kaspersky

Our commitment to Integrity

In today's vast and complex digital world, transparency is a vital element in our pursuit of combatting cybercrime.

Our initiatives and commitments provide us with the foundation to engage with the wider cybersecurity community and stakeholders, giving us invaluable insights into global trends, as well as providing everyone with an opportunity to validate and verify the trustworthiness of our products, internal processes and business operations.

Contents

“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.

Introduction

Kaspersky, one of the largest privately-owned cybersecurity firms in the world, has protected individuals and enterprises throughout the world for 25 years. We have a proud global outlook.

Amidst the current challenging and uncertain times, trust has been shaken internationally within the technology and cyber environment. We are proud of the quality of our products and processes to protect our users from cyberthreats and we are pleased to share the information so that you can be confident in trusting Kaspersky.

We have a proven track record in protecting our four hundred million-plus users and in demonstrating that we are are transparent and independent.

As technology unites the world as never before, trust and cooperation between members of the global cybersecurity industry is paramount. Kaspersky is proud to lead the international fight against cybercrime, through our innovative products and unrivalled threat intelligence. We are also committed to working with partners and to being open and transparent about everything we do.

Our geographical roots may be Russian, but we are — officially, culturally and strategically — a global company. We do not have any ties to any government, including the Russian government.

Our holding company is registered in the UK, we have over 4,500 employees in more than 30 countries, our R&D and security experts are based on four continents, and the majority of our revenue comes from outside of Russia.

Over the following pages, we bring together a wealth of external evidence to demonstrate that we are proven, transparent and independent.

Global Kaspersky

400 million-plus users and **over 240,000 corporate clients worldwide** are protected by our security solutions.

We have more than **25 years' experience** in cybersecurity.

We **operate in 200 countries and territories** across the globe.

And have **34 offices in 31 countries.**

Over **4,500 highly qualified specialists** work for Kaspersky.

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

At Kaspersky, we are guided by the notion that cybercrime has no nationality and knows no borders. It can only be beaten by a truly international approach, marked by collaboration.

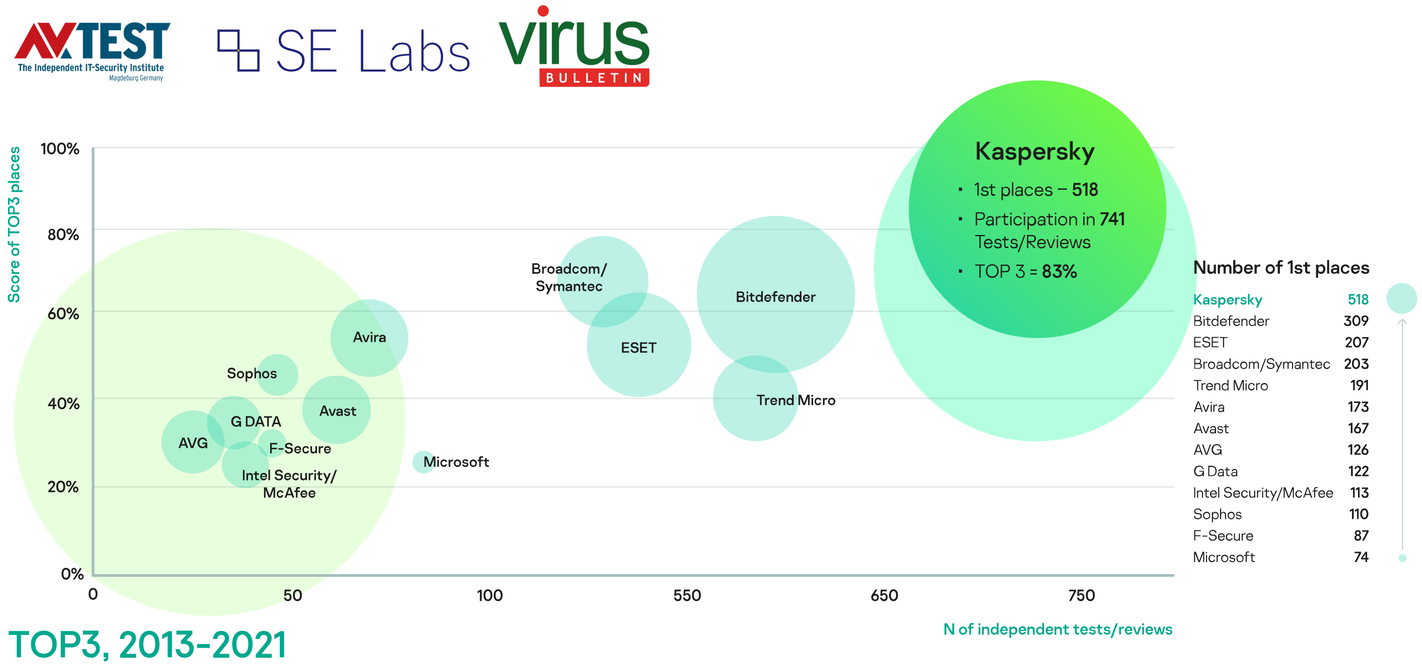
Proven

We are proud of our comprehensive portfolio of security solutions and services. But don’t just take our word for it. Our products excel in third party assessments, against the most rigorous international standard tests and certifications.

Most tested, most awarded.

Kaspersky's enterprise and consumer products routinely score the highest marks in independent ratings and surveys, conducted by some of the best-known labs in the world, such as AV-TEST, SE Labs and Virus Bulletin.

For the past eight years, we have topped the TOP3 metric of global independent tests of over 80 vendors in the security industry. These are the most exacting assessments in the sector and demonstrate that we outperform the competition, time and time again, over a sustained period.



TOP3, 2013-2021

From 2013-2021, Kaspersky took part in 741 independent tests and reviews, with:

- 518 first places
- 612 top three finishes
- Ranking top three in 83% of all assessments

Learn more

Proven

Common Criteria

Kaspersky's Endpoint Security for Windows application, a core part of Kaspersky Endpoint Security for Business, is certified under the Common Criteria for Information Technology Security Evaluation (CC).

This is an international standard for security products; formal recognition that vendors' claims about a security product are valid and have been independently tested to a formalised methodology. It is a global mark of consistency, quality, integrity of code and reliability.

Our Endpoint Security for Windows product has recently been recertified for version 11.6; Kaspersky is one of only two vendors to achieve this certification.

View the certificate

SOC 2

Kaspersky regularly passes security audits to confirm the security and reliability of its engineering practices. In 2022 the company has again successfully passed the Service and Organization Controls 2 (SOC 2) Type 1 audit by a Big Four accountancy firm.

Developed by the American Institute of Certified Public Accountants (AICPA) and recognised globally, this audit is conducted to AICPA's Trust Services Criteria: security, availability, processing integrity, confidentiality and privacy.

The independent assessment confirms that Kaspersky's antivirus bases are protected against unauthorised changes by security controls.

Find out more

ISO 27001

Kaspersky also regularly certifies its data systems under the ISO 27001 international standard for information security, by external analysts TÜV Austria.

More formally known as the ISO/IEC 27001:2013, this is another international standard; a collection of best practices for security management measures to protect information and customer's data. We are proud that recertification once again demonstrates our commitment to strong information security.

View the certificate

Working with the global IT security community

Kaspersky cooperates closely with numerous international organisations and law enforcement agencies, participating in joint operations, cyber threat investigations, cyber diplomacy and promoting an open and safe internet.

This multi-stakeholder approach is based on trust, collaboration and transparency. Notable examples include:

INTERPOL

As part of our long-term relationship with INTERPOL, we provide human resources support, training, digital forensics tools and threat intelligence data on the latest cybercriminal activity. Cybercrime is borderless and our work with INTERPOL is vital to prevent attacks across the globe.

No More Ransom

Kaspersky founded the No More Ransom initiative with Europol, the Dutch national police and McAffee in 2016, to help victims of ransomware to decrypt files. There are now 188 partners and the initiative has supported more than 1.5 million people worldwide.

ENISA

We are involved with several studies and publications with the European Cyber Security Agency, ENISA.

Kaspersky security researchers provide their expertise and contribute to ENISA reports.

The Geneva Dialogue on Responsible Behaviour in Cyberspace

Kaspersky is a member of this international process to discuss the security of digital products, led by the Swiss Federal Department of Foreign Affairs and implemented by DiploFoundation.

PARIS CALL

Kaspersky is a signatory to this initiative to promote trust and security in cyberspace, launched by French President Emmanuel Macron in 2018.

Proven

Coalition against Stalkerware

In cooperation with a wide variety of international partners, we helped to launch this initiative against a type of commercial spyware, so protecting users against stalking, domestic violence, harassment and sexual abuse.

The coalition continues to grow and is backed by non-governmental organisations and partners working in domestic violence survivor support, digital rights advocacy, IT security and academic research.

Coalition Against Stalkerware

Multi-stakeholder cooperation

- **The Council of Europe** to promote an open and safe internet
- The **German platform Industrie 4.0**
- Four European Union **Horizon 2020** projects

ENGAGIERT IN DER PLATTFORM INDUSTRIE 4.0

Horizon 2020 Programme

Transparent

We believe in being open, honest and ethical in everything we do.

Global Transparency Initiative

We launched our pioneering Global Transparency Initiative (GTI) in 2017 and it's become an international benchmark for digital trust and accountability. It aims to engage the broader international security community and other stakeholders in validating and verifying the trustworthiness of Kaspersky products, internal processes and business operations.

Find out more

Transparent

Through GTI, we have taken these clear and accountable steps:

1 Relocation of the cyberthreat-related data processing and storage to Switzerland

Cyberthreat-related data shared by our users in Europe, North and Latin America, the Middle East and several countries in Asia-Pacific has been relocated to two world-class data centers in Zurich, Switzerland. Here, it is securely processed and stored under Switzerland's strict data protection regulations.

2 A global network of Transparency Centers

We have established a network of Transparency Centers, where our trusted partners and government stakeholders can review our products' source code, software updates and threat detection rules, to satisfy themselves that we are open and transparent about our solutions' features and capabilities.

No other cybersecurity provider has undertaken a similar initiative on this scale.

Visitors can also learn more about our portfolio, engineering and data processing practices. We are also happy to arrange remote visits.

The Centers are located in:

- Zurich, Switzerland
- Madrid, Spain
- Kuala Lumpur, Malaysia
- Sao Paulo, Brazil
- Utrecht, the Netherlands
- Rome, Italy
- Tokyo, Japan
- Singapore
- Woburn, MA, USA

Find out more

3 Third party auditing

Rigorous independent auditing confirms the integrity of our solutions and processes. See details on our SOC 2 Type 1 audit and ISO 27001 certification on page 8 for more information.

Learn more about SOC2

Learn more about Kaspersky's ISO 27001

4 Vulnerability management program

Our Bug Bounty initiative offers rewards of up to $100,000 for the discovery of critical flaws in our leading products.

With this initiative, we strive to maintain the security of our programs. We are careful not to create new risks and problems as we identify any errors and adhere to five ethical principles for responsible vulnerability disclosure.

5 Cyber capacity building program

A dedicated training programme in evaluating product security. This is aimed at businesses, governmental organisations and academic institutions, to help them develop the knowledge and skills to assess supply chain cyber resilience.

Find out more

6 Transparency report

Kaspersky regularly and publicly shares its approach in responding to requests from global government and law enforcement agencies for two categories: user data and technical expertise. We also disclose the number of requests per country. See page 16.

The company also receives requests from its users to learn about personal data processing and every six months Kaspersky shares a number of such requests.

Find out more

Data security

Kaspersky's approach to processing data is based on respecting and protecting people's privacy, as well as on a commitment to transparency and accountability.

For the functionality of its cybersecurity solutions, Kaspersky may process cyberthreat-related data and statistics. The cyberthreat-related data includes suspicious or previously unknown malicious files that the company's products send to the Kaspersky Security Network (KSN) for automated malware analysis, if Kaspersky users agree to do so (and accept the KSN Statement).

Whenever data is processed, we use the highest standards for data protection to protect user data and guarantee the security and privacy of our users. Kaspersky's security measures for protecting data include a number of tools such as encryption, digital certificates, and strict access policies.

We comply with the laws of all countries in which we operate and make every effort to ensure that user data is secure.

Dealing with government and law enforcement agency requests

As part of our transparent and accountable approach, Kaspersky responds to requests for data from various countries. However, we will only share information if the request is legally justified, complies with other legal requirements and does not create risks to the security and integrity of our products. In every case, we assess whether or not to approve requests according to our core principles.

We never:

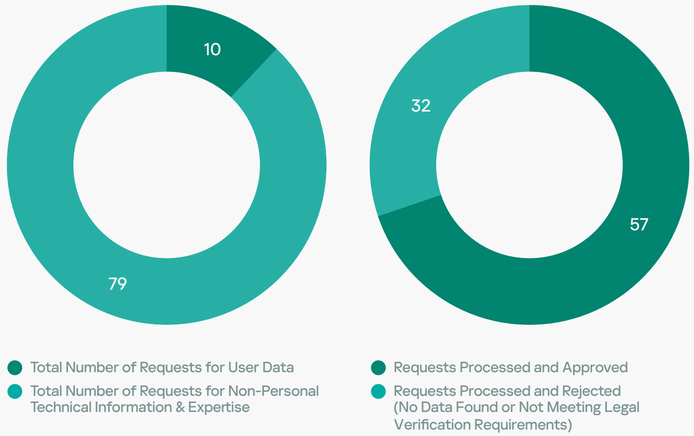
- Provide governments or law enforcement agencies with access to user data or the company's infrastructure
- Provide them with encryption keys, or add undeclared capabilities to our products and services

We always:

- Ensure that our response to requests complies with all applicable laws and procedures

We regularly share our approach towards working with these requests and in 2021 we began to report on both the number of requests we receive — and whether we accepted or rejected them.

In the first half of 2022, we received a total number of 89 requests andrejected 32% of them



Read full report

Independent

As a private company we are independent from short term business considerations and institutional influence.

We share our expertise, knowledge and technicalfindings with the world's security community. Kaspersky has no ties to any government or country.

Our finances

Although our geographical roots are Russian, we operate across the world and the majority of our revenue comes from outside of Russia. Our holding company, Kaspersky Labs Limited (KLL) is registered in the UK, in London.

There are plenty of legally independent Kaspersky national companies operating worldwide, including 11 entities in Europe, all subsidiaries of KLL. All pay their taxes, salaries and social security contributions in Europe. Our local businesses are run by local entities, which gives us the opportunity to independently control our international and local operations.

Global Research and Analysis Team (GReAT)

Established in 2008, the GReAT team is at the very heart of Kaspersky. It is one of our most important assets in fighting cybercrime and comprises over 35 top security researchers from all over the world: Europe, Russia, the Americas, Asia and the Middle East. GReAT is managed from Bucharest, Romania.

They bring unrivalled expertise, passion and curiosity to the discovery and analysis of cyber threats and have detected some of the biggest campaigns, from Stuxnet in 2010 to the more recent Lazarus, BlueNoroff and Moonlight Maze.

They track, analyse, interpret and mitigate constantly evolving threats, whatever their origin and whatever their purpose. There are no limits on which threat actors to track. Over the years, GReAT has published a number of reports about APT attacks with Russian language included in the code.

In 2020, the GReAT team won Industry Team of the Year at the Annual Cyber Security Awards for their ongoing leadership and expertise in the field and for their response to the Covid-19 pandemic.

They are committed to sharing information with other researchers around the world so that, together, global experts can fight computer viruses more effectively.

Language	Threat
Russian	RedOctober, CloudAtlas, Miniduke, CosmicDuke, Epic Turla, Penguin Turla, Turla, Black Energy, Agent. BTZ, Teamspy, Sofacy, Lurk, GCMAN, Metel, Carbanak, MontysThree
English	Regin, Equation, Duqu 2.0, Flame, ProjectSauron
Chinese	IceFog, SabPub, Nettraveler, Danti, MosaicRegressor, CosmicStrand
Spanish	Careto/Mask, El Machete
Korean	DarkHotel, Kimsuky, Lazarus, BlueNoroff
French	Animal Farm
Arabic:	Desert Falcons, StoneDrill, Shamoon

Cybersecurity is a constantly evolving practice, dealing with ever changing threats. At Kaspersky, we want the very best for our customers; this has always been our mission.

If you have any questions, please reach out to us via email at **B2B@kaspersky.com**
We'll get back to you as soon as we can.

www.kaspersky.com