Kaspersky Corporate Kit

Updated: March 2021
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
Kaspersky at a glance
Facts about us

**Essentials**

- Founded in 1997 and led by Eugene Kaspersky
- Present on 6 continents in almost 200 countries and territories
- Provides innovative IT security solutions and services for business and consumers

**Numbers**

- > 14 million product activations per year
- > 4,000 highly qualified specialists
- US$ 685 million — global non-audited revenue in 2019

**Achievements and recognition**

- One of the five biggest endpoint security vendors*
- Kaspersky has been recognized as a 2020 Customers’ Choice for Endpoint Detection & Response Solutions by Gartner Peer Insights**
- Kaspersky Internet Security was honored with the **Product of the Year 2020** award by independent test lab AV-Comparatives***

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

---

* The company was ranked fifth in the IDC ‘Worldwide Endpoint Security Market Shares, 2018: Large Vendors Write a New Market Narrative’ (Doc #US45055319 May 2019).
** Kaspersky recognized as the highest ranking vendor in the 2020 Gartner Peer Insights Customers’ Choice for Endpoint Detection & Response. Gartner Peer Insights Customers’ Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology. They neither represent the views of nor constitute endorsement by, Gartner or its affiliates. https://www.gartner.com/reviews/market/endpointdetection-and-response-solutions
*** Kaspersky’s flagship home user security solution—Kaspersky Internet Security—was honored with the **Product of the Year 2020** award for an impressive sixth time, in an annual report released by independent test lab AV-Comparatives. Kaspersky was acknowledged ahead of 16 peers by achieving Advanced+ awards in seven rigorous tests, to rank the company highest overall across the participating Windows security products.
Geography

200 countries and territories we operate in

34 representative regional offices

North America
Mexico
USA

Europe
Austria
Czech Republic
Denmark
France
Germany
Israel
Italy
Netherlands
Poland
Portugal
Romania
Russia (HQ)
Spain
Switzerland
UK

South America
Brazil

Asia
China
Hong Kong
India
Japan
Kazakhstan
Malaysia
Singapore
South Korea
Turkey
UAE

Africa
South Africa

Transparency Centers
Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia
New Brunswick, Canada
(to be open in 2021)
Our role in the global IT security community

We participate in joint operations and cyberthreat investigations with the global IT security community, international organizations such as INTERPOL and Europol, law enforcement agencies and CERTs worldwide.

We cooperate with INTERPOL and provide the organization with human resources support, training, and threat intelligence data on the latest cybercriminal activities.

In cooperation with non-profit organizations, digital activists, and cybersecurity vendors, we launched the Coalition against Stalkerware* to protect users against stalking and domestic violence.

Kaspersky is a member of the Advisory Group on the Internet Security at the European Cybercrime Centre (EC3) at Europol.

Together with Cigref, we are co-chairing the Working Group 6 as part of the Paris Call for Trust and Security in Cyberspace. The aim of this working group is to develop concrete proposals for solutions to improve the level of security in cyberspace.

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.

*Stalkerware – a type of a commercial spyware deemed to be legal. Learn more [http://stopstalkerware.org/](http://stopstalkerware.org/)
The No More Ransom Initiative

In July 2016, the Dutch National Police, Europol, McAfee and Kaspersky announced the launch of the No More Ransom project - a non-commercial initiative that united public and private organizations and aims to inform people of the dangers of ransomware, and helps them to recover their data without having to pay the criminals.

NO MORE RANSOM!

- 100+ free decryption tools.
- 160+ project partners representing organizations from around the globe.
- The site is available in 37 languages.
Our 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 governments and law enforcement agencies to fight cyberthreats.

We are committed to the trustworthy development of our technologies and solutions.

We cooperate with the IT security industry in joint cyberthreat investigations.
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 its products, internal processes, and business operations.

It includes a number of actionable and concrete measures:

- Independent code and update review
- Engineering practices, external audit & certification
- Vulnerability management program
- R&D infrastructure relocation
- Cyber-capacity Building program
Kaspersky moved core infrastructure to Switzerland and opens Transparency Centers

Customer data storage and processing
Malicious and suspicious files received from users of Kaspersky products in Europe, the United States, Canada and several countries in Asia-Pacific region* are processed and stored on Swiss servers.

- Madrid, Spain  
  - Transparency Center

- New Brunswick, Canada  
  - Transparency Center (to be open in 2021)

- São Paulo, Brazil  
  - Transparency Center

- Zurich, Switzerland  
  - Transparency Center
  - Data centers

- Kuala Lumpur, Malaysia  
  - Transparency Center

Transparency Centers
A facility for trusted partners and government stakeholders to review the company’s code, software updates and threat detection rules, along with other activities.

Independent review
Third-party assessment of internal processes to verify the integrity of Kaspersky solutions and processes.
In 2019 Kaspersky has achieved the SOC 2 Type 1 report in accordance with the SSAE 18 standard (Security criteria) issued by one of the Big Four accounting firms.

Bug bounty program
Aimed to make Kaspersky more secure, it encourages independent security researchers to supplement the company’s own work in vulnerability detection and mitigation.

*Australia, New Zealand, Japan, Bangladesh, Brunei, Cambodia, India, Indonesia, South Korea, Laos, Malaysia, Nepal, Pakistan, Philippines, Singapore, Sri Lanka, Thailand, and Vietnam.
Digital trust

As cybersecurity becomes vital for every individual and entity, the question of provider trust is becoming essential. Our mission is to maintain the trust of customers, in addition to our already proven quality.

What people think

Trust security provider’s use of data
87% of businesses and 82% of consumers trust their security provider to behave ethically when collecting and using their data.

Biggest threat?
45% of businesses and 47% of consumers worry about protecting online data from cybercriminals.

But also: national and foreigngvs, employers, families & more

Worry about security provider’s use of data
65%–78% of businesses and 54%–80% of consumers worry provider will access and share private data, opinions, location or online behavior.

Who is the most responsible for your protection online?
57% of businesses: my IT security team
57% of consumers: I am
45% (consumers), 43% (businesses): my cybersecurity provider

What matters when choosing

Governments should choose highest quality product or service even if it is by a foreign company
55% businesses agree
66% consumers

82% businesses agree
78% consumers

In general
In areas critical to national security

What matters most when you choose a security provider?
Honesty, integrity, independence, product quality – all 90% + Country of origin 86%/80%
Kaspersky and Digital Trust

- Data storage & processing relocation for European customers to Switzerland
- Building your Private Security Cloud Network with the highest privacy (KPSN)

- SOC2 audit by a 'Big Four' auditor confirms that Kaspersky has strong security controls for development and release of its anti-virus bases
- Integrity and highest performance of Kaspersky products based on results of 62 tests

- Dedicated Transparency Centers in Zurich, Madrid (first in the EU), São Paulo and Kuala Lumpur for source code review. Transparency Center in New Brunswick, Canada to open in 2021.
- Vulnerabilities management with the continuous Bug Bounty Program
- Independent assessment for GDPR compliance

- Private & independent company with 23-year history on the global market
- Company's DNA for continuous development of new technologies
- Our GReAT team plus one third of our employees are R&D specialists
Kaspersky has achieved the SOC 2 Type 1 report in accordance with the SSAE 18 Security Criteria issued by an independent third-party ‘Big Four’ auditor.

The audit concludes that the development and release of Kaspersky’s antivirus bases are protected from unauthorized changes by strong security controls.

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).
ISO 27001 certification

Kaspersky has achieved ISO/IEC 27001:2013 certification issued by TÜV AUSTRIA.

The certification confirms that the company’s data security systems, including Kaspersky Security Network, meet industry best practices. It is valid for the company’s data services located in Data Centers in Zurich, Frankfurt, Toronto and Moscow.

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.
Bug Bounty Program

Kaspersky has run its public bug bounty program from 2016 in partnership with the famous HackerOne platform. The company also supports the Disclose.io framework, which provides Safe Harbor for vulnerability researchers concerned about negative legal consequences of their discoveries.

Who can participate

- Individuals over the age of thirteen (13) at the time of entry.
- All researchers except employees of Kaspersky, their subsidiaries, and their immediate families.

Scope products

- Kaspersky Internet Security 2019
- Kaspersky Endpoint Security 11
- Kaspersky Endpoint Security for Linux
- Kaspersky Password Manager
- Kaspersky Secure Connection

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.

More details are available in the [bug bounty program description on the HackerOne platform website](#).
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.
Threat research

>1,000,000,000
cyberthreats
detected by Kaspersky since the company’s inception

10,000,000,000
cyberattacks
detected by Kaspersky in 2020

360,000
new malicious files
detected by Kaspersky every day
Advanced persistent threat landscape in 2020

Kaspersky’s Global Research and Analysis Team (GReAT) is well-known for the discovery and dissemination of the most advanced cyberthreats.

According to their data, in 2020 the top targets for advanced persistent threats (APT) were governments, and the most significant threat actor was Lazarus.

Top 10 targets:
- Government
- Banks
- Financial Institutions
- Diplomatic
- Telecommunications
- Educational
- Defense
- Energy
- Military
- IT companies

Top 12 targeted countries:
- Chile
- Mexico
- Brazil
- France
- UK
- Turkey
- India
- Russia
- China
- Japan
- South Korea
- Hong Kong

Top 10 significant threat actors:
1. Lazarus
2. DeathStalker
3. CactusPete
4. IAMTheKing
5. TransparentTribe
6. StrongPity
7. Sofacy
8. CoughingDown
9. MuddyWater
10. SixLittleMonkeys

apt.securelist.com

Based on the data up to 31.12.2020
## Our major discoveries and research

<table>
<thead>
<tr>
<th>Detection</th>
<th>SOFACTY</th>
<th>DUQU 2.0</th>
<th>LURK</th>
<th>LAZARUS</th>
<th>PROJECT SAURON</th>
<th>EXPERT/NOTPETYA</th>
<th>SHADOWPAD</th>
<th>OLYMPIC DESTROYER</th>
<th>SHADOW HAMMER</th>
<th>TAJMAHAL</th>
<th>MOSAIC REGRESSOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classification</td>
<td>Cyber-espionage malware</td>
<td>Complex cyberattack platform</td>
<td>Cybercriminal operation</td>
<td>Cyber-espionage &amp; sabotage, financial attacks</td>
<td>Cyber-espionage malware</td>
<td>Data wiping campaign</td>
<td>Modular cyber-attack platform</td>
<td>Cyber-espionage malware</td>
<td>Cyber-espionage malware</td>
<td>Cyber-espionage platform</td>
<td>Cyber-espionage platform</td>
</tr>
<tr>
<td>Description</td>
<td>Sofacy (also known as &quot;Fancy Bear&quot;, &quot;Sedac&quot;, &quot;STRONTIIUM&quot; and &quot;APT28&quot;) is a highly professional threat actor. Suspected of a connection to the notorious Mindiuexactors. Sofacy has been notable for its extensive use of zero-day exploits</td>
<td>A highly sophisticated malware platform exploiting up to three zero-day vulnerabilities</td>
<td>The gang responsible for creating infected computer networks that resulted in the theft of more than $45M from banks, other financial institutions and businesses since 2011. The group was looking for a way into remote banking services so that it could steal money from customer accounts</td>
<td>A threat actor attacking state organizations. Project Sauron deliberately avoids patterns, customizing its implants and infrastructure for each individual target, and never using them, making traditional indicators of compromise almost useless</td>
<td>A wiper pretending to be ransomware, using modified code of BlueEye and EternalRomance exploits. Some observations point to a link between Ex-Petr and BlackEnergy APT</td>
<td>ShadowPad is one of the largest known supply-chain attacks. Affected server management software NetSarang used by hundreds of large businesses around the world. Attackers deployed the platform in victim networks to gain flexible remote control capabilities</td>
<td>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</td>
<td>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 certificates</td>
<td>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</td>
<td>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</td>
<td></td>
</tr>
<tr>
<td>Targets</td>
<td>Military and government entities worldwide</td>
<td>Malware infections linked to the PFAS events and venues for high level meetings between world leaders</td>
<td>Banks, other financial institutions and businesses</td>
<td>Media, financial institutions, casinos, software developers for investment companies, cryptocurrency businesses</td>
<td>Mainly state organizations. Over 30 victims in Russia, Iran and Rwanda</td>
<td>Spread around the world, primarily targeting businesses in Ukraine, Russia and Western Europe. &gt;50% of organizations attacked were industrial companies</td>
<td>Banking and financial industry, software, media, energy and utilities, insurance, industrial and construction, manufacturing, and other industries</td>
<td>Organizations related to Winter Olympic Games 2018 biological and chemical threat prevention organizations in EU Financial institutions in Russia</td>
<td>Special instructions in malware code were aimed at targeting only 600 systems, identified by specific MAC addresses</td>
<td>Diplomatic entities with possible affiliation to DPRK</td>
<td>Diplomatic entities</td>
</tr>
</tbody>
</table>
Targeted attack research

- Metel
  - ProjectSauron
    - Adwind
    - Saguaro
      - Lazarus
        - StrongPity
        - Lurk
        - Dropping Elephant
      - ScarCruft
    - StoneDrill
      - Shamoon 2.0
        - ExPetr/NotPetya
        - WannaCry
    - GCMAn
      - Ghoul
        - Poseidon
          - Fruity Armor
        - Danti
    - ATMitch
      - Moonlight Maze
      - ShadowPad
        - ZooPark
        - BlackOasis
        - WhiteBear
        - Silence
        - Octopus
      - Hades
        - Titanium
      - AppleJeus
      - FinSpy
    - Olympic Destroyer
    - Topi
      - Cycldek
      - SixLittleMonkeys (aka Microcin)
      - CactusPete
      - DeathStalker
      - MATA
      - TransparentTribe
      - SneakyPastes
      - WellMess
      - TwoSail Junk
      - MontysThree
      - MosaicRegressor
      - VHD Ransomware
      - WildPressure
      - PhantomLance
Kaspersky solutions & services
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.

- Enterprises
- Industrial facilities
- Small and medium businesses
- Very small businesses
- Consumers

>240,000 Corporate clients worldwide

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

creates an environment where a vulnerability or bad code is no longer a big deal

aims to protect software and data systems from the consequences of the intrusion of malicious code, viruses and hacker attacks

with The Kaspersky Security System (KSS) protection component controls interactions across the whole system, rendering the exploitation of vulnerabilities useless
KasperskyOS

- Proprietary microkernel – developed in-house by Kaspersky, no Linux inside
- Secure-by-design – developed with security in mind and remains secure during its whole lifecycle
- Static security configuration based on default deny principles – any interaction that is not allowed will be rejected
- Business logic is separated from security features – easier to develop and support, decrease time to market, increase security and safety
- Multi-level compatibility – POSIX API compatible (well 98% of the API)
- Runs on Intel x86, x64 and ARM (v6, v7, v8)
KasperskyOS

KasperskyOS is designed for embedded connected systems with specific requirements for cyber security.

Telecommunication

Transportation

Internet of things

Industrial

Small and big screens

Kaspersky IoT Secure Gateway

- Device detection & classification
- Secure boot & secure update
- Access through web-interface
- Firewall
- IPS/IDS
- Remote and centralized management via KSC
- MQTT broker
## Next Generation solutions for enterprise

### Technological

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Management and Defense</td>
<td>Advanced Protection empowered by Threat Intelligence</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td>The leading multi-layered endpoint protection platform, based on NextGen cybersecurity technologies</td>
</tr>
<tr>
<td>Hybrid Cloud Security</td>
<td>Borderless security engineered for your hybrid cloud environment</td>
</tr>
<tr>
<td>Cybersecurity Services</td>
<td>Intelligence and expertise providing a new level of cyber-immunity</td>
</tr>
<tr>
<td>Internet of Things and Embedded Security</td>
<td>Minimizing risk and addressing cybersecurity threats to IoT systems and embedded devices</td>
</tr>
<tr>
<td>Fraud Prevention</td>
<td>Advanced solution for seamless user experience and proactive prevention of fraud in real-time</td>
</tr>
</tbody>
</table>

### By Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Cybersecurity</td>
<td>Meeting the most stringent security requirements and ensuring supreme protection for highly critical infrastructures</td>
</tr>
<tr>
<td>Finance Services Cybersecurity</td>
<td>Raising security levels through predicting preventing and responding to financially motivated cybercrime</td>
</tr>
<tr>
<td>Transportation Cybersecurity</td>
<td>Securing all areas of transportation IT infrastructure</td>
</tr>
<tr>
<td>Telecom Cybersecurity</td>
<td>Securing telecoms data, applications and networks against the most advanced cyberthreats</td>
</tr>
<tr>
<td>Industrial Cybersecurity</td>
<td>Specialized protection for industrial control systems</td>
</tr>
<tr>
<td>Healthcare Cybersecurity</td>
<td>True Cybersecurity where it matters most</td>
</tr>
<tr>
<td>Retail Cybersecurity</td>
<td>Rigorous security and compliance for POS terminals, workstations, mobile devices and back-office systems</td>
</tr>
<tr>
<td>Blockchain Security</td>
<td>The ultimate cybersecurity for the Crypto-Economy</td>
</tr>
</tbody>
</table>
Industrial cybersecurity

KasperskyOS
(Secure Operating System)
- Security-by-design approach
- Proprietary lightweight microkernel and independent security engine.
- Cyber-immunity

Supported Industrial Endpoints:
- SCADA Servers
- SCADA Clients
- Human-Machine Interfaces (HMI)
- Engineering Workstations
- Historians
- OPC Gateways

Industrial Endpoint Protection
- KICS for Nodes
- KICS for Networks
- KICS Security Center

Industrial Anomaly and Breach Detection

Centralized security management

Kaspersky Industrial CyberSecurity

PRODUCTS

Kaspersky ICS-CERT

Industrial Systems Emergency Response Team offering expert intelligence and consulting services.

SERVICES

Training and awareness
- Kaspersky Security Awareness
- Kaspersky Security Trainings

Expert services and intelligence
- Kaspersky Security Assessment
- Kaspersky Incident Response
- Kaspersky Threat Intelligence

End of Point protection capabilities:
- Application whitelisting
- Antimalware engine
- Device control
- File Integrity Monitoring
- Exploit Prevention
- Wireless access control
- Log Inspection
- PLC integrity checker
- Ransomware protection
- Firewall

Network security capabilities:
- Network Visualization
- Network Activity Monitoring
- Asset Discovery
- Deep Packet Inspection
- Machine Learning for Anomaly Detection
- Remote Access Detection
- Malware Spreading Detection
- Event Correlation
- Safe Non-Invasive Mode
- SOC/SIEM Integration

Awareness and training programs:
- Industrial Cybersecurity Awareness (1 day)
- Advanced Industrial Cybersecurity in Practice (1-2 days)
- ICS Digital Forensics for Professionals (4 days+)
- ICS Penetration Testing for Professionals (5 days)
- IoT vulnerability research and exploitation training (4 days)
- Capture the flag (CTF) competition
- Become a Trainer—Train the Trainer
- Kaspersky Interactive Protection Simulation (KIPS)

Export services features:
- Penetration testing and threat modeling
- Secure network architecture and controls recommendations
- Emergency support to localize incident and digital forensics (available on demand or via subscription)
- ICS Adversary Update Reports (TTPs, targets, attribution)
- Vulnerability database and advisory
Next Generation solutions for SMBs

As easy as home antivirus
- Kaspersky Small Office Security
  - Works out of the box, no configuration required
  - Financial protection with Safe Money
  - Client and personal data protection. Encryption backup
  - Storing all passwords with Password Manager

Rapid protection for limited resources
- Kaspersky Endpoint Security Cloud
  - Cloud-based console for flexible, simple administration, no need for additional hardware
  - Protect PCs, laptops, mobile devices and file servers
  - Default security policies for immediate protection
  - The latest, most up-to-date software - always

The best enterprise-grade security solution
- Kaspersky Endpoint Security for Business
  - EDR at the core and an automated Sandbox to work with your endpoint protection
  - Prevents employees from exposing themselves, and you, to an attack
  - Maximizes the number of incidents processed, without increasing your manpower costs
  - Scales easily, securing diverse environments and platforms
Next Generation solutions for Business

Multi-layered security for physical, virtual, mobile environments and servers

Targeted products including:

- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Mail Server
- Kaspersky Security for Office 365

Superior detection rate

The complete security platform

Managed from one central console
Managed Services with Kaspersky

BUILD SERVICES

- Endpoint Protection and hardening
- Vulnerability and Patch Management
- Office365 Protection

Kaspersky
- Endpoint Security for Business
- Endpoint Security Cloud
- Security for Microsoft Office 365

MSP

Incident Response
- Security Awareness
- Managed Web and Email Protection

24/7 Security Monitoring
- Threat Detection and Response
- Proactive Threat Hunting

MSSP

Kaspersky
- EDR Optimum
- Hybrid Cloud Security
- Sandbox
- Automated Security Awareness Platform
- Security for Mail Server
- Security for Web Gateway

Kaspersky EDR Expert
- Anti Targeted Attack
- Threat Lookup
- Threat Data Feeds
- Intelligence Reporting

KASPERSKY INTELLIGENCE AND EXPERTISE

Automation and integration
- RMM and PSA Integrations
- Subscription-based model and LMP

Knowledge and Expertise
- Training for MSP
- MSA Premium Support for MSP
The future of consumer cybersecurity

Personalized digital security powered by artificial intelligence, machine learning and other technologies of tomorrow.

Our complete collection of apps under one easy-to-manage account protects users' privacy and data and optimizes their device performance. Protects users beyond their devices:

- Informs if personal data from their accounts is leaked online.
- Alerts if an intruder joins their home network.

Works fast and smoothly on all platforms thanks to cloud-based technologies.

Kaspersky Security Cloud

Available on: 🖥️ 📱 🍊 🍁

Comes in Personal & Family plans

The Family plan includes everything the personal one does – anti-malware, payment protection, password security, VPN & more. Plus it comes with parental controls and allows users to install security on family devices remotely and manage it from their online account.
Giving consumers the confidence to thrive

Protection for your children, privacy, identity & mobiles

- Kaspersky VPN Secure Connection
  - Win | Android | Mac | iOS
- Kaspersky Password Manager
  - Win | Android | Mac | iOS
- Kaspersky Safe Kids
  - Win | Android | Mac | iOS
- Kaspersky Internet Security for Android

Best-selling security suites

- Kaspersky Total Security
  - Win | Android | Mac | iOS
- Kaspersky Internet Security
  - Win | Android | Mac

Free apps and utilities

- Kaspersky QR Scanner
  - Android | iOS
- Kaspersky Battery Life
  - Android
- Kaspersky Security Cloud Free
  - Win | Android | iOS

We inspire our customers to embrace new technologies and make the most of all the opportunities they bring – because they know we’re keeping them safe.
MOST TESTED*  
MOST AWarded*  
KASPERSKY PROTECTION

* kaspersky.com/top3

---

As cybersecurity becomes vital for 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 2020, Kaspersky products participated in 62 independent tests and reviews. Our products were awarded 45 firsts and received 50 top-three finishes.

---

* 62 independent tests were completed by Kaspersky products in 2020 alongside 13 competitors. More than 100 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.
Kaspersky Innovation Hub

**MISSION:** We are constantly looking for the most advanced projects working at the edge of cybersecurity, to support the growth of new joint business activities and enrich our cybersecurity offerings in different industries. We engage with the ecosystem as part of our main goal of making the world cyber-immune.

The **Kaspersky Innovation Hub** is a core element in our growth strategy, established to encourage corporate innovations and foster collaboration between our company and the brilliant minds inside and outside of the business in developing new technologies.

- **Employees**
- **kaspersky**
- **Business Units**
- **iHub**
- **Kaspersky Innovation Hub**
- **Startups**
- **Venture Capitalist**

**Benefits:**
- Improve existing products
- Validation of new ideas
- Emerging trend
- Analyze
- Minimize risks
- Revenue enhancement
- Ecosystem builder
- Build a dream team
Kaspersky in the market
Customer recognition

Kaspersky recognized as the highest ranking vendor in the 2020 Gartner Peer Insights Customers’ Choice for Endpoint Detection & Response

Gartner Peer Insights Customers’ Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. [https://www.gartner.com/reviews/market/endpointdetection-and-response-solutions](https://www.gartner.com/reviews/market/endpointdetection-and-response-solutions)

The GARTNER PEER INSIGHTS CUSTOMERS’ CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers’ Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.
Customer recognition


Gartner Peer Insights Customers’ Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates. [https://www.kaspersky.com/enterprise-security/security-awareness](https://www.kaspersky.com/enterprise-security/security-awareness)

The GARTNER PEER INSIGHTS CUSTOMERS’ CHOICE badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. Gartner Peer Insights Customers’ Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.
Kaspersky Threat Intelligence

Kaspersky has been recognized as a ‘Leader’ in ‘The Forrester Wave™: External Threat Intelligence Services Q1, 2021’ report.

Kaspersky’s current offering ranks among the Top 2 on the market.

*The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester Wave™ is a graphical representation of Forrester’s call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.
Kaspersky was recognized as “Global Company of the Year” in the Industrial (OT/ICS) Cybersecurity Market by Frost and Sullivan*.

Kaspersky has been ranked number one for the quality of its partner program in the Canalys Worldwide Vendor Benchmark*. The company achieved the highest overall rating of 87.8%.

The benchmark is an objective comparison of channel partner programs, measuring how vendors perform in a number of key categories. Kaspersky received over 679 reviews from the channel for its program, an increase of 588% over the past 12 months.

Kaspersky has been recognized as a **Champion** in the Canalys Global Cybersecurity Leadership Matrix 2020*.

Champions are vendors with high Vendor Benchmark scores that have also demonstrated continued progress in further developing their channel ecosystems over the last 12 months.

Our customers

We work in a wide range of industry sectors. Our solutions and services successfully protect over 240,000 clients around the world, regardless of size or complexity.
As we work to create a safer future, we are concerned about the well-being of the world not only in the context of its digital reality. Gender equality, accessible knowledge, volunteering, child safety, animal protection and more are all issues that are crucial for us.

We are also committed to social responsibility through volunteerism and philanthropy in different regions where the company operates.

We cooperate with non-profit organizations, support charity initiatives and create our own social programs. Read Kaspersky CSR report here.
Women in Tech

Kaspersky runs an Internet community called Women in CyberSecurity that helps supercharge the career growth of women entering the cybersecurity industry and those already working in the field. The company also hosts Empower Women project aimed at supporting the career growth of women who are up for the challenge of protecting the world from cyber threats by sharing role models.

Fighting against stalkerware

In November 2019, Kaspersky with nine other organizations from IT Security industry and non-profit sector launched a global initiative to protect users against stalking and domestic violence.

Already since April 2019 our users of Kaspersky Internet Security for Android receive a Privacy Alert – a specially designed notification to warn the user if their private information is being covertly monitored by a third party. For this initiative, we cooperated with the Electronic Frontier Foundation.

Preserving the World

We understand the importance of preserving past cultures, for the benefit of future generations. That is why Kaspersky has been cooperating with the Archeological Society at Athens (ASA) since 2015, to develop its Akrotiri project. This project is dedicated to saving the remains of the historic Cycladic/Minoan settlement on Santorini Island – widely known as the Greek “Pompeii”.
Kaspersky runs an Internet community called Women in CyberSecurity that helps supercharge the career growth of women entering the cybersecurity industry and those already working in the field. The company also hosts Empower Women project aimed at supporting the career growth of women who are up for the challenge of protecting the world from cyber threats by sharing role models.
Fighting against stalkerware

Kaspersky has been at the forefront of protecting victims of stalkerware. Since April 2019, users of Kaspersky Internet Security for Android have received a Privacy Alert – a new feature that warns the user if their private information is being covertly monitored by a third party. For this initiative, we cooperated with the Electronic Frontier Foundation.

In 2019, Kaspersky and nine other organizations from both the IT Security industry and the advocacy/non-profit sector launched a global initiative “Coalition Against Stalkerware” to protect users against stalking and domestic violence. In its first year, the Coalition has more than doubled its membership to 26 partners.

The company’s GReAT researchers developed TinyCheck, an easy to use open-source tool which relies on Raspberry Pi and detects stalkerware and spyware.
Preserving the World

We understand the importance of preserving past cultures, for the benefit of future generations. That is why Kaspersky has been cooperating with the Archeological Society at Athens (ASA) since 2015, to develop its Akrotiri project. This project is dedicated to saving the remains of the historic Cycladic/Minoan settlement on Santorini Island – widely known as the Greek “Pompeii”. The company has become the major sponsor of the project, providing support for a number of activities to help the scientists advance their work. This includes the restoration of excavations, the conservation of spectacular wall paintings and the project’s architectural conservation work.
Preserving the World

In July 2019 Kaspersky sponsored the Kuril Islands expedition with a renowned team of environmentalists, film makers and photographers, aimed to give people the opportunity to explore the remarkable nature of the isolated islands and bring attention to the current ecological situation faced by the region.
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 different ages and professions all around the world about cybersecurity.
School

Kaspersky intends to educate young users about being safe online. We globally distribute the children's book “Kasper, Sky and the Green Bear” – a joint publication with Dutch writer Marlies Slegers.

We have a Kaspersky School project in Moscow, Russia, aimed at giving schoolchildren a foundational base in mathematics. The project is also intended to educate schoolchildren and teachers about the basics of cybersecurity.

University

As part of our international educational project Kaspersky.Academy, we promote knowledge of cybersecurity among students worldwide. The company supports young talent in IT, including organizing a global student competition – Secur’IT Cup – and contributing to the development of top-notch educational cybersecurity programs.

Business

Kaspersky collaborates with business schools, such as INSEAD, one of the of the top three schools for Executive Education and leading MBA programs in the world, to introduce students to the cybersecurity world through keynote lectures.

Within the framework of the Kaspersky.Academy project, we offer an MBA training course aimed at increasing knowledge of information security and the development of organizational security policies.
Kaspersky intends to educate young users about being safe online. We globally distribute the children’s book “Kasper, Sky and the Green Bear” – a joint publication with Dutch writer Marlies Sleegers.

We have a Kaspersky School project in Moscow, Russia, aimed at giving schoolchildren a foundational base in mathematics. The project is also intended to educate schoolchildren and teachers about the basics of cybersecurity.
University

As part of our international educational project Kaspersky.Academy, we promote knowledge of cybersecurity among students worldwide. The company supports young talent in IT, including organizing a global student competition – Secur'IT Cup – and contributing to the development of top-notch educational cybersecurity programs.
Business

Today we are witnessing growing business concerns about cybersecurity, and we are proud to share our expertise with top managers from various industries. Kaspersky collaborates with business schools, such as INSEAD, one of the top three schools for Executive Education and leading MBA programs in the world, to introduce students to the cybersecurity world through keynote lectures.

Within the framework of the Kaspersky.Academy project, we offer an MBA training course aimed at increasing knowledge of information security and the development of organizational security policies.

Photo: Maxence Torilloux for INSEAD
Sponsorships & Partnerships

As a global innovative company, Kaspersky cares about the future by not only providing cybersecurity to different industries, but also by supporting promising talent in various countries.

We contribute to the development of science and modern art, help preserve the world and provide the opportunity for sportspeople to achieve their full potential.
Sport

We have built strong relationships with Scuderia Ferrari in Formula One and the Eintracht Frankfurt football club. In 2021 we became a sponsor of Aprilia Racing. In addition, the company supports talented drivers across various other racing series, including Giancarlo Fisichella, Antonio Giovinazzi, Giuliano Alesi, Antonio Fuoco, Amna and Hamda Al Qubaisi.

Science & Space

Kaspersky is a strategic partner of the Gagarin Research and Test Cosmonaut Training Center, located in Star City, Russia, where cosmonauts from all over the world prepare to go to space. Moreover, the company has supported Starmus – the world’s most ambitious science and music festival.

Chess

Kaspersky is an official cybersecurity partner of the FIDE World Championship series – the world’s most prestigious chess tournament, and provides complex protection for the FIDE Online Arena gaming platform.

The company also supports young chess players including Dinara Saduakassova and Andrey Tsvetkov.

Art

Kaspersky is a partner of the Moniker International Art Fair in London, and it supports special commissions from internationally-acclaimed artists such as Ben Eine. Additionally, we worked on a significant creative collaboration with renowned street artists D*Face, SHOCK-1 and Felipe Pantone.
Sports

We have built strong relationships with Scuderia Ferrari in Formula One and the Eintracht Frankfurt football club.

In 2021 we became a sponsor of Aprilia Racing – one of the most successful teams in motorcycle racing history.

In addition, the company supports talented drivers across various other racing series, including Giancarlo Fisichella, Antonio Giovinazzi, Giuliano Alesi, Antonio Fuoco, Amna and Hamda Al Qubaisi.
Kaspersky is an official cybersecurity partner of the FIDE World Championship series – the world’s most prestigious chess tournament, and provides complex protection for the FIDE Online Arena gaming platform.

The company also supports young chess players including Dinara Saduakassova and Andrey Tsvetkov.
Science & Space

Kaspersky is a strategic partner of the Gagarin Research and Test Cosmonaut Training Center, located in Star City, Russia, where cosmonauts from all over the world prepare to go to space. Moreover, the company has supported Starmus – the world’s most ambitious science and music festival.
Kaspersky is a partner of the Moniker International Art Fair in London, and it supports special commissions from internationally-acclaimed artists, such as Ben Eine. We worked on a significant creative collaboration with British multimedia street artist D*Face.

At the 10th Anniversary of Moniker International in 2019, we unveiled an artistic collaboration with the British street artist SHOK-1, famous for his X-ray paintings. In 2021 Kaspersky teamed up with contemporary artist Felipe Pantone to raise awareness on Data Privacy Day.
Thank you!
kaspersky