KASPERSKY lab

What You Should Know

About Kaspersky Lab

Kaspersky Lab is a private, international company that operates in almost 200 countries and territories, protecting over 400 million people and 270,000 companies worldwide.

The company has R&D centers and anti-malware experts around the world, including the United States, Europe, Japan, Israel, China, Russia and Latin America. More than 80 percent of its sales and operations are outside of Russia.

The company's North American headquarters is located in Woburn, Massachusetts. Kaspersky Lab employs more than 300 people in North America, including cyber experts from the company's renowned Global Research and Analysis Team (GReAT).

With more than 20 years of experience, Kaspersky Lab is the world's largest privately owned cybersecurity company, and it consistently ranks among the world's top four vendors of security solutions for endpoint users (IDC, 2017).[1] In addition to leading endpoint protection, the company's comprehensive security portfolio includes a number of specialized solutions and services to fight sophisticated and evolving digital threats.

1. IDC, *Worldwide Endpoint Security Market Shares, 2016: Competition Gets Fierce,* # US42553717, May 2017

Kaspersky Lab Principles for Fighting Cyberthreats

As an IT security company, Kaspersky Lab is determined to detect and neutralize all forms of malicious programs, regardless of their origin or purpose. One of Kaspersky Lab's most important assets in fighting cybercrime is its Global Research & Analysis Team (GReAT), comprised of elite security researchers located in every major region across the world. The company's research team is actively involved in the discovery and disclosure of a significant proportion of the world's major malware attacks.

Kaspersky Lab remediates any malware it discovers, regardless of its potential origin. The company is committed to protecting the world from cyberthreats, and Kaspersky Lab has not, and will never, help any government with its cyberespionage activities. The company only develops defensive capabilities that protect people and businesses from digital attacks, and it will never assist any government or organization with its offensive efforts in cyberspace.

Cooperation with Law Enforcement Agencies and Governments

As a private company, Kaspersky Lab has no political ties to any government, and the company routinely collaborates with local, regional and international law enforcement agencies, along with the global IT security community, to fight cybercrime. Collaborating partners include (but are not limited to) INTERPOL, Europol, Microsoft Digital Crimes Unit, The National High Tech Crime Unit (NHTCU) of the Netherlands' Police Agency, CyberSecurity Malaysia and The City of London Police, as well as Computer Emergency Response Teams (CERTs) worldwide. Kaspersky Lab works with these organizations in the best interests of international cybersecurity, providing technical expertise and forensic analysis of malicious programs, during investigations and in compliance with court orders.

In July 2016, the Dutch National Police, Europol, Intel Security and Kaspersky Lab launched the No More Ransom project, a non-commercial initiative that unites public and private organizations to inform people on the dangers of ransomware. Through No More Ransom's 40 free decryption tools, five of which Kaspersky Lab developed, people can recover their data without having to pay cybercriminals. For more information, visit https://www.nomoreransom.org.

Kaspersky Lab Does Not Have Political Ties to ANY Government

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 with its cyberespionage efforts. For 20 years, Kaspersky Lab has focused on protecting people and organizations from cyberthreats, and the location of its headquarters does not change that mission.

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 with its cyberespionage efforts.

Ongoing Cooperation with the IT Security Industry

Kaspersky Lab believes that joint effort is the most effective way of fighting cybercriminals. The company openly shares its knowledge and technical findings with the world's IT security community. It regularly publishes its research for the wider public to protect organizations from identified threats, encourage collaborative security practices and increase international cooperation.

Kaspersky Lab also collaborates in joint cyberthreat investigations with companies and organizations such as Adobe, AlienVault Labs, Dell Secureworks, Crowdstrike, OpenDNS Security Research Team, GoDaddy Network Abuse Department, Seculert, SurfNET, Kyrus Tech Inc. and Honeynet Project.

Kaspersky Lab fully supports and abides by the industry best practice of confidentially reporting vulnerabilities discovered during cybersecurity research in order to allow vendors adequate time to develop and release security updates that protect users. In addition, as a security vendor itself, Kaspersky Lab supports the use of coordinated vulnerability disclosure programs like bug bounties, which incentivize security researchers to test and improve the resiliency of its own products.

Trusted, Tested and Proven Technologies and Solutions

For more than 20 years, Kaspersky Lab has been dedicated to excellence and continuously evolving its solutions to address the dynamic cyberthreat landscape. To continue detecting and preventing cybercrimes effectively, the company invests in the best specialists, education, research and development of new solutions to ensure industry-leading protection.

Kaspersky Lab routinely scores at the highest level in numerous independent ratings and surveys. The company has received some of the most prestigious international awards and several first and top-three places in independent tests conducted by leading entities in North America, Europe and Asia (such as AV-Test of Germany, AV-Comparatives in Austria, Dennis Technology Labs in London, etc.).

Kaspersky Lab technologies are trusted by more than 120 global technology and OEM partners including Microsoft, Amazon Web Services, Cisco, Kaseya, Asus, Lenovo, Juniper Networks, Check Point, D-Link, Clearswift, Netgear, ZyXel, Alt-N, Parallels, H3C and Trustwave.

Kaspersky Lab Product Certifications

Kaspersky Lab routinely attains licenses and certifications from the countries it operates in, including one from the U.S. National Institute of Standards and Technology, certifying the company's encryption technologies for businesses as fully compliant with the Federal Information Processing Standards (FIPS) 140-2. These certifications and licenses demonstrate Kaspersky Lab products are trusted to secure sensitive data and are protecting organizations without any issues or unexpected behaviors.

Principles of Protecting Privacy

Privacy is a basic right, and Kaspersky Lab is diligently investing time and resources into protecting privacy on a global scale. The company investigates advanced cyberespionage and surveillance campaigns violating people's privacy such as HackingTeam's legal spyware or Computrace software, and this research often leads to the disruption of such cybercriminal activities.

Hundreds of millions of people around the globe trust Kaspersky Lab to protect the data that matters most to them. Kaspersky Lab takes this responsibility seriously, which is why its products and technologies do not process private data. Kaspersky Security Network (KSN) is an automated cloud-enabled system that processes depersonalized cybersecurity-related data streams from millions of voluntary participants around the world. This data helps to identify emerging threats more quickly and precisely to incorporate new protection measures as fast as possible.

Unlike in many other products on the market today, Kaspersky Lab users have full control over telemetry (data) sharing with their participation in KSN being voluntary, and they may disable telemetry reporting completely at any given time. In addition, business and government users may choose to install a local and private KSN center on their premises to make sure the data never leaves their facility.

Kaspersky Lab Investigates and Reports on All Cyberthreats it Discovers

Kaspersky Lab reports on any kind of threat discovered, and it does not matter which language the threat 'speaks' - Russian, Chinese, Spanish, German or English. The company's experts published at least 17 reports about APT attacks with Russian-language included in the code. Due to the company's unique and global customer base, Kaspersky Lab will continue demonstrating its leadership by finding and reporting global cyberthreat campaigns, regardless of the origin or intention.

The following list, as reported by the GReAT team, provides a sample of threats and the language used in each case:

- **Russian language:** RedOctober, CloudAtlas, Miniduke, CosmicDuke, Epic Turla, Penquin Turla, Black Energy, Agent.BTZ, Teamspy, Satellite Turla, CozyDuke, Sofacy, xDedic, KopiLuwak Turla
- **Chinese language:** IceFog, SabPub, Nettraveler, Naikon, Danti
- **Arabic language:** Desert Falcons, Shamoon / StoneDrill
- **Spanish language:** Careto/Mask, El Machete, Saguaro
- **Korean language:** Darkhotel, Kimsuky, Lazarus
- **English language:** Regin, Equation, Duqu 2.0, ProjectSauron
- **French language:** Animal Farm


Duqu 2.0


Regin


IceFog


Darkhotel


Animal Farm


Desert Falcons

Kaspersky Lab Does Not Provide Attribution

Attribution of threat actors on the Internet is incredibly difficult given that attackers often include false information to mislead investigators. The company's policy is to focus on the technical analysis of cyberthreats and the sharing of Indicators of Compromise (IOCs) to help protect customers around the world. Therefore, Kaspersky Lab does not definitively attribute attacks to specific entities or nation-states.

Facts Refuting False Allegations and Erroneous Conclusions

U.S. government intelligence sources have questioned the relationship between Kaspersky Lab and the Russian government, given that the company's headquarters is located in Moscow.

As a private company, Kaspersky Lab has no ties to any government, and the company has never helped, nor will help, any government in the world with its cyberespionage efforts. In addition, during the last 10 years, Kaspersky Lab has discovered and publicly reported on multiple Russian-speaking cyber espionage campaigns, which is more than any other U.S.-based company.

Unlike in many other products, Kaspersky Lab users have full control over telemetry (data) sharing with their participation being voluntary, and they can disable telemetry reporting completely at any given time. Additionally, business and government users may choose to install a local and private Kaspersky Security Network (KSN) center on their premises to make sure the data never leaves their facility.

The company has a 20-year history in the IT security industry of always abiding by the highest ethical business practices. Kaspersky Lab is available to assist all concerned government organizations with any investigations, and the company ardently believes a deeper examination of Kaspersky Lab will confirm that these allegations are unfounded.

For 20 years, Kaspersky Lab has been focused on protecting people and organizations from cyberthreats, and its headquarters' location doesn't change that mission--just as a U.S.-based cybersecurity company doesn't allow access to or send any sensitive data from its products to the U.S. government, Kaspersky Lab products also do not allow any access or provide any private data to any country's government.

Kaspersky Lab routinely attains licenses and certifications from the countries it operates in, including one from the U.S. National Institute of Standards and Technology, certifying the company's encryption technologies for businesses as fully compliant with the Federal Information Processing Standards (FIPS) 140-2. These certifications and licenses demonstrate Kaspersky Lab products are trusted to secure sensitive data and are protecting organizations without any issues or unexpected behaviors.

About Our Chairman and CEO, Eugene Kaspersky

Eugene Kaspersky has been the CEO of Kaspersky Lab since 2007. He grew up in the Soviet era, when almost every education opportunity was sponsored by the government in some manner. After graduating from a prestigious Soviet high school with a focus in mathematics, he then studied cryptography at a university that was sponsored by four state institutions, one of which was the KGB. Upon graduating in 1987, he was placed at a Ministry of Defense (MoD) scientific institute, where he served as a software engineer. Contrary to misinformed sources, serving as a software engineer was the extent of his military experience, and he never worked for the KGB.

Eugene's interest in cybersecurity began when he discovered the 'Cascade' virus on his computer. His specialized education in cryptography helped him to analyze the encrypted virus and develop a removal tool. Eugene's curiosity and passion for computer technology drove him to start analyzing additional malicious programs and developing disinfection modules, and this unique antivirus module collection would eventually become the foundation for the Kaspersky Lab antivirus database.

In 1991, the year the Soviet Union ended, Eugene left the research institute and formed a small antivirus division at an emerging commercial holding company. A few years later, he and a small group of associates founded Kaspersky Lab in 1997. Today, the company operates in almost 200 countries and territories worldwide, employs nearly 3,700 professionals and protects more than 400 million users around the world.

Eugene Kaspersky
Chairman and CEO, Kaspersky Lab

Learn more about internet security: **www.securelist.com**
Find a partner near you: **www.kaspersky.com/buyoffline**

www.usa.kaspersky.com
#truecybersecurity

AO Kaspersky Lab
500 Unicorn Park, 3rd Floor Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com