Kaspersky Corporate Kit

kaspersky

Updated: November 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

Bring on the future

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

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.

>240,000
Corporate clients worldwide

>400,000,000
Users worldwide are protected by our technologies

Enterprises

Industrial facilities

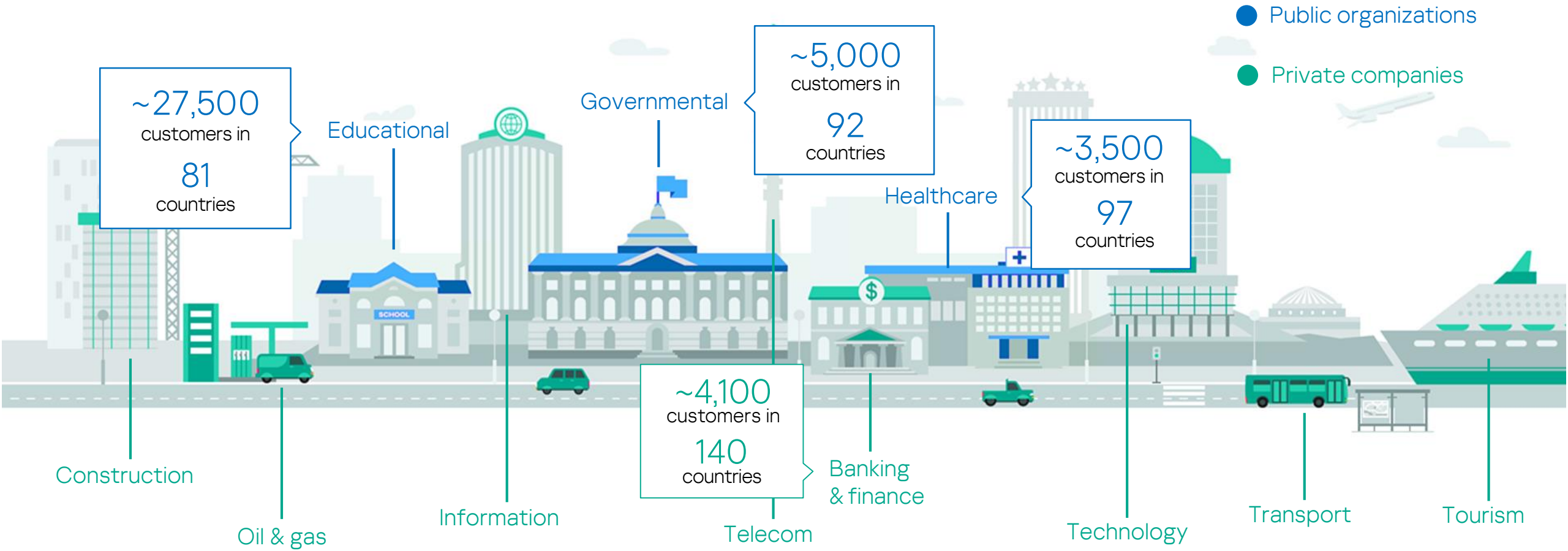
Small and medium businesses

Very small businesses

Consumers

Our customers

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

Our role in the global IT security community

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

INTERPOL

Learn more

Coalition Against Stalkerware

Learn more

PARIS CALL
FOR TRUST AND SECURITY IN CYBERSPACE
11 • 12 • 2018

Learn more

industrial internet CONSORTIUM

Learn more

Global Transparency Initiative

- Key transparency principles
- Global Transparency Initiative
- Independent assessments and certifications
- Bug Bounty Program

Our key 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 international organizations to fight cybercrime.

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

We cooperate with the IT security industry in joint cybercrime investigations.

Global Transparency Initiative

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

It includes a number of actionable and concrete measures:

Cyberthreat-related data infrastructure relocation to Switzerland.

Creation of a global network of Transparency Centers in some regions, where Kaspersky's trusted partners and government stakeholders can review the company's code, software updates and threat detection rules.

Third-party security assessments of Kaspersky's engineering and data management practices 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, softwvare updates and threat detection rules, along with other activities.

Independent reviews

Regular third-party assessment of internal protcesses to confirm the security of Kaspersky's processes and systems, including:

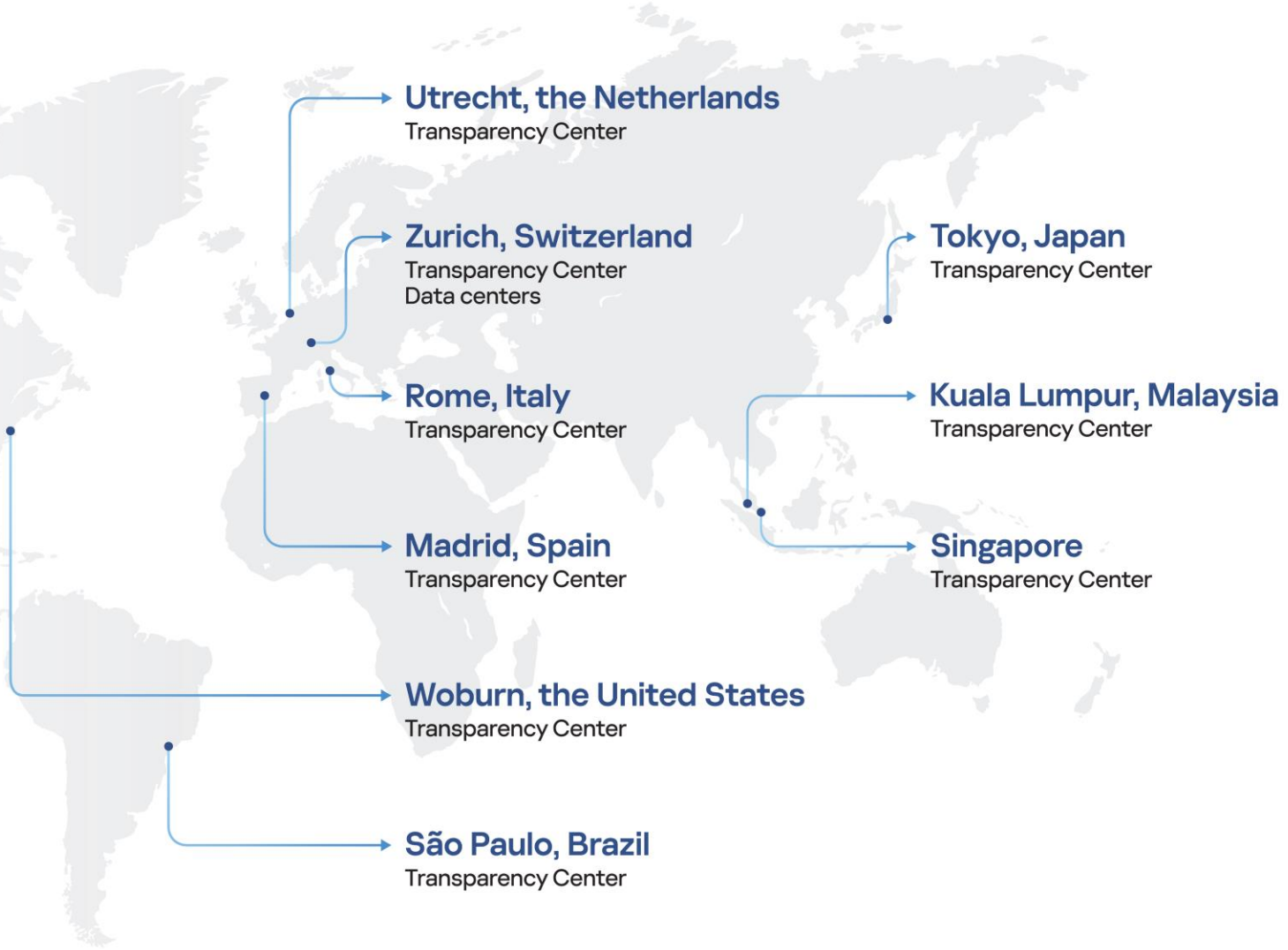
- SOC 2 audits by a Big Four firm
- ISO 27001 certifications for the company's data systems

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)

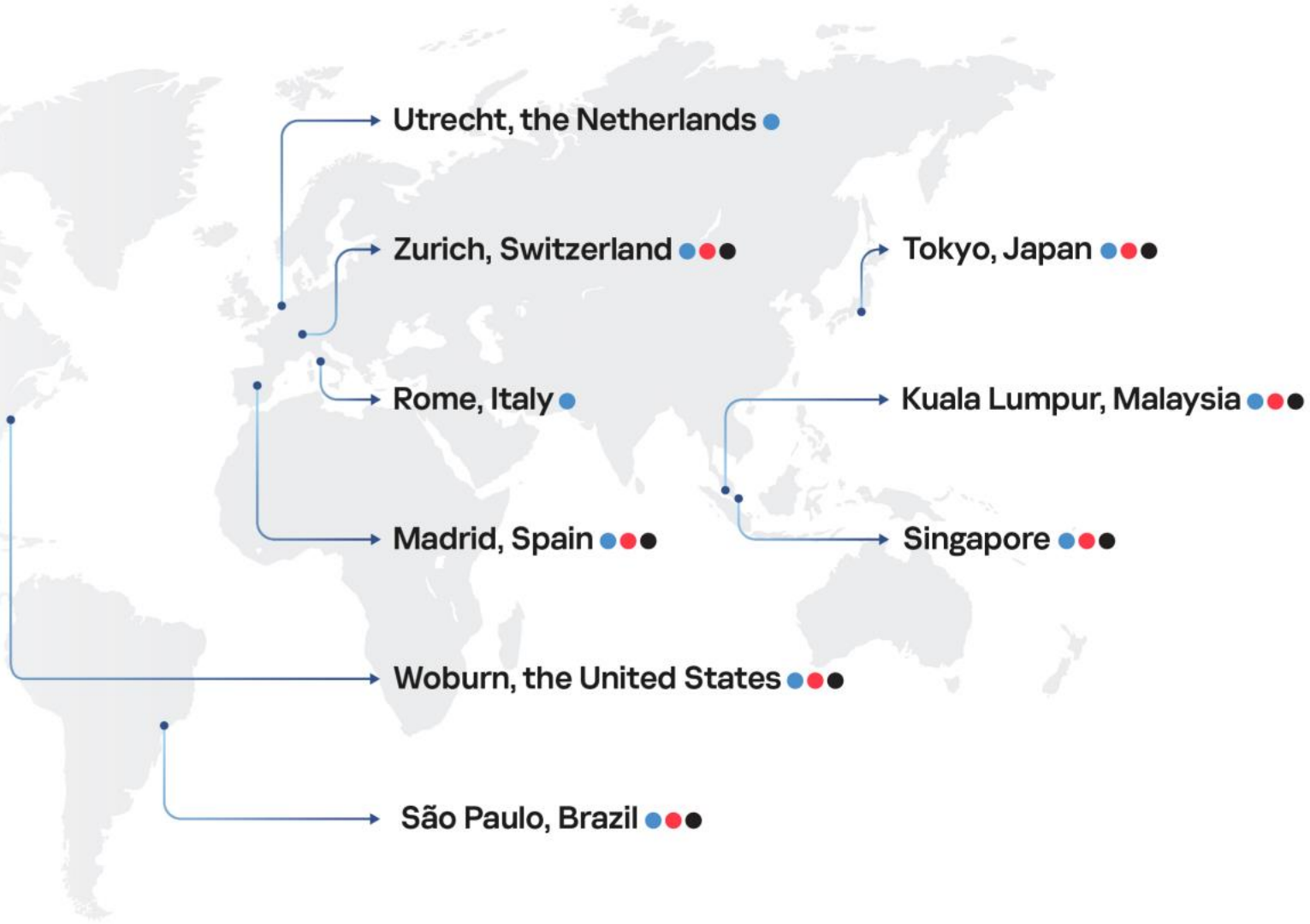
An overview of Kaspersky's transparency practices, products and services, as well as data management practices.

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

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.

Learn more

ISO/IEC 27001

The most widely used information security standard prepared and published by the International Organization for Standardization (ISO), the world's largest developer of voluntary international standards. Information security management system of Kaspersky has been certified against ISO/IEC 27001:2013 international standard.

Learn more

Bug Bounty Program

Kaspersky is committed to the principles of ethical vulnerability disclosure approach. To ensure the integrity of our products, Kaspersky has been running its public bug bounty program since 2016. 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).

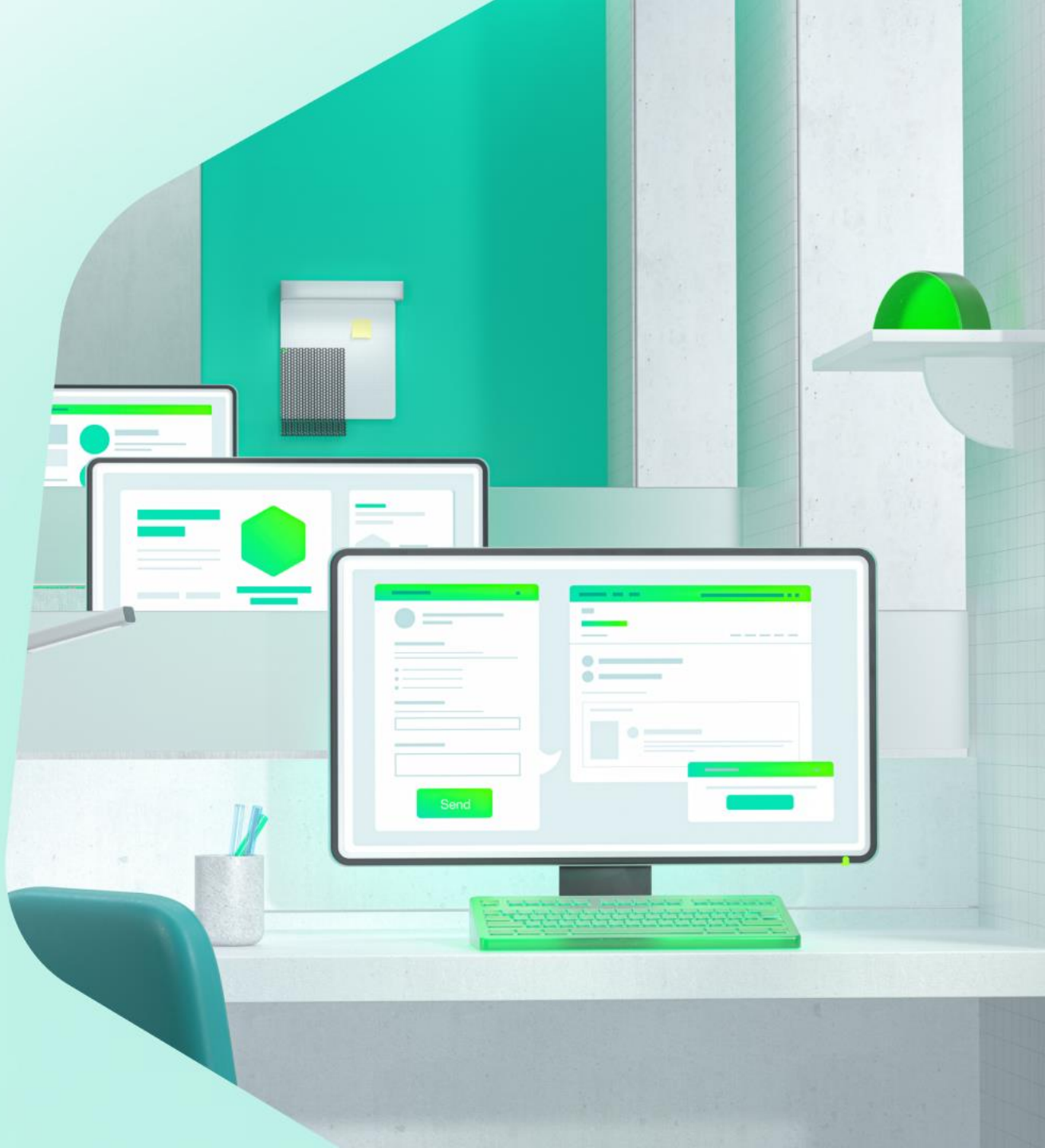
$5,000 – $20,000
for the discovery of vulnerabilities allowing different and less severe types of remote code execution.

$1,000 – $5,000
for discovery of bugs allowing local privilege escalation, or leading to sensitive data disclosure.

Learn more

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

Threat research

>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.

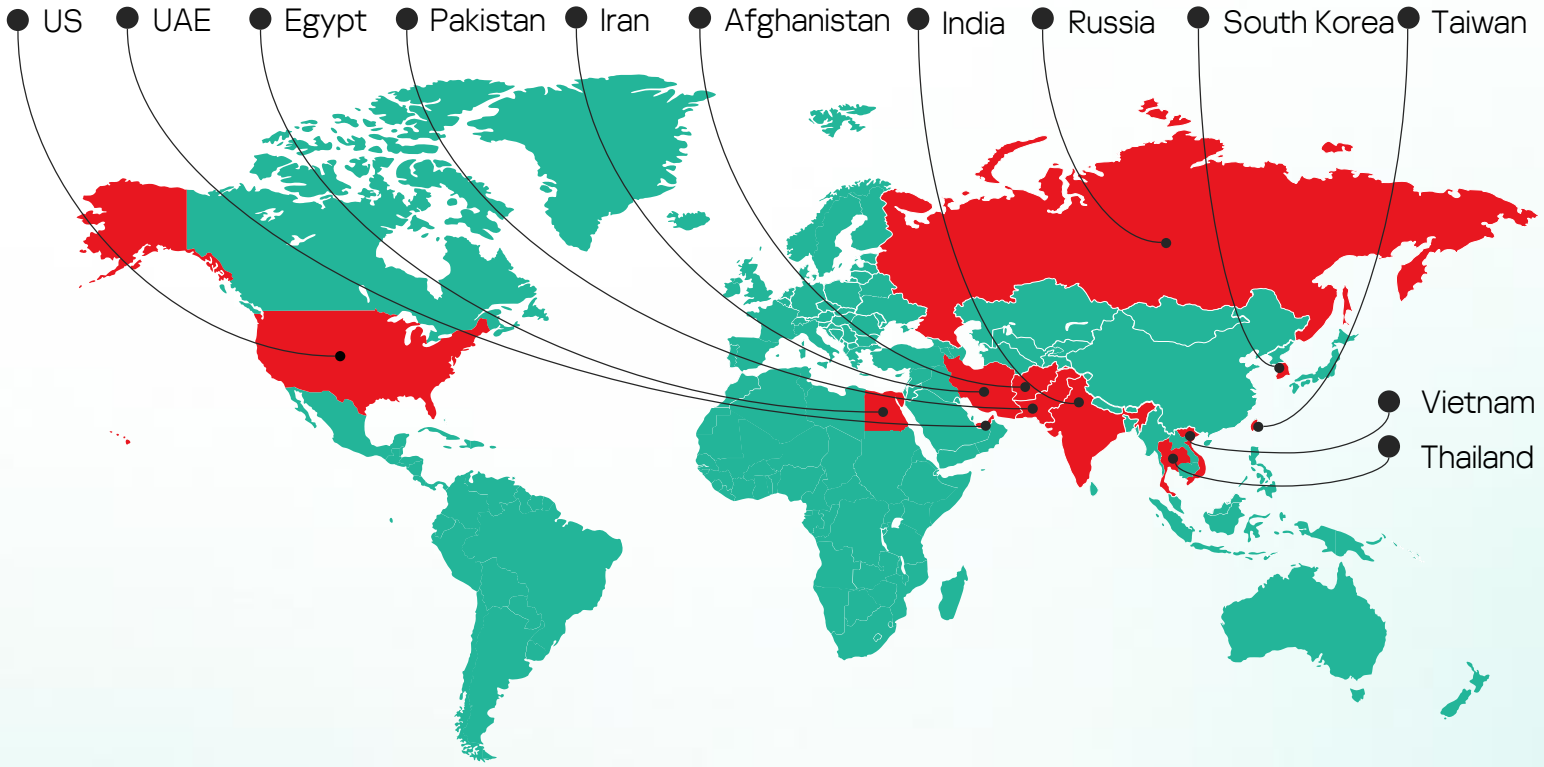
Top 10 targets

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

Top 10 significant threat actors

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

Top 12 targeted countries



apt.securelist.com

Based on the data up to 31.12.2021

Our major discoveries and research

	Sofacy	Duqu 2.0	Lazarus	Project Sauron	Expetr/ Notpetya	Shadowpad	Olympic destroyer	Shadow hammer	Tajmahal	Mosaic-regressor	Ghostemperor
Detection	2014	2015	2016	2016	2017	2017	2018	2018	2019	2020	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
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 Telecommunication companies
	Link	Link	Link	Link	Link	Link	Link	Link	Link	Link	Link

Targeted attack research

2016

- ProjectSauron
- StrongPity
- Lazarus
- Fruity Armor
- ScarCruft
- Poseidon
- Danti
- Dropping Elephant

2017

- WannaCry
- Shamoon 2.0
- StoneDrill
- BlueNoroff
- ExPetr/NotPetya
- Moonlight Maze
- ShadowPad
- BlackOasis
- Silence
- WhiteBear

2018

- Zebrocy
- DarkTequila
- MuddyWater
- Skygofree
- Olympic Destroyer
- ZooPark
- Hades
- Octopus
- AppleJeus

2019

- Topinambour
- ShadowHammer
- SneakyPastes
- FinSpy
- DarkUniverse
- COMpfun
- Titanium

2020

- Cycldek
- SixLittleMonkeys (aka Microcin)
- CactusPete
- DeathStalker
- MATA
- TransparentTribe
- WellMess
- TwoSail Junk
- MontysThree
- MosaicRegressor
- VHD Ransomware
- WildPressure
- PhantomLance

2021

- GhostEmperor
- ExCone
- BlackShadow
- BountyGlad
- EdwardsPhesant
- HotCousin
- GoldenJackal
- FerociousKitten
- ReconHellcat
- CoughingDown
- MysterySnail
- CraneLand

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

Learn more

Privacy checklist

Easy to grasp definitive checklist for those who care about their privacy

Learn more

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

Learn more

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

KasperskyOS

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.

IoT & Industrial IoT

Controllers for smart cities

Virtual desktop infrastructure

Transportation

Professional mobile devices

Trusted execution environment

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 Enterprise Solutions

Targeted Solutions

- Kaspersky Industrial CyberSecurity
- Kaspersky Fraud Prevention
- Kaspersky Research Sandbox
- Kaspersky Threat Attribution Engine
- Kaspersky Private Security Network

Stage 3

Complex and apt-like attacks

Expert Security

Mature IT security capability or a SOC team

- Internal Expertise
  - Kaspersky Cybersecurity Training
- Intelligence
  - Kaspersky Threat Intelligence
- Extended Detection and Response
  - Kaspersky Endpoint Detection and Response Expert
  - Kaspersky Anti Targeted Attack
- Assessment
  - Kaspersky Security Assessment
- External Guidance
  - Kaspersky Incident Response
- People
  - Kaspersky Security Awareness Ultimate

Stage2

Evasive threats

Optimum Security

IT Security

- People
  - Kaspersky Security Awareness Advanced
- Visibility and response
  - Kaspersky Endpoint Detection and Response Optimum
- Detection Enrichment
  - Kaspersky Threat Intelligence Portal

Stage 1

Commodity Threats

Security Foundations

IT

- Endpoint
  - Kaspersky Endpoint Security for Business
  - Kaspersky Embedded Systems Security
  - Kaspersky Hybrid Cloud Security
- Network
  - Kaspersky Security for Mail Server
  - Kaspersky Security for Internet Gateway
- Data
  - Kaspersky Security for Storage
- People
  - Kaspersky Security Awareness Essential
- Support
  - Kaspersky Premium Support and Professional Services

Kaspersky Managed Detection and Response

Kaspersky Industrial Cybersecurity Solution

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
- **Industrial Anomaly and Breach Detection**
  - Kaspersky Machine Learning for Anomaly Detection
- **Centralized Security Management**
  - KICS for Networks
  - Kaspersky Security Center

Services

- **Training and Awareness**
  - Kaspersky Security Awareness
  - Kaspersky Security Trainings
- **Expert Services and Intelligence**
  - Kaspersky Security Assessment
  - Kaspersky Incident Response
  - Kaspersky Threat Intelligence

Some of the supported devices & protocols

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

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

- 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 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

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 Safe Kids
Win | Android | Mac | iOS

Kaspersky QR Scanner
Android | iOS

Kaspersky Battery Life
Android

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**.

Learn more

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

Recognitions

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.

ESG

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.

ESG

Women in Tech

As a cybersecurity company, we play a key role in tackling the gender gap issue and ensuring that real progress is happening.

Learn more

Fighting against stalkerware

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.

Learn more

Preserving the World

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).

Learn more

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.

Education

School

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.

Learn more

University

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

Learn more

Business

Kaspersky collaborates with business schools to deliver courses on information security for business leaders, top managers and senior executives.

Learn more

Sponsorships & Partnerships

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.

Learn more

Science & Space

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

Learn more

Art

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

Learn more

Gaming

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

Learn more

Motorsport

Kaspersky is sponsoring Aprilia Racing, one of the most decorated brands in motorcycle racing history.

Learn more

Bring on the future