Our mission is simple — building a safer world.

And in fulfilling that mission we aim to become the global leader in cybersecurity — by securing technology to make sure that the possibilities it brings become opportunities for each and every one of us.

Bring on endless possibilities.
Bring on a safer tomorrow.

Eugene Kaspersky, CEO
Our promise

We believe in a tomorrow where technology improves all of our lives. Which is why we secure it, so everyone, everywhere, can benefit from the endless opportunities it brings.
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 6 continents in almost 200 countries and territories

Provides innovative IT security solutions and services for business and consumers

Numbers

> 15 million consumer product activations per year

> 4,500 highly qualified specialists

US $ 752 million global non-audited IFRS revenue in 2021
Our Next Generation solutions and services are available for a wide range of clients: from individual home users to large and small organizations, including big enterprises, critical infrastructure networks and governments.

>240,000
Corporate clients worldwide

>400,000,000
Users worldwide are protected by our technologies
We work in a wide range of industry sectors. Our solutions and services successfully protect over 240,000 clients around the world, regardless of size or complexity.
We are an international cybersecurity company

200 countries and territories we operate in

34 representative regional offices

- Africa
  - South Africa

- Asia
  - China
  - Hong Kong
  - India
  - Japan
  - Kazakhstan
  - Malaysia
  - Singapore
  - South Korea

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

- Middle East
  - Saudi Arabia
  - Turkey
  - UAE

- North America
  - Mexico
  - USA

- South America
  - Brazil

- Transparency Centers
  - Zurich, Switzerland
  - Madrid, Spain
  - São Paulo, Brazil
  - Kuala Lumpur, Malaysia
  - Woburn, USA
  - Singapore, Singapore
  - Tokyo, Japan
  - Rome, Italy
  - Utrecht, the Netherlands
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.
Global Transparency Initiative

- Key transparency principles
- Global Transparency Initiative
- Independent assessments and certifications
- Bug Bounty Program
Data sent to Kaspersky is crucial for protecting users, it is robustly protected 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.
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:

1. Cyberthreat-related data infrastructure relocation to Switzerland.
2. 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.
3. Third-party security assessments of Kaspersky's engineering and data management practices to verify the security of the company's solutions.
Global Transparency Initiative

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 received.

Cyber Capacity Building Program – a dedicated training to share security evaluation knowledge with a 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:
- SOC 2 audits by a Big Four firm
- 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

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.
Kaspersky Global Transparency Initiative: our results in numbers

2 Additional data locations in Switzerland — globally known as a neutral country, and with strict data protection regulation. Here we process and store cyberthreat-related user data from Europe, North and Latin America, the Middle East, and also several countries in Asia-Pacific region.

9 Transparency Centers in Brazil, Italy, Japan, Malaysia, the Netherlands, Singapore, Spain, Switzerland, and the United States.

2 Regular third-party independent assessments confirming the trustworthiness of Kaspersky engineering practices:
- SOC 2 audit by a ‘Big Four’ accountancy firm
- ISO 27001 certification

30+ Transparency Center visits by public and private stakeholders, including two ‘red piste’ visits with a source code review.

53 Bug Bounty report awarded with total payments equal to $75,750.
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 renewed SOC 2 audit in 2022.

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 renewed SOC 2 audit in 2022.

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. Information security management system of Kaspersky has been certified against ISO/IEC 27001:2013 international standard.
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. The company also supports the Disclose.io framework, which provides Safe Harbor for vulnerability researchers concerned about negative legal consequences of their discoveries.

**Rewards**

**$100,000**

for the discovery and coordinated disclosure of severe vulnerabilities (high-quality report 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 discovery of bugs allowing local privilege escalation, or leading to sensitive data disclosure.
Threat intelligence and research

- 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.

>4,500 highly qualified specialists

50% of our employees are R&D specialists

35+ world-leading security experts: our elite group
>1,000,000,000

cyberthreats
detected by Kaspersky since the company's inception

8,000,000,000

cyberattacks
detected by Kaspersky in 2021

380,000

new malicious files
detected by Kaspersky every day
Advanced persistent threat landscape in 2021

Kaspersky’s Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats. According to their data, in 2021 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets

- Government
- Diplomatic
- Telecommunications
- Military
- Defense
- IT companies
- Educational
- Civil Aviation
- Logistics
- Pharmaceutical

Top 12 targeted countries

- US
- UAE
- Egypt
- Pakistan
- Iran
- Afghanistan
- India
- Russia
- South Korea
- Taiwan
- Vietnam
- Thailand

Based on the data up to 31.12.2021
## Our major discoveries and research

<table>
<thead>
<tr>
<th>Classification</th>
<th>Detection</th>
<th>Active since</th>
<th>Targets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber-espionage &amp; sabotage, financial attacks</td>
<td>Lazarus</td>
<td>2016</td>
<td>Malware infections linked to the P5+1 events and venues for high level meetings between world leaders</td>
</tr>
<tr>
<td>Cyber-espionage malware</td>
<td>Project Sauron</td>
<td>2016</td>
<td>Media, financial institutions, casinos, software developers for investment companies, cryptocurrency businesses</td>
</tr>
<tr>
<td>Modular cyber-attack platform</td>
<td>Shadowpad</td>
<td>2017</td>
<td>Mainly state organizations. Over 30 victims in Russia, Iran and Rwanda</td>
</tr>
<tr>
<td>Cyber-espionage malware</td>
<td>Olympic destroyer</td>
<td>2018</td>
<td>Spread around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. &gt;50% of organizations attacked were industrial companies</td>
</tr>
<tr>
<td>Cyber-espionage malware</td>
<td>Shadow hammer</td>
<td>2018</td>
<td>Banking and financial industry, software, media, energy and utilities, insurance, industrial and construction, manufacturing, and other industries</td>
</tr>
<tr>
<td>Cyber-espionage malware</td>
<td>Tajmahal</td>
<td>2019</td>
<td>Organizations related to Winter Olympic Games 2018, biological and chemical threat prevention organizations in EU, financial institutions in Russia</td>
</tr>
<tr>
<td>Cyber-espionage platform</td>
<td>Mosaic-regressor</td>
<td>2020</td>
<td>Banking and financial industry, software, media, energy and utilities, insurance, industrial and construction, manufacturing, and other industries</td>
</tr>
<tr>
<td>Cyber-espionage platform</td>
<td>Ghostemperor</td>
<td>2021</td>
<td>Special instructions in malware code were aimed at targeting only 600 systems, identified by specific MAC addresses</td>
</tr>
</tbody>
</table>

**Targets:**
- Military and government entities worldwide
- Malware infections linked to the P5+1 events and venues for high level meetings between world leaders
## Targeted attack research

<table>
<thead>
<tr>
<th>Year</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>ProjectSauron, StrongPity, Lazarus, Fruity Armor, ScarCruft, Poseidon, Danti, Dropping Elephant, WannaCry, Shamoon 2.0, StoneDrill, BlueNoroff, ExPetr/NotPetya, Moonlight Maze, ShadowPad, BlackOasis, Silence, WhiteBear</td>
</tr>
<tr>
<td>2017</td>
<td>WannaCry, Shamoon 2.0, StoneDrill, BlueNoroff, ExPetr/NotPetya, Moonlight Maze, ShadowPad, BlackOasis, Silence, WhiteBear</td>
</tr>
<tr>
<td>2018</td>
<td>Zebrocy, DarkTequila, MuddyWater, Skygofree, Olympic Destroyer, ZooPark, Hades, Octopus, AppleJeus</td>
</tr>
<tr>
<td>2019</td>
<td>Topinambour, ShadowHammer, SneakyPastes, FinSpy, DarkUniverse, COMpfun, Titanium</td>
</tr>
<tr>
<td>2021</td>
<td>GhostEmperor, ExCone, BlackShadow, BountyGlad, EdwardsPhesant, HotCousin, GoldenJackal, FerociousKitten, ReconHellcat, CoughingDown, MysterySnail, MysterySnail, MysterySnail</td>
</tr>
</tbody>
</table>
Privacy has become a commodity of value with more and more users understanding its importance and the need to change their habits to protect their digital presence. Being not just a cybersecurity company, but a privacy company, Kaspersky invests not only in privacy features, but also works to enable users to protect their data and digital privacy through educational assets and hands-on tools.

Enabling a privacy-minded world

Privacy has become a commodity of value with more and more users understanding its importance and the need to change their habits to protect their digital presence. Being not just a cybersecurity company, but a privacy company, Kaspersky invests not only in privacy features, but also works to enable users to protect their data and digital privacy through educational assets and hands-on tools.

- **Anti-doxing course**: Learn the basics about doxing dangers and how to defend against it.
- **Privacy checklist**: Easy to grasp definitive checklist for those who care about their privacy.
- **Stalkerware protection**: Kaspersky’s Internet Security for Android solution offers users best-in-class protection and detection of software used to secretly spy on people.
- **Privacy Checker**: Instructions on how to set up social media accounts and OS privacy levels.

Learn more
Products & solutions

- Cyber Immunity approach
- KasperskyOS
- Enterprise Solutions
- Industrial Cybersecurity Solution
- SMB Next Generation Solutions
- MSP Solutions
- B2C Solutions
From cybersecurity to Cyber Immunity

Traditional (cybersecurity)

Endless vulnerability/antidot race
Virus/antivirus, email fishing/email protection

Secure by Design (Cyber Immunity)

Defined by product goal and security objective
Microkernel, isolated domains, security policies
Architectural approach creates an environment where a vulnerability or bad code is no longer a big deal.

- IT system’s “inherent” protection – its ability to withstand cyberattacks without any additional (applied) security tools

- The hands-on methodology to create IT systems with “innate” protection

- The platform for building Cyber Immune IT-systems – KasperskyOS, proprietary microkernel operating system for IT-products with high demands on cybersecurity
KasperskyOS areas of application

KasperskyOS-based solutions have “innate” protection against the consequences of the intrusion of malicious code and hacker attacks.

They perform its functions even in an aggressive environment without additional security features.
KasperskyOS-based product portfolio

Kaspersky IoT Infrastructure Security
A solution for protecting internet of things (IoT), as well as connecting to clouds, with secure gateways as its key elements

Kaspersky IoT Secure Gateway

KISG 100
Siemens SIMATIC IOT2040 hardware platform

KISG 1000
Advantech UTX-3117 hardware platform

Kaspersky Security Center

Kaspersky Secure Remote Workspace
A solution for convenient and predictable operation as well as centralized administration of thin client infrastructure

Kaspersky Thin Client

Kaspersky Security Center

Kaspersky Security Management Suite

Powered by KasperskyOS
Kaspersky SMB Next Generation Solutions

**Kaspersky Small Office Security**
- As easy as home antivirus
- Works out of the box, no configuration required
- Financial protection with Safe Money
- Client and personal data protection. Encryption back-up
- Storing all passwords with Password Manager

**Kaspersky Endpoint Security Cloud**
- Rapid protection for limited resources
- Cloud-based console for flexible, simple administration, no need for additional hardware
- Protects PCs, laptops, mobile devices and file servers
- Security for Microsoft Office 365 and ‘Shadow IT’ control
- The latest, most up-to-date software - always

**Kaspersky Optimum Security**
- The best enterprise-grade security solution
- Essential EDR functionality to combat evasive threats
- Managed protection brings security to a whole new level
- Reduces your cybersecurity team's workload
- Cloud-native solution that covers diverse infrastructures
Kaspersky Services for Managed Service Providers

**Build services**
- Endpoint Protection and hardening
- Vulnerability and Patch Management
- Office365 Protection
- Incident Response
- Security Awareness
- Managed Web and Email Protection

**MSP**
- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Automated Security Awareness Platform
- Kaspersky Security for Mail Server
- Kaspersky Security for Web Gateway

**MSSP**
- Kaspersky EDR Optimum
- Kaspersky EDR Expert
- Kaspersky Anti Targeted Attack
- Kaspersky Threat Lookup
- Kaspersky Threat Data Feeds
- Kaspersky Intelligence Reporting

**Automation and integration**
- RMM and PSA Integrations
- Subscription-based model and LMP

**Knowledge and Expertise**
- Kaspersky Cybersecurity Training
- Kaspersky Premium Support and Professional Services

Kaspersky at a glance
- Global Transparency Initiative
- Threat Intelligence and research
- Products & solutions
- Awards
- ESG
- Education
- Sponsorships & Partnerships
B2C Solutions: New product portfolio

Kaspersky announces early access to new and reimagined consumer product portfolio

Our range of plans answer the needs of every consumer
B2C Solutions: Giving consumers the confidence to thrive

We inspire our customers to embrace new technologies and make the most of all the opportunities they bring — because they know we’re keeping them safe.

Kaspersky B2C Solutions

- Kaspersky VPN Secure Connection
  - Win | Android | Mac | iOS
- Kaspersky Password Manager
  - Win | Android | Mac | iOS
- Kaspersky QR Scanner
  - Android | iOS
- Kaspersky Battery Life
  - Android
- Kaspersky Safe Kids
  - Win | Android | Mac | iOS
- Kaspersky Security Cloud Free
  - Win | Android | iOS
Kaspersky awards

- Overview
- Top 3 metrics
More than 600 awards

One of the five biggest endpoint security vendors*.

Kaspersky Internet Security was honored with the Product of the Year 2020 award by independent test lab AV-Comparatives**.


**Kaspersky’s flagship home user security solution – Kaspersky Internet Security – was honored with the Product of the Year 2020 award for an impressive sixth time, in an annual report released by independent test lab AV-Comparatives. Kaspersky was acknowledged ahead of 16 peers by achieving Advanced+ awards in seven rigorous tests, to rank the company highest overall across the participating Windows security products.
Recognitions

Most Tested*  
Most Awarded*  
Kaspersky Protection

*Kaspersky.com/top3

As cybersecurity becomes vital for every individual and entity, trust in providers is essential. We protect home users and corporate clients worldwide, and market recognition is really important for us. In 2021, Kaspersky products participated in 75 independent tests and reviews. Our products were awarded 57 firsts and received 63 top-three finishes.

* 75 independent tests were completed by Kaspersky products in 2021 alongside 13 competitors. More than 80 vendors took part in the tests, but only those who participated in 35% or more of the tests had their results represented in the chart.
As we work to create a safer future, we are concerned about the well-being of the world not beyond in the context of its digital reality. Gender equality, accessible knowledge, volunteering, child safety, animal protection and more are all issues that are crucial to us.

We are also committed to social responsibility through volunteerism and philanthropy in the different regions in which the company operates.

We cooperate with non-profit organizations, support charity initiatives and create our own social programs.

Read Kaspersky CSR report [here](#).
As a cybersecurity company, we play a key role in tackling the gender gap issue and ensuring that real progress is happening.

Kaspersky, with 40+ partners from the IT Security industry and non-profit sector, supports the Coalition Against Stalkerware global initiative, and protects users from stalking and domestic violence.

We understand the importance of preserving past cultures, for the benefit of future generations. Since 2015, Kaspersky has been cooperating with the Archeological Society at Athens (ASA).
Education

The concept of Cyber Immunity implies both protecting users’ devices and major critical systems, as well as teaching people the basics of cybersecurity.

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.
Learn more

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.

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

Kaspersky collaborates with business schools to deliver courses on information security for business leaders, top managers and senior executives.
As an innovative global company, Kaspersky cares for the future by not only providing cybersecurity to different industries, but by also supporting promising talent in various countries.

We contribute to the development of science and modern art, we help to preserve the world, and we provide the opportunity for sportspeople to achieve their full potential.
Sponsorships & Partnerships

**Chess**
Kaspersky is an official cybersecurity partner of the FIDE World Championship.

**Science & Space**
Kaspersky has a long history of supporting initiatives in the area of space science, including special cybersecurity training for cosmonauts.

**Art**
Kaspersky was a partner of the Moniker International Art Fair in London, and it supported artists, such as Ben Eine.

**Gaming**
Kaspersky has partnered with several esports teams across the globe to ensure the best of gamers’ experience.

**Motorsport**
Kaspersky is sponsoring Aprilia Racing, one of the most decorated brands in motorcycle racing history.
Bring on the future