

What you should know about Kaspersky Lab



Proven.
Transparent.
Independent.

Fighting for your digital freedom

Your data and privacy are under attack by cybercriminals and spy agencies, so you need a partner who is not afraid of standing beside you to protect what matters to you most. For over 20 years, Kaspersky Lab has been catching all kinds of cyberthreats. No matter whether they come from script kiddies, cybercriminals or governments, or from the north, south, east or west. We believe the online world should be free from attack and state-sponsored espionage, and will continue fighting for a truly free and safe digital world.

Proven

Kaspersky Lab routinely scores the highest marks in independent ratings and surveys.

- Measured alongside **more than 100** other well-known vendors in the industry
- **72 first places** in 86 tests in 2017
- **Top 3 ranking*** in 91% of all product tests
- In 2017, Kaspersky Lab received **Platinum Status** for Gartner's Peer Insight** Customer Choice Award 2017, in the Endpoint Protection Platforms market

Our Global Research and Analysis Team has been actively involved in the discovery and disclosure of some of the most prominent malware attacks with links to governments and state organizations.

Transparent

We are totally transparent and are making it even easier to understand what we do:

- Independent review of the company's source code, software updates and threat detection rules
- Independent review of internal processes
- Three transparency centers by 2020
- Increased bug bounty rewards with up to \$100K per discovered vulnerability

* www.kaspersky.com/top3

** <https://www.gartner.com/reviews/customer-choice-awards/endpoint-protection-platforms>

Independent

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

We share our expertise, knowledge and technical findings with the world's security community, IT security vendors, international organizations, and law enforcement agencies.

Our research team is spread across the world and includes some of the most renowned security experts in the world. We detect and neutralize all forms of advanced APTs, regardless of their origin or purpose.

About Kaspersky Lab

We are one of the world's largest privately-owned cybersecurity companies.



We operate in **200** countries and territories



and have **35** offices in **31** countries.



Over **4,000** highly-qualified specialists work for Kaspersky Lab.



We pride ourselves on developing world-leading security that keeps us – and every one of our **400 million** users protected by our technologies,



and **270,000** corporate clients – one step ahead of potential threats.

Kaspersky Lab is a global cybersecurity company which has been operating in the market for over 20 years. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into next generation security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats.

As a private company, Kaspersky Lab does not have ties to any government, and the company has never helped, nor will help, any government in the world in its cyberespionage efforts.



Our Global Transparency Initiative

Kaspersky Lab is committed to protecting customers from cyberthreats, regardless of their origin or purpose. The company's Global Transparency Initiative is aimed at engaging the broader information security community and other stakeholders in validating and verifying the trustworthiness of its products, internal processes, and business operations. It also introduces additional accountability mechanisms by which the company can further demonstrate that it addresses any security issues promptly and thoroughly.

The initial phase of Kaspersky Lab's Global Transparency Initiative will include:

1. Initiating an independent review of the company's source code with similar reviews of the company's software updates and threat detection rules to follow;
2. Commencing an independent assessment of (i) the company's secure development lifecycle processes, and (ii) its software and supply chain risk mitigation strategies;
3. Development of additional controls to govern the company's data processing practices in coordination with an independent party that can attest to the company's compliance with said controls;
4. Formation of three Transparency Centers globally, with plans to establish the first one in 2018, to address any security issues together with customers, trusted partners and government stakeholders; the centers will serve as a facility for trusted partners to access reviews on the company's code, software updates, and threat detection rules, along with other activities. The Transparency Centers will open by 2020;
5. Increasing bug bounty awards up to \$100,000 for the most severe vulnerabilities found under Kaspersky Lab's Coordinated Vulnerability Disclosure program, to further incentivize independent security researchers to supplement the company's vulnerability detection and mitigation efforts.



«Internet balkanization benefits no one except cybercriminals. Reduced cooperation among countries helps the bad guys in their operations, and public-private partnerships don't work like they should. We need to reestablish trust in relationships between companies, governments and citizens».

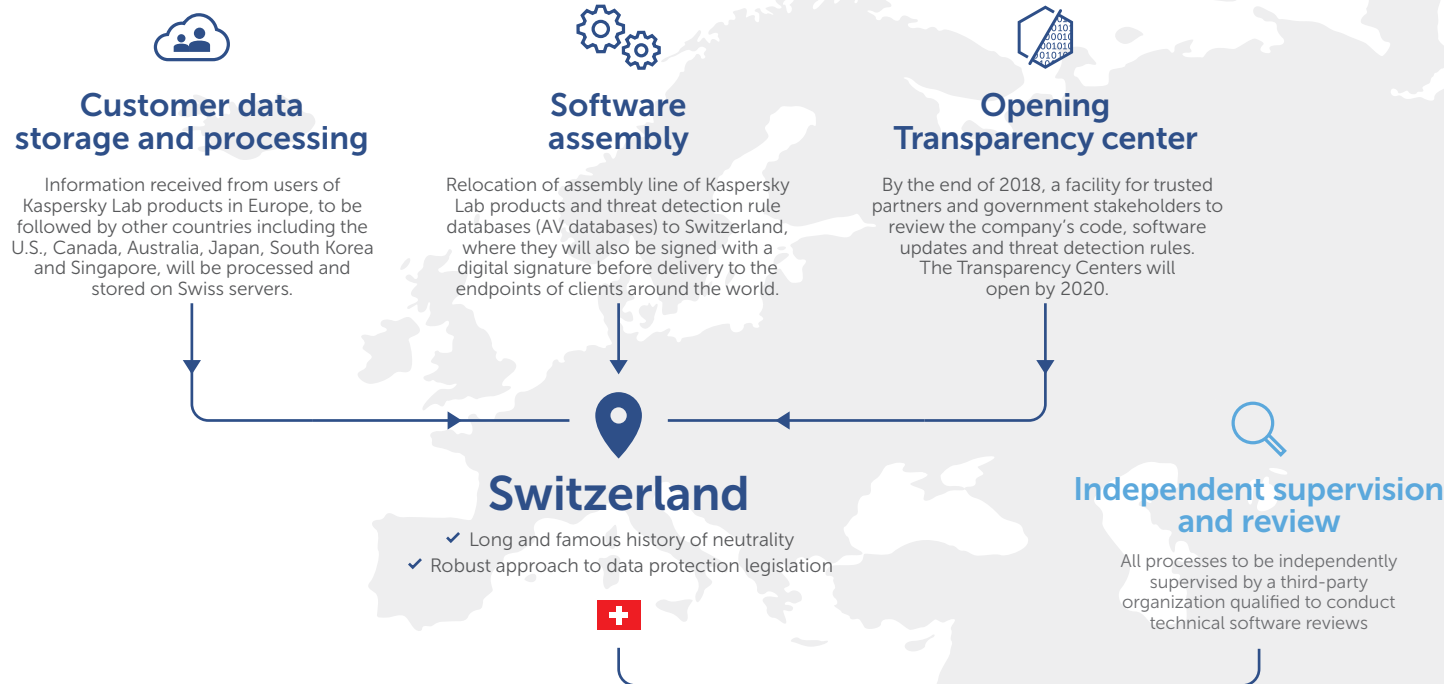
Our Global Transparency Initiative:

Kaspersky Lab moves core infrastructure to Switzerland

As part of its Global Transparency Initiative, Kaspersky Lab is adapting its infrastructure to move a number of core processes from Russia to Switzerland.

This includes customer data storage and processing, as well as software assembly, including threat detection updates.

To ensure full transparency and integrity, Kaspersky Lab is arranging for this activity to be supervised by an independent third party, also based in Switzerland.



Kaspersky Lab's principles for fighting cyberthreats

Kaspersky Lab is determined to detect and neutralize all forms of malicious programs, regardless of their origin or purpose. It does not matter which language the threat "speaks": Russian, Chinese, Spanish, German, or English. The company's experts have published at least 17 reports about APT attacks with Russian-language included in the code. This is more than any other U.S.-based company.

The following list of threats, as reported by Kaspersky Lab's GReAT team, shows the different languages used in each threat:

- **Russian language:** Moonlight Maze, RedOctober, CloudAtlas, Miniduke, CosmicDuke, Epic Turla, Penguin Turla, Turla, Black Energy, Agent.BTZ, Teamspy, Sofacy (aka Fancy Bear, APT28), CozyDuke
- **English language:** Regin, Equation, Duqu 2.0, Lamberts, ProjectSauron
- **Chinese language:** IceFog, SabPub, Nettraveler, Spring Dragon, Blue Termite
- **Spanish language:** Careto/Mask, El Machete
- **Korean language:** Darkhotel, Kimsuky, Lazarus
- **French language:** Animal Farm
- **Arabic language:** Desert Falcons, Stonedrill and Shamoon













One of Kaspersky Lab's most important assets in fighting cybercrime is its Global Research & Analysis Team (GReAT), comprising top security researchers from all over the world – Europe, Russia, the Americas, Asia, and the Middle East.

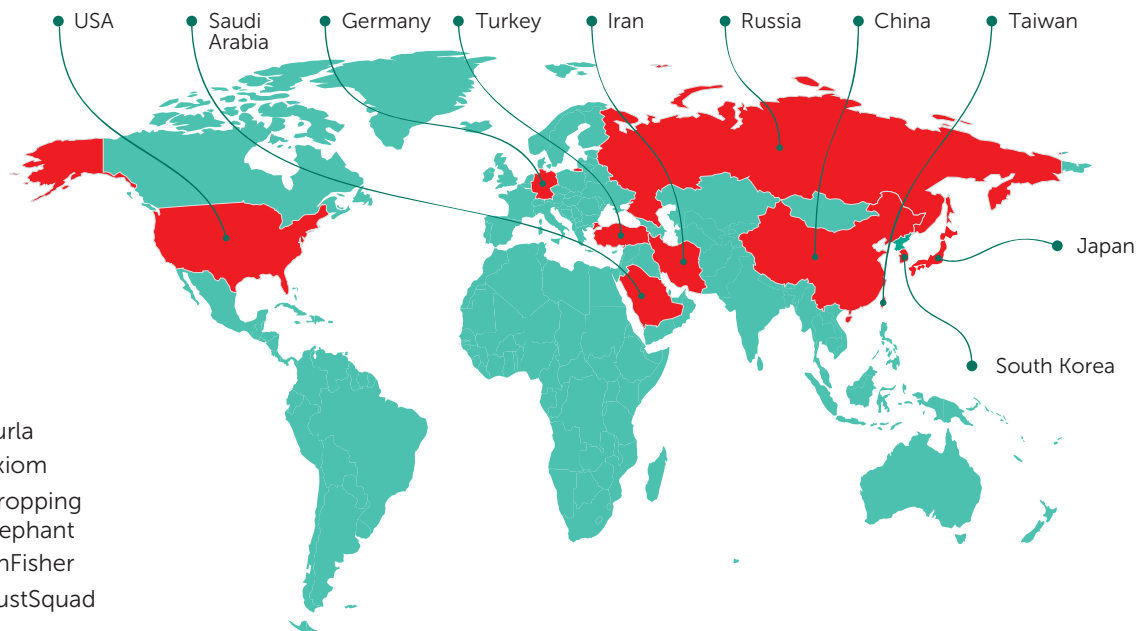
Advanced Persistent Threat Landscape in 2017

According to Kaspersky Lab's GReAT team, in 2017 the top target for APTs were governments; and the most significant threat actor was Lazarus.

Top 10 targets:

-  Government
-  Education
-  Financial institutions
-  Military
-  Diplomatic
-  Energy
-  IT companies
-  Telecommunications
-  Political parties
-  Military contractors

Top 10 targeted countries:



Top 10 significant actors:

- | | |
|--|---|
|  1 Lazarus |  6 Turla |
|  2 Sofacy |  7 Axiom |
|  3 Lamberts |  8 Dropping Elephant |
|  4 BlueNoroff (part of Lazarus) |  9 FinFisher |
|  5 Equation group |  10 DustSquad |



Principles for the processing of user data

Respecting and protecting people's privacy is a fundamental principle of Kaspersky Lab's approach to processing users' data. The data that is processed is crucial for identifying new and as yet unknown threats – such as WannaCry and ExPetr – and offering better protection products to users. Analyzing big data from millions of devices to strengthen protection capabilities is an industry best practice that is applied by IT security vendors around the world. It is a must for securing users' digital lives from cyberthreats.

Users of Kaspersky Lab products can always choose how much data they provide, based on the product or service used and the respective agreements accepted. All data processed and/or transferred is robustly secured through encryption, digital certificates, segregated storage, strict data access policies and by other methods.

What is Kaspersky Security Network?

Kaspersky Security Network (KSN) is one of Kaspersky Lab's main cloud systems that was created to maximize the effectiveness of discovering new and unknown cyberthreats and thereby ensure the quickest and most effective protection for users. KSN is an advanced cloud-based system that automatically processes cyberthreat-related data received from millions of devices owned by Kaspersky Lab users across the world, who have voluntarily opted to use this system.

This cloud-based system approach is now the industry standard, applied by many global IT security vendors.

How do you anonymize the data you process?

Kaspersky Lab takes user privacy extremely seriously. The company implements the following measures to anonymize obtained data:

- The information is used in the form of aggregated statistics;
- Logins and passwords are filtered out from transmitted URLs, even if they are stored in the initial browser request from the user;
- When we process possible threat data, by default we do not use the suspicious file. Instead we use hash-sum, which is a one-way math function that provides a unique file identifier;
- Where possible, we obscure IP addresses and device information from the data received;
- The data is stored on separated servers with strict policies regarding access rights, and all the information transferred between the user and the cloud is securely encrypted.

Kaspersky Lab's role in the global IT security community

Kaspersky Lab participates in joint operations and cyberthreat investigations with the global IT security community, international organizations such as INTERPOL, law enforcement agencies and CERTs worldwide. Kaspersky Lab is the official partner of Europol.

- We hold **regular training courses** for INTERPOL officers and the police forces of many countries, e.g. City of London Police.
- We provide **expert speakers** at conferences around the globe, e.g. World Economic Forum in Davos.
- We host the **annual Kaspersky Lab Security Analyst Summit** which brings together the world's foremost IT security experts.
- We are a part of the **Securing Smart Cities** not-for-profit global initiative that aims to solve the existing and future cybersecurity problems of smart cities.
- We are a **member of the Industrial Internet Consortium** that helps organizations to more easily connect and optimize assets and operations to drive agility across all industrial sectors.
- We launched the **No More Ransom** initiative in July 2016 jointly with the Dutch National Police, Europol and Intel Security. The non-commercial initiative that united public and private organisations and aims to inform people of the dangers of ransomware, and helps them to recover their data without having to pay the criminals.

Cooperation with law enforcement agencies

As a private company, we have no political ties to any government but are proud to collaborate with the authorities of many countries, as well as international law enforcement agencies, and commercial and public entities in fighting cybercrime. We work with local authorities in the best interests of international cybersecurity, providing technical consultations or expert analysis of malicious programs, in compliance with court orders or during investigations – all in accordance with industry standards.

What others say

«IDC believes that, before making their own decisions, organizations should demand convincing evidence and, until this is presented, continue buying and using Kaspersky Lab's products.»

Dominic Trott,
Associate Research Director – European Security at IDC,
commenting on the European Parliament vote on Report
on Cyber Defence that includes referencing Kaspersky Lab
based on untrue statements.

«Balkanization, especially in the cyber security community, is happening and needs to be corrected. Kaspersky Lab is fighting against cyber criminals, and working with governments and companies across the world to address the issue.»

Noboru Nakatani,
Former Executive Director of Global Complex
for Innovation, Interpol

«Given that no evidence has been presented, other than the fact that Kaspersky Lab is a Russian company and Eugene Kaspersky worked as a software engineer for Soviet military intelligence, the targeting of Kaspersky Lab feels like a Cold War witch hunt.»

James Nuns,
Journalist CBROnline

«Martijn Grooten, editor of the Virus Bulletin, a U.K.-based information portal on information security, said he hoped the move would help 'take away some of the distrust between Kaspersky and Western governments, as I don't think there's a good reason for this distrust'.»

David Gauthier-Villars and Dan Strumpf,
The Wall Street Journal

«'Our government hasn't even been clear about what they're accusing Kaspersky of,' says Rob Graham, a security consultant for the firm Erratasec. 'We're just getting propaganda on this issue and no hard data. And that's bad'.»

Andy Greenberg,
WIRED

«Nowadays the political turmoil has zoomed in on and singled out your company, without reflecting all you and your company have done in over 20 years for security and the fight against digital crime. These decisions are not made by us and unfortunately also not ours to make. Politicians make those decisions based on their agendas which in too many cases are not in our interests.»

Dr. ir Johannes Drooghaag
in an open letter to Eugene Kaspersky

Do you work with governments?

Kaspersky Lab has no political ties to any government or country. We do, indeed, regularly cooperate with international organizations, such as INTERPOL, to help fight global cybercrime, and work with law enforcement agencies in a number of countries, including the U.S. and within the EU, providing technical analysis of malicious programs during investigations.

Are you a Russian company?

Officially, culturally and strategically we are a global cybersecurity company even though our geographical roots are Russian. Our holding company is registered in the U.K., we have over 4,000 employees in 31 countries, our research centers are based on three continents, and over 82% of our revenue comes from outside of Russia. This further demonstrates that working inappropriately with any government would be detrimental to the company's bottom line, as we would then risk the largest part of our business.

Eugene Kaspersky, CEO, Kaspersky Lab

Eugene Kaspersky is a world-renowned cybersecurity expert and successful entrepreneur. He has been the Chief Executive Officer of Kaspersky Lab since 2007.

Eugene began his career in cybersecurity accidentally when his computer became infected with the 'Cascade' virus in 1989. Eugene's specialized education in cryptography helped him analyze the encrypted virus and understand its behavior and then develop a removal tool for it.



After successfully removing the virus, Eugene's curiosity and passion for computer technology drove him to start analyzing more malicious programs and developing disinfection modules for them.

Further pursuing his passion for defensive technologies, in 1990 Eugene started gathering a team of like-minded enthusiast researchers to create the AVP Toolkit Pro antivirus program, which four years later, was recognized by the University of Hamburg as the most effective antivirus software in the world. Wishing to combine their successful track record of antivirus programming with their entrepreneurial vision, Eugene and his colleagues decided to establish their own independent company. In 1997 Kaspersky Lab was founded, with Eugene heading the company's antivirus research.

In 2007 Eugene Kaspersky was named Kaspersky Lab's CEO.

Eugene has earned a number of international awards for his technological, scientific and entrepreneurial achievements. He was voted the World's Most Powerful Security Exec by SYS-CON

Media in 2011, awarded an Honorary Doctorate of Science from Plymouth University in 2012, and named one of Foreign Policy Magazine's 2012 Top Global Thinkers for his contribution to IT security awareness on a global scale.

Does or did your CEO work for Russian intelligence agencies?

The only affiliation Eugene ever had with the KGB, was studying cryptography and mathematics at the Higher School, co-sponsored by the KGB and the Soviet Ministry of Defense. After studying there, Eugene served as a software engineer in the Soviet Ministry of Defense, which is not the KGB. He has got a military rank, as all graduates of the Higher School received a rank automatically upon graduation. Eugene has no relationship with high ranking governmental officials in Russia. For the 20 years that Kaspersky Lab has existed, the company has never had any inappropriate ties with any government or law enforcement agencies.



© 2018 Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.