Kaspersky Corporate Kit

kaspersky

Updated: April 2023

Our mission is simple — building a safer world.

In fulfilling that mission we aim to become the global leaders in cybersecurity — by securing technology to ensure 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. This 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 six continents in almost 200 countries and territories

Provides innovative IT security solutions and services for businesses and consumers

Numbers

> 15 million
consumer product activations per year

> 4,500
highly qualified specialists

US $ 758 million
global 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.

>220,000
Corporate clients worldwide

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

Enterprises

Industrial facilities

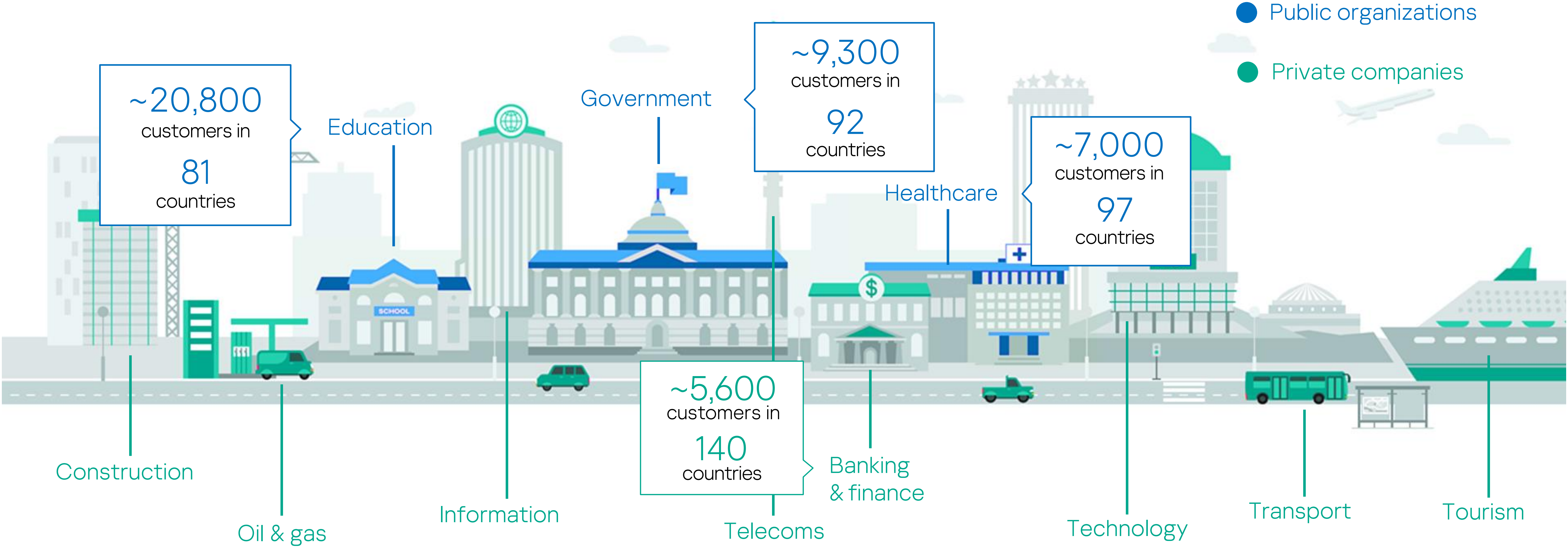
Small and medium businesses

Very small businesses

Consumers

Our customers

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



● Public organizations

● Private companies

~20,800 customers in 81 countries

~9,300 customers in 92 countries

~7,000 customers in 97 countries

~5,600 customers in 140 countries

We are an international cybersecurity company

200 countries and territories where we operate

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.

OIPC ICPO INTERPOL
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 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.

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 confirm the security of Kaspersky's processes and systems, including:

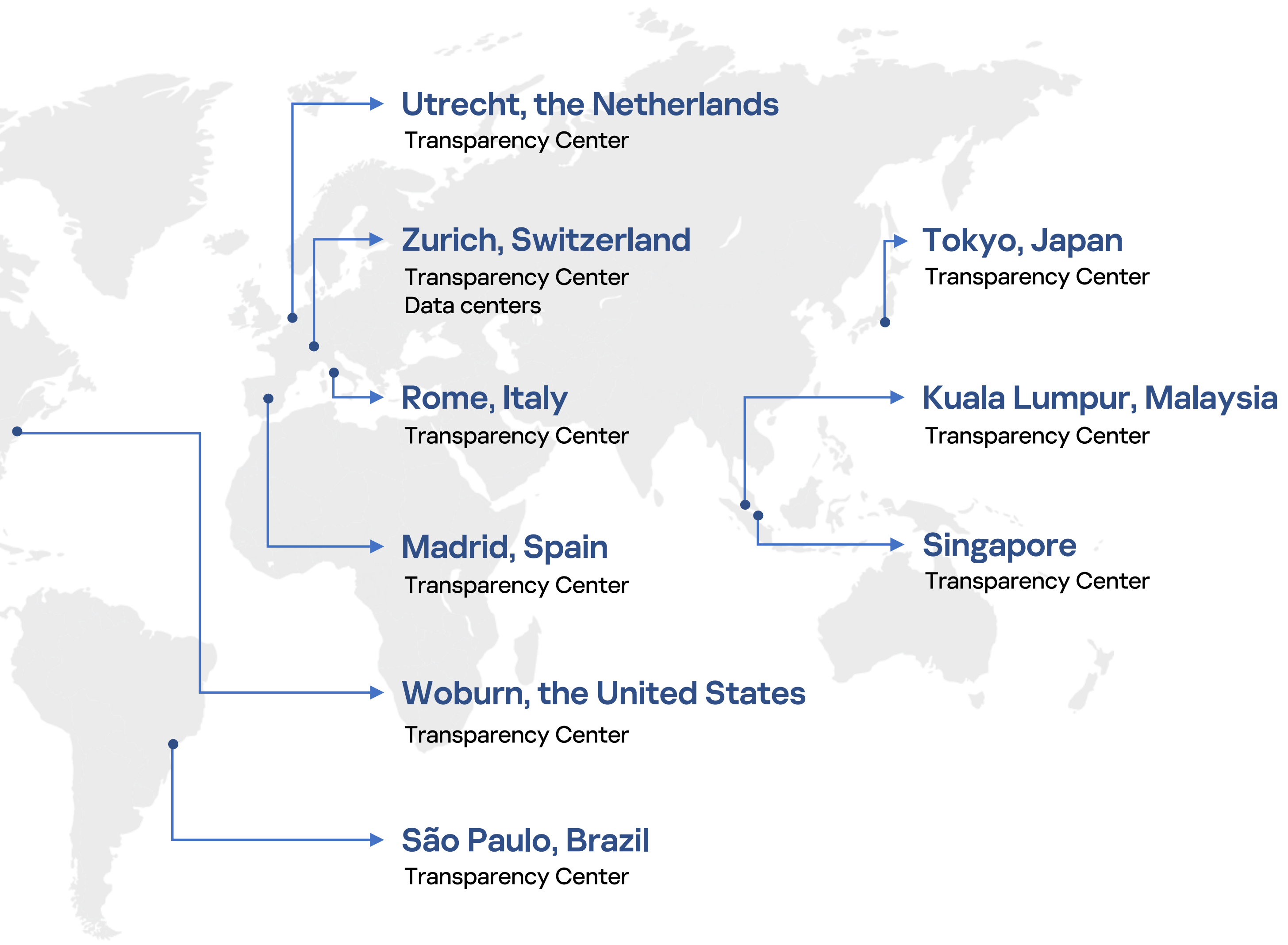
- SOC 2 audits by a Big Four firm
- ISO 27001 certifications for the company's data systems

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.



Utrecht, the Netherlands
Transparency Center

Zurich, Switzerland
Transparency Center
Data centers

Rome, Italy
Transparency Center

Madrid, Spain
Transparency Center

Woburn, the United States
Transparency Center

São Paulo, Brazil
Transparency Center

Tokyo, Japan
Transparency Center

Kuala Lumpur, Malaysia
Transparency Center

Singapore
Transparency Center

Kaspersky Transparency Centers

Review options:

Blue Piste (both remote & physical)

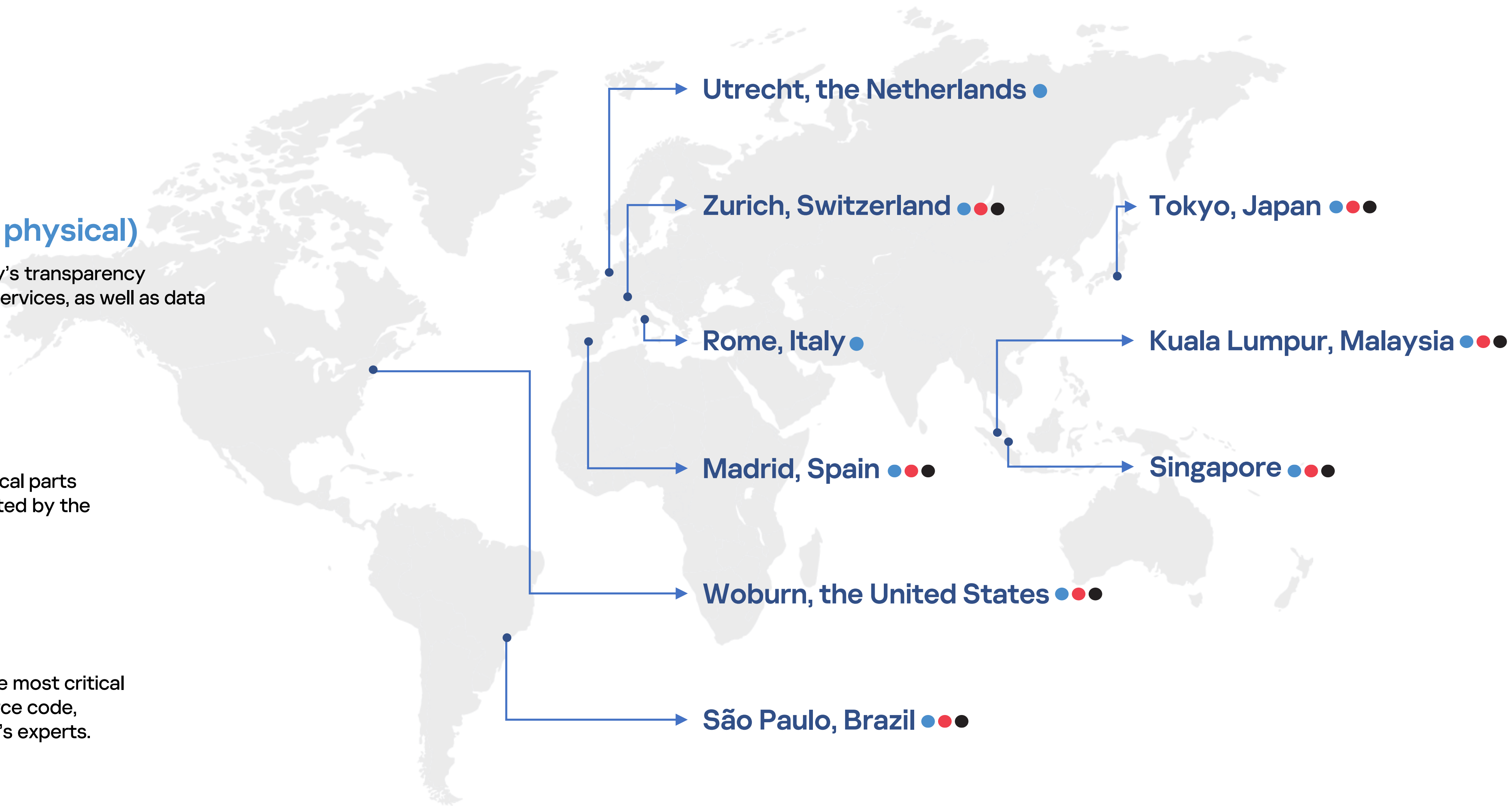
An overview of Kaspersky's transparency practices, products and services, as well as data management practices.

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.



Utrecht, the Netherlands ●

Zurich, Switzerland ●●●

Tokyo, Japan ●●●

Rome, Italy ●

Kuala Lumpur, Malaysia ●●●

Madrid, Spain ●●●

Singapore ●●●

Woburn, the United States ●●●

São Paulo, Brazil ●●●

Kaspersky Global Transparency Initiative: our results in numbers

2 Additional data locations

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 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

54 Bug Bounty report awarded

with total payments equal to $76,550

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.

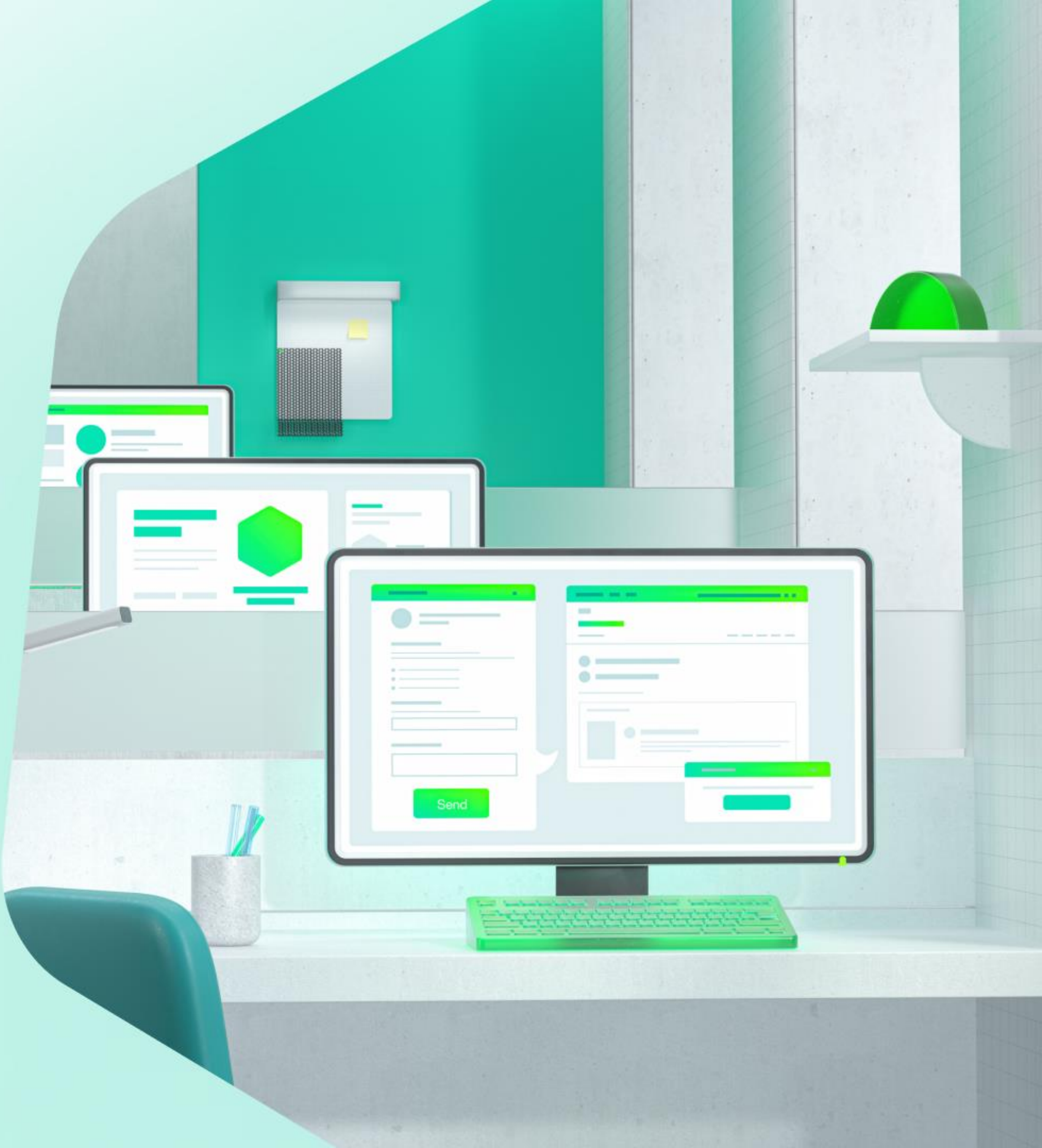
$1,000 – $5,000

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+ members in our group of elite world-leading security experts - GReAT

Threat research

>1,000,000,000

cyberthreats

detected by Kaspersky since
the company's inception

7,000,000,000

cyberattacks

detected by Kaspersky in 2022

400,000

new malicious files

detected by Kaspersky every day

Advanced persistent threat landscape in 2022

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 2022 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

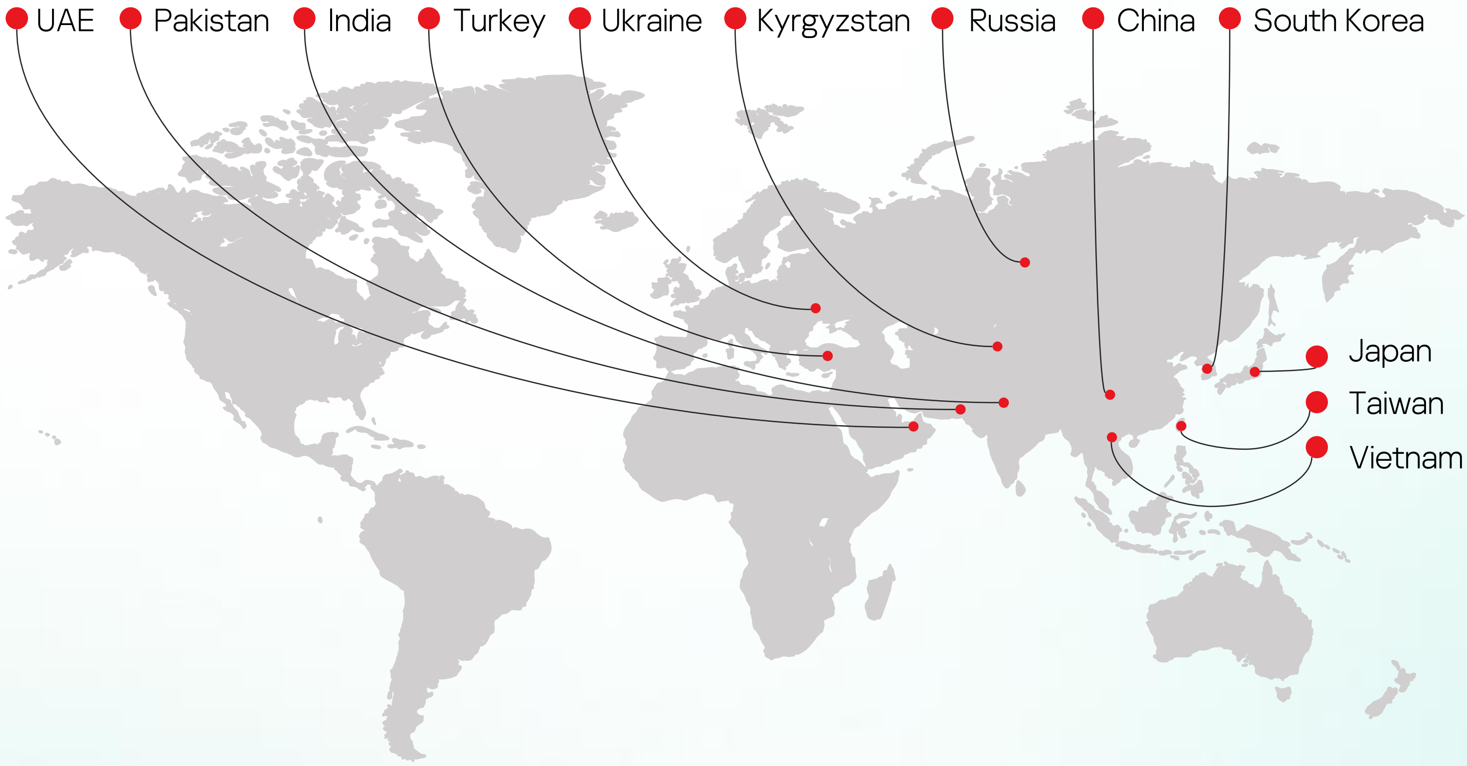
Top 10 targets

- Government
- Military
- Diplomatic
- IT companies
- Educational
- Telecommunications
- Media
- Software Development
- Manufacturing
- Logistics

Top 10 significant threat actors

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

Top 12 targeted countries



apt.securelist.com

Based on the data up to 31.12.2022

Our major discoveries and research

	Sofacy	Duqu 2.0	Lazarus	Project Sauron	Expetr/ Notpetya	Olympic destroyer	Shadow hammer	Tajmahal	Mosaic-regressor	Ghostemperor	Moonbounce
Detection	2014	2015	2016	2016	2017	2018	2018	2019	2020	2021	2022
Active since	2008	2014	2009	2011	2017	2017	2018	2013	2017	2020	2021
Classification	Cyber-espionage malware	Complex cyberattack platform	Cyber-espionage & sabotage, financial attacks	Cyber-espionage malware	Data wiping campaign	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage platform	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	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.	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.
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	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 organizations and Telecommunication companies	Holding companies and industrial suppliers

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
- Tomiris

2022

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

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 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 consumer security solutions 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

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

Kaspersky Cyber Immunity

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

- 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 IT 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.

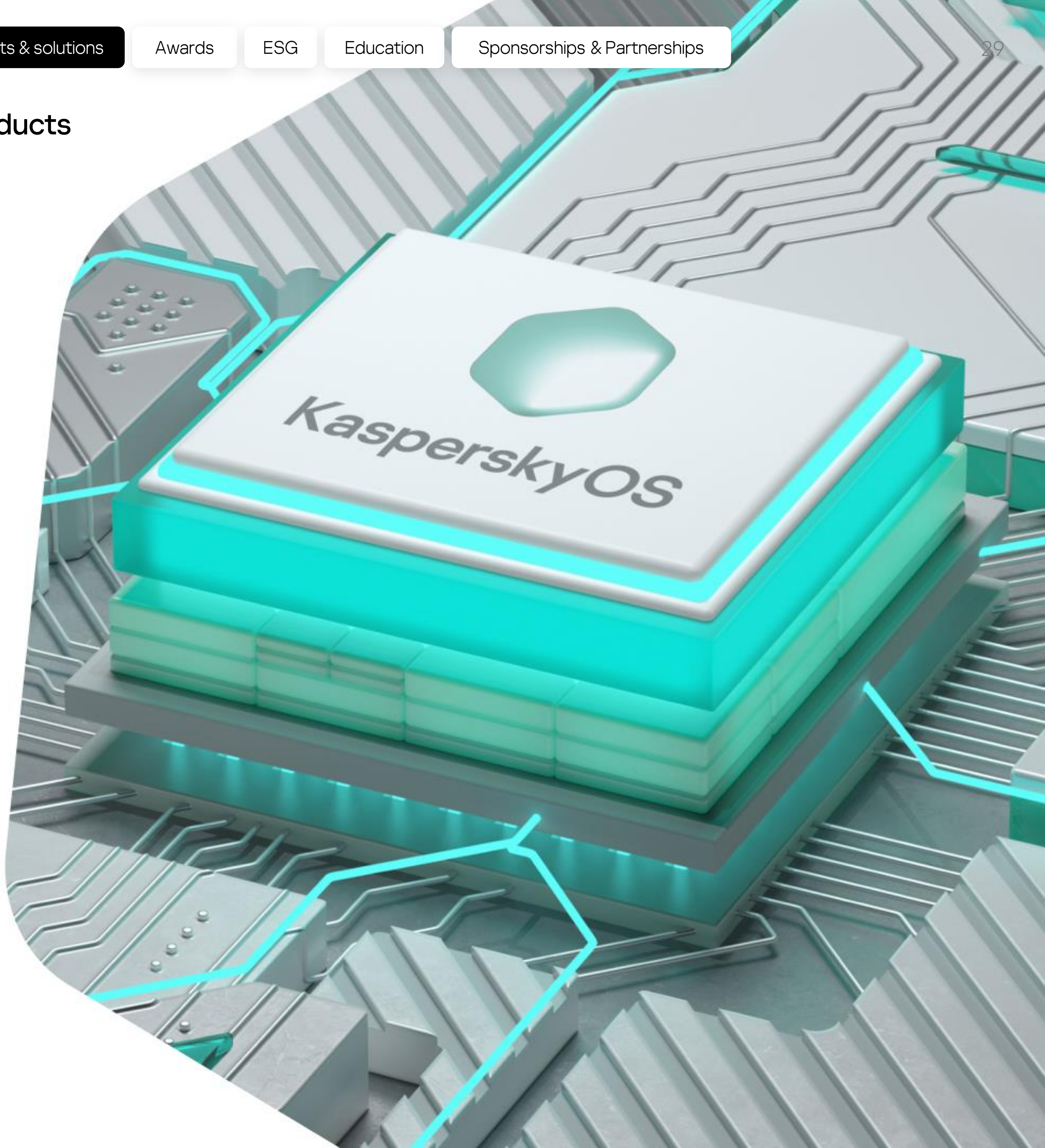
They perform functions even in an aggressive environment without additional security features.

- IoT & Industrial IoT
- Smart cities
- Thin client infrastructure
- Transportation
- Professional mobile devices

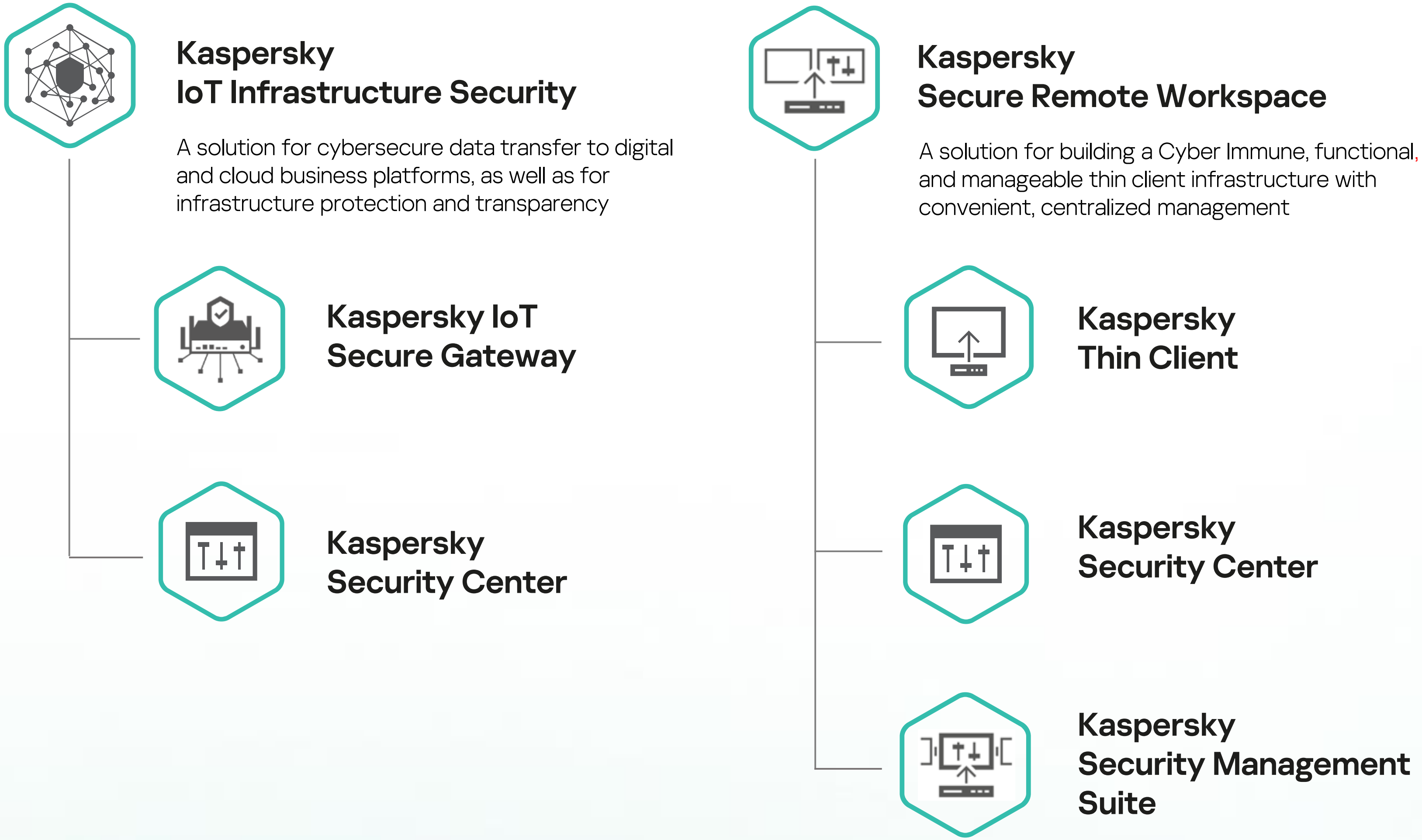
KasperskyOS is an effective platform to create Cyber Immune products

Microkernel operating system for IT systems with high demands on cybersecurity

- grants a platform for creating secure by design solutions
- creates an environment that does not allow apps to execute undeclared functions and prevents 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 Secure Remote Workspace

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

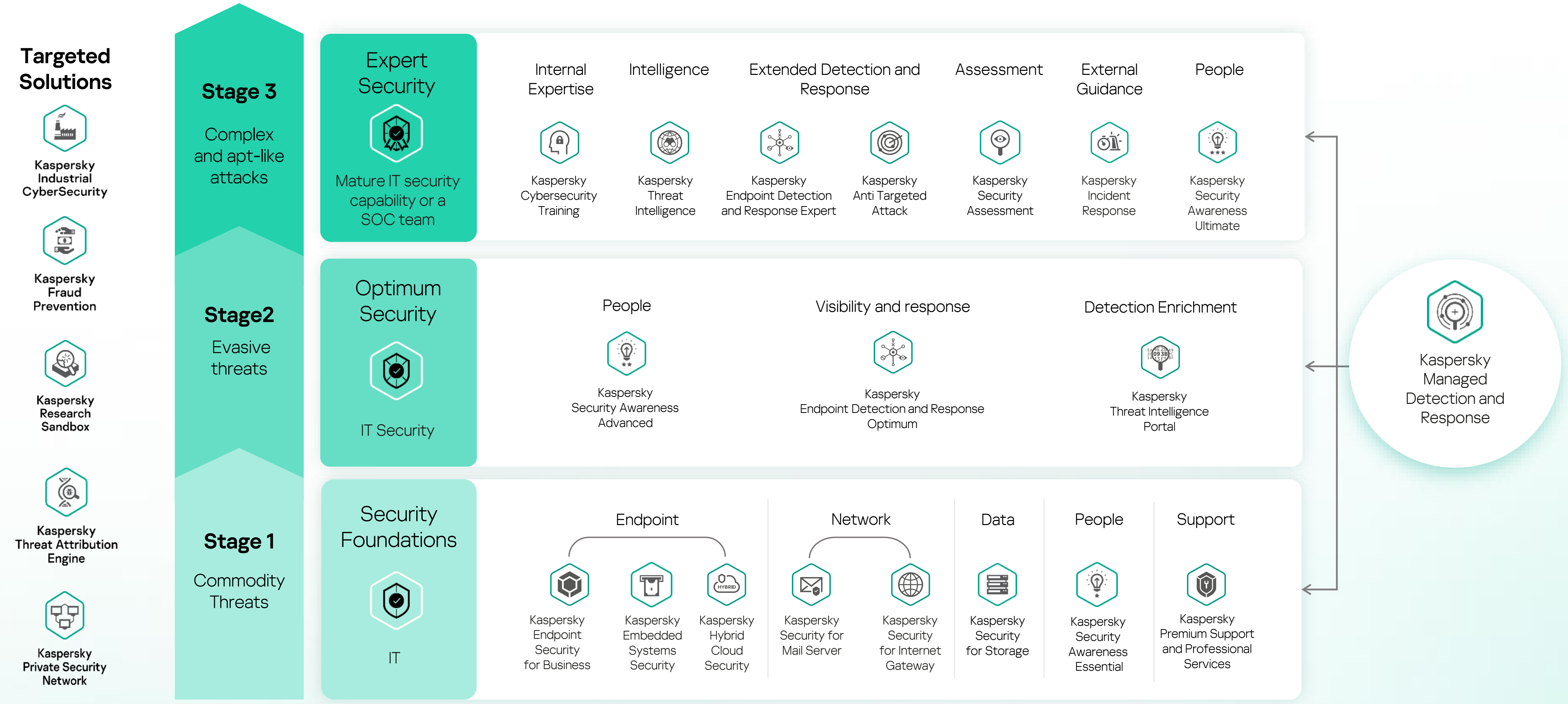
Kaspersky Thin Client

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

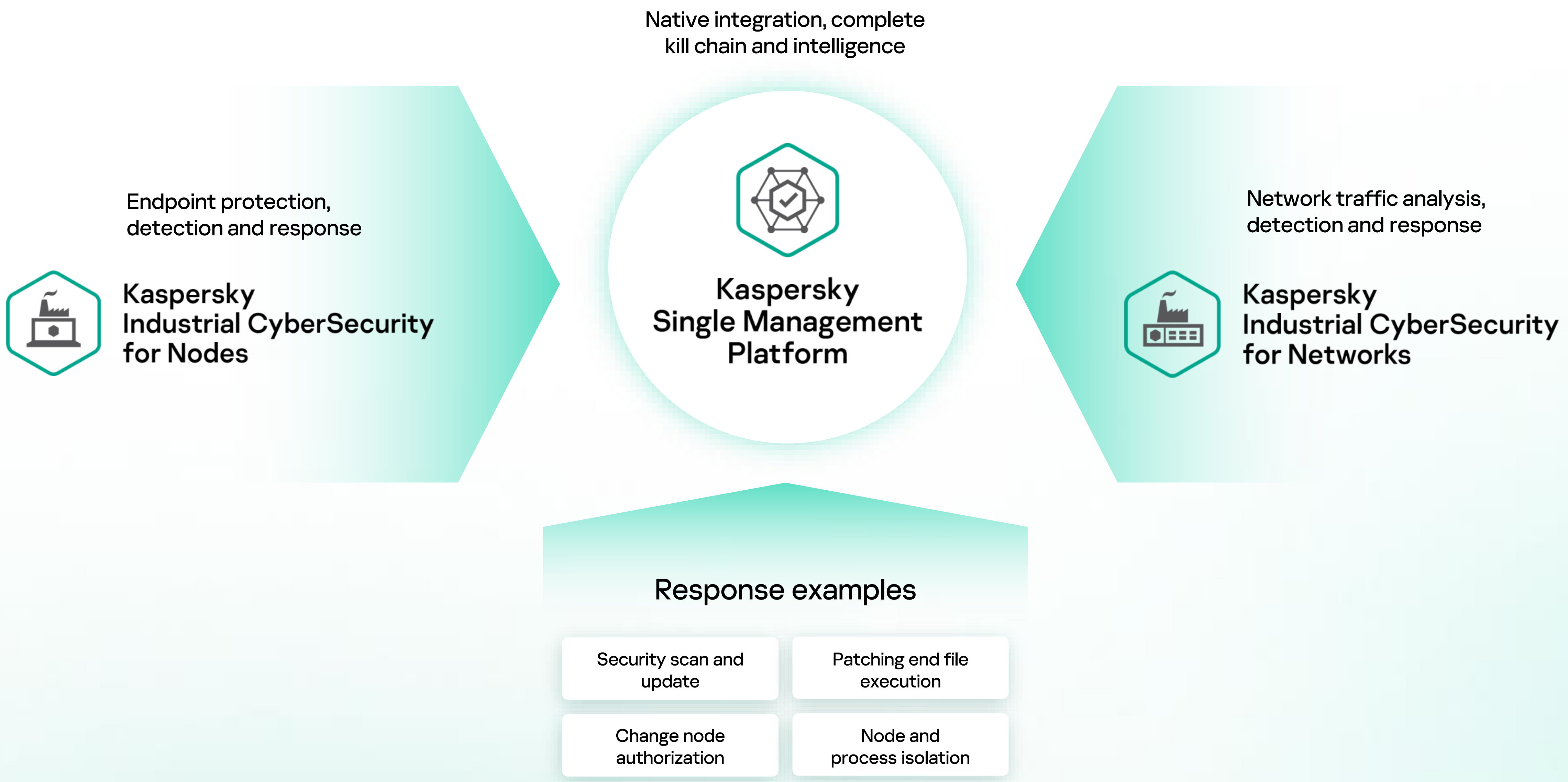
Security Foundations

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

Natively integrated platform for OT



Native integration, complete kill chain and intelligence

Endpoint protection, detection and response

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Single Management Platform

Network traffic analysis, detection and response

Kaspersky Industrial CyberSecurity for Networks

Response examples

- Security scan and update
- Patching end file execution
- Change node authorization
- Node and process isolation

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

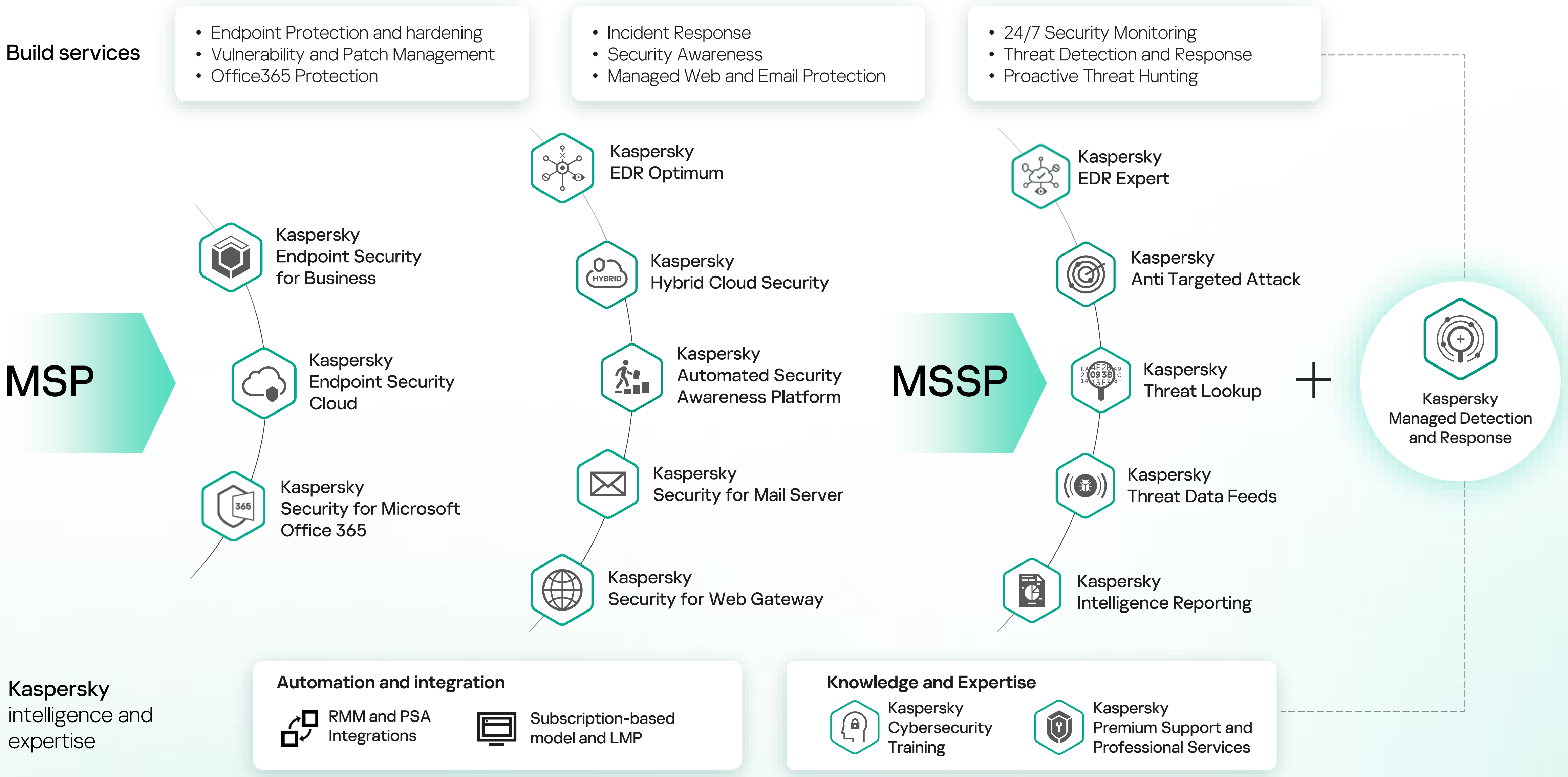
- Cloud-based console for flexible, simple administration, no need for additional hardware
- Protects PCs, laptops, mobile devices and file servers
- Security for Microsoft Office 365 and 'Shadow IT' control
- The latest, most up-to-date software - always

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

Our bold new plans cover the full range of customer needs

Complete protection for your digital life

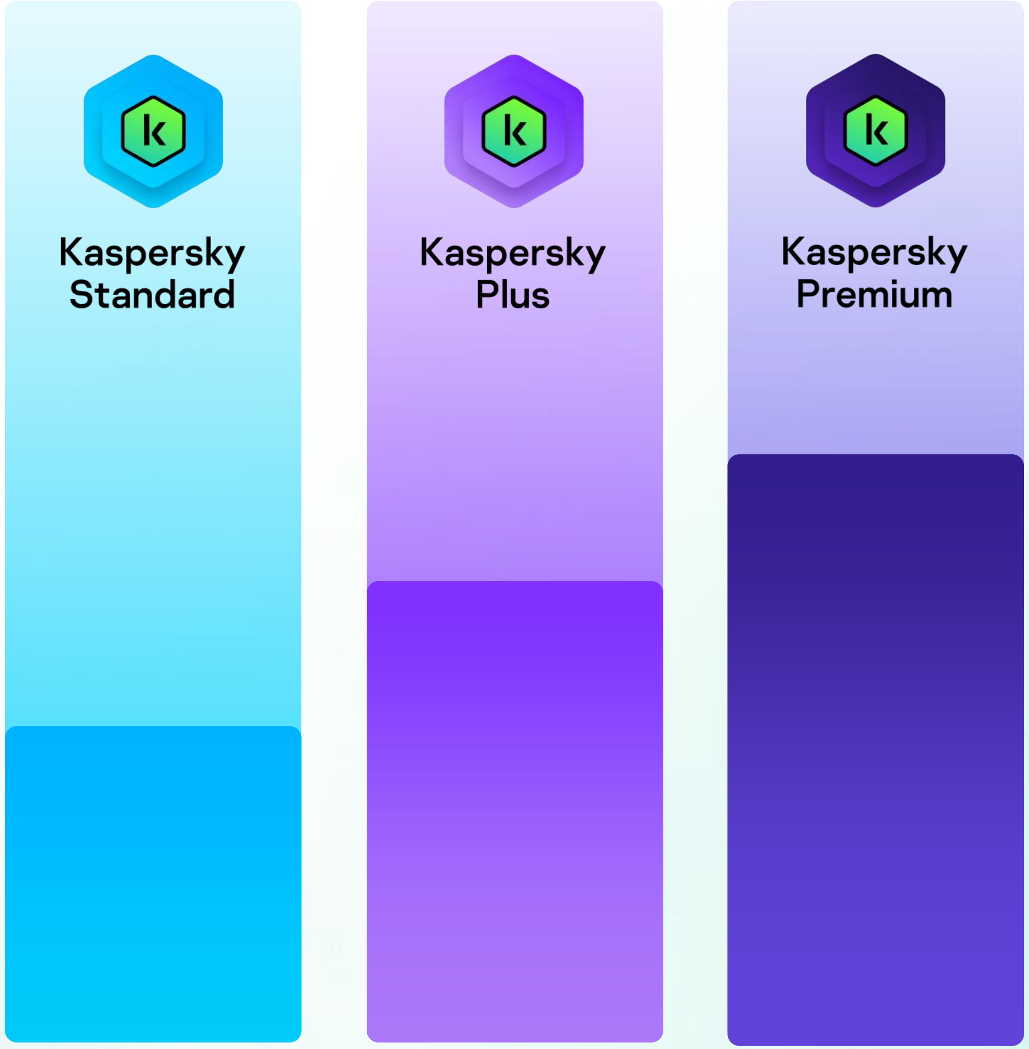
PREMIUM SERVICES

IDENTITY

PRIVACY

PERFORMANCE

SECURITY



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 Plus
Win | Android | Mac | iOS

Kaspersky Premium
Win | Android | Mac | iOS

Kaspersky VPN Secure Connection
Win | Android | Mac | iOS

Kaspersky Safe Kids
Win | Android | Mac | iOS

Kaspersky Password Manager
Win | Android | Mac | iOS

Kaspersky Who Calls*
Android | iOS
*Only available in Russia, Kazakhstan and Indonesia

Kaspersky awards

- Overview
- Top 3 metrics

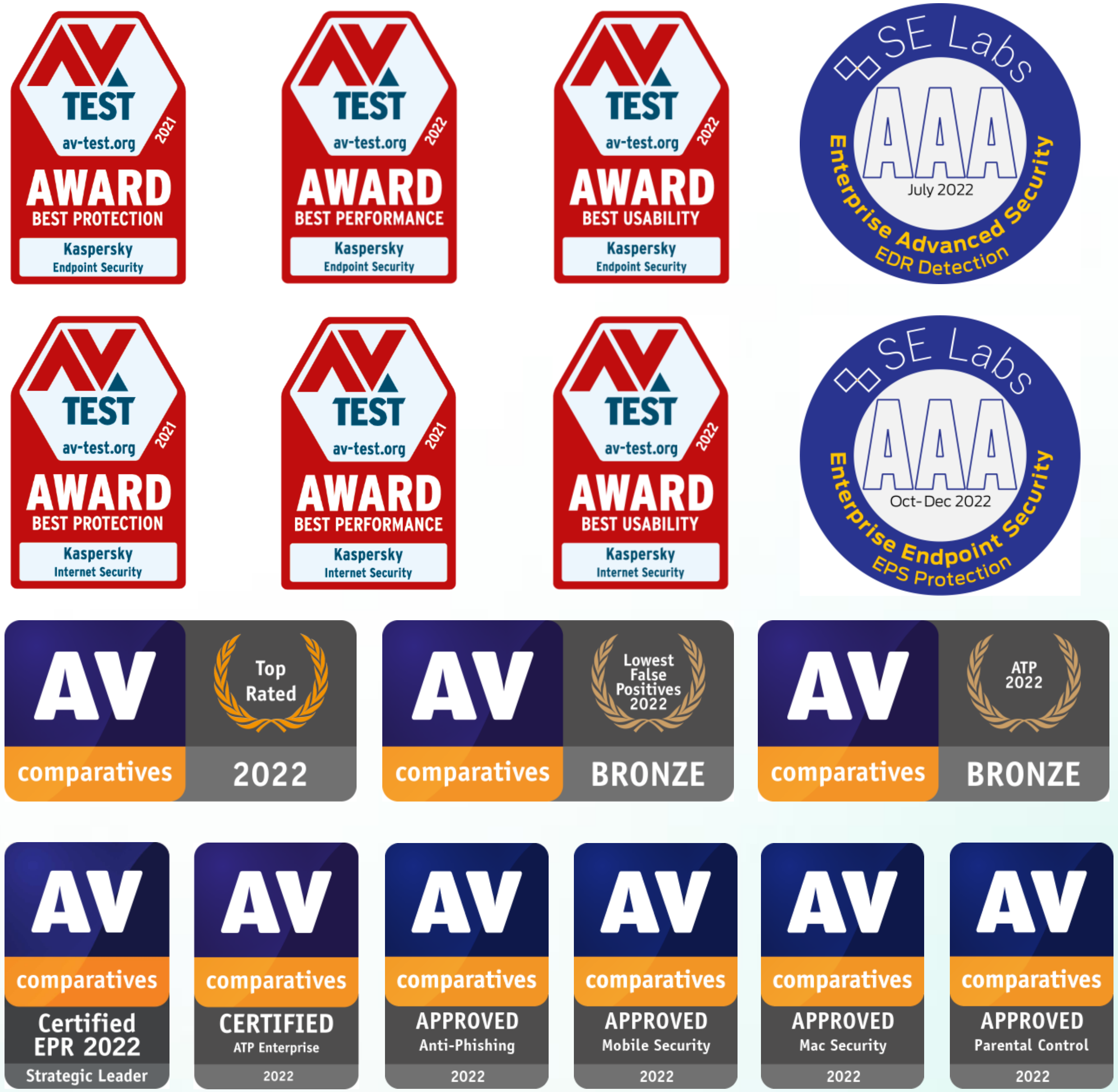
More than 600 awards

One of the five biggest endpoint security vendors*.

Kaspersky Internet Security was honored with the **Top Rated 2022** annual award by independent test lab AV-Comparatives**.

Kaspersky EDR Expert continues to demonstrate top results: Total Accuracy Rating of 100% in Advanced Security EDR test by SE Labs***; and 100% protection from targeted attacks and **Strategic Leader** status from AV-Comparatives****.

Learn more


AV TEST av-test.org 2021 AWARD BEST PROTECTION Kaspersky Endpoint Security
AV TEST av-test.org 2022 AWARD BEST PERFORMANCE Kaspersky Endpoint Security
AV TEST av-test.org 2022 AWARD BEST USABILITY Kaspersky Endpoint Security
SE Labs AAA July 2022 Enterprise Advanced Security EDR Detection
AV TEST av-test.org 2021 AWARD BEST PROTECTION Kaspersky Internet Security
AV TEST av-test.org 2021 AWARD BEST PERFORMANCE Kaspersky Internet Security
AV TEST av-test.org 2022 AWARD BEST USABILITY Kaspersky Internet Security
SE Labs AAA Oct-Dec 2022 Enterprise Endpoint Security EPS Protection
AV comparatives Top Rated 2022
AV comparatives Lowest False Positives 2022 BRONZE
AV comparatives ATP 2022 BRONZE
AV comparatives Certified EPR 2022 Strategic Leader
AV comparatives CERTIFIED ATP Enterprise 2022
AV comparatives APPROVED Anti-Phishing 2022
AV comparatives APPROVED Mobile Security 2022
AV comparatives APPROVED Mac Security 2022
AV comparatives APPROVED Parental Control 2022

*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 Internet Security – was honored with the annual Top Rated 2022 award for high results in 8 Real-World tests, 2 Malware Protection tests, 2 Performance tests, and Enhanced Real-World test of 2022.

Awards

Most Tested*
Most Awarded*
Kaspersky Protection

*Kaspersky.com/top3

86

Tests/Reviews

69

First Places

85%

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 really important for us. In 2022, Kaspersky products participated in 86 independent tests and reviews. Our products were awarded 69 firsts and received 33 top-three finishes.

* 86 independent tests were completed by Kaspersky products in 2022 alongside 14 competitors. More than 90 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

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

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.

Connectivity delivers key benefits
More advanced IPGs connect and communicate with smartphones or tablets over Bluetooth, with apps for clinicians and patients – easier to use and enable better treatment
Firmware can be updated over the air, with new features or bug patches
Growing tension between usability, safety and security. For example, implants need to have a software backdoor and override capability in case of a medical emergency. This makes them safer, but more insecure
Kaspersky.Academy
Partners Summit

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 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 we provide athletes with the opportunity to reach their full potential.

Sponsorships & Partnerships

Chess

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

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

Motorsport

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

Learn more

Gaming

Kaspersky is partnering with several eSports teams across the globe to ensure the best experience for gamers.

Learn more

Bring on the future