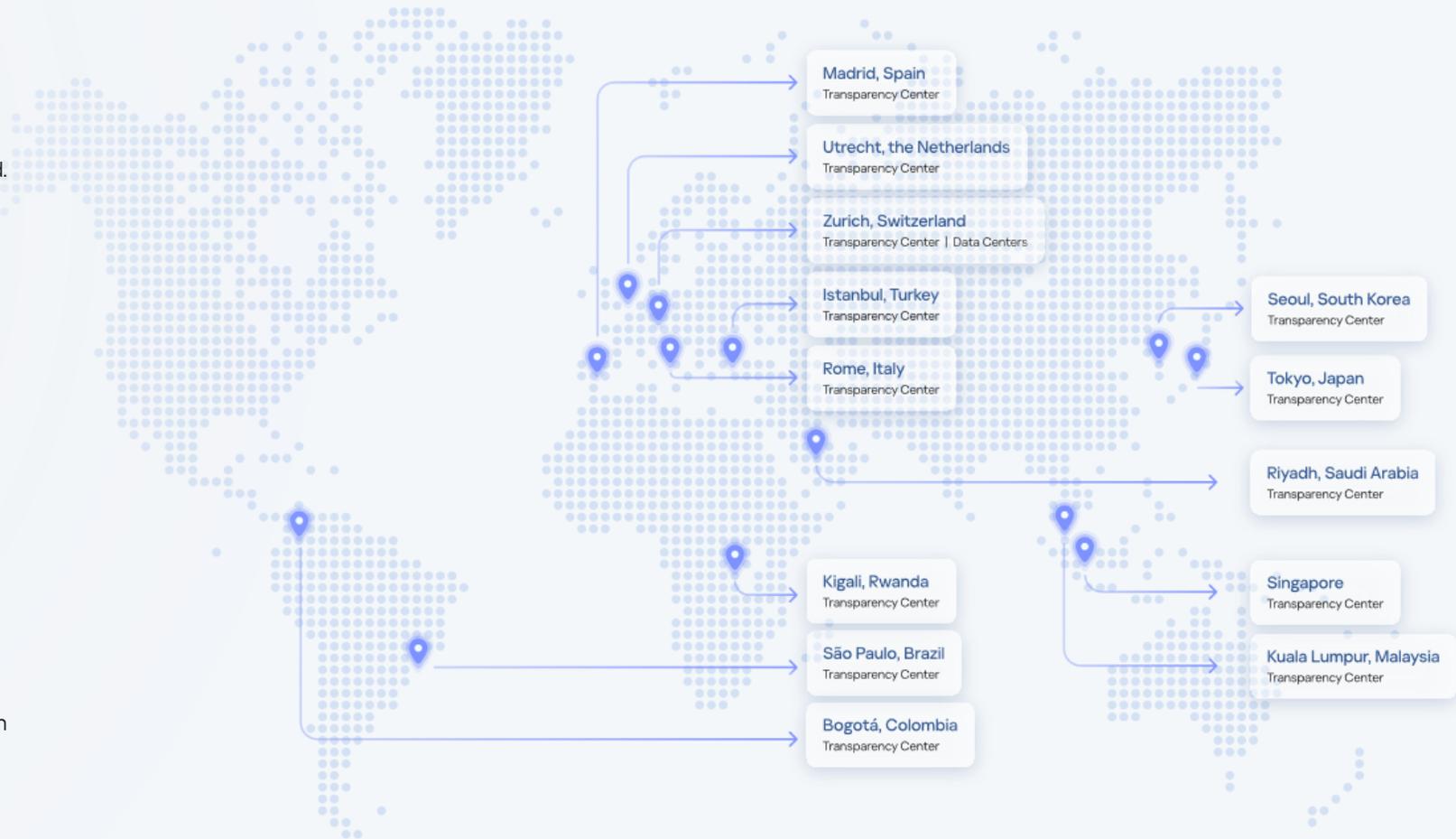
Bug bounty program

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.



Kaspersky Transparency Centers

Immerse yourself in the history of [Global Transparency Initiative](#)

Blue Piste (both remote & physical)

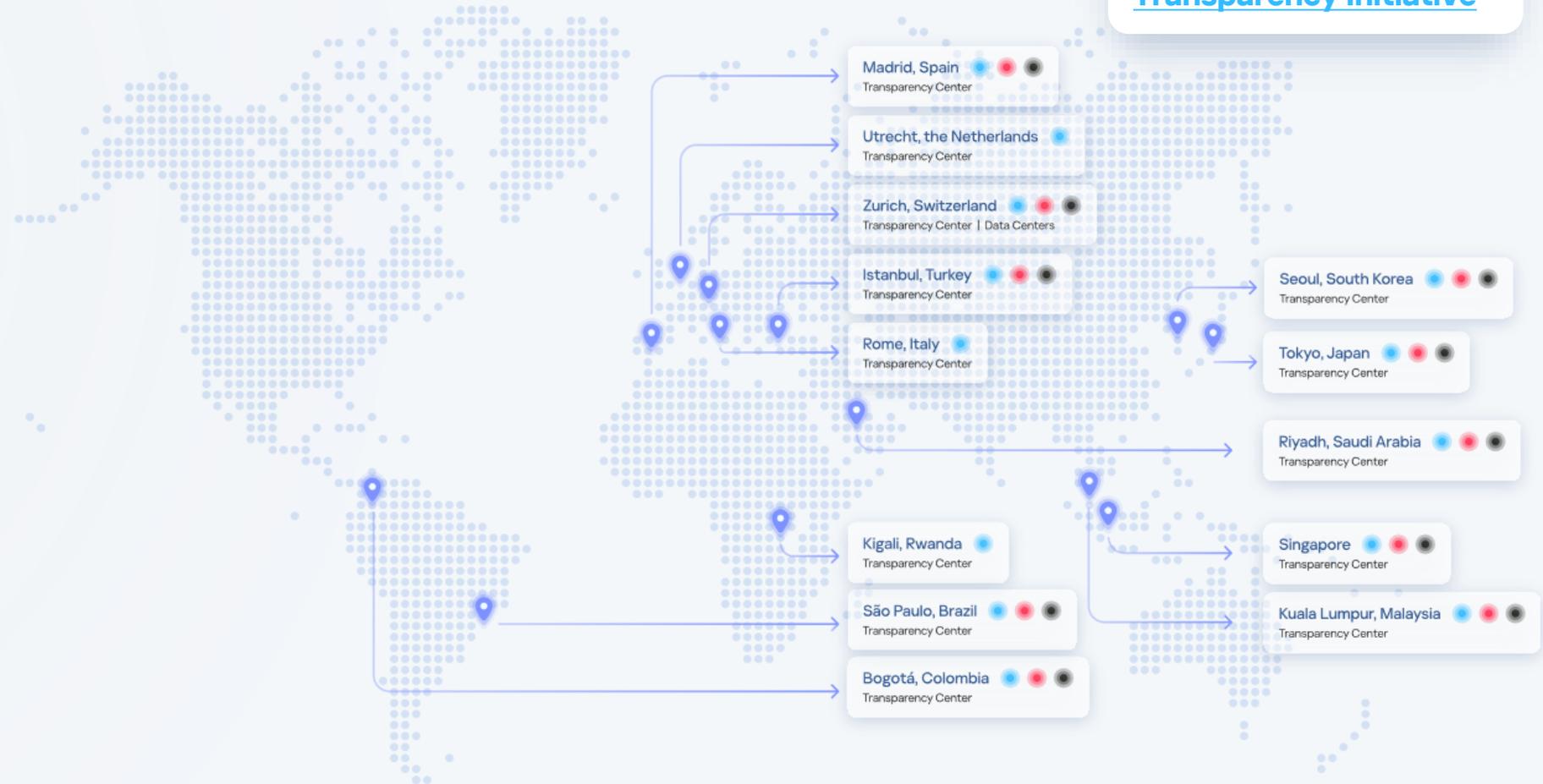
An overview of Kaspersky's transparency practices, products and services, as well as data management practices.

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.



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.



66 Transparency Center reviews

by public and private stakeholders



74 Bug Bounty report awarded

with total payments equal to \$93,510

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 2025.



[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 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

03

Expertise

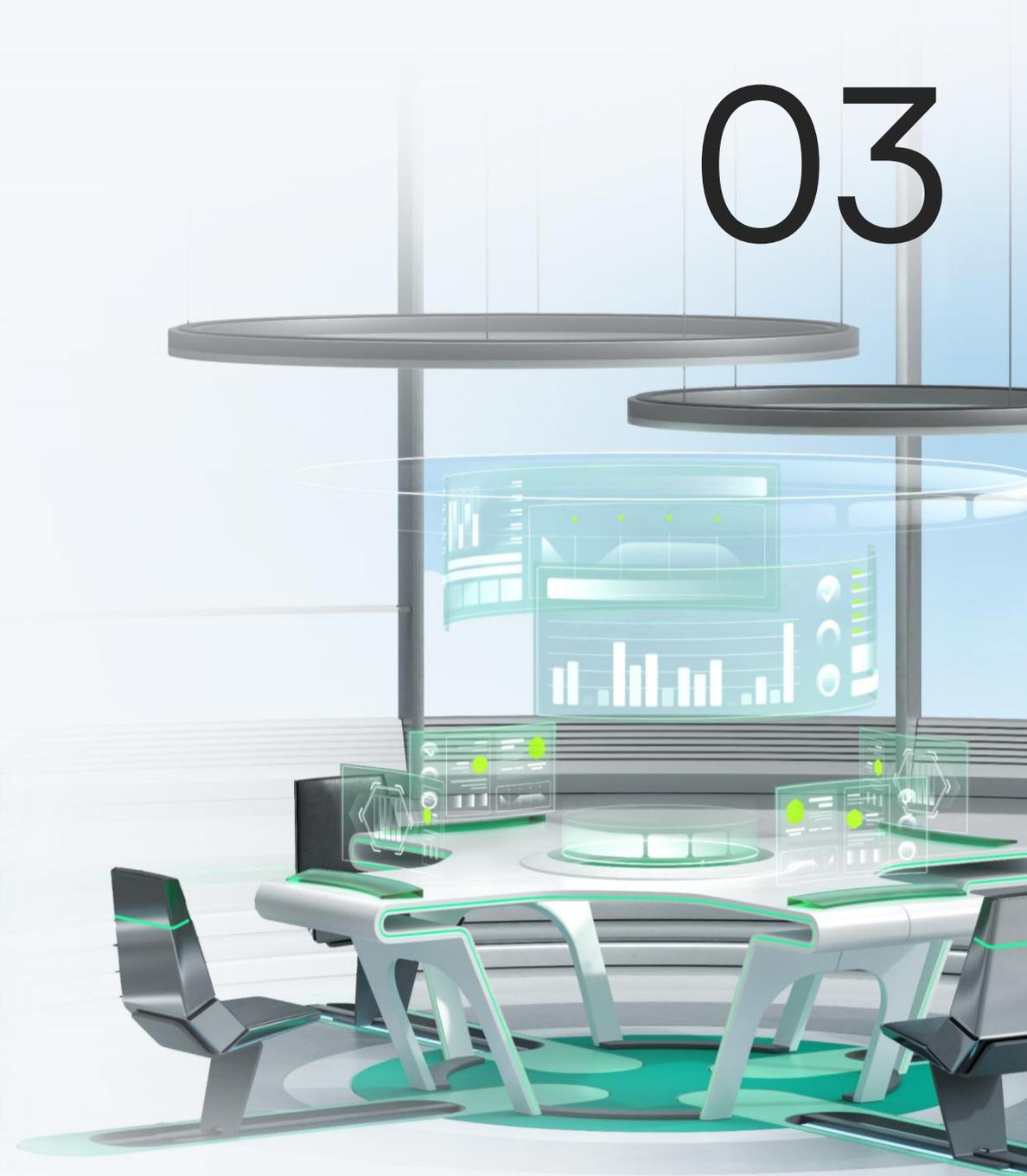
Threat research

Current advanced persistent threat landscape

Major discoveries and research

Targeted attack research

Enabling a privacy-minded world



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.

>5,500

Highly-qualified specialists

>50%

of our employees are R&D specialists

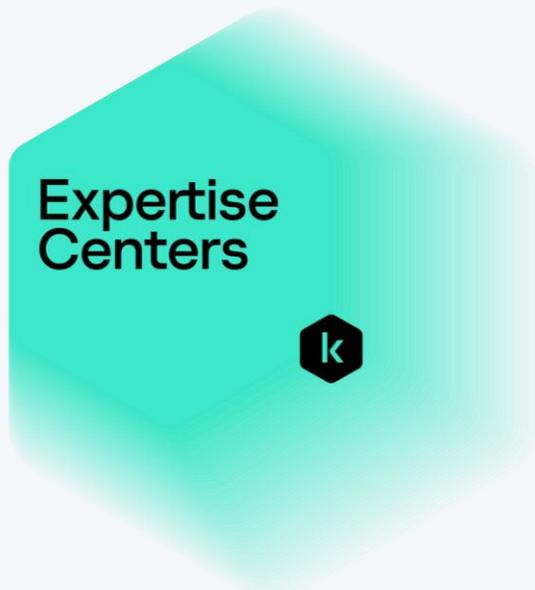
40+

Members in our group of elite world-leading security experts – GREAT



Technology leadership enriched with global expertise

● Threat Research ● Incident Investigation



The unmatched power of expertise: The core of our cybersecurity portfolio

[Learn more](#)

● ●

Kaspersky Global Research and Analysis Team

GREAT

- Research of the most complex threats; APTs, cyber espionage campaigns, global cyber epidemics, etc.
- Investigation of sophisticated financial cybercrime
- Security of future-focused technologies

●

Kaspersky Threat Research

Threat Research

- SSDLC & Secure-by-Design methodologies
- Content filtering research
- Threat research from malware to APTs and detection logic development

●

Kaspersky AI Technology Research

AI Technology Research

- AI-powered threat detection / solutions
- AI cybersecurity
- GenAI Research

● ●

Kaspersky Security Services

Security Services

- MDR
- Incident Response
- Security Assessment
- SOC Consulting
- Compromise assessment
- Digital Footprint Intelligence

● ●

Kaspersky ICS CERT

ICS CERT

- Threat analysis in industrial infrastructure
- ICS vulnerability research and assessment
- Technology associations, analytics and standards

Threat research

>2,100,000,000 cyberthreats

detected by Kaspersky since the company's inception

4,900,000,000
cyberattacks

detected by Kaspersky in 2024

500,000
new malicious files

detected by Kaspersky every day

Advanced persistent threat landscape in 2024

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 2024 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targeted industries

- | | |
|--|---|
|  Government |  Manufacturing |
|  Telecommunications |  Defense |
|  Financial Institutions |  IT companies |
|  Education |  Construction |
|  Energy |  Commercial |

Top 10 significant actors

- | | |
|----------------|---------------------|
| • Lazarus | • Charming Kitten |
| • HoneyMyte | • Gamaredon |
| • Kimsuky | • SideWinder |
| • DeathStalker | • Awaken Likho |
| • BlindEagle | • Transparent Tribe |

Top 12 targeted countries and territories



Our major discoveries and research

	 Expetr/ Notpetya	 Olympic destroyer	 Shadow hammer	 Tajmahal	 Mosaicregressor	 Ghostemperor	 Moonbounce	 Operation Triangulation	 Grandoreiro
Detection	2017	2018	2018	2019	2020	2021	2022	2023	2024
Active since	2017	2017	2018	2013	2017	2020	2021	2019	2016
Classification	Data wiping campaign	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	APT campaign	Financial cybercrime
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 legitimate certificate	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	A sophisticated Brazilian banking trojan under the Tetrade malware family, enabling attackers to bypass banking security and commit fraud. Despite arrests in 2021 and 2024, it remains active, with recent lighter versions targeting 30 banks in Mexico. Responsible for 5% of global banking trojan attacks this year, Grandoreiro has targeted users of over 1,700 banks, making it one of the most persistent threats worldwide
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 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	Financial institutions in more than 40 countries in North and Latin America, and Europe

Targeted attack research

2017



WannaCry



Shamoon 2.0



StoneDrill



BlueNoroff

ExPetr/
NotPetyaMoonlight
Maze

ShadowPad



BlackOasis



Silence



WhiteBear

2018



Zebrocy



DarkTequila



MuddyWater



Skygofree

Olympic
Destroyer

ZooPark



Hades



Octopus



AppleJeus

2019



Topinambour



ShadowHammer



SneakyPastes



FinSpy



DarkUniverse



COMpfun



Titanium

2020



Cycldek

SixLittleMonkeys
(aka Microcin)

CactusPete



DeathStalker



MATA



TransparentTribe



WellMess



TwoSail Junk



MontysThree



MosaicRegressor



VHD Ransomware



WildPressure



PhantomLance

2021



GhostEmperor



ExCone



BlackShadow



BountyGlad



EdwardsPheasant



HotCousin



GoldenJackal



FerociousKitten



ReconHellcat



CoughingDown



MysterySnail



CraneLand

2022



Tomiris



ZexCone



SilentMarten



MoonBounce



ToddyCat



MagicKarakurt



CosmicStrand



SBZ



StripedFly



DiceyF



MurenShark

2023



PowerMagic



CommonMagic



Trila



LoneZerda



CloudWizard

Operation
Triangulation

BlindEagle

Mysterious
Elephant

BadRory



Dark Caracal



HrServ

2024



CloudSourcerer



PipeMagic



Zanubis



SambaSpy



SideWinder



BellaCPP



EastWind



PassiveNeuron



Awaken Likho

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.



Course on cyberhygiene

In the course, Kaspersky experts explain, in simple and clear language, how to safely live your online life and protect yourself and your loved ones from cyberthreats.

[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

04

Corporate Cybersecurity

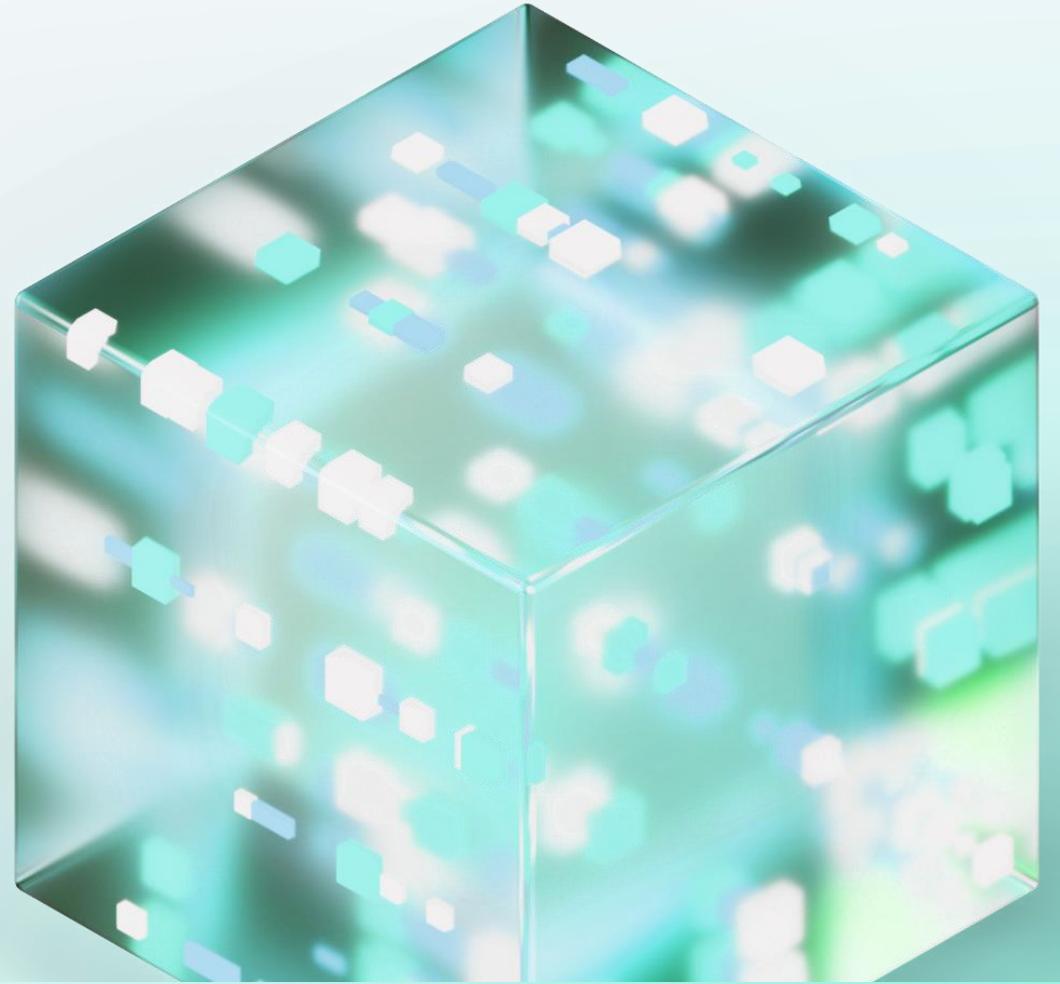
Industrial Cybersecurity

Threat Intelligence

MSSP / MSP Offering

Cyber Immunity approach

Consumer Cybersecurity



Kaspersky proposal for IT environment



Corporate cybersecurity

- 1 Solutions
- 2 Threat Intelligence & Training
- 3 Expert Services



Kaspersky Expert Security

Expert approach to protecting the corporate business segment

1

XDR Corporate



Kaspersky Next XDR Expert

Highest tier expert solutions



Kaspersky Anti Targeted Attack



Kaspersky Next EDR Expert



Kaspersky SIEM



Kaspersky Container Security



Kaspersky SD-WAN



Kaspersky Fraud Prevention



Kaspersky Scan Engine

Targeted solutions

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



Open Single Management Platform



Industrial cybersecurity

XDR Industrial



Kaspersky Industrial Cybersecurity

for Nodes

for Networks

Kaspersky proposal for OT environment



Corporate cybersecurity

XDR Corporate



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

XDR Industrial



Kaspersky Industrial Cybersecurity

for Nodes

for Networks

Specialized solutions



Kaspersky Antidrone



Kaspersky Machine Learning for Anomaly Detection



Kaspersky SD-WAN



Kaspersky Thin Client



Kaspersky Automotive Secure Gateway

Cyber Immune solutions

1

Awareness



Kaspersky Security Awareness

Threat Intelligence



Kaspersky ICS Threat Intelligence

Trainings



Kaspersky ICS CERT Training

3

Assessment



Kaspersky ICS Security Assessment

Managed security



Kaspersky Managed Detection and Response

Response



Kaspersky Incident Response

- 1 Solutions
- 2 Threat Intelligence & Training
- 3 Expert Services

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

Kaspersky Intelligence Reporting

Kaspersky Digital Footprint Intelligence

Kaspersky Next: B2B flagship product line



SMB



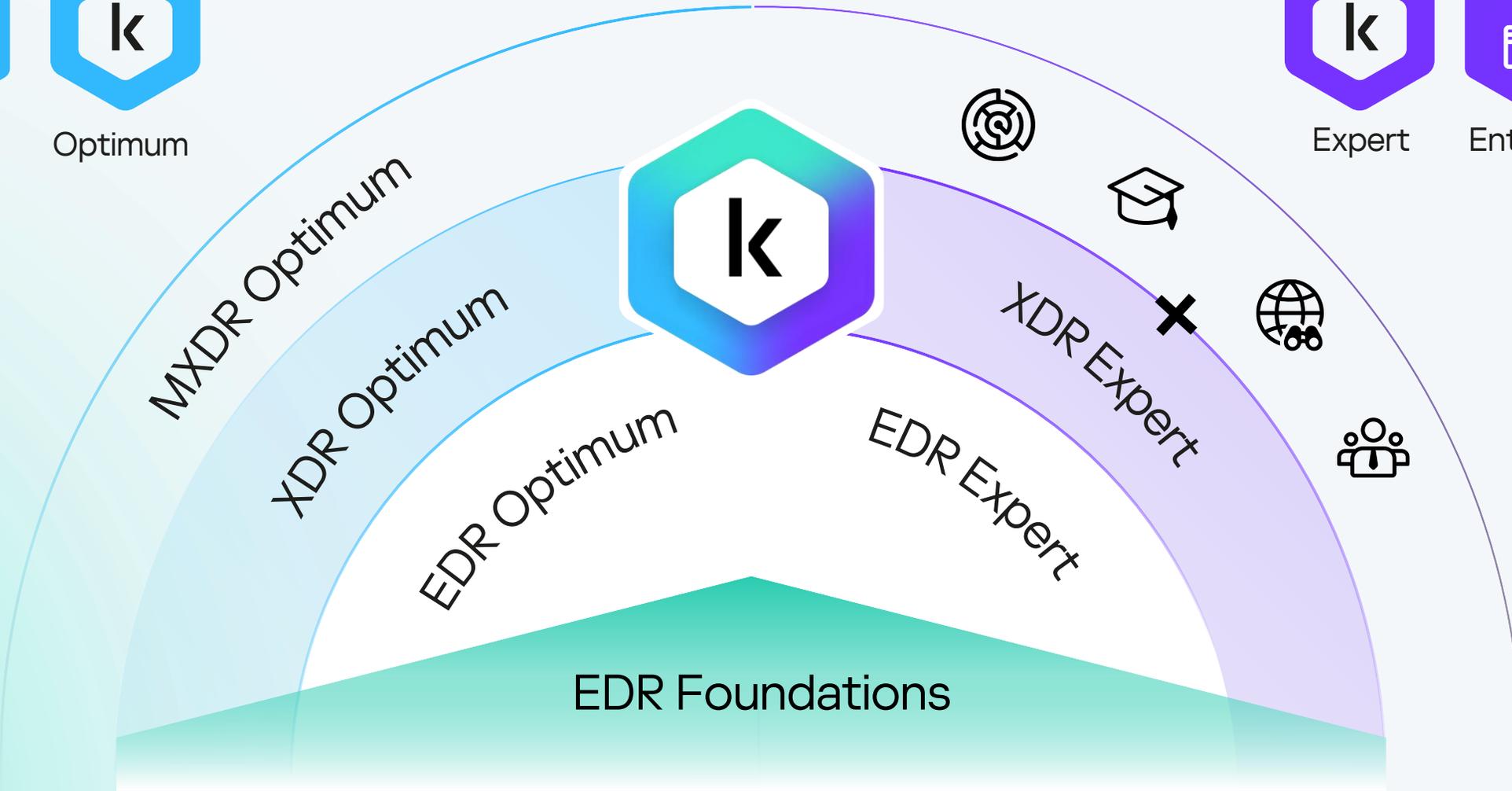
Optimum



Expert



Enterprise



Comprehensive MSP and MSSP offering to build security services

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

Build services:

MSP

1 Managed Protection Services

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

Base your services on:

Knowledge and Support

- Kaspersky Cybersecurity Training
- Kaspersky Premium Support
- Kaspersky Professional Services
- Kaspersky SOC Consulting
- Kaspersky Incident Response

- 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

Managed Detection & Response Service

- Essential MDR
- Kaspersky Managed Detection and Response

MSSP

2 Managed Detection & Response Services

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

- Kaspersky Anti Targeted Attack
- Kaspersky Next EDR Expert

3 Managed Threat Intelligence Services

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

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

4 SOC as a Services

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

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

AI in Kaspersky: A long and exciting journey

2008

In-lab Auto-Analyst that compares incoming files based on static characteristics with already known malware

2010

In-Lab Auto-Analyst module that uses emulation logs as an additional criterion for clustering of executable files

2011

Pattern-Based Similarity System, with Emulator logs processed on the user's side, with newly found patterns sent to Kaspersky's cloud services and analyzed using ML

2013

TrueForest: in-lab ML-powered creation of Smart Records using Decision Tree algorithmics and their application in Kaspersky frameworks

2014

SmartHash: in-Lab ML-powered creation of Smart Records using Locality-Sensitive Hashes to detect malware families

2015

A module for in-lab Auto-Analyst using System Watcher behavior logs from Sandbox for sample clusterization

2016–2017

Decision trees - based detection models delivered and applied on the user's device

2018

- AI Analyst for Kaspersky MDR
- The application of ML learning algorithms is becoming more prevalent in user-facing products, with a focus on analyzing the behavior of executable files
- Adaptive Anomaly Control: uses normal system behavior baseline to detect anomalies
- MLAD. Predictive analytics system for detection of anomalies in industrial data

2020

- Spam quarantine system based on deep neural networks
- 1st Russian neuromorphic processor for peripheral AI - AltAI

2022

- New AI-based phishing detection system

2023

- Web page graph analysis system for detection of malicious activities
- Custom ML models in MLAD

2024

- Open source release of Kaspersky Neuromorphic Platform with AltAI backend
- AI security service – AI-cert.kaspersky.com
- AI for KUMA/XDR (risk score calculation for hosts)
- GenAI-based TI summaries
- KIRA - Kaspersky Investigation and Response Assistant

2025

- Detection of DLL Hijacking in KUMA
- Detection of stolen accounts in MDR and KUMA/XDR
- Development of KIRA across KUMA, XDR, EDR, and KCS
- Integration of AI agents with VM



kasperskyOS

Secure, flexible and scalable operating system to build a reliable foundation for your IT environment

Microkernel Architecture

Ensures transparency and strict code quality control, fault tolerance, and OS scalability.

Component Isolation

All components are fully isolated from each other and from the external environment, eliminating uncontrolled interaction.

Proprietary Microkernel

Inter-process Communication Control

Any interaction between components that is not explicitly allowed by the security policy is automatically denied.

Cyber Immunity

According to definite methodology and processes, products and solutions built on KasperskyOS have innate resilience to even unknown threats.

Solution areas



Thin client infrastructure

Operating system for thin clients based on the KasperskyOS microkernel.



Kaspersky Thin Client



Transportation

Software for high-performance controllers of vehicles that combines the functions of a telematic control unit and a secure gateway.



Kaspersky Automotive Secure Gateway



Corporate mobile devices

Operating system for corporate-owned mobile devices based on the KasperskyOS microkernel.

* Available only through Early Access Program for our customers and partners.



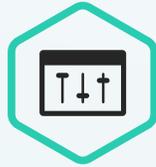
KasperskyOS Mobile

KasperskyOS-based product portfolio



Kaspersky Thin Client

Cyber Immune and feature-rich Thin Client infrastructure



Kaspersky Security Center



Kaspersky Security Management Suite



Kaspersky USB Redirector



Kaspersky Appcenter

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



Kaspersky Automotive Secure Gateway

Building reliable IT systems for connected vehicles



Kaspersky Automotive Adaptive Platform



Kaspersky Automotive Secure Broker Framework



Kaspersky OTA Agent



Kaspersky Vehicle SOC Agent



Kaspersky Remote Diagnostic Agent



KasperskyOS Mobile

Secure operating system for corporate mobile devices



Kaspersky Security Center



KasperskyOS Mobile Device Management



B2C Solutions: Core product portfolio

Our comprehensive plans cover the full range of customer needs

Complete protection for your digital life



Premium services



Privacy



Identity



Performance



Smart Home



Security



Kaspersky
Standard



Kaspersky
Plus



Kaspersky
Premium

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 VPN Secure Connection

Win | Android | Mac | iOS



Kaspersky Who Calls*

Android | iOS

Only available in Russia, Kazakhstan, Indonesia, and Latin America



Kaspersky Plus

Win | Android | Mac | iOS



Kaspersky Safe Kids

Win | Android | Mac | iOS



Kaspersky eSIM Store

Android | iOS | Web



Kaspersky Premium

Win | Android | Mac | iOS



Kaspersky Password Manager

Win | Android | Mac | iOS

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.

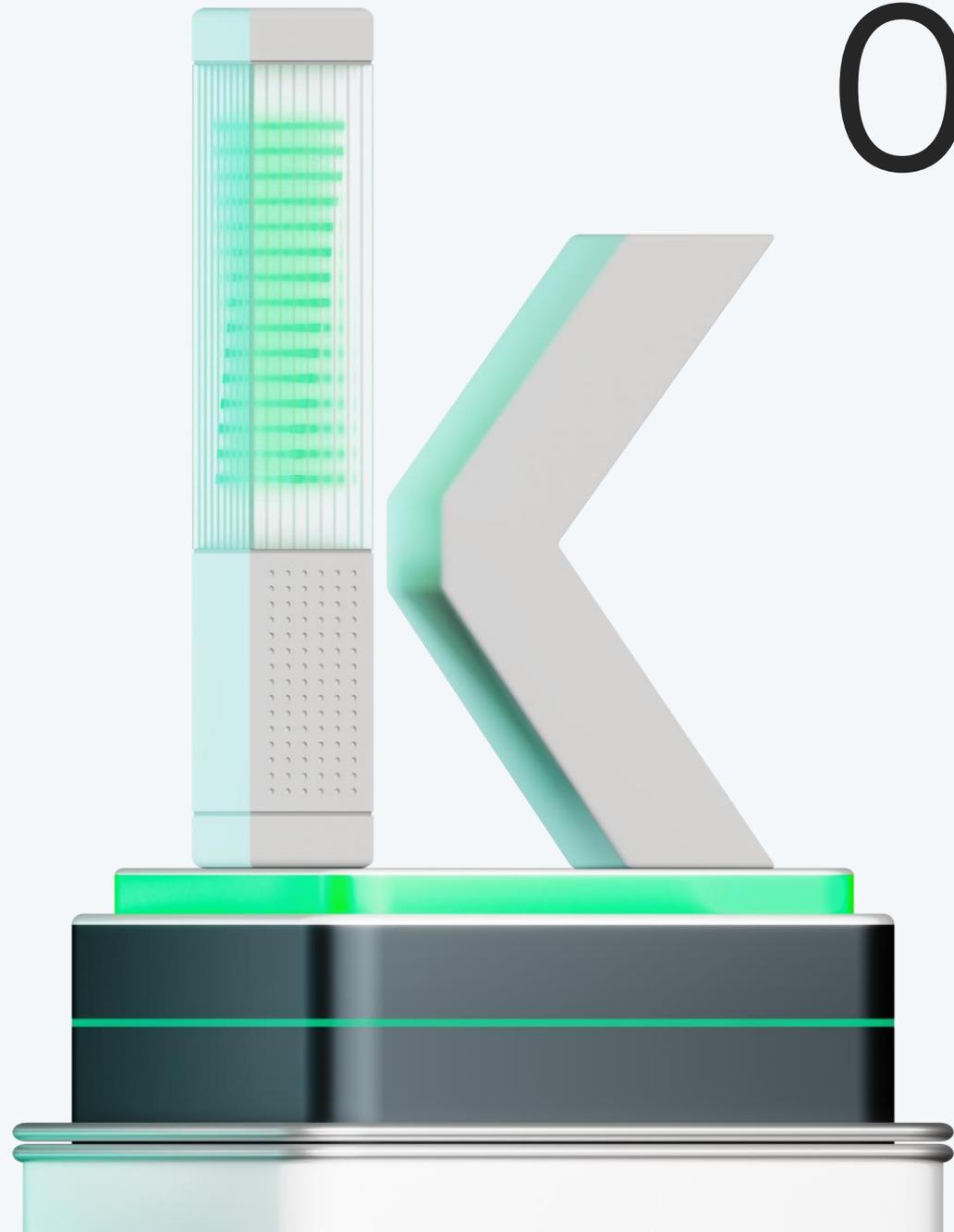
Kaspersky awards

05

Overview

Top 3 metrics

Recognitions



More than 800 awards*

Kaspersky Standard was honored with the **Product of the Year 2023 and Top Rated 2024 annual awards** by independent test lab AV-Comparatives**.

Kaspersky EDR Expert continually delivers top results:

- 100% protection from targeted attacks, **Strategic Leader** status in 2022, 2023, 2024, and Certified in 2025 from AV-Comparatives***;
- AAA recognition and Total Accuracy Rating of 100% in Advanced Security EDR tests by SE Labs****;
- regular rating “Approved” by AV-Test*****.

According to AV-Comparatives Security Survey 2025, Kaspersky was named the most popular desktop security solution in Europe, Asia, South and Central Americas*****.

[Learn more](#)

* The number includes independent test results of corporate and consumer products during 2013-2024. Check [TOP3](#) and the [awards](#) pages.

** 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. The product was awarded [Top Rated Product 2024](#) based on test results of the year 2024.

*** Endpoint Detection and Response tests of [2022](#), [2023](#), [2024](#) and [2025](#) by AV-Comparatives.

**** Enterprise Advanced Security EDR test of [2022](#) and [2023](#) by SE Labs.

***** Advanced EDR Tests of [2023](#) and [2024](#) by AV-TEST.

***** [AV-Comparatives Security Survey 2025](#).



Most Tested Most Awarded* Kaspersky Protection

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 2024, Kaspersky products participated in 95 independent tests and reviews. Our products were awarded 91 firsts and received 92 top-three finishes.

[Learn more](#)

* 95 independent tests and reviews were completed by Kaspersky products in 2024 along other participating vendor products. More than 95 vendors took part in the tests in 2024, but only 8 participated in 35% or more of the tests, and were represented in the chart. Additionally, we considered valuable to have another 6 vendors' results represented in the chart.



95

Tests / Reviews

91

First Places

97%

Top 3

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, Frost & Sullivan, Canalis, ISG, QKS Group, and others.

In 2025, Kaspersky was noted as the vendor “who shaped the year” in IDC's Worldwide Consumer Digital Life Protection 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.

Kaspersky has been [named](#) a Leader in the 2024 Frost Radar™ for Cyber Threat Intelligence (CTI) recognized for innovation in the CTI market.



* IDC Worldwide Modern Endpoint Security Market Shares 2024 (May 2025)

** IDC Worldwide Consumer Digital Life Protection Market Shares 2024 (June 2025)

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.

Find out more about the company's ESG strategy in our Sustainability report.

[Learn more](#)



ESG strategic development

Our main accomplishments:

[Learn more](#)

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

Education

07

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.



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.

Online course on career orientation

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.

Expert Trainings

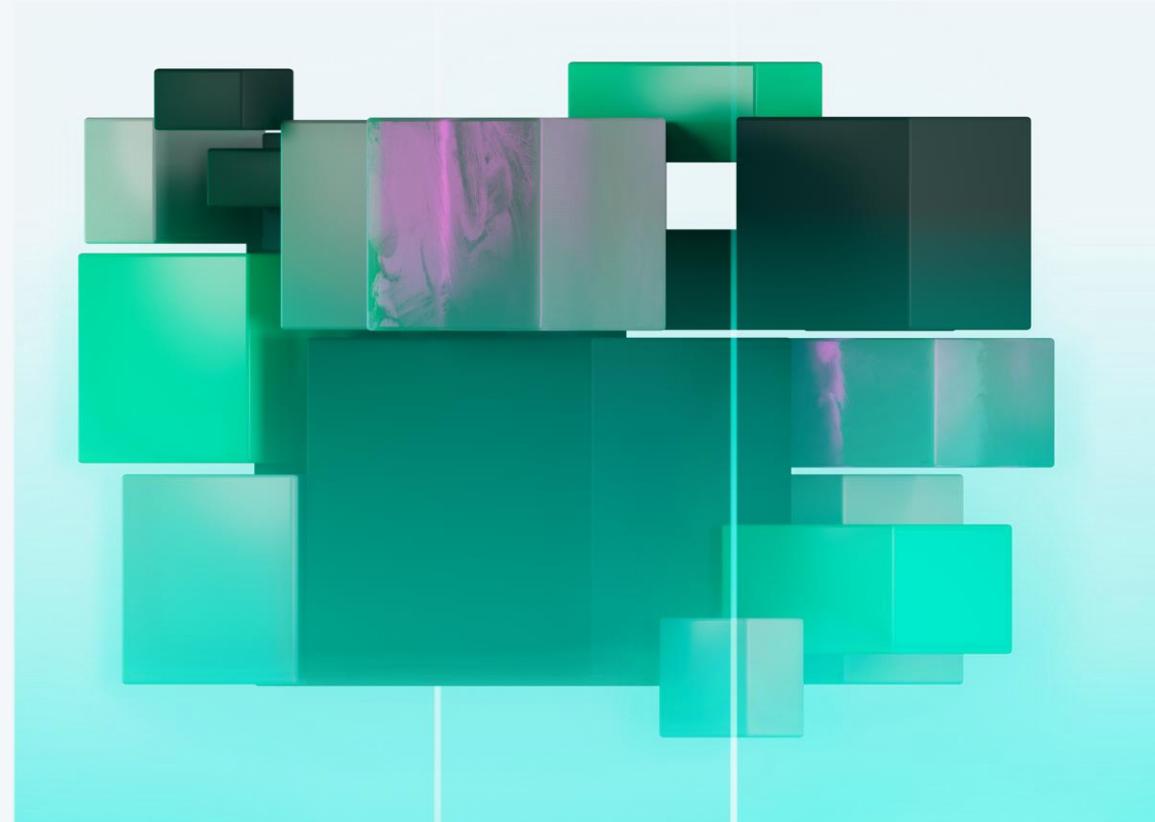
Cybersecurity for Executives Online

Sponsorships & Partnerships

08

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.



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 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



kaspersky