kaspersky

Kaspersky Overview: Our values, business, solutions and services

Updated: April 2025

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 of Kaspersky

For over 25 years committed to building a safer world

Kaspersky is a global cybersecurity and digital privacy company building a safer digital world for over 25 years. In this time, we have evolved from offering endpoint security to complete business and consumer protection. With a team of more than 5,000 professionals, we continue to build our cybersecurity ecosystem, aiming to meet the entire range of security needs for organizations and users to ensure a Cyber Immune future.

Innovating the IT industry with a Cyber Immunity approach

Technological breakthroughs have always been driven by the desire to innovate. However, with innovation comes the risk that technologies might be exploited beyond their intended use. Leveraging its long-standing and successful experience in tackling sophisticated cybercrime, Kaspersky has pioneered security for the IT industry with its Cyber Immunity approach, aiming to create cyber-physical systems that are inherently safe and secure, a concept close to the heart of KasperskyOS.

A billion devices have been protected by Kaspersky to date[1]

Kaspersky's solutions protect businesses, critical infrastructure, governments and consumers around the globe from sophisticated and evolving digital threats. This includes protection from the most notorious Advanced Persistent Threat (APT) groups and ransomware, among many others. The company's unique product portfolio includes innovative security solutions ranging from leading endpoint protection to specialized security solutions and services.

A comprehensive ecosystem

We don't just sell solutions – we provide an ecosystem of strategic solutions that protect customers now and in the future, as their business develops. And we're not just a vendor - we're a partner, analyzing customers' cybersecurity resources and requirements to ensure they get exactly what they need. Our products and services are built on extensive, relentless and ongoing threat research and development – over half of our 5,000-strong staff are R&D specialists. Our innovation speaks for itself – with more than 1,500 patents granted worldwide, we continue to shape the future of cybersecurity and the proof of this unique make-up is in the fact that we are the most tested, most awarded cybersecurity vendor on the planet.

Our portfolio is designed to support businesses of every size, from small local companies to global powerhouses. We know that as organizations change and grow, adopt new technologies, face more serious security challenges and have access to more resources, their cybersecurity needs change and grow too, and requires additional options. Our stage-by-stage approach is in sync with this natural development.

[1] 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.

kaspersky

Threat intelligence with a truly global reach

Operating in more than 200 countries and territories, Kaspersky gathers real-time intelligence from all over the globe, helping to protect users from threats that other companies might overlook. We are the first to know about new threats, and our global coverage helps us to swiftly prevent them from spreading.

A unique team of security experts at the forefront of your protection

Our vastly experienced teams of experts across five Expertise Centers work around-the-clock to combat mass attacks, malware, targeted and APT attacks, industry- and infrastructure-specific threats to keep our customers safe.

- The **Kaspersky Global Research and Analysis Team (GReAT)** researches and discovers the most sophisticated threats (from the infamous Duqu, Equation or Carbanak to the latest Operation Triangulation)
- The **Kaspersky Threat Research** group conducts anti-malware and content filtering research, develops key threat-fighting technologies and contributes to our unique SSDLC[2] and Secure by Design methodologies.
- The **Kaspersky AI Technology Research** center handles general AI research and AI-powered threat detection and solutions.
- **Kaspersky Security Services** include MDR, Incident Response, Security Assessments, SOC Consulting, and Digital Footprint Intelligence.
- **Kaspersky ICS CERT** excels in the area of industrial infrastructures specifics, carrying out OT threat analysis, vulnerability research and assessment, and working with technology associations and product vendors to establish high security standards for the next-generation technologies.

Work done in Kaspersky's Expertise Centers all feed into our solutions and services to keep our customers safe and ahead of even the most sophisticated threats.

Combining security expertise with the power of Artificial Intelligence

From smart home devices to robotic manufacturing and business, artificial intelligence (AI) continues to gain momentum, revolutionizing many industries. Kaspersky has extensive experience with AI and has been using it to solve specific problems for almost 20 years.

AI technologies are an integral part of our solutions and products, finding their place in Kaspersky's own infrastructure as well as client-side solutions. To mention just a few, Kaspersky Security Network (KSN) is a cloud data-processing powerhouse that accumulates global threat-related data, detects new malware and helps build new on-premise detection models for subsequent deployment, integrated into multiple Kaspersky products. Kaspersky Industrial CyberSecurity (KICS) and Machine Learning for Anomaly Detection (MLAD) use AI algorithmics to discern indirect attack indicators and subtle activity anomalies in highly specific industrial environments. The Managed Detection and Response (MDR) platform employs the help of AI-based Autoanalyst which leans on SOC team alert processing to later process them automatically, relieving SOC analysts from significant amount of manual work.

[2] Secure Software Development Life Cycle

kaspersky

At the current point in the development of AI, we believe that the most effective solutions are created when humans and machines work together, maximizing their combined strengths. Our team at the Kaspersky AI Technology Research Center has been working with AI in cybersecurity and Ethical AI for almost two decades to help discover and counter the broadest range of threats. Their work is proof that blending AI capabilities with human expertise and comprehensive threat intelligence from big data creates the most effective, most reliable security.

Top quality confirmed by multiple tests and awards

Our products regularly undergo independent external reviews and tests, and receive the highest marks and award recognitions. According to AV-Comparatives Security Survey 2025, Kaspersky was named the most popular desktop security solution in Europe, Asia, Central and South Americas. With over 600[3] industry awards received for its security solutions, Kaspersky remains one of the most endorsed security vendors on the market. Our technologies and processes are comprehensively audited and certified in accordance with the world's most respected standards to ensure the most robust security for our customers.

Read more about independent assessments and certifications

Kaspersky is working on reviewing its internal processes with independent auditors, including:

- The Service Organization Control (SOC) 2 for Service Organizations audits have been undertaken by Kaspersky since 2019. In 2024, Kaspersky also renewed comprehensive SOC 2 Type 2 audit for the effectiveness of controls implemented to protect the process of the antivirus databases development.
- ISO/IEC 27001:2013 certification: the international standard outlining best practices for information security management systems, achieved by Kaspersky in 2020 and subsequent re-certification with expanded scope in 2022.

We are transparent in how we work to protect you and your businesses

Kaspersky is the first cybersecurity company to publicly offer our source code for external review and has also made our Software Bill of Materials (SBOM) available for our customers and partners. Our international network of Transparency Centers allows stakeholders to learn about our internal processes and data management practices, providing confidence in the high levels of data protection we offer.

Read more about Kaspersky's Global Transparency Initiative

Kaspersky is committed to protecting customers from cyberthreats, regardless of their origin or purpose. The company's Global Transparency Initiative (GTI) 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 also introduces additional accountability mechanisms by which the company can further demonstrate that it addresses any security issues promptly and thoroughly. You can learn more about the history of the GTI development and its global expansion on the website.

Kaspersky's Global Transparency Initiative includes a number of actionable and concrete measures:

- **External review** of the company's source code, software updates and threat detection rules;
- **Independent review** of the company's secure development lifecycle processes, and its software and supply chain risk mitigation strategies;
- **Relocation of threat-related data storage and processing to Switzerland** for customers in Europe, North and Latin America, the Middle East, and also several countries in the Asia-Pacific region.

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

- **Transparency Centers across the globe** to address any security concerns, together with customers, trusted partners and government stakeholders. Kaspersky Transparency Centers are located across META, Asia-Pacific, Europe, and Latin America.
- **Increased bug bounty rewards** of up to US$100,000 for the most severe vulnerabilities found under Kaspersky's Vulnerability Disclosure program. Since 2022, Kaspersky has been running its public bug bounty program on the Yogosha platform. The company also supports the Disclose.io framework which provides Safe Harbor for vulnerability researchers concerned about negative legal consequences of their discoveries.
- **Making the company's approach in its Responsible Vulnerability Disclosure transparent** by publishing its ethical principles.
- **Transparency Reports** disclosing the number of requests from law enforcement and government agencies to provide information on user data, expertise, and technical information for the investigation of threats.
- **The launching of the Cyber Capacity Building Program** – a dedicated training course on product security evaluation for greater security and cyber-resilience of the ICT ecosystem, available also online.

We believe education and cooperation will lead to a safer digital era

Kaspersky educates its users on the evolving cyberthreat landscape and speaks about complex digital topics in a simple way. The company works to enrich children's online safety and supports the development of young talent by contributing to the international IT community. We also lead global associations and joint projects aimed at protecting those in need. Together we can build a safer world.

Read more about our role in the global IT community

Cooperation is the most effective way of building a safer world and fighting cybercriminals. We believe there are no borders to providing security. To this end, we share our expertise, knowledge and technical findings with the world's security community. Our company has been taking part in investigations with companies such as Adobe, AlienVault Labs, Novetta, CrowdStrike, OpenDNS and others.

We are proud to collaborate with global IT security vendors, international organizations, and national and regional law enforcement agencies all over the world in fighting cybercrime.

Along with law enforcement agencies and CERTs worldwide, Kaspersky cooperates with INTERPOL in the joint fight against cybercrime. The company provides the organization with human resources support, training, and threat intelligence data on the latest cybercriminal activities. Specifically, Kaspersky researchers have provided trainings to INTERPOL law enforcement officials since 2019, with the company conducting more than 10 cybersecurity training events for INTERPOL.

To further enhance global efforts to combat cyber offenses, Kaspersky and AFRIPOL have signed a cooperation agreement in preventing and fighting cybercrime. Having a long record of joint cooperation projects, the two organizations have been active contributors to the assessment of the African threat landscape, as well as disrupting cybercrime, namely Africa Cyber Surge Operation and Africa Cyber Surge Operation II.

Kaspersky is also a member of initiatives and organizations such as Securing Smart Cities, the Industrial Internet Consortium, AUTOSAR, the International Telecommunication Union, and the International Organization for Standardization. We are founding members of the Coalition Against Stalkerware and the NoMoreRansom Initiative, and participate as partners in the Geneva Dialogue – a multistakeholder cooperation group leading an international process and conversation on the security of digital products. We take part in joint cyberthreat investigations and conduct training for cybersecurity specialists and for international police organizations. Collaboration between the Dutch police and Kaspersky led to the arrest of suspects behind the Coinvault ransomware attacks.

Kaspersky also proactively engages with UN initiatives, including the Global Digital Compact, the Open-Ended Working Group on the Security and Use of ICT and the Ad Hoc Committee to Elaborate a Comprehensive

International Convention on Countering the Use of ICT for Criminal Purposes. Kaspersky has been a frequent participant in the Internet Governance Forum (IGF) under the aegis of the United Nations, having presented its "Ethical principles for the use of AI in Cybersecurity" as well as its guidelines for the secure development and deployment of AI systems as part of the forum.

Read more about our educational initiatives

We believe that encouraging dialogue and launching educational programs are essential steps towards international collaboration in the fight against cybercrime. That is why we run the Kaspersky Academy – an international educational project established by Kaspersky in 2010. Through this program, we promote worldwide knowledge of cybersecurity, supporting young talent in IT and contributing to the development of high-quality cybersecurity educational programs.

To equip young talents with the wide knowledge of cybersecurity professional paths and make their future IT journey more vivid, Kaspersky also launched the Tech Valley project, which focuses on senior scholars and college students. In 2023, Kaspersky Academy launched Kaspersky Academy Alliance, a special program for universities to integrate the cybersecurity expertise and the latest Kaspersky technologies into teaching to enhance student's academic outcome.

In 2023, Kaspersky announced its Kids' Cyber Resilience project. The goal of this project is to establish collaborative and proactive approach to online safety and security, helping children manage stress and recover from setbacks in a digital environment. In 2024, Kaspersky expanded its initiative from Vietnam, in the Asia-Pacific (APAC) region to the Middle East and CIS countries. That same year, Kaspersky also published a book "Cybersecurity Alphabet" for kids 5-12 years old. In this book, they get to know new technologies, learn the main cyber hygiene rules, find out how to avoid online threats and recognize fraudsters' tricks. Furthermore, in 2025 Kaspersky announced the opening of its Cyber Research Center at KidZania Santa Fe to educate young users about the importance of digital security.

Apart from youth education, the project also equips parents and educators with the knowledge and tools needed to guide children to identify issues online, i.e. sources of stress and discomfort, reduce or mitigate potential cyber risks, and provide support for those who may have been impacted by cyber bullying and other negative forms of online experiences. Kaspersky experts also contribute to study materials for Junior High schools.

Kaspersky also conducts Kaspersky Expert training, aimed at professionals to help them learn effective threat detection and mitigation strategies to battle the evolving dangers of today's cyber-reality.

Read more about our social projects

In our efforts to build a safer future, we are not only concerned with the digital well-being of the world. Reducing the environmental impact of our infrastructure, business activities and products, employee care, inclusivity and availability of technologies are the key areas of Kaspersky's sustainable development. The company has been releasing its sustainability reports since 2023, drafting in accordance with international GRI and SASB standards. The latest report is available here.

Women in Cybersecurity is an online community created by Kaspersky, that helps supercharge the careers of women entering the cybersecurity industry, along with those already in the field. We've also launched the Empower Women digital project with the goal of further building bridges between women and men at every level of the company via knowledge sharing – helping to create a working environment where everyone can reach their full potential, regardless of gender. Kaspersky has consistently led efforts to address digital violence and technology-facilitated abuse. In 2019, the company introduced spyware protection in its Android app, becoming the first to offer users a robust defense against stalkerware – a commercial spyware, which is deemed legal, but can be used to secretly monitor and track a partner's device and often leads to domestic abuse. That same year, Kaspersky co-founded the Coalition Against Stalkerware, uniting private IT companies, NGOs, research institutions, and law enforcement agencies to combat intrusive software and raise awareness about digital abuse. What began with 10 stakeholders has now grown into a network of over 40 organizations and has also received support from INTERPOL,

all working collaboratively to combat cyberstalking and support victims for five years on. On top of this, Kaspersky supports non-profit organizations (NPOs) working with the victims of domestic abuse.

Building on its commitment to combating both online and offline stalking, Kaspersky recently introduced the Who's Spying on Me feature in its Android apps. This innovation not only detects stalkerware but also identifies suspicious Bluetooth devices that could be used for offline tracking. By expanding its protective capabilities, Kaspersky continues to empower individuals to take control of their safety and privacy.

In 2024, Kaspersky launched an Anti-stalking Awareness Guide — a new initiative engaging psychologists and victims of stalking. Combining expertise from multiple disciplines, this guide doesn't just help users identify signs of stalking and take protective measures, but also amplifies the voices of survivors, inspiring others to reclaim their sense of safety and control.

Furthermore, Kaspersky was a partner in the EU-wide "DeStalk" project, running from 2021-2023, which the European Commission chose to support with its Rights, Equality and Citizenship Program. DeStalk addresses the issues of cyberviolence and stalkerware, representing new, widespread and hidden forms of online gender-based violence.