

kaspersky

**Kaspersky Overview:
Our values, business,
solutions and services**

Updated: March 2024

“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 date¹

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.

[Read more information about our product portfolio](#)

Kaspersky’s portfolio encompasses solutions to suit a wide range of customers. We are not just a service or a product vendor, we are a partner. We analyze the business needs, decompose the requirements, and find the best solutions for its stable growth and development, regardless of its size, field, and expertise.

We provide customers with not just separate products and services, but with a complete ecosystem – comprehensive solutions that complement and enhance each other. We do not only solve a specific task – we think strategically about everything the company needs now and in the future. In order to address any problem in the field of cybersecurity, we utilize our products and services that are built upon ongoing research and extensive experience in studying threats. Behind each of our solutions, there are numerous researches, technological innovations, and new approaches conducted and implemented.

We empower consumers with a range of products to secure their privacy, money and other values that are really important. We understand the needs of small businesses and have a unique multi-layered solution especially for them, which is easy to manage and offers effective protection. We cover all the cybersecurity needs of large

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.

enterprises with our full enterprise platform that helps to prevent all types of cyberthreats, detecting even the most sophisticated attacks, responds to security incidents and predicts the evolution of the threat landscape.

Our comprehensive portfolio of solutions achieves all of this thanks to the combination of our unique expertise, threat intelligence and machine learning that enables us to develop robust technologies to detect, block and prevent cyberattacks.

As a technology-driven company we invest heavily in R&D to support the innovative ideas we believe in. That is why half of the company's employees are R&D specialists; developing and maintaining our solutions in-house – key to providing a holistic approach to security.

Kaspersky is consistently awarded top scores in more independent tests [than any other vendor](#).

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

On a daily basis, 24/7, hundreds top cybersecurity professionals are working to combat the threats of massive malware, APT, industrial, and automotive cybersecurity, IoT and other threats to ensure you and your business remain protected. Our experts have firsthand experience dealing with any kind of security challenges and put this expertise into our state-of-the-art protection technologies to be sure their quality is unsurpassed. Our elite group of international experts – Kaspersky's Global Research and Analysis Team (GReAT) – is globally recognized and performs on the most influential cybersecurity conferences such as BlackHat, AVAR, Virus Bulletin, and others. These cybersecurity experts conduct research and reveal the most sophisticated threats targeting users and organizations all around the world. In 2023, Kaspersky GReAT experts have uncovered an ongoing mobile Advanced Persistent Threat (APT) campaign dubbed '[Operation Triangulation](#)', targeting iOS devices with previously unknown malware with the final goal to hiddenly spy on users.

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. With over 600² 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 users.

[Read more about independent assessments and certifications](#)

Kaspersky is working with independent auditors to review its internal processes, including:

- The Service Organization Control (SOC) 2 for Service Organizations audits have been undertaken by Kaspersky since 2019. In 2023, Kaspersky also [passed](#) comprehensive SOC 2 Type 2 audit for the effectiveness of controls implemented to protect the process of the antivirus databases development.

² The number includes independent test results of corporate and consumer products during 2013-2023.

- [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.

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

- **Independent 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.
- **Transparency Centers across the globe** to address any security concerns, together with customers, trusted partners and government stakeholders. These facilities are in Zurich, Utrecht, Madrid, Rome, Kuala Lumpur, São Paulo, Tokyo, Singapore, Woburn, Riyadh, and Kigali.
- **Increased bug bounty rewards** of up to US\$100,000 for the most severe vulnerabilities found under Kaspersky's Coordinated 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 the 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. Moreover, Kaspersky was included in the list of Vulnerability Top Contributors by [Microsoft](#). 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.

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](#). Other partners include law enforcement agencies and CERTs worldwide. 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 also regularly participates in the Internet Governance Forum (IGF) under the aegis of the United Nations. At the IGF 2023 (Kyoto, Japan), Kaspersky organized the workshop on "Ethical principles for the use of AI in Cybersecurity" and attended the IGF Parliamentary Track.

[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.

Kaspersky also runs the [SecurIT Cup](#) – a global competition for students from all over the world and from various academic backgrounds. Participants have the chance to win US\$10,000 and benefit from competing alongside like-minded students while building an understanding of what it is like to work in the industry. They are welcome to suggest their own project ideas to help solve global cybersecurity issues.

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 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.

Apart from kids' education, the process includes equipping parents and educators with knowledge and tools to guide kids 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 forms of negative online experiences. Kaspersky experts also contribute to study materials for Junior High schools.

Additionally, Kaspersky conducts [Kaspersky Expert training](#), which is aimed at professionals and helps 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. In 2023, the company released its first [Sustainable \(ESG\) report](#) covering results for 2021 and mid-2022 as well as key objectives for 2023.

[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 also been at the forefront of protecting victims of 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. Kaspersky was the first in the industry to warn customers about third-party tracking of this type, and our anti-spyware feature, warning the user if their private information is being covertly monitored by a third party, is available to customers in Kaspersky for Android.

In 2019, Kaspersky and nine other organizations working within the IT security industry or working with the victims and perpetrators of stalkerware launched the [Coalition Against Stalkerware](#) - a global initiative to protect users from stalking and domestic violence. To date, it has united more than 40 business partners and has also received support from INTERPOL. On top of this, Kaspersky supports non-profit organizations (NPOs) working with the victims of domestic abuse.

In 2020, the company's GReAT researchers developed [TinyCheck](#), an easy to use, open-source tool detecting stalkerware and spyware designed to assist those in need. In collaboration with various victim service organizations and tech communities, TinyCheck has developed further. 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.