

How we turn knowledge into protection

GRI 3-3

By investing in R&D and creating innovative technologies, we transform knowledge and expertise into new practical solutions for protecting the digital world.

We invest in research and new products

~3,000

Kaspersky employees work in R&D

We believe that to effectively protect people and businesses from cyberthreats, we must constantly evolve and stay one step ahead of attackers. Accordingly, research and work to improve security solutions are among the key areas we focus on at Kaspersky.

Kaspersky’s R&D departments employ approximately 3,000 specialists — engineers, analysts, researchers and developers. Their shared mission is to transform cyberthreat expertise and knowledge into practical security solutions that help clients feel more confident in the digital environment.

During 2024–2025, our experts prepared 373 unique research and analytical publications. In them, we share research findings, observations about emerging threats, approaches to protection, and practices that help the market and community better understand the modern cyber-risk landscape.

373

unique research publications for 2024–2025



Main areas of development

In the reporting period, Kaspersky primarily invested in three new and extremely promising areas:

- We enhance corporate network security protection with NGFW
- development and sales of Kaspersky Container Security
- creation of cloud products for the international market (XDR Optimum, Cloud XDR)

Kaspersky also develops innovative solutions at the intersection of the cybersecurity and physical security of industrial facilities. For example, our [Kaspersky Antidrone](#) system is designed to detect and protect against drones.

The Kaspersky Antidrone project has four patents in Russia, two patents in the United States, and three patents in Europe. The system has been awarded the AGBA Cybersecurity Innovation Award and the Industrial Design Award.



We enhance corporate network security protection with NGFW

We developed and launched a next-generation firewall (NGFW) based on our global expertise and advanced technologies.

This solution helps businesses:

- protect the corporate network from a wide range of cyberthreats
- monitor the activity of applications and services
- manage traffic effectively to ensure a more stable network
- optimize infrastructure performance, reducing the risk of downtime and incidents.

We make container and cloud environments more secure with Kaspersky Container Security

Kaspersky Container Security (KCS) is a solution that protects containerized applications at all stages of their life cycle, from development to operation.

KCS helps organizations:

- protect business processes and reduce the likelihood of incidents
- comply with security standards and regulations
- build security into development processes and follow DevSecOps principles, according to which security is implemented from the very beginning, at all stages of the product life cycle
- free up information security resources for other tasks by automating certain checks and controls
- reduce time to market by enabling faster development and faster releases while complying with security requirements

Kaspersky Container Security is designed with container environments in mind and provides protection at multiple levels: from container images to the host operating system—the environment the containers run on.

KCS is part of [Kaspersky Cloud Workload Security](#), our comprehensive solution for protecting cloud workloads. As part of this platform, KCS helps reliably protect against cyberattacks and reduce the time required to detect threats in cloud environments and respond to them.



We make it simpler to detect sophisticated attacks with cloud-based XDR products

We create cloud-based XDR products, XDR Optimum and Cloud XDR, for the international market to make it easier for companies to detect and stop sophisticated cyberattacks.

XDR is an information security concept that helps:

- proactively identify threats at various levels of infrastructure
- respond quickly to incidents
- repel complex attacks that are not always noticeable by a single indicator

XDR combines endpoint device protection (EDR) capabilities with other security tools from a single vendor and connects additional data sources. As a result, specialists get:

- a single point for decision making
- a user-friendly interface
- advanced capabilities for investigating complex cyber incidents

For the international market, we are developing this product as a cloud-based service—this format helps companies significantly reduce the cost of using the solution and achieve benefits faster without complicating their infrastructure.