

We scale security by combining knowledge and experience

GRI 3-3

Our goal is to protect users and organizations from cyberthreats using advanced technologies and our accumulated expertise.

Kaspersky solutions:

In 2025, Kaspersky solutions blocked a worldwide total of

>14 million

attacks involving malware, adware or unwanted mobile software.

>144 million

malicious email attachments blocked by Kaspersky Mail Anti-Virus

Detected and blocked web threats¹ on the devices of

34%

of users globally in 2025

Detected local threats² (on-device threats) on the devices of

37%

of users globally

At Kaspersky, countering modern cyberthreats begins with an analysis of how the modern digital world is structured, what threats arise there, and how they evolve. Accordingly, all our activities in this area are underpinned by the work of our Expertise Centers – multidisciplinary teams whose work we are truly proud of.

They bring together researchers, analysts, engineers and practitioners, who study cyberthreats, investigate cyberattacks, develop new security technologies, and help organizations around the world manage incidents.



¹ Web threats are cyberthreats that penetrate devices via the internet.

² Here we mean cyberthreats that are spread via removable USB drives, CDs and DVDs, or that initially get on the computer in a disguised form, for example, in installation files or encrypted files.

Kaspersky's five Expertise Centers

Today, Kaspersky concentrates its expertise in [five](#) specialized centers, each of which addresses its own tasks but also works closely with all the others. Together, they let us not only respond to threats, but also understand their nature, anticipate how attacks will unfold, and transform knowledge into reliable protection.



1. Kaspersky Global Research and Analysis Team (GReAT)

As well as researching the most complex [APTs](#) and the actors behind them, GReAT experts investigate organized cybercriminal groups and lead the way in exploring the security risks of cutting-edge technologies – often before anyone else has even attempted to compromise them.

Thanks to the joint effort of GReAT and other Threat Research teams, our clients receive access to enhanced mechanisms of protection against advanced threats and exclusive reports on [APT threats](#) and [threats specific to financial crime](#) which feature a breakdown of tactics, techniques, and procedures (TTP) employed by attackers and indicators of compromise (IoC) necessary for the creation of a robust security system.

GReAT experts also provide unique threat research tools to their colleagues from other centers, aiding both internal and commercial services.



2. Kaspersky Threat Research

Kaspersky Threat Research experts focus on deep analysis of all types of cyberthreats, and develop protective

technologies and threat intelligence data that allow organizations to monitor and counter the broadest range of malicious activities.

They shape technological and methodological foundations that make our solutions resilient against compromise.



3. Kaspersky AI Technology Research

The AI Technology Research team explores one of the most significant technological breakthroughs of the 21st century. They excel in driving AI-powered technologies to tackle real-world cybersecurity challenges, navigate the uncharted territory of GenerativeAI applications – in cybersecurity and beyond – and strengthen the security of existing AI-based systems against compromise.



4. Kaspersky Security Services

Renowned for delivering Security Services globally, the team goes beyond customer engagements, uncovering

new TTPs, enriching the MITRE ATT&CK framework, developing proprietary tools and enhancing detection capabilities in Kaspersky products.

They also share their expertise through webinars, reports and training to help professionals stay ahead of threats.



5. Kaspersky ICS CERT

Kaspersky ICS CERT leverages deep expertise to combat ICS-specific cyberthreats, identify vulnerabilities in disruption-sensitive environments, and serve as trusted analysts and thought leaders in global industrial associations.

The results of this expertise underpin our Industrial (ICS) Threat Intelligence¹ services, which are available through the [TIP](#)². These include research reports, machine-readable feeds of [indicators of compromise \(IoC\)](#), and [information about vulnerabilities](#).

Another important area for ICS CERT is assisting software and hardware vendors. The center helps check the level of cybersecurity maturity of their solutions and make these solutions more secure.

¹ Specialized cyberthreat analytics focused on industrial systems and critical infrastructure.
² TIP (Threat Intelligence Platform) is a platform for working with threat analytics.