

# Kaspersky Corporate Kit

**kaspersky**

Updated: April 2024



# Our mission is simple — building a safer world.

We do that by becoming the global leader in cybersecurity. By securing technology we ensure that it stays free of cyberthreats — providing nothing but positive possibilities for everyone.

**Bring on endless possibilities.  
Bring on a safer tomorrow.**

Eugene Kaspersky, CEO

# Our key values that drive our work



## Be there for you

We'll always be there for you, for our customers, partners, prospects & colleagues. We **never lose sight of the people** we build our solutions for.



## Be committed experts

Through our **recognized technology expertise**, we are committed to providing **trust, safety and confidence**. We never give up on our mission to make the digital world a safer place. And on this duty we always play fair.



## Be cleverly inventive

Focused and ready to act – we share cutting-edge information with customers, partners, colleagues and prospects to keep them ahead of the curve.



## Be powered by challenges

We constantly challenge ourselves and the status quo to **do what others can't**. We deliver outstanding solutions to overcome obstacles of all kinds, and **this is proven** across our 25-year history.

# 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 six continents in more  
than 200 countries and territories

Provides innovative IT security  
solutions and services for  
businesses and consumers

# Numbers

**> 13 million**

consumer product activations per year

**> 5,000**

highly qualified specialists

**US \$752 million**

global non-audited IFRS revenue in 2022

## 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.

# >220,000

Corporate clients worldwide choose our protection

# 1,000,000,000

Devices protected by Kaspersky to date\*



Enterprises



Industrial facilities



Small and medium businesses



Very small businesses

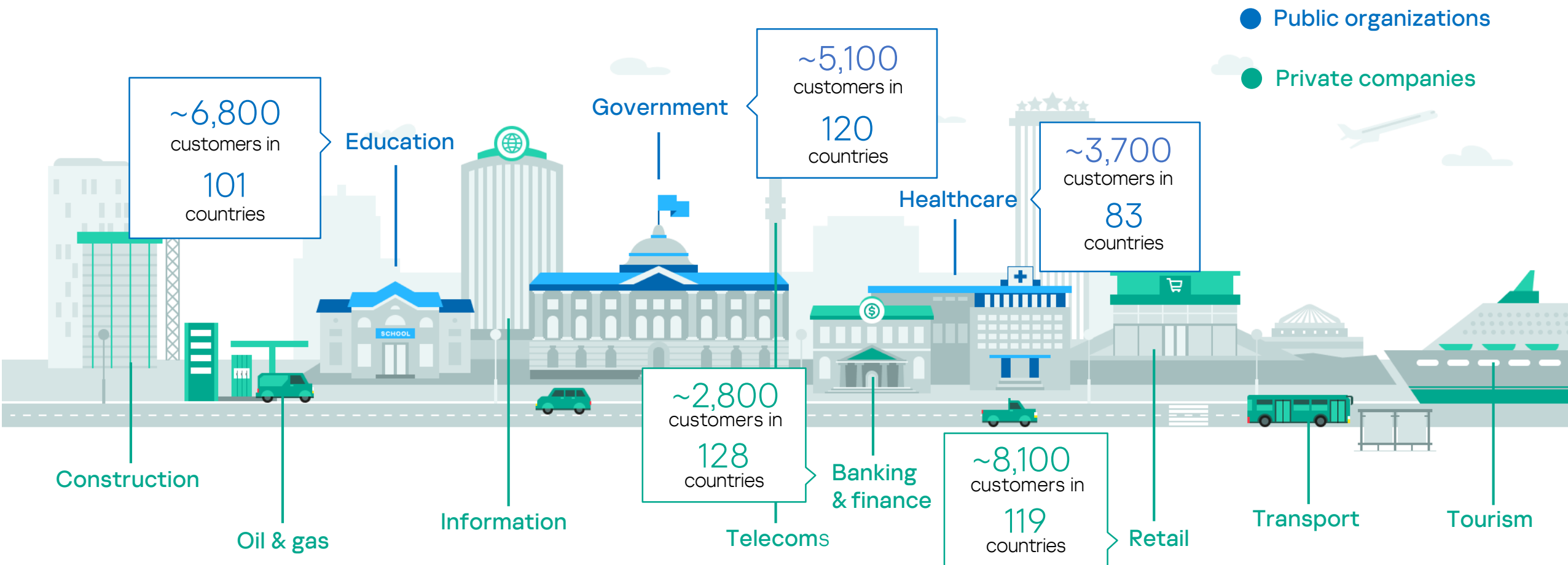


Consumers

\*The figure is based on the data of Kaspersky Security Network (KSN) for automated malware analysis and includes records starting from 2011, when the system was rolled out.

## Our customers

We work in a wide range of industry sectors. Our solutions and services successfully protect over 220,000 clients around the world, regardless of size or complexity





## We are an international cybersecurity company



**200** countries and territories  
where we operate



**30+** representative  
regional offices



### Africa

South Africa  
Kenya  
Rwanda

### Asia

Greater China  
(China, Hong  
Kong)  
India  
Japan  
Kazakhstan  
Malaysia  
Singapore  
South Korea

### Transparency Centers

Zurich, Switzerland  
Madrid, Spain  
São Paulo, Brazil  
Kuala Lumpur, Malaysia  
Woburn, USA  
Kigali, Rwanda

### Europe

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

### Middle East

Saudi Arabia  
Turkey  
UAE

### North America

USA

### Latin America

Brazil  
Mexico

Singapore  
Tokyo, Japan  
Rome, Italy  
Utrecht, the Netherlands  
Riyadh, Saudi Arabia



## 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](#)



[Learn more](#)



[Learn more](#)



[Learn more](#)

# Global Transparency Initiative

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



## Our key transparency principles



Data sent to Kaspersky is crucial for protecting users, it is robustly secured 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 pillars

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.

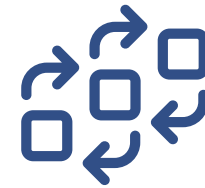
**It includes a number of actionable and concrete measures:**



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 verify the security of the company's solutions.

## Global Transparency Initiative pillars

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.



Cyber Capacity Building Program – dedicated training to share security evaluation knowledge with the 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:

- Regular SOC 2 audits
- ISO 27001 certifications for the company's data systems



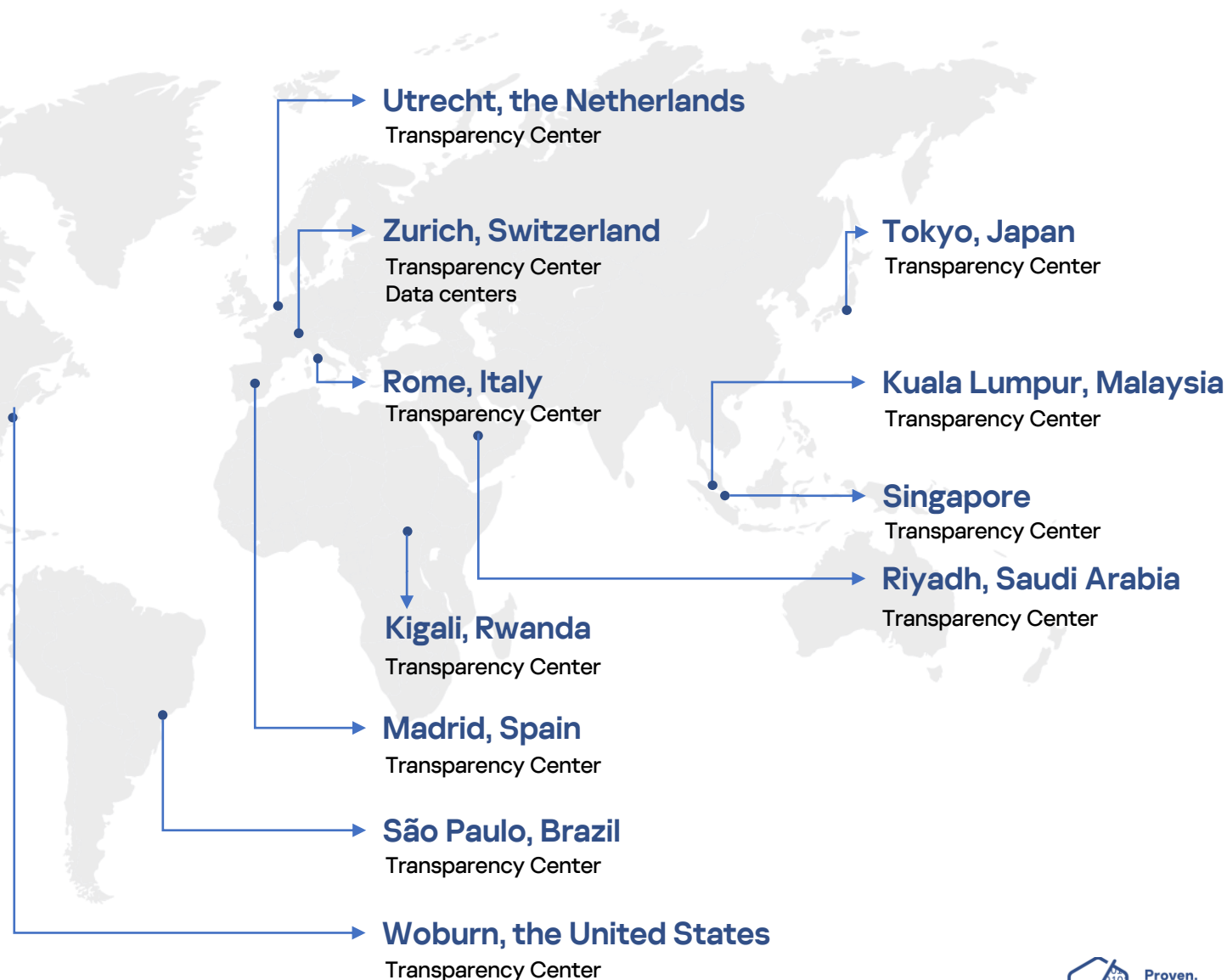
### Bug bounty program

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)

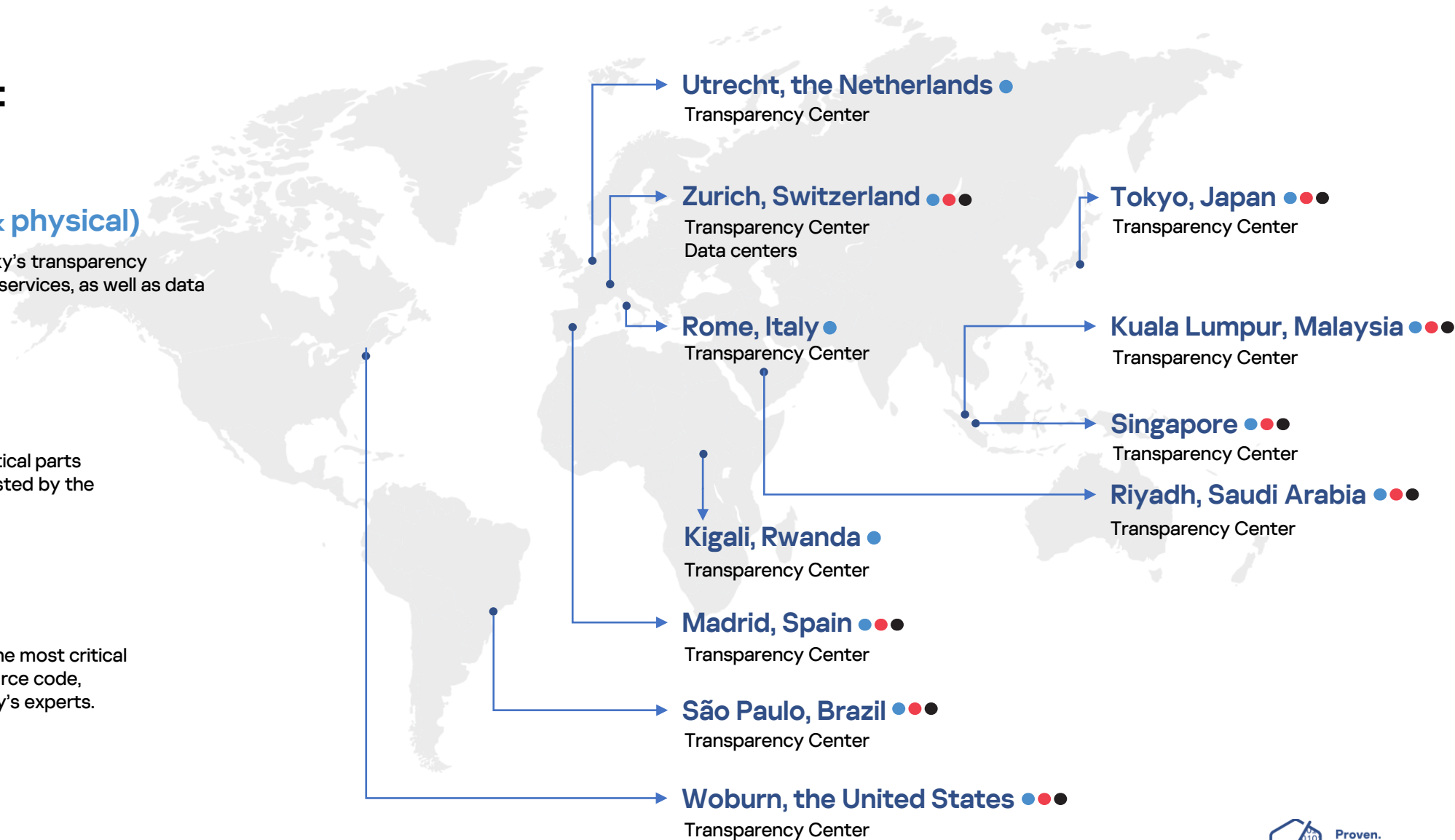
An overview of Kaspersky's transparency practices, products and services, as well as data management practices.

### 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



in Switzerland: globally known as a neutral country, it contains strict data protection regulation.

Here we process and store cyberthreat-related user data from Europe, North and Latin America, the Middle East, and several countries in Asia-Pacific region.



in Brazil, Italy, Japan, Malaysia, the Netherlands, Singapore, Rwanda, Spain, Switzerland, Saudi Arabia, and the United States



confirming the trustworthiness of Kaspersky's engineering practices::

- SOC 2 audit
- ISO 27001 certification



Since 2018, Kaspersky has invested over \$8.4 million in the program, which includes \$5.6 million for equipment for the data centers in Zurich.



by public and private stakeholders



with total payments equal to \$81,750

## 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 passed a comprehensive SOC 2 Type 2 audit in 2023.

[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. Kaspersky's information security management system 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, and since 2022, it operates on the [Yogosha platform](#). The company also supports the Disclose.io framework, which provides a “Safe Harbor” for vulnerability researchers concerned about the negative legal consequences of their discoveries.

## Rewards

### \$100,000

for the discovery and coordinated disclosure of severe vulnerabilities (high-quality reports with PoC).

### \$5,000 – \$20,000

for the discovery of vulnerabilities allowing different and less severe types of remote code execution.

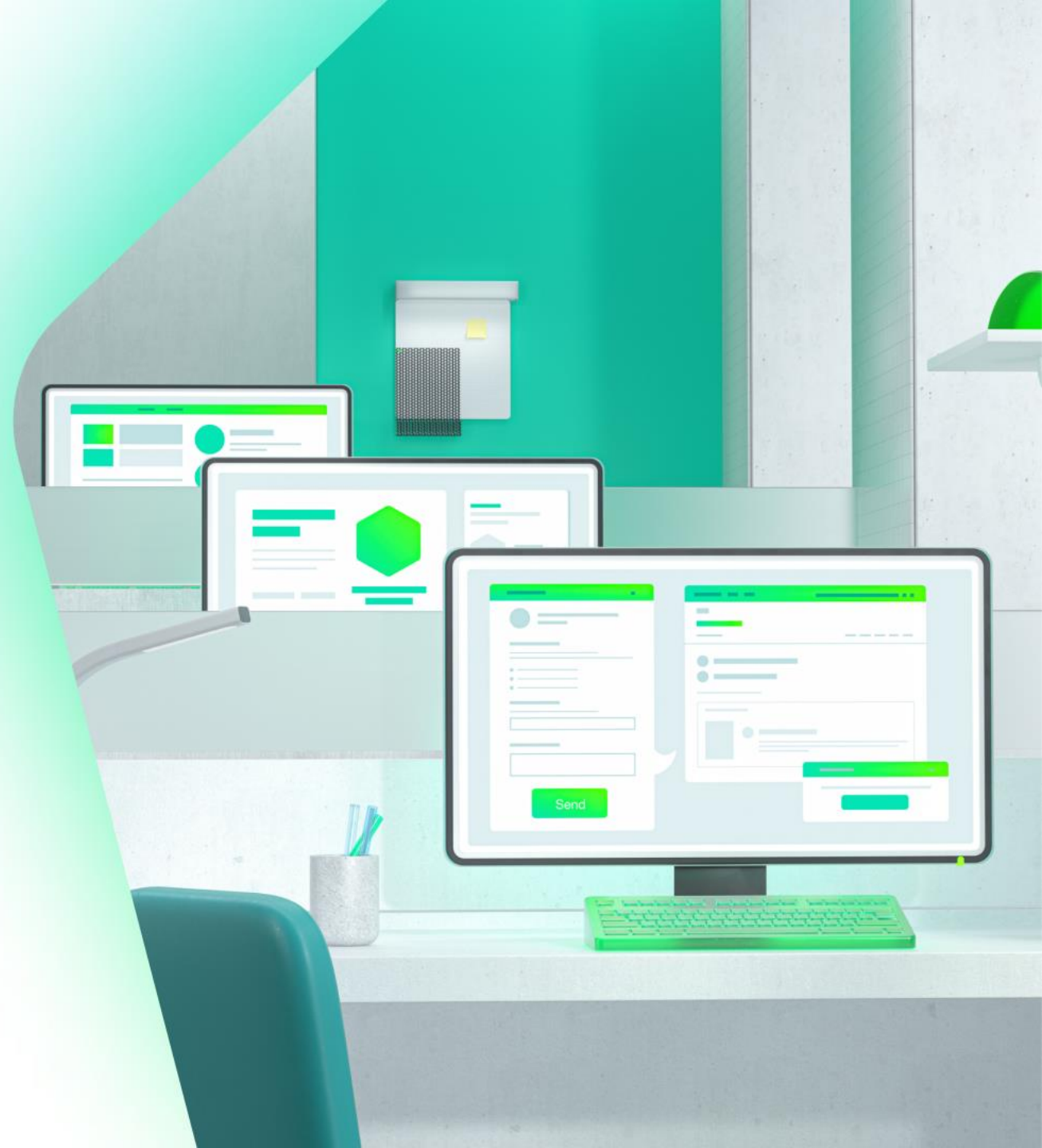
### \$1,000 – \$5,000

for the 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.

**>5,000** Highly-qualified specialists

**50%** of our employees are R&D specialists

**35+** Members in our group of elite world-leading security experts - GREAT





## Threat research

# >1,400,000,000

## cyberthreats

detected by Kaspersky since  
the company's inception

# 6,100,000,000

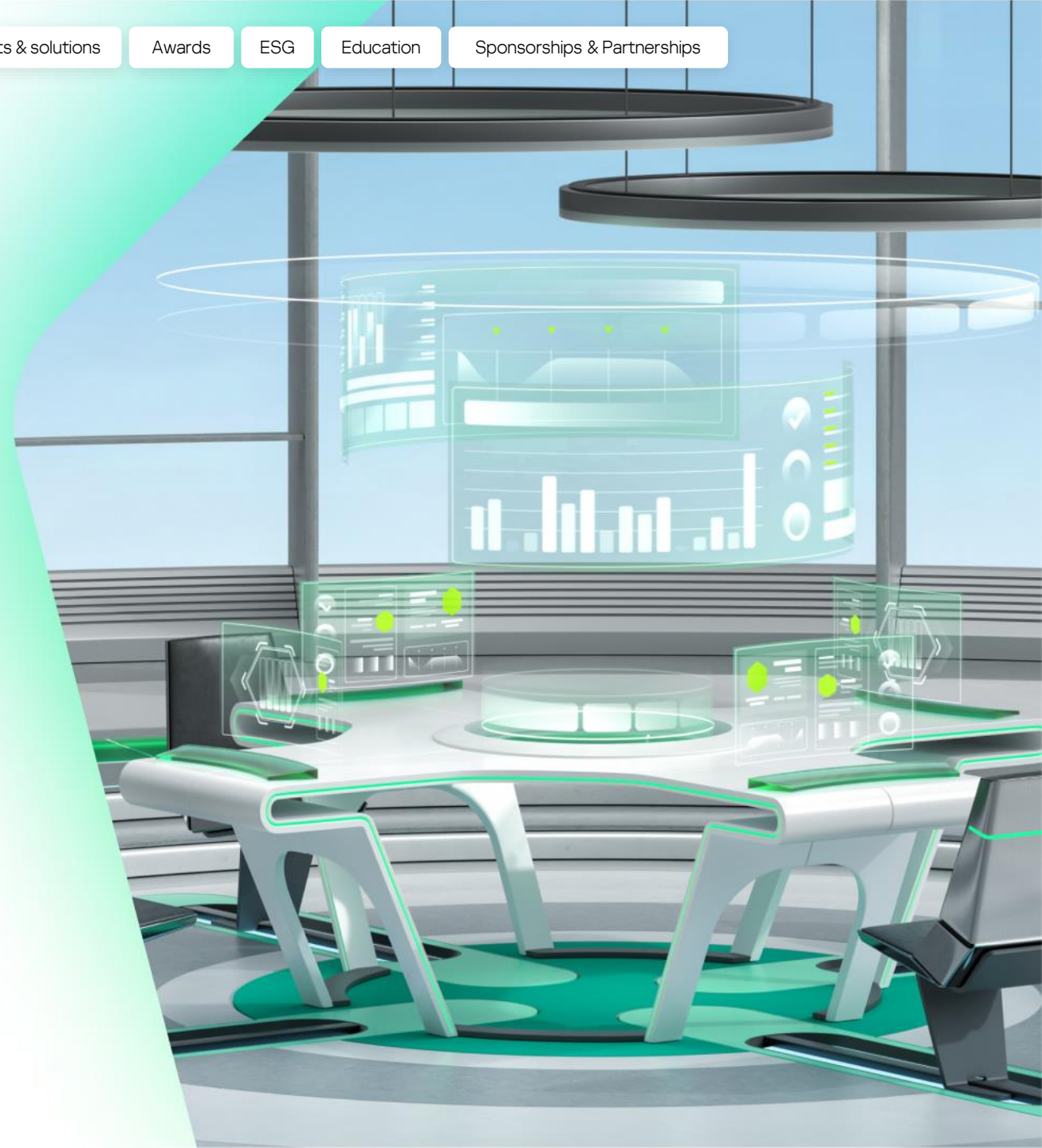
## cyberattacks

detected by Kaspersky in 2023

# 411,000

## new malicious files

detected by Kaspersky every day



## Advanced persistent threat landscape in 2023

Kaspersky's Global Research and Analysis Team (GReAT) is well-known for the discovery and analysis of the most advanced cyberthreats. According to their data, in 2023 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

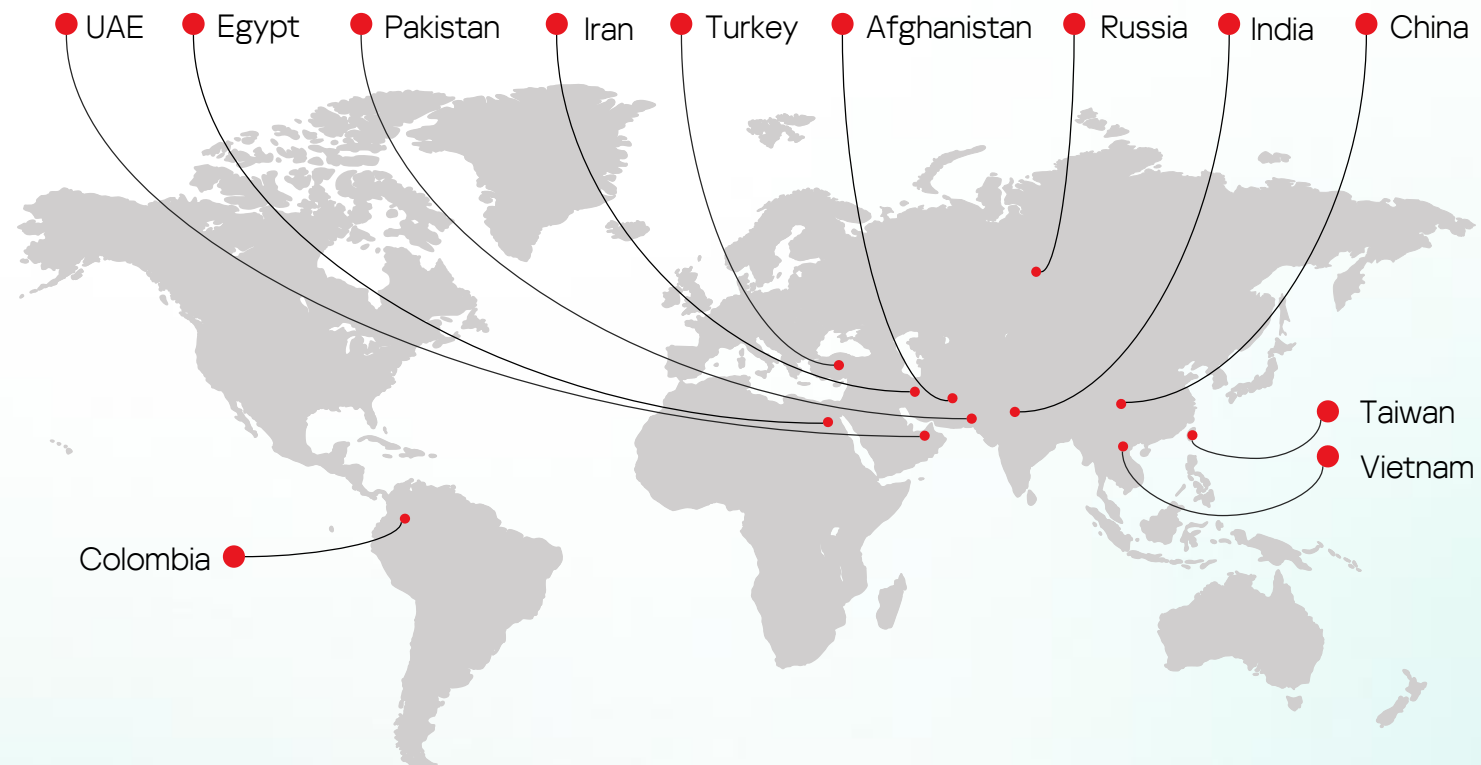
### Top 10 targets

- |  |   |
|--|---|
|  Government   |  Telecommunications  |
|  Military     |  Cryptocurrency      |
|  Diplomatic   |  Industrial          |
|  IT companies |  Manufacturing       |
|  Energy       |  Technology Research |

### Top 10 significant threat actors









- |           |                |
|-----------|----------------|
| ① Lazarus | ⑥ Ghostwriter  |
| ② APT10   | ⑦ DeathStalker |
| ③ Kimsuky | ⑧ BitterAPT    |
| ④ ZexCone | ⑨ SideCopy     |
| ⑤ Tomiris | ⑩ Gelsemium    |

### Top 12 targeted countries and territories









## Our major discoveries and research










								
	<b>Expetr/ Notpetya</b>	<b>Olympic destroyer</b>	<b>Shadow hammer</b>	<b>Tajmahal</b>	<b>Mosaicregressor</b>	<b>Ghostemperor</b>	<b>Moonbounce</b>	<b>Operation Triangulation</b>
Detection	<b>2017</b>	<b>2018</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>	<b>2022</b>	<b>2023</b>
Active since	<b>2017</b>	<b>2017</b>	<b>2018</b>	<b>2013</b>	<b>2017</b>	<b>2020</b>	<b>2021</b>	<b>2019</b>
Classification	Data wiping campaign	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	Cyber-espionage platform	APT campaign
Description	A wiper pretending to be ransomware, using modified EternalBlue and EternalRomance exploits. Some observations point to a link between ExpPetr and BlackEnergy APT	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 a legitimate certificate	A 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.	A highly sophisticated, complex UEFI firmware rootkit we attributed to APT41, which allows the attackers to persistently execute a malware stager on the operating system via a malicious driver.	The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data. The targets are infected using zero-click exploits via the iMessage platform, and the malware runs with root privileges, gaining complete control over the device and user data.
Targets	Spread around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. >50% of organizations attacked were industrial companies	Organizations related to Winter Olympic Games 2018; biological and chemical threat prevention organizations in the 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 organizations and Telecommunication companies	Holding companies and industrial suppliers	iOS devices

## Targeted attack research








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

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

2022

-  ZexCone
-  SilentMarten
-  MoonBounce
-  ToddyCat
-  MagicKarakurt
-  CosmicStrand
-  SBZ
-  StripedFly
-  DiceyF
-  MurenShark

2023

-  PowerMagic
-  CommonMagic
-  Trila
-  LoneZerda
-  CloudWizard
-  Operation Triangulation
-  BlindEagle
-  Mysterious Elephant
-  BadRory
-  Dark Caracal
-  HrServ

## Enabling a privacy-minded world

Privacy has become a valuable commodity as more and more users understand its importance and the need to change their habits to protect their digital presence. Being not just a cybersecurity firm, but a privacy company, Kaspersky invests in features that enable users to protect their data and digital privacy through educational assets and hands-on tools.



### Anti-doxing course

Learn what the basic dangers of doxing are and how to protect yourself from it

[Learn more](#)

### Privacy checklist

An easy to grasp definitive checklist for those who care about their privacy

[Learn more](#)

### Stalkerware protection

Kaspersky's consumer security 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 social media accounts and OS privacy levels

[Learn more](#)

# Products & solutions

- Kaspersky Cyber Immunity approach
- KasperskyOS-based product portfolio
- Enterprise Solutions
- Industrial Cybersecurity Solutions
- SMB Next Generation Solutions
- MSP Solutions
- B2C Solutions





## Kaspersky Cyber Immunity

Kaspersky's approach and methodology for developing secure-by-design cyber-physical systems

- The architectural approach creates an environment where a vulnerability or bad code is no longer a big deal
- Methodology, technologies and tools for creating Cyber Immune solutions
- **KasperskyOS** – an optimal platform for building Cyber Immune cyber-physical systems

The overwhelming majority of attacks on a Cyber Immune system are the types that cannot impact its critical function



## Kaspersky Cyber Immunity areas of application

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

They perform functions even in an aggressive environment without additional security features.



IoT & Industrial IoT



Smart cities



Thin client infrastructure



Transportation

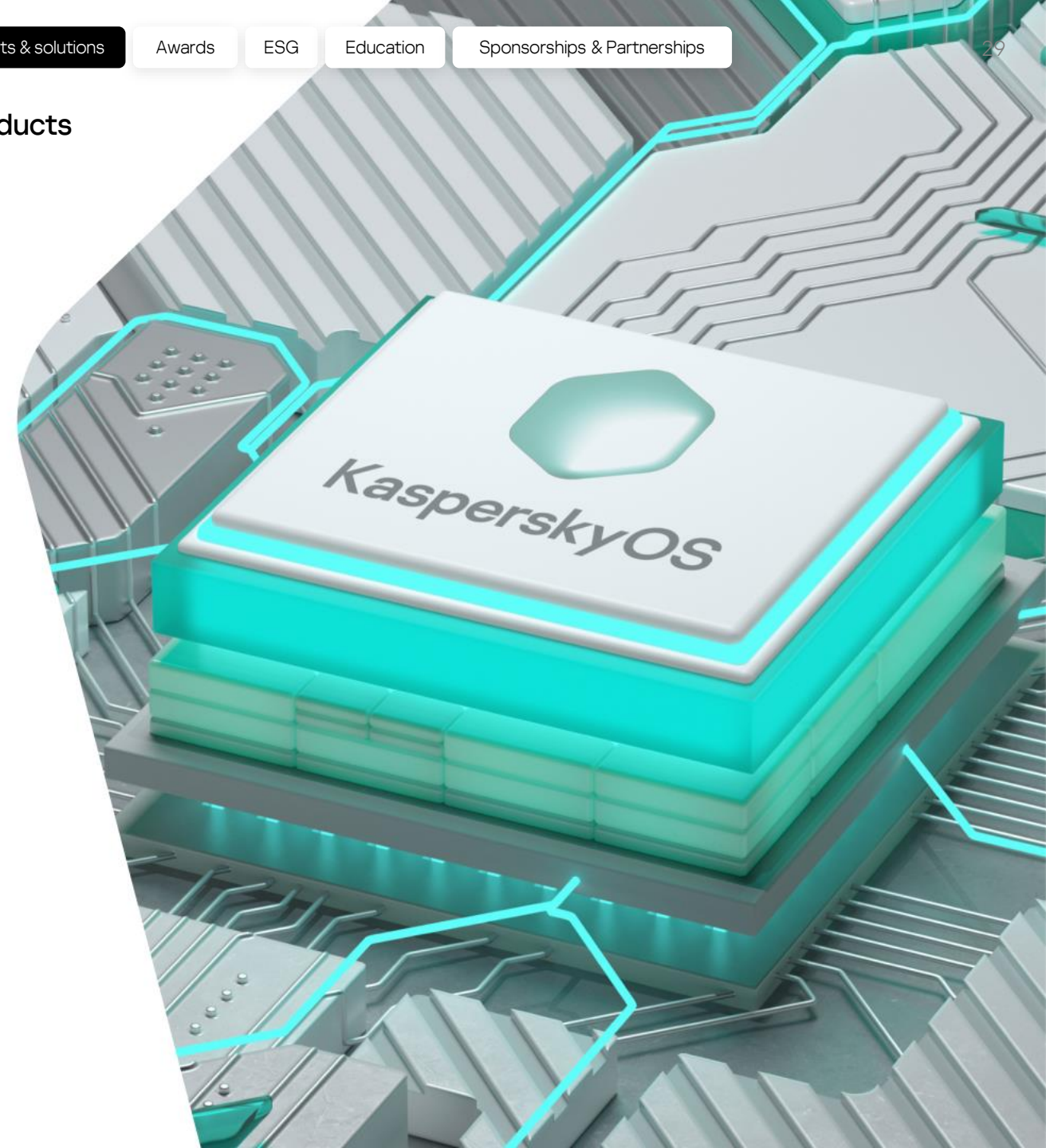


Professional mobile devices

## KasperskyOS is an effective platform to create Cyber Immune products

Microkernel operating system for cyber-physical systems with high cybersecurity demands

- Grants a platform for creating secure-by-design solutions
- Creates an environment that does not allow apps to execute undeclared functions and prevents the exploitation of vulnerabilities
- Provides full transparency, flexible configuration of security policies and control over interactions across the whole system





# KasperskyOS-based product portfolio

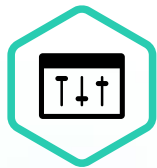


## Kaspersky IoT Infrastructure Security

A solution for cybersecure data transfer to digital and cloud business platforms, as well as for infrastructure protection and transparency



### Kaspersky IoT Secure Gateway

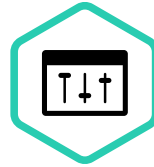


### Kaspersky Security Center



## Kaspersky Thin Client

A solution for building a Cyber Immune, functional, and manageable thin client infrastructure with convenient, centralized management



### Kaspersky Security Center

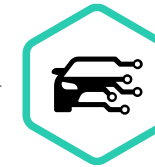


### Kaspersky Security Management Suite



## Kaspersky Automotive Secure Gateway

Building reliable IT systems for smart road vehicles



### Kaspersky Automotive Adaptive Platform



### Kaspersky Automotive Secure Broker Framework



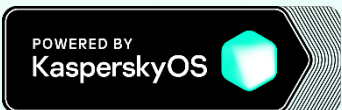
### Kaspersky OTA Agent



### Kaspersky Vehicle SOC Agent



### Kaspersky Remote Diagnostic Agent



# Kaspersky Enterprise Solutions

## Targeted Solutions



Kaspersky Industrial CyberSecurity



Kaspersky Fraud Prevention



Kaspersky Threat Analysis



Kaspersky Private Security Network



**Expert Security**



Mature IT security capability or a SOC team

**Optimum Security**

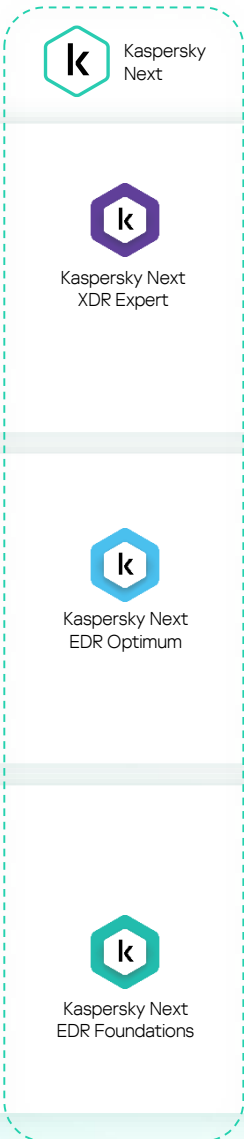


IT Security

**Security Foundations**













IT







Internal Expertise    Threat Intelligence    Extended Detection and Response    Security information and event management    Assessment    Expert Guidance    Investigation    People

Native XDR    Open XDR








Kaspersky Cybersecurity Training    Kaspersky Threat Intelligence    Kaspersky Anti Targeted Attack    Kaspersky Extended Detection and Response    Kaspersky Unified Monitoring and Analysis Platform    Kaspersky Security Assessment    Kaspersky Compromise Assessment    Kaspersky SOC Consulting    Kaspersky Incident Response    Kaspersky Security Awareness Ultimate

People    Detection Enrichment    Containers

Kaspersky Security Awareness Advanced    Kaspersky Threat Data Feeds    Kaspersky Threat Lookup    Kaspersky Container Security

Endpoint    Network    Data    People    Cloud, Virtual server, VDI    Support

Kaspersky Embedded Systems Security    Kaspersky Security for Mail Server    Kaspersky Security for Internet Gateway    Kaspersky Security for Storage    Kaspersky Security Awareness Essential    Kaspersky Hybrid Cloud Security    Kaspersky Premium Support and Professional Services



Kaspersky Managed Detection and Response



Kaspersky SD-WAN



### Kaspersky OT CyberSecurity

Cyber-physical security ecosystem for industrial enterprises



### Kaspersky Extended Detection and Response

IT-OT Convergence

#### Technologies

##### Specialized Solutions



Kaspersky Antidrone



Kaspersky Machine Learning for Anomaly Detection



Kaspersky SD-WAN

#### Native XDR



Kaspersky Industrial CyberSecurity



for Nodes

Endpoint Protection, Detection and Response



for Networks

Network Traffic Analysis, Detection and Response

##### KasperskyOS solutions



Kaspersky IOT Secure Gateway



Kaspersky Thin Client



Kaspersky Automotive Secure Gateway

#### Knowledge

##### Cyber hygiene



Kaspersky Security Awareness

##### Threat intelligence



Kaspersky ICS Threat Intelligence

##### Training



Kaspersky ICS CERT Training

#### Expertise

##### Discovery



Kaspersky ICS Security Assessment

##### Managed Service



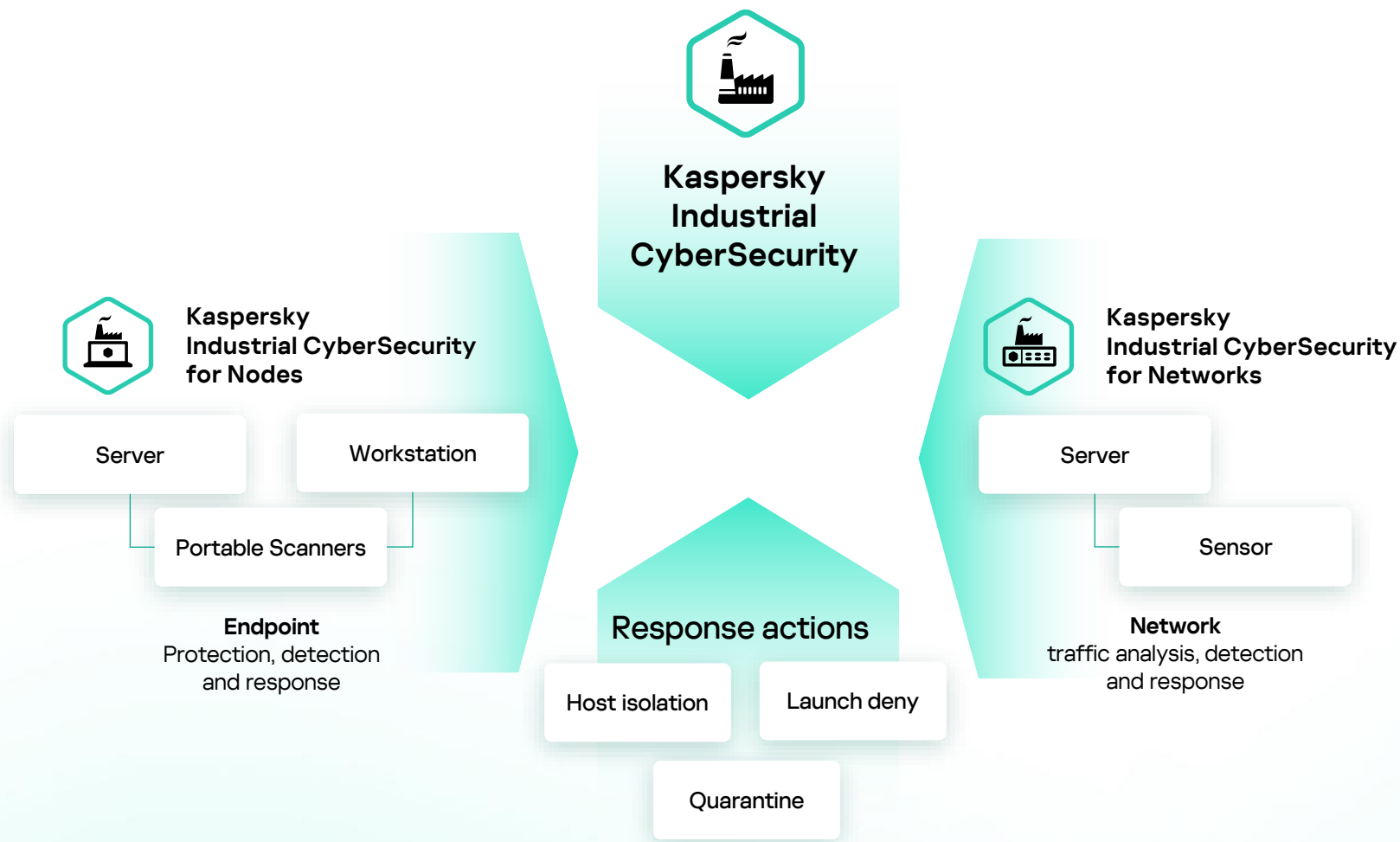
Kaspersky Managed Detection and Response

##### Response



Kaspersky Incident Response Readiness

## Native XDR platform for critical infrastructure protection



### Network: detection and response

Network traffic analysis and endpoint sensors to detect intrusions on the lowest level (ICS Protocols DPI and IDS signatures)

### Audit, risk and asset management

Passive asset detection and active polling of OT components. Risk-oriented reporting, clear situational awareness, vulnerability management and OVAL-based audit.

### Endpoint: detection and response

Antimalware, software & device whitelisting and more. ICS EDR enables root cause analysis of incidents in OT

## 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



Unlimited, fast VPN to enjoy global  
content without compromising on  
privacy, security or speed



Storing all passwords with  
Password Manager



### Kaspersky Next EDR Foundations

#### 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



Key IT scenarios covered



Cloud monitoring for detecting  
'Shadow IT'



### Kaspersky Next EDR Optimum

#### The best enterprise-grade security solution



Essential EDR functionality to combat  
evasive threats



Cloud-native solution that  
covers diverse infrastructures



Reduces your cybersecurity  
team's workload



Security for Microsoft Office 365  
and 'Shadow IT' control

## Kaspersky Services for Managed Service Providers

### Offer #1

#### Managed Protection

Kaspersky Managed Protection offering provides top notch endpoint, cloud, web and mail protection



Kaspersky Next  
EDR Foundations



Kaspersky Next  
EDR Optimum



Kaspersky  
Security for  
Mail Server



Kaspersky  
Security for  
Office 365



Kaspersky  
Security for  
Internet Gateway



Kaspersky  
Hybrid Cloud  
Security



Kaspersky  
Automated Security  
Awareness Platform

### Offer #2

#### Managed Detection & Response

Kaspersky MDR delivers a fully managed, 24/7 detection, prioritization, investigation and response service, without having to actually establish their own SOC team.



Kaspersky  
Endpoint Detection  
and Response



Kaspersky  
Anti Targeted  
Attack



Kaspersky  
Managed Detection  
and Response

### Offer #3

#### SOC as a service

Our SIEM Kaspersky Unified Monitoring and Analysis Platform serves as a core of a modern SOC, allowing to unify Kaspersky and 3<sup>rd</sup> parties products in a single system.



Kaspersky  
Unified Monitoring  
and Analysis Platform

### Offer #4

#### Threat Intelligence

Our award-winning TI will help you to mitigate attacks on your customers with unique IoCs and IoAs.



Kaspersky  
Threat Intelligence

### Offer #5

#### Managed XDR

The ultimate bundle that include all the above and complies with the XDR concept, thus allowing to provide best cybersecurity services even for the most demanding customers.

## B2C Solutions: New product portfolio

Our bold new plans cover the full range of customer needs

# Complete protection for your digital life



PREMIUM SERVICES



IDENTITY



PRIVACY



PERFORMANCE



SECURITY



Kaspersky  
Standard



Kaspersky  
Plus



Kaspersky  
Premium



## Complete protection for consumers' digital lives

With our diverse collection of security products, we inspire customers to embrace new technologies – because they know we're guarding them and their families.

### Kaspersky B2C Solutions



#### Kaspersky Standard

Win | Android | Mac | iOS



#### Kaspersky VPN Secure Connection

Win | Android | Mac | iOS



#### Kaspersky Who Calls\*

Android | iOS

\*Only available in Russia, Kazakhstan and Indonesia



#### Kaspersky Plus

Win | Android | Mac | iOS



#### Kaspersky Safe Kids

Win | Android | Mac | iOS



#### Kaspersky Premium

Win | Android | Mac | iOS



#### Kaspersky Password Manager

Win | Android | Mac | iOS

# Kaspersky awards

- Overview
- Top 3 metrics
- Recognitions



# More than 600 awards\*

One of the five biggest endpoint security vendors\*\*.

Kaspersky Standard was honored with the **Product of the Year 2023** annual award by independent test lab AV-Comparatives\*\*\*.

Kaspersky EDR Expert continually delivers top results: Total Accuracy Rating of 100% in Advanced Security EDR tests of 2022&2023 by SE Labs\*\*\*\*; 100% protection from targeted attacks, and **Strategic Leader** status from AV-Comparatives\*\*\*\*\*, and got approved by AV-Test\*\*\*\*\*.

[Learn more](#)

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

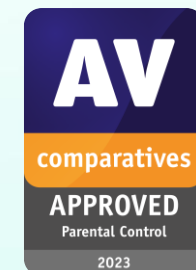
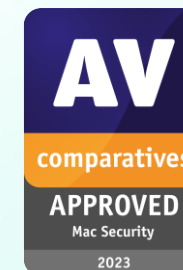
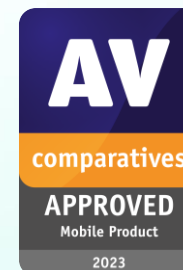
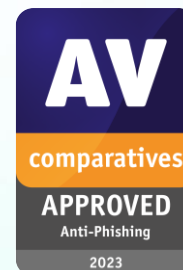
\*\*The company was ranked fifth by IDC estimations in Worldwide Consumer Digital Life Protection Market Shares (9 June 2022)

\*\*\* Kaspersky's flagship home user security solution – Kaspersky Standard – was honored with the annual [Product of the Year 2023](#) award for high results in 8 Real-World tests, 2 Malware Protection tests, 2 Performance tests, and Enhanced Real-World test of 2023.

\*\*\*\* Enterprise Advanced Security EDR test reports of [2022](#) and [2023](#)

\*\*\*\*\* Endpoint Detection and Response tests of [2022](#) and [2023](#)

\*\*\*\*\* Advanced EDR Test [2023](#)



## Awards



# Most Tested Most Awarded\* Kaspersky Protection

[\\*Kaspersky.com/top3](https://kaspersky.com/top3)

# 100

Tests/Reviews

# 93

First Places

# 94%

Top 3

As cybersecurity becomes vital to every individual and entity, trust in providers is essential. We protect home users and corporate clients worldwide, and market recognition is very important for us. In 2023, Kaspersky products participated in 100 independent tests and reviews. Our products were awarded 93 firsts and received 94 top-three finishes.

\*100 independent tests and reviews were completed by Kaspersky products in 2023 along other participating vendor products. More than 90 vendors took part in the test in 2023, but only 10 participated in 35% or more of the tests, and were represented in the chart. Additionally, we considered valuable to have another 5 vendors' results represented in the chart.



## Recognitions

Kaspersky products are regularly assessed by global research firms, and our cyber protection expertise is proven by the number of recognitions by industrial analysts.

Among those are IDC, Canals, ISG, Quadrant Knowledge Solutions, Info-Tech, and many others.

In 2023, Kaspersky was [noted](#) as the vendor “who shaped the year” in IDC's Worldwide Modern Endpoint Security Market Shares report.\*



# ESG

Our company's mission is to build a safe and sustainable digital world so that people can use technological solutions to improve not only their daily lives but also life on the planet as a whole.

We fulfill this mission by increasing the resilience of the digital space against threats through the creation of Cyber Immunity while paying special attention to social projects and environmental awareness.

Read the first Sustainability (ESG) report covering results for 2021 and mid-2022 as well as key objectives for 2023 [here](#).





## ESG strategic development

Kaspersky's sustainable development is grounded in five key areas

1

### Ethics and transparency

- Source code and process transparency
- Data protection and the right to privacy
- Management transparency and business resilience

2

### Safer cyberworld

- Critical infrastructure protection
- Assistance in the investigation of cybercrimes on a global level
- Protection of users against cyberthreats

3

### Safer planet

- Reducing the environmental impact of our infrastructure, business activities and products

4

### People empowerment

- Employee care
- Women in STEM
- Inclusivity and availability of technologies
- Talent development in IT

5

### Future tech

- Cyber Immunity for new technologies

Learn more about our main accomplishments [here](#).

# Education

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, and create a life-long learning journey for passionate cybersecurity experts.



## Education: Cybersecurity is for life-long learning



### School: Primary

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.

Kids Cyber Resilience

Kids book



### School: Secondary

Kaspersky is keen to help young talents to explore the field of cybersecurity and make their future professional journey to IT more vivid.

Tech Valley



### University

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

Secut'IT Cup

Kaspersky Academy Alliance

SafeBoard



### Professional

Kaspersky provides a wide range of knowledge on information security for IT professionals, business leaders, top managers and senior executives.

xTraining

Cybersecurity for Executives Online

# Sponsorships & Partnerships

As an innovative global company, Kaspersky cares about future by providing cybersecurity to different industries and by supporting promising talent in various countries.

We contribute to the development of science and contemporary art, help to preserve the world, and provide athletes with the opportunity to reach their full potential.





## Sponsorships & Partnerships



### 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 partners with multiple eSports teams worldwide: Nasr (UAE), Sangal (Turkey), Reckoning (India), and Red Canids (Brazil) to enhance the gaming experience of eSports enthusiasts by providing advanced cyber security measures

[Learn more](#)



### Motorsport

Kaspersky supports talented drivers such as Amna and Hamda Al Qubaisi, the first Emirati female drivers.

[Learn more](#)

**Bring on the future**