Kaspersky Corporate Kit

kaspersky

Updated: April 2022

Our mission is simple — building a safer world.

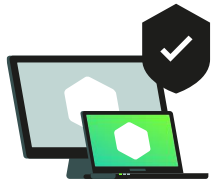
And in fulfilling that mission we aim to become the global leader in cybersecurity — by securing technology to make sure that the possibilities it brings become opportunities for each and every one of us.

Bring on endless possibilities.
Bring on a safer tomorrow.

Eugene Kaspersky, CEO

Kaspersky at a glance

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

> 14 million product activations per year

> 4,500 highly qualified specialists

US$ 704 million — global non-audited revenue in 2020

Achievements and recognition

One of the six biggest endpoint security vendors*

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

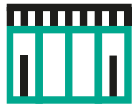
* The company was ranked sixth by IDC estimations in 'Worldwide Consumer Endpoint Security Market Shares, 2020: The COVID-19 Pandemic Contributed to a Market Surge' (DOC #US47714321 / JUN 3, 2021) and 'Worldwide Corporate Endpoint Security Market Shares, 2020: Pandemic and Expanding Functionality Propelled Market Growth' (DOC #US47768021 / JUN 7, 2021).
** 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.

Customer reach

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.

Enterprises

Industrial facilities



Small and medium businesses

Very small businesses

Consumers

>240,000

Corporate clients worldwide

>400,000,000

Users worldwide are protected by our technologies

We are an international cybersecurity company

200 countries and territories we operate in

34 representative regional offices

North America
Mexico
USA

South America
Brazil

Africa
South Africa

Australia

Europe
Austria
Czech Republic
Denmark
France
Germany
Israel
Italy
Netherlands
Poland
Portugal
Romania
Russia
Spain
Switzerland
UK

Asia
China
Hong Kong
India
Japan
Kazakhstan
Malaysia
Singapore
South Korea
Turkey
UAE

Transparency Centers
Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia

Our role in the global IT security community

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

We cooperate with INTERPOL and provide the organization with human resources support, training, and threat intelligence data on the latest cybercriminal activities.

In cooperation with non-profit organizations, digital activists, and cybersecurity vendors, we launched the Coalition against Stalkerware* to protect users against stalking and domestic violence.

Together with Cigref, we are co-chairing the Working Group 6 as part of the Paris Call for Trust and Security in Cyberspace. The aim of this working group is to develop concrete proposals for solutions to improve the level of security in cyberspace.

We are a member of the Industrial Internet Consortium that helps organizations to more easily connect and optimize assets and operations to drive agility across all industrial sectors.

*Stalkerware – a type of a commercial spyware deemed to be legal.
Learn more http://stopstalkerware.org/

Our transparency principles

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 governments and law enforcement agencies to fight cyberthreats

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

We cooperate with the IT security industry in joint cyberthreat investigations

Our Global Transparency Initiative

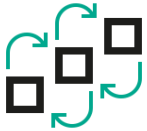
Launched in 2017, Kaspersky's Global Transparency Initiative is aimed at engaging the broader information security community and other stakeholders in validating and verifying the trustworthiness of its products, internal processes, and business operations.

It includes a number of actionable and concrete measures:

Independent code and update review

Engineering practices, external audit & certification

Vulnerability management program



R&D infrastructure relocation

Cyber-capacity Building program

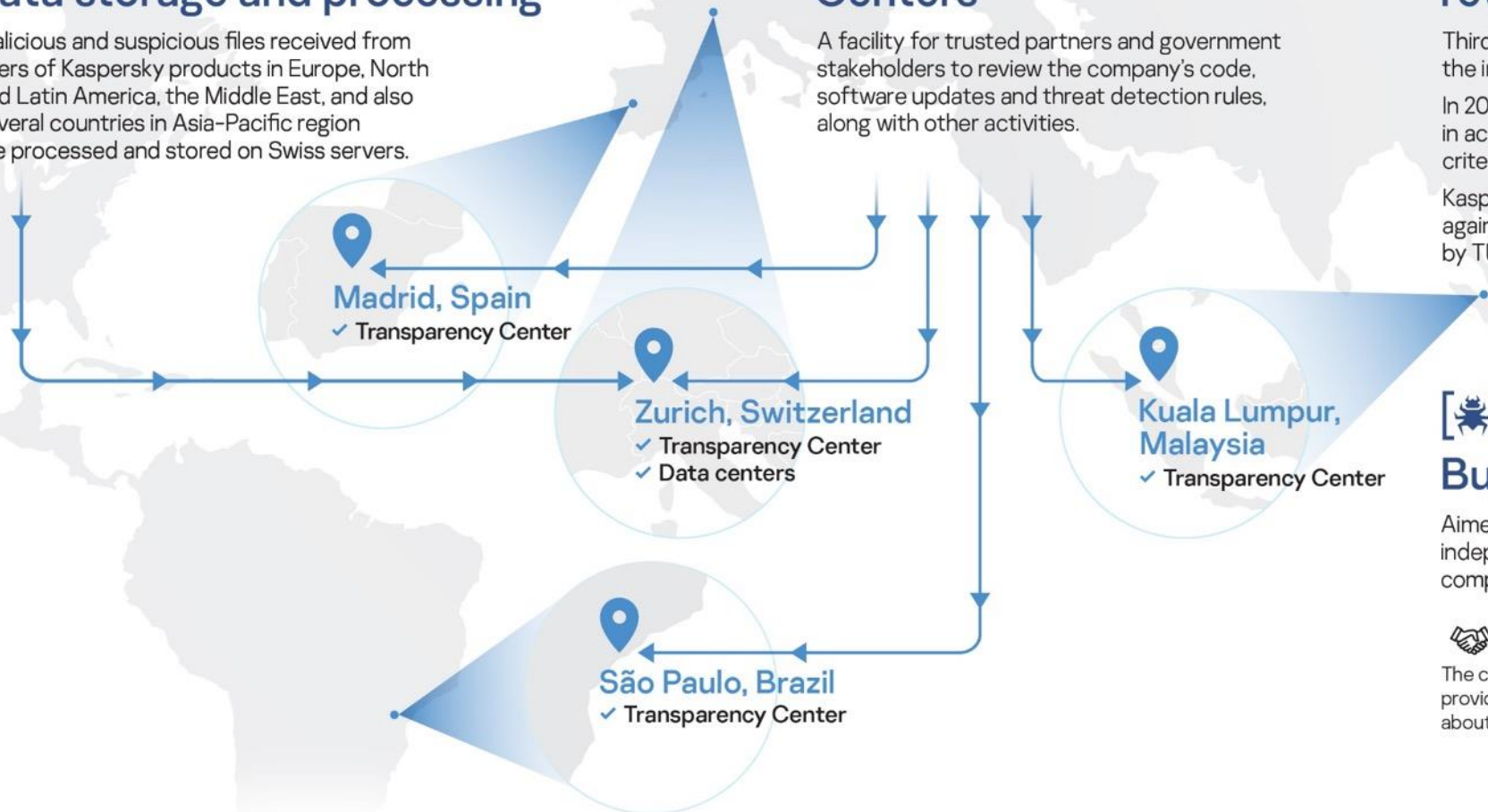
Kaspersky Global Transparency Initiative

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 several countries in Asia-Pacific region are processed and stored on Swiss servers.

Transparency Centers

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



Independent review

Third-party assessment of internal processes to verify the integrity of Kaspersky solutions and processes.

In 2019 Kaspersky has achieved the SOC 2 Type 1 report in accordance with the SSAE 18 standard (Security criteria) issued by one of the Big Four accounting firms.

Kaspersky's data services have also been certified against ISO/IEC 27001:2013 international standard by TÜV AUSTRIA.

Bug bounty program

Aimed to make Kaspersky more secure, it encourages independent security researchers to supplement the company's own work in vulnerability detection and mitigation.

The company also supports the Disclose.io framework which provides Safe Harbor for vulnerability researchers concerned about possible negative legal consequences of their discoveries.

kaspersky BRING ON THE FUTURE

Proven. Transparent. Independent.

As cybersecurity becomes vital for every individual and entity, the question of provider trust is becoming essential. Our mission is to maintain the trust of customers, in addition to our already proven quality.

What people think

Trust security provider's use of data

87% of businesses and **82%** of consumers trust their security provider to behave ethically when collecting and using their data

Worry about security provider's use of data

65%-78% of businesses and **54%-80%** of consumers worry provider will access and share private data, opinions, location or online behavior

Biggest threat?

45% of businesses and **47%** of consumers worry about protecting online data from cybercriminals.

But also: national and foreign govs, employers, families & more

Who is the most responsible for your protection online?

57% of businesses: my IT security team
57% of consumers: I am
45% (consumers), **43%** (businesses): my cybersecurity provider

What matters when choosing

Governments should choose highest quality product or service even if it is by a foreign company

55% businesses agree
66% consumers

In general

82% businesses agree
78% consumers

In areas critical to national security

What matters most when you choose a security provider?

Honesty, integrity, independence, product quality — all **90% +**
Country of origin **86%/80%**

Results of the report The Boundaries of Trust: Privacy and Protection in Cyberspace
https://www.kaspersky.com/blog/the-boundaries-of-trust/

SOC 2 audit

Kaspersky has achieved the SOC 2 Type 1 report in accordance with the SSAE 18 Security Criteria issued by an independent third-party 'Big Four' auditor.

The audit concludes that the development and release of Kaspersky's antivirus bases are protected from unauthorized changes by strong security controls.

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).

ISO 27001 certification

Kaspersky has achieved ISO/IEC 27001:2013 certification issued by TÜV AUSTRIA.

The certification confirms that the company's data security systems, including Kaspersky Security Network, meet industry best practices. It is valid for the company's data services located in Data Centers in Zurich, Frankfurt, Toronto, Beijing and Moscow.

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.

Bug Bounty Program

Kaspersky has run its public bug bounty program from 2016. The company also supports the Disclose.io framework, which provides Safe Harbor for vulnerability researchers concerned about negative legal consequences of their discoveries.

Who can participate

- Individuals over the age of thirteen (13) at the time of entry.
- All researchers except employees of Kaspersky, their subsidiaries, and their immediate families.

Scope products

- Kaspersky Internet Security 2019
- Kaspersky Endpoint Security 11
- Kaspersky Endpoint Security for Linux
- Kaspersky Password Manager
- Kaspersky Secure Connection

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.

More details are available in the bug bounty program description on Kaspersky website.

Threat landscape

Expertise

>4,500 highly qualified specialists

50% of our employees are R&D specialists

40+ world-leading security experts: our elite group

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.

>1,000,000,000
cyberthreats

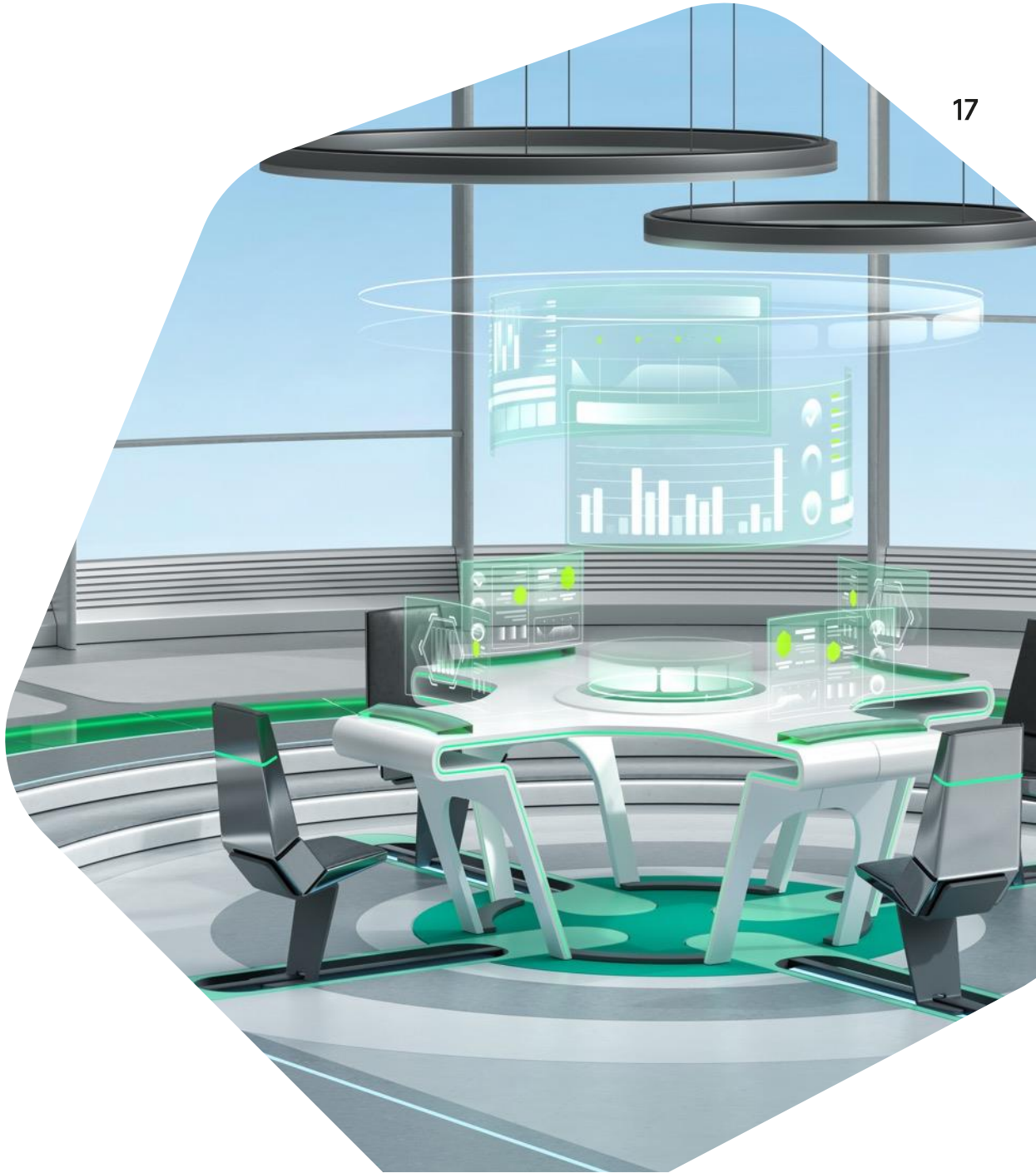
detected by Kaspersky since the company's inception

8,000,000,000
cyberattacks

detected by Kaspersky in 2021

380,000
new malicious files

detected by Kaspersky every day



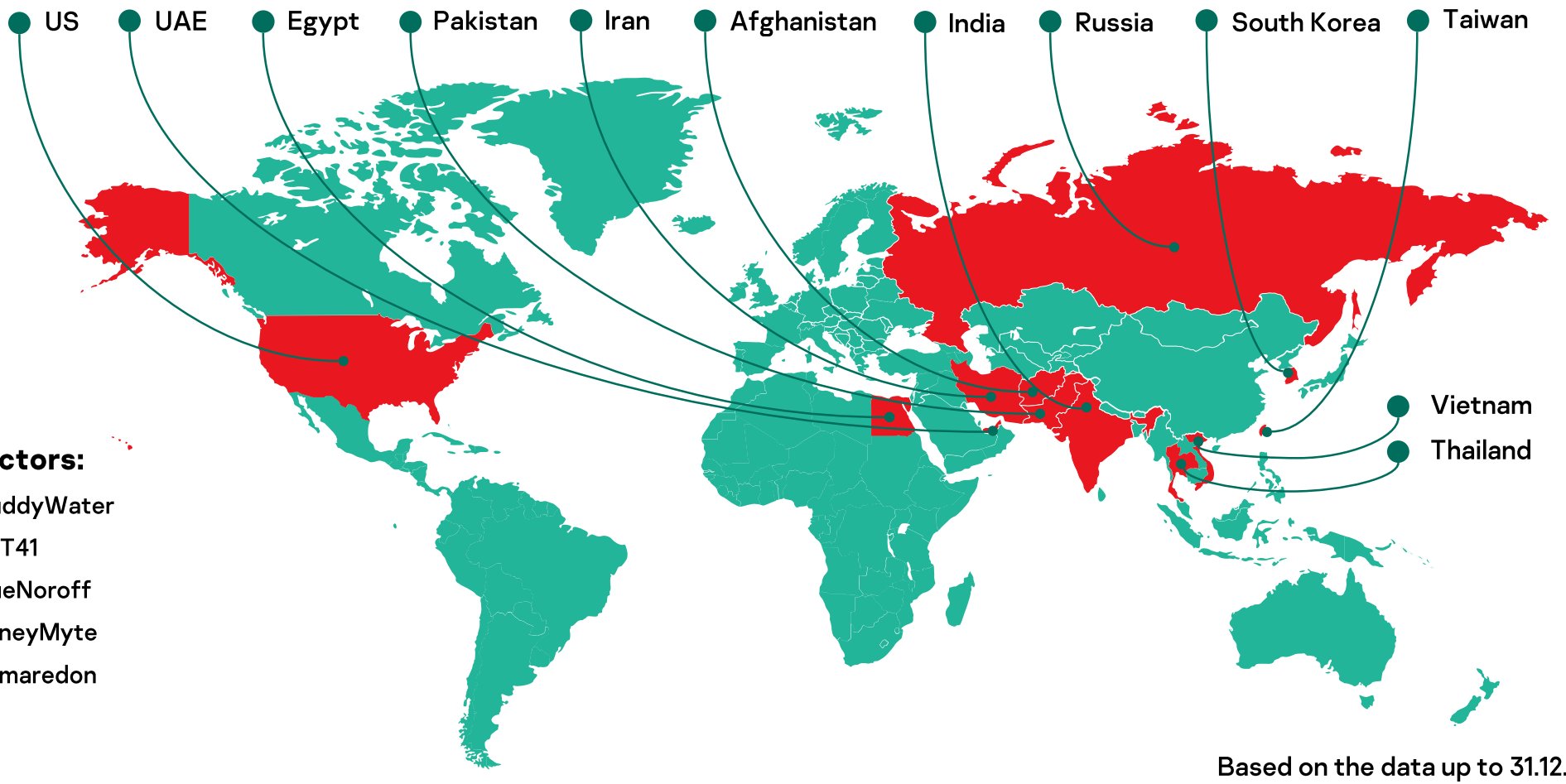
Advanced persistent threat landscape in 2021

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:



Top 10 significant threat actors:

1. Lazarus
2. DarkHalo
3. CloudComputating
4. Turla
5. SideCopy
6. MuddyWater
7. APT41
8. BlueNoroff
9. HoneyMyte
10. Gamaredon

apt.securelist.com

Based on the data up to 31.12.2021

Our major discoveries and research

Detection	SOFACY 2014	DUQU 2.0 2015	LAZARUS 2016	PROJECT SAURON 2016	EXPETR/ NOTPETYA 2017	SHADOWPAD 2017	OLYMPIC DESTROYER 2018	SHADOW HAMMER 2018	TAJMAHAL 2019	MOSAICREGRESSOR 2020	GHOSTEMPEROR 2021
Active since	2008	2014	2009	2011	2017	2017	2017	2018	2013	2017	2020
Classification	Cyber-espionage malware	Complex cyberattack platform	Cyber-espionage & sabotage, financial attacks	Cyber-espionage malware	Data wiping campaign	Modular cyber-attack platform	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform
Description	Sofacy (also known as "Fancy Bear", "Sednit", "STRONTIUM" and "APT28") is a highly professional threat actor. Suspected of a connection to the notorious Miniduke actors, Sofacy has been notable for its extensive use of zero-day exploits	A highly sophisticated malware platform exploiting up to three zero-day vulnerabilities	A group believed to be behind the attacks on Sony Pictures Entertainment in 2014 and the Central Bank of Bangladesh in 2016. Responsible for data destruction, money theft as well as conventional cyber-espionage operations against multiple companies around the world	A threat actor attacking state organizations. Project Sauron deliberately avoids patterns, customizing its implants and infrastructure for each individual target, and never reusing them, making traditional indicators of compromise almost useless	A wiper pretending to be ransomware, using modified EternalBlue and EternalRomance exploits. Some observations point to a link between ExPetr and BlackEnergy APT	ShadowPad is one of the largest known supply-chain attacks. Affected server management software NetSarang used by hundreds of large businesses around the world. Attackers deployed the platform in victim networks to gain flexible remote control capabilities	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.
Targets	Military and government entities worldwide	Malware infections linked to the P5+1 events and venues for high level meetings between world leaders	Media, financial institutions, casinos, software developers for investment companies, cryptocurrency businesses	Mainly state organizations. Over 30 victims in Russia, Iran and Rwanda	Spread around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. >50% of organizations attacked were industrial companies	Banking and financial industry, software, media, energy and utilities, insurance, industrial and construction, manufacturing, and other industries	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 organisations and Telecommunicati on companies

Targeted attack research

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

Kaspersky solutions & services

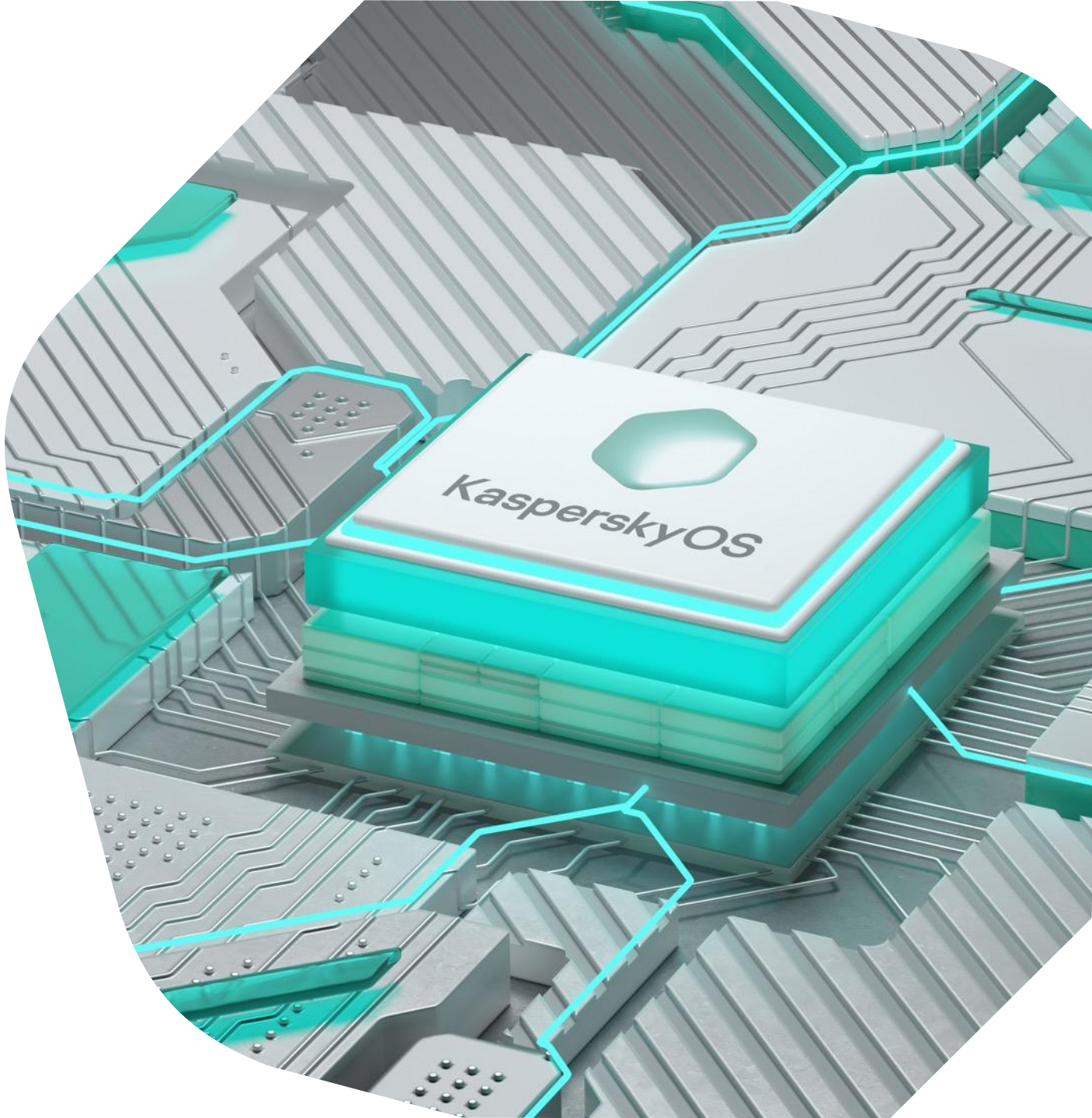
KasperskyOS

Cyber Immune operating system for connected systems with high demands on cybersecurity

Creates an environment where a vulnerability or bad code is no longer a big deal

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

Grants a platform for creating secure-by-design solutions for a number of industries with special requirements to safety and security



Key technologies

KasperskyOS is designed with security in mind and remains secure during its whole lifecycle

Cyber Immunity

System stays secure when everything that can be hacked is hacked

Microkernel

Proprietary Kaspersky's microkernel, developed in-house, no Linux inside. Vastly reduced attack surface

Secure-by-design

Mature multiple independent layers of security (MILS) implementation, high level of isolation between domains

Default deny

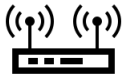
Security functions are separated from business logic in security monitor which controls all communications in the system. Any interaction that is not allowed will be rejected

Multi-level compatibility

POSIX API compatible (well 98% of the API).
Runs on Intel x86, x64, ARM v6, v7, v8

KasperskyOS

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

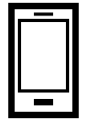


IoT & Industrial IoT

Transportation

Industrial automation

Virtual desktop infrastructure



Corporate mobile devices

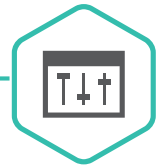
Trusted execution environment

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

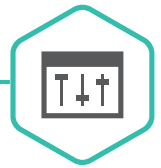


Kaspersky Security Center

Kaspersky Secure Remote Workspace β

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

Kaspersky Automotive Adaptive Platform β

Specialized SDK for development of secure automotive software

β - The current version of the product is intended for non-commercial piloting

Kaspersky enterprise solutions

Kaspersky Security Foundations

Who's it for?

- IT teams in organizations of every size
- Decision-makers who want to build a solid security foundation now and avoid costly future problems

What is it?

The cloud-managed threat prevention stage enabling every organization to automatically stop commodity cyberthreats on any device, VDI and hybrid server infrastructure. Delivers an average 441% ROI as confirmed in Forrester's TEI interviews with customers.

What does it do?

- Protects every device — including specialized and legacy endpoints
- Delivers visibility and control over every IT asset
- Helps prevent or mitigate user mistakes
- Provides the systems management automation you need, without breaking the bank

Kaspersky Optimum Security

What is it?

- Kaspersky Optimum Security helps protect businesses from new, unknown and evasive threats
- Effective threat detection and response solution, easy on resources
- 24/7 security monitoring, automated threat hunting and guided and managed responses supported by Kaspersky experts

Who's it for?

- Small dedicated IT security team, typically of one to three people
- Limited cybersecurity resource
- Emerging cybersecurity expertise

What does it do?

- Upgrades endpoint protection against evasive threats
- Supports building essential incident response processes
- Optimizes cybersecurity resource use

Kaspersky Expert Security

What is it?

Kaspersky Expert Security is a comprehensive defensive approach, designed to meet the day-to-day needs of any IT security-matured enterprise in dealing with the most sophisticated current threats, including APTs (Advanced Persistent Threats) and targeted attacks.

Who's it for?

- Mature and fully formed IT security team or a Security Operations Center
- Organizations with a complex and distributed IT environment
- Companies with a low risk appetite due to the high potential costs of security incidents and data breaches

What does it do?

- Optimizes your experts' workloads
- Uplifts their knowledge and skills
- Backs up your experts

Kaspersky Industrial Cybersecurity

KasperskyOS
(Secure Operating System)
- Secure-by-design approach
- Proprietary lightweight microkernel and independent security engine.
- Cyber-Immunity

Kaspersky Industrial CyberSecurity

Authorized to Use CERT™
CERT is a mark owned by Carnegie Mellon University

Kaspersky ICS-CERT

Industrial Systems Emergency Response Team offering expert intelligence and consulting services.

Products

Industrial Secure Gateway

Kaspersky IoT Secure Gateway

Industrial Endpoint Protection

KICS for Nodes

Endpoint protection capabilities:
- Application whitelisting
- Antimalware engine
- Device control
- File Integrity Monitoring
- Exploit Prevention
- Wireless access control
- Log Inspection
- PLC integrity checker
- Ransomware protection
- Firewall

Industrial Anomaly and Breach Detection

Kaspersky Machine Learning for Anomaly Detection

Centralized Security Management

KICS for Networks

Network security capabilities:
- Network Visualization
- Network Activity Monitoring
- Asset Discovery
- Deep Packet Inspection
- Machine Learning for Anomaly Detection
- Remote Access Detection
- Malware Spreading Detection
- Event Correlation
- Safe Non-Invasive Mode
- SOC/SIEM Integration

Kaspersky Security Center

Supported Industrial Endpoints:
- SCADA Servers
- SCADA Clients
- Human Machine Interfaces (HMI)
- Engineering Workstations
- Historians
- OPC Gateways

Services

Training and Awareness

Kaspersky Security Awareness

Kaspersky Security Trainings

Awareness and training programs:
- Industrial Cybersecurity Awareness (1 day)
- Advanced Industrial Cybersecurity in Practice (1-2 days)
- ICS Digital Forensics for Professionals (4 days +)
- ICS Penetration Testing for Professionals (5 days)
- IoT vulnerability research and exploitation training (4 days)
- Capture the flag (CTF) competition
- Become a Trainer – Train the Trainer
- Kaspersky Interactive Protection Simulation (KIPS)

Kaspersky Security Assessment

Expert Services and Intelligence

Kaspersky Incident Response

Kaspersky Threat Intelligence

Expert services features:
- Penetration testing and threat modelling
- Secure network architecture and controls recommendations
- Emergency support to localize incident and digital forensics (available in demand or via subscription)
- ICS Adversary Update Reports (TTPs, targets, attribution)
- Vulnerability database and advisory

Some of the supported devices & protocols

ABB CODESYS EMERSON MITSUBISHI ELECTRIC OMRON Rockwell Automation Schneider Electric SIEMENS YOKOGAWA

Next generation solutions for SMBs

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
- Protect PCs, laptops, mobile devices and file servers
- Default security policies for immediate protection
- The latest, most up-to-date software - always

Kaspersky Optimum Security

The best enterprise-grade security solution

- EDR at the core and an automated Sandbox to work with your endpoint protection
- Prevents employees from exposing themselves, and you, to an attack
- Maximizes the number of incidents processed, without increasing your manpower costs
- Scales easily, securing diverse environments and platforms

Diversity of managed services with Kaspersky

BUILD SERVICES

- Endpoint Protection and hardening
- Vulnerability and Patch Management
- Office365 Protection

- Incident Response
- Security Awareness
- Managed Web and Email Protection

- 24/7 Security Monitoring
- Threat Detection and Response
- Proactive Threat Hunting

MSP

- Kaspersky Endpoint Security for Business
- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365

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

MSSP

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

\+ Kaspersky Managed Detection and Response

KASPERSKY INTELLIGENCE AND EXPERTISE

Automation and integration

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

Knowledge and Expertise

- Kaspersky Cybersecurity Training
- Kaspersky Premium Support and Professional Services

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.

Protection for your children, privacy, identity & mobiles

Kaspersky VPN Secure Connection
Win | Android | Mac | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Security for Android

Best-selling security suites

Kaspersky Total Security
Win | Android | Mac | iOS

Kaspersky Internet Security
Win | Android | Mac

Free apps and utilities

Kaspersky QR Scanner
Android | iOS

Kaspersky Battery Life
Android

Kaspersky Security Cloud Free
Win | Android | iOS

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION

*kaspersky.com/top3

75
Tests/Reviews

57
First Places

84%
Top 3

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.

Kaspersky in the market

Kaspersky B2B Industry Recognitions

Industry Analysts

Partners

Analyst recognition

Kaspersky was recognized as “Global Company of the Year” in the Industrial (OT/ICS) Cybersecurity Market by Frost and Sullivan*.

* Frost and Sullivan 2020 Global Industrial (OT/ICS) Cybersecurity market analysis.
Read the full analysis and evaluation here: https://www.kaspersky.com/acq-lp/kicsaward2020-ungated

Kaspersky has been ranked for the quality of its partner program in the Canalys Worldwide Vendor Benchmark* for the second consecutive year with an increase of +12.7% in the overall partner rating.

The benchmark is an objective comparison of channel partner programs, measuring how vendors perform in a number of key categories. Kaspersky received over 679 reviews from the channel for its program, an increase of 588% over the past 12 months.

* Canalys worldwide vendor benchmark report, December 2020.

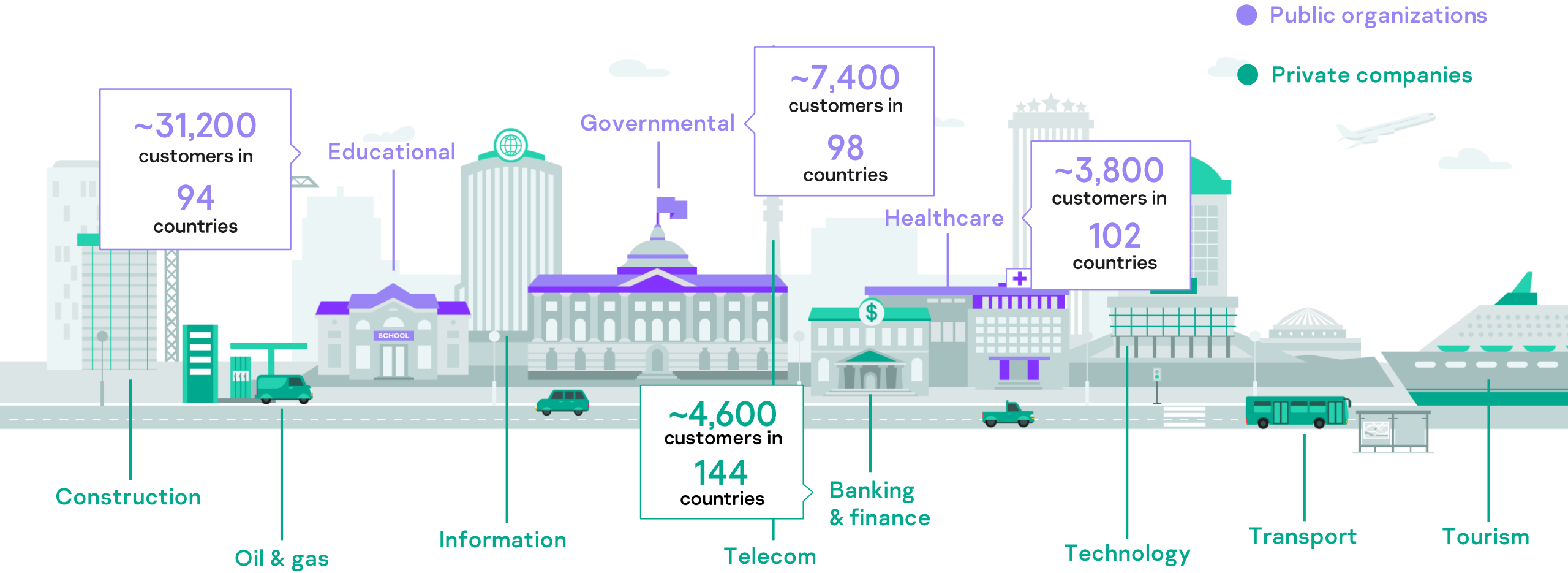
Analyst recognition

Kaspersky named Champion for the second consecutive year in the 2021 Canalys Global Cybersecurity Matrix*.

Champion status recognizes vendors demonstrating the highest level of excellence in channel management. Kaspersky was rated to have the highest global channel feedback score of 87.5% ahead of all vendors.

* Canalys Global Cybersecurity Matrix 2021. Access the report: https://media.kaspersky.com/en/canalys-global-cybersecurity-leadership-matrix-2021.pdf

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



ESG

As we work to create a safer future, we are concerned about the well-being of the world not only in the context of its digital reality. Gender equality, accessible knowledge, volunteering, child safety, animal protection and more are all issues that are crucial for us.

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

We cooperate with non-profit organizations, support charity initiatives and create our own social programs.
Read Kaspersky CSR report here.

Women in Tech

Kaspersky runs an Internet community called Women in CyberSecurity that helps supercharge the career growth of women entering the cybersecurity industry and those already working in the field. The company also hosts Empower Women project aimed at supporting the career growth of women who are up for the challenge of protecting the world from cyber threats by sharing role models.

Fighting against stalkerware

In November 2019, Kaspersky with nine other organizations from IT Security industry and non-profit sector launched the Coalition Against Stalkerware as a global initiative to protect users against stalking and domestic violence. Supported by INTERPOL, it unites more than 40 partners today.

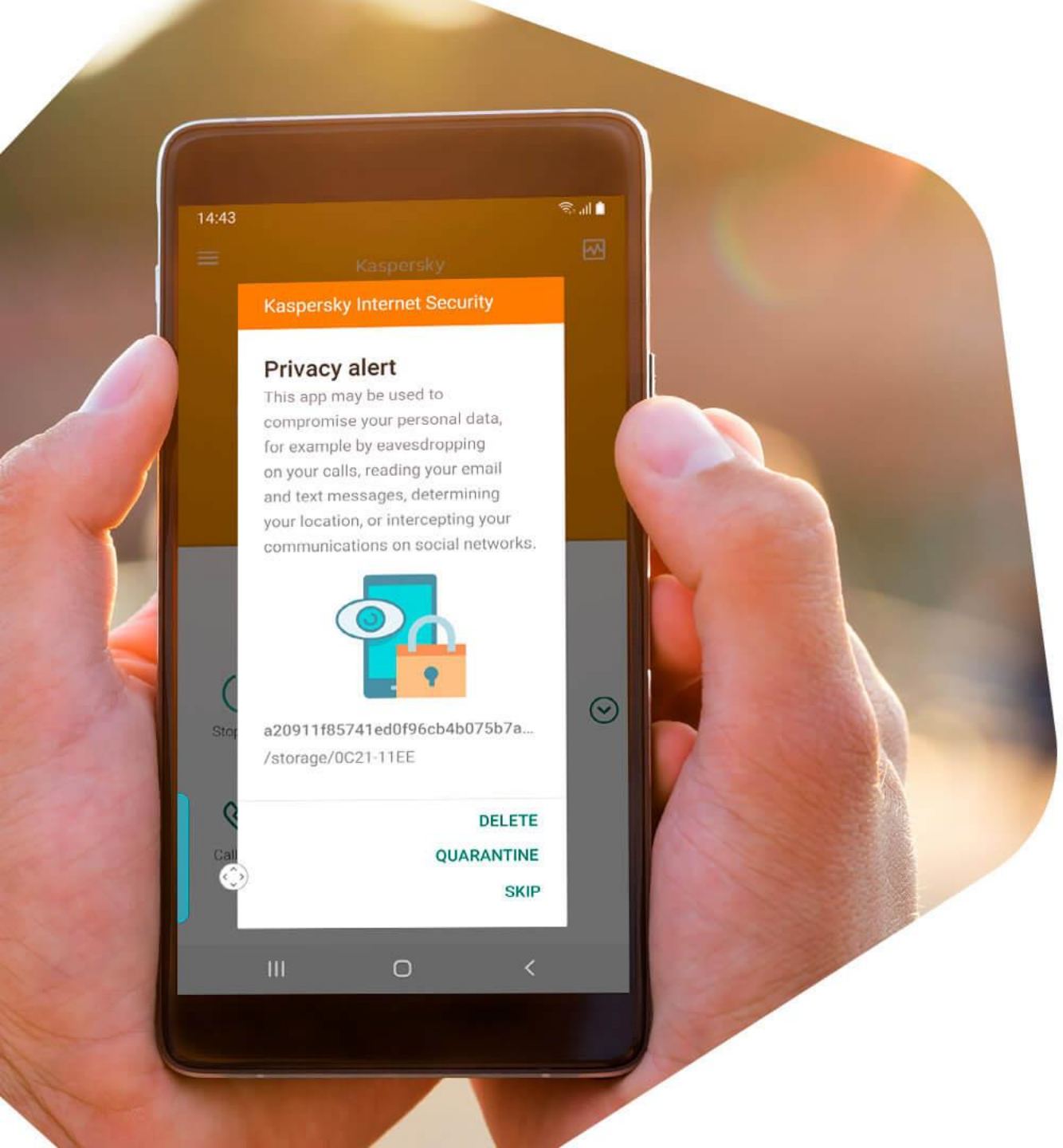
Already since April 2019 our users of Kaspersky Internet Security for Android receive a Privacy Alert – a specially designed notification to warn the user if their private information is being covertly monitored by a third party.

Preserving the World

We understand the importance of preserving past cultures, for the benefit of future generations. That is why Kaspersky has been cooperating with the Archeological Society at Athens (ASA) since 2015, to develop its Akrotiri project. This project is dedicated to saving the remains of the historic Cycladic/Minoan settlement on Santorini Island – widely known as the Greek “Pompeii”.

Women in Tech

Kaspersky runs an Internet community called Women in CyberSecurity that helps supercharge the career growth of women entering the cybersecurity industry and those already working in the field. The company also hosts Empower Women project aimed at supporting the career growth of women who are up for the challenge of protecting the world from cyber threats by sharing role models..



Fighting against stalkerware

Kaspersky is at the forefront of protecting victims of stalkerware. Kaspersky supports NGOs, law enforcement agencies, regulators and researchers by sharing its technical knowledge on stalkerware, conducting training and contributing to the discussions on definition, identification criteria, statistics and trends.

In 2019, Kaspersky and nine other organizations working with victims, perpetrators, or in the IT security industry launched the Coalition Against Stalkerware, to protect users against cyberstalking and domestic violence. Supported by INTERPOL, it unites more than 40 partners now.

In 2020, our GReAT researchers developed TinyCheck, an easy to use, open-source tool detecting stalkerware and spyware.

Since 2021, Kaspersky has been part of the EU-wide 'DeStalk' project, supporting the European Commission's Rights, Equality and Citizenship Program.

Preserving the World

We understand the importance of preserving past cultures, for the benefit of future generations. That is why Kaspersky has been cooperating with the Archeological Society at Athens (ASA) since 2015, to develop its Akrotiri project. This project is dedicated to saving the remains of the historic Cycladic/Minoan settlement on Santorini Island – widely known as the Greek “Pompeii”. The company has become the major sponsor of the project, providing support for a number of activities to help the scientists advance their work. This includes the restoration of excavations, the conservation of spectacular wall paintings and the project’s architectural conservation work.

Preserving the World

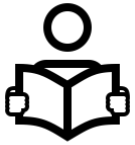
In July 2019 Kaspersky sponsored the Kuril Islands expedition with a renowned team of environmentalists, film makers and photographers, aimed to give people the opportunity to explore the remarkable nature of the isolated islands and bring attention to the current ecological situation faced by the region.

Kaspersky has also supported the fundraising initiative organized by Dr. Burkanov and members of the expedition team, aimed at collecting robust environmental data that will help to inform sound policy and scientific projections of the future. To date over $40,000 have been raised.

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 different ages and professions all around the world about cybersecurity.



School

Kaspersky intends to educate young users about being safe online. We globally distribute the children's book 'Midori Kuma and a Very Special Race', written by well-known children's book author and journalist Alessia Cruciani.

We have a Kaspersky School project in Moscow, Russia, aimed at giving schoolchildren a foundational base in mathematics. The project is also intended to educate schoolchildren and teachers about the basics of cybersecurity.

University

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

The company supports young talent in IT, including organizing the Safeboard Global internship program, the Secur'IT Cup student competition and contributing to the development of top-notch educational cybersecurity programs.

Business

Kaspersky collaborates with business schools, such as INSEAD, one of the of the top three schools for Executive Education and leading MBA programs in the world, to introduce students to the cybersecurity world through keynote lectures.

Within the framework of the Kaspersky.Academy project, we offer an MBA training course aimed at increasing knowledge of information security and the development of organizational security policies.

School

Kaspersky intends to educate young users about being safe online. We globally distribute the children's book 'Midori Kuma and a Very Special Race', written by well-known children's book author and journalist Alessia Cruciani.

We have a Kaspersky School project in Moscow, Russia, aimed at giving schoolchildren a foundational base in mathematics. The project is also intended to educate schoolchildren and teachers about the basics of cybersecurity.

University

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

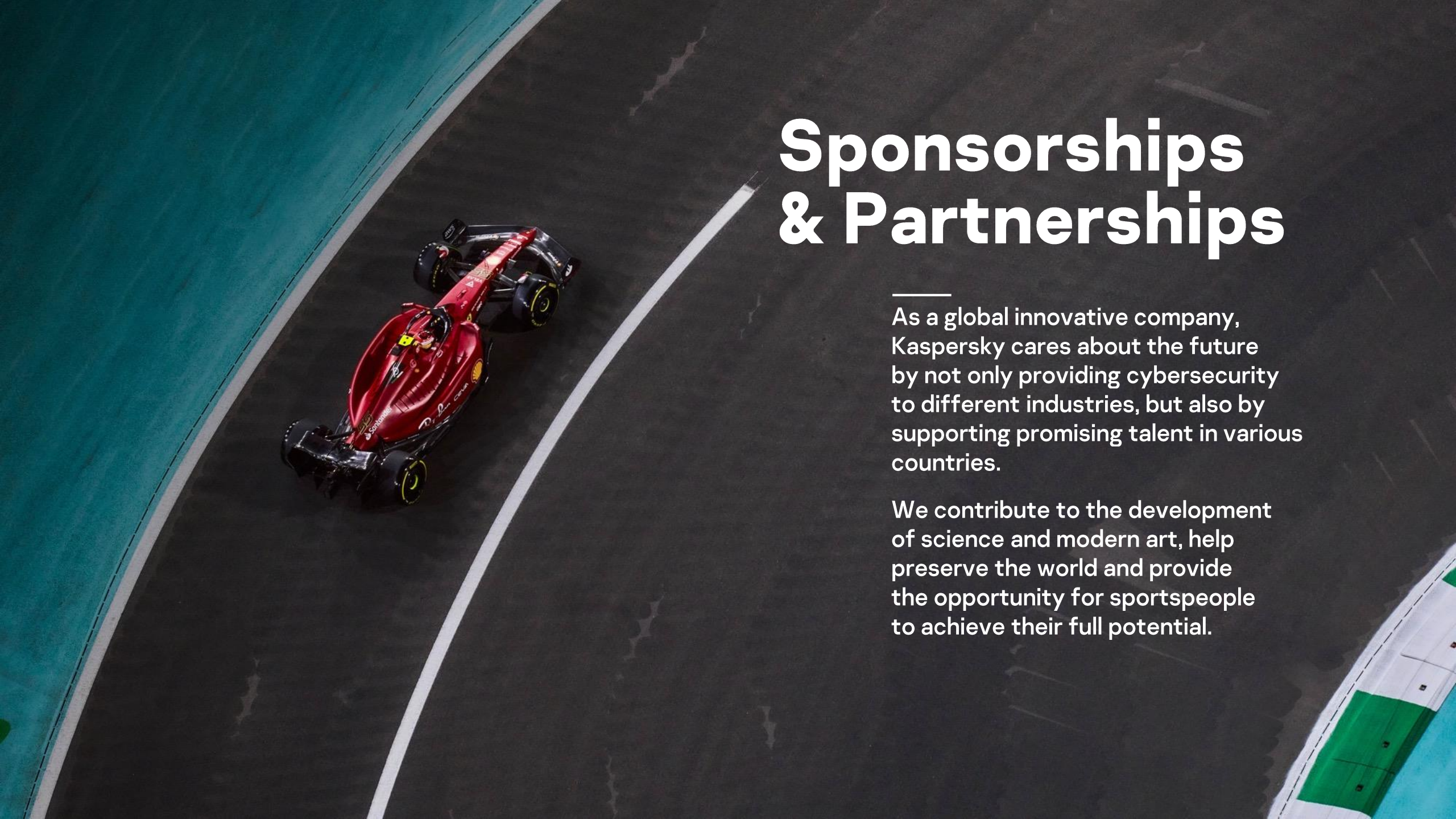
The company supports young talent in IT, including organizing the Safeboard Global internship program, the Secur'IT Cup student competition and contributing to the development of top-notch educational cybersecurity programs.

Business

Today we are witnessing growing business concerns about cybersecurity, and we are proud to share our expertise with top managers from various industries. Kaspersky collaborates with business schools, such as INSEAD, one of the top three schools for Executive Education and leading MBA programs in the world, to introduce students to the cybersecurity world through keynote lectures.

Within the framework of the Kaspersky.Academy project, we offer an MBA training course aimed at increasing knowledge of information security and the development of organizational security policies.

Photo: Maxence Torilloux for INSEAD



Sponsorships & Partnerships

As a global innovative company, Kaspersky cares about the future by not only providing cybersecurity to different industries, but also by supporting promising talent in various countries.

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

Sponsorships & Partnerships

Sport

We have built a strong relationship with Scuderia Ferrari by sponsoring them in Formula One as well as their Esport team and the official Ferrari Esport Series.
In 2021 we became a sponsor of Aprilia Racing competing in the MotoGP championship. In addition, the company supports talented drivers across various other racing series, such as Amna and Hamda Al Qubaisi, first emirati female drivers.

Science & Space

Kaspersky was a strategic partner of the Gagarin Research and Test Cosmonaut Training Center, located in Star City, Russia, where cosmonauts from all over the world prepare to go to space. Moreover, the company has supported Starmus – the world's most ambitious science and music festival.

Chess

Kaspersky is an official cybersecurity partner of the FIDE World Championship series – the world's most prestigious chess tournament, and provides complex protection for the FIDE Online Arena gaming platform.

The company also supports young chess players including Andrey Tsvetkov.

Art

Kaspersky is a partner of the Moniker International Art Fair in London, and it supports special commissions from internationally-acclaimed artists such as Ben Eine. Additionally, we worked on a significant creative collaboration with renown street artists D*Face, SHOCK-1 and Felipe Pantone.

Sports

We have built a strong relationships with Scuderia Ferrari by sponsoring them in Formula One as well as their Esport team and the official Ferrari Esport Series.

In 2021 we became a sponsor of Aprilia Racing – one of the most successful teams in motorcycle racing history – competing in the MotoGP championship.

In addition, the company supports talented drivers across various other racing series, such as Amna and Hamda Al Qubaisi, first Emirati female drivers.

Chess

Kaspersky is an official cybersecurity partner of the FIDE World Championship series — the world's most prestigious chess tournament, and provides complex protection for the FIDE Online Arena gaming platform.

The company also supports young chess players including Andrey Tsvetkov.

Science & Space

Kaspersky was a strategic partner of the Gagarin Research and Test Cosmonaut Training Center, located in Star City, Russia, where cosmonauts from all over the world prepare to go to space. Moreover, the company has supported Starmus – the world's most ambitious science and music festival.

Art

Kaspersky is a partner of the Moniker International Art Fair in London, and it supports special commissions from internationally-acclaimed artists, such as Ben Eine. We worked on a significant creative collaboration with British multimedia street artist D*Face.

At the 10th Anniversary of Moniker International in 2019, we unveiled an artistic collaboration with the British street artist SHOK-1, famous for his X-ray paintings. In 2021 Kaspersky teamed up with contemporary artist Felipe Pantone to raise awareness on Data Privacy Day.

Gaming and eSports

As a company with a mission to build a safer world, Kaspersky is committed to ensuring that gamers safely enjoy the best of their gaming experiences. Kaspersky has previously partnered with the high-performance eSports brand Fnatic and is currently a partner of Ferrari's Esport team. Our company has been also a partner of the European Speedrunner Assembly - the largest organizer of speedrunning* festivals in Europe.

Kaspersky is a partner of the Real Race eSports.Lamborghini competition 2021 — a global esports races for players of all levels on Assetto Corsa Competizione.

* Speedrunning – a type of gaming where players compete to complete a game or a level as fast as possible.

Thank you!

kaspersky