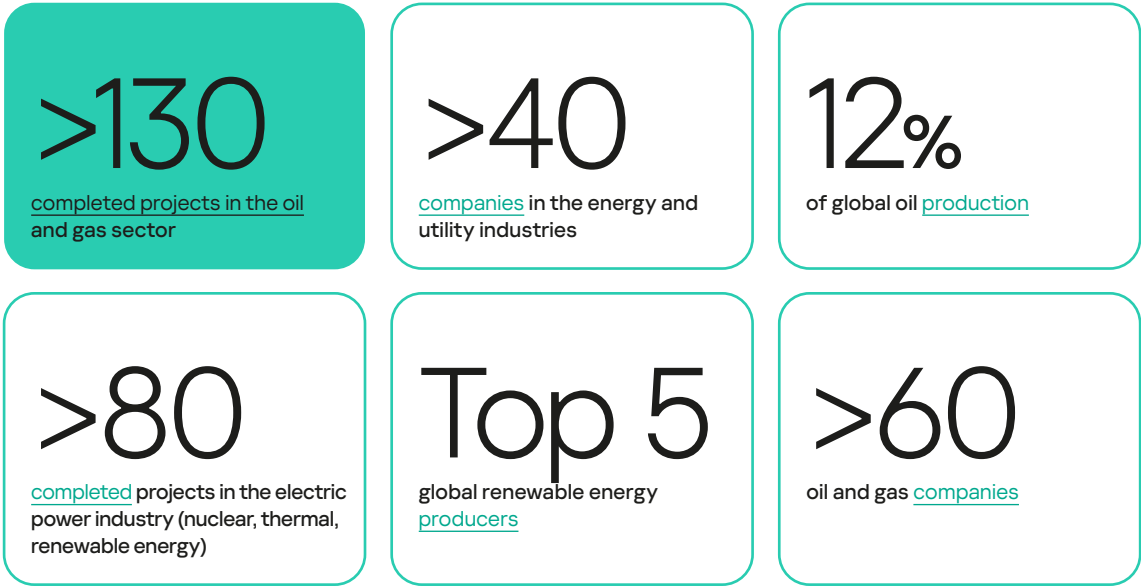


How we protect critical infrastructure

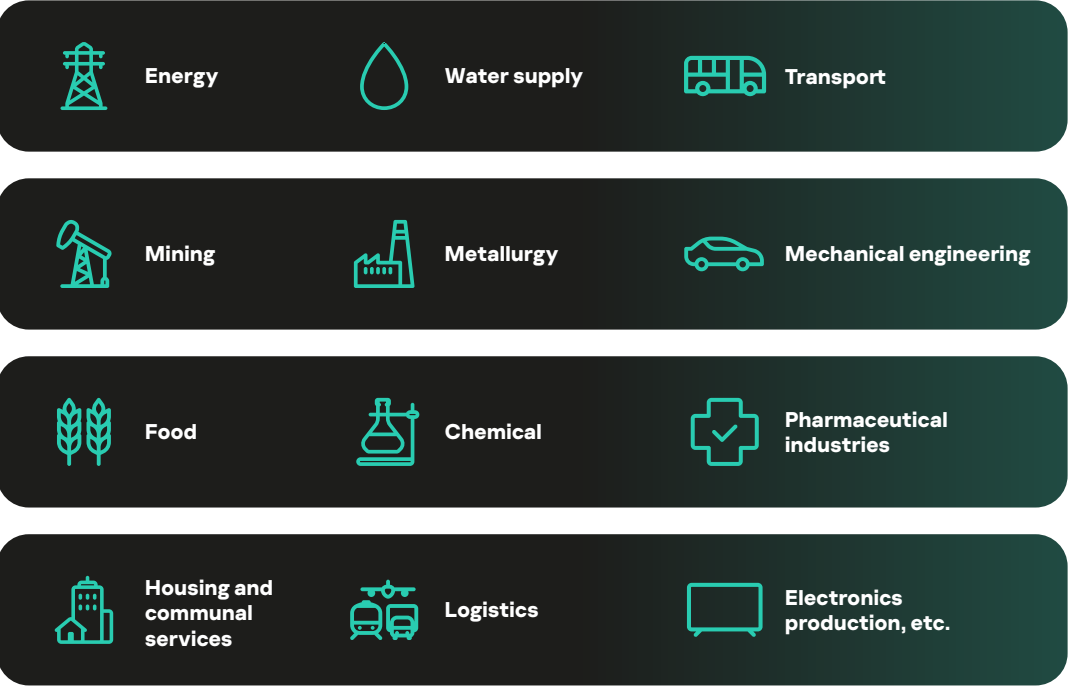
Our goal is to ensure that cyber-physical systems can operate without interruption at critical infrastructure facilities and in industry through the use of modern technologies, knowledge, and experience.

Protected by Kaspersky solutions



Critical infrastructure is systems that directly influence the sustainable functioning of the economy, state, and society.

Examples of critical infrastructure



Why this matters

Modern industrial automation systems are increasingly digital, connected, and intelligent, utilizing the cloud, AI, the Internet of Things, and digital twins. This makes production more efficient but also increases risks: the attack surface grows, and the critical infrastructure facilities themselves become attractive targets for attackers. Moreover, many critical systems were originally designed to operate in an isolated environment but are now forced to operate in a highly open and connected environment.

Today, the world faces a growing number of cyberattacks on critical infrastructure, and these attacks are becoming increasingly sophisticated.

Key researches in 2024–2025

- At the beginning of 2025, Kaspersky ICS CERT [announced](#) it discovered SalmonSlalom - a campaign targeting industrial organizations in the Asia-Pacific region. The attackers used legitimate cloud services to manage malware and employed a complicated multi-stage malware delivery scheme using legitimate software to avoid detection. As a result, they could

spread malware over victim organizations' networks, install remote administration tools, manipulate devices, steal and delete confidential information.

- At the Security Analyst Summit 2025, Kaspersky ICS CERT [presented](#) the results of a security audit that has exposed a significant security flaw enabling unauthorized access to all connected vehicles of one automotive manufacturer. By exploiting a zero-day vulnerability in a contractor's publicly accessible application, it was possible to gain control over the vehicle telematics system, compromising the physical safety of drivers and passengers. For instance, attackers could force gear shifts or turn off the engine when the vehicle is driving. The findings highlight potential cybersecurity weaknesses in the automotive industry, prompting calls for enhanced security measures.
- In 2025, Kaspersky ICS CERT [discovered](#) a hardware-level vulnerability affecting Qualcomm chipsets that are widely used in a range of consumer and industrial devices, including smartphones and tablets, car components, IoT devices and more. The vulnerability resides in the BootROM – firmware embedded at the hardware level. Attackers could potentially get access to any data stored on the device or device sensors like camera and microphone, implement complicated attack scenarios and in some circumstances get full control of the device.

Energy, water supply, and transport—sectors that directly impact people's daily lives and a country's sustainable development—are increasingly vulnerable.

At the same time, the manufacturing sector remains the main target of attackers. According to our quarterly [reports](#) of the main incidents in industrial cybersecurity, the vast majority of organizations attacked in 2024–2025 were in manufacturing.

Our approach to protecting critical infrastructure

We view cybersecurity as a continuous cycle: preparation, monitoring and early detection, response, rapid recovery.

Today, cyber resilience goes beyond traditional cybersecurity. This means that simply blocking attacks is no longer enough: the entire OT infrastructure¹ must be kept stable even during incidents.

Therefore, we are building a security platform for cyber-physical systems, where Kaspersky solutions protect IT, OT and IIoT² environments and help organizations implement digital technologies without compromising business stability, human safety, or the environment.

We help minimize risks and evaluate the benefits of investments in protecting critical infrastructure.

How our solutions help businesses save money and make informed decisions

By disrupting industrial operations, cyberattacks can cause significant losses, ranging from equipment downtime to product loss and reputational damage. To help companies more accurately assess the risks and effectiveness of cybersecurity investments, we conducted an international [study](#), together with VDC Research, an analytics firm.

What was the result?

The joint study found that implementing a comprehensive solution (protecting industrial nodes and monitoring network traffic) can reduce the potential damage from cyber incidents:

- by up to 45% for energy firms and enterprises offering housing and communal services
- by up to 76% for the manufacturing sector.

¹ OT (Operational Technology) infrastructure is the systems, equipment, and software that directly control physical processes in industry and at critical infrastructure facilities.

² Industrial Internet of Things.

We protect at every level

Kaspersky OT CyberSecurity

Kaspersky offers a dedicated OT CyberSecurity Ecosystem that delivers comprehensive protection for industrial environments. At the heart of this ecosystem lies Kaspersky Industrial CyberSecurity (KICS) – a native Extended Detection and Response platform that protects all levels of industrial and critical infrastructure systems and networks.



Level 2

Monitoring and management

- IIoT¹, perimeter protection and upper-level automation (SCADA)
- Access control, auditing, and increased visibility of OT systems
- Expert support on the customer's side

Level 3

Enterprise systems

- Convergence of IT and OT, correlation of data from all available sources
- Unified security processes and approaches using Hybrid XDR
- Training programs, consulting and advanced threat intelligence

Level 1

Controllers and protection

- Detection of intrusions, hacking attempts and compromised microprocessor equipment in low-level automation
- Deep packet inspection (DPI), protection of embedded operating systems from network threats and attempts to change process parameters
- Machine learning for detecting anomalies in industrial processes

Level 0

Industrial process

- Monitoring cyber-physical threats to key equipment
- Ensuring the security of connected vehicles and other physical objects

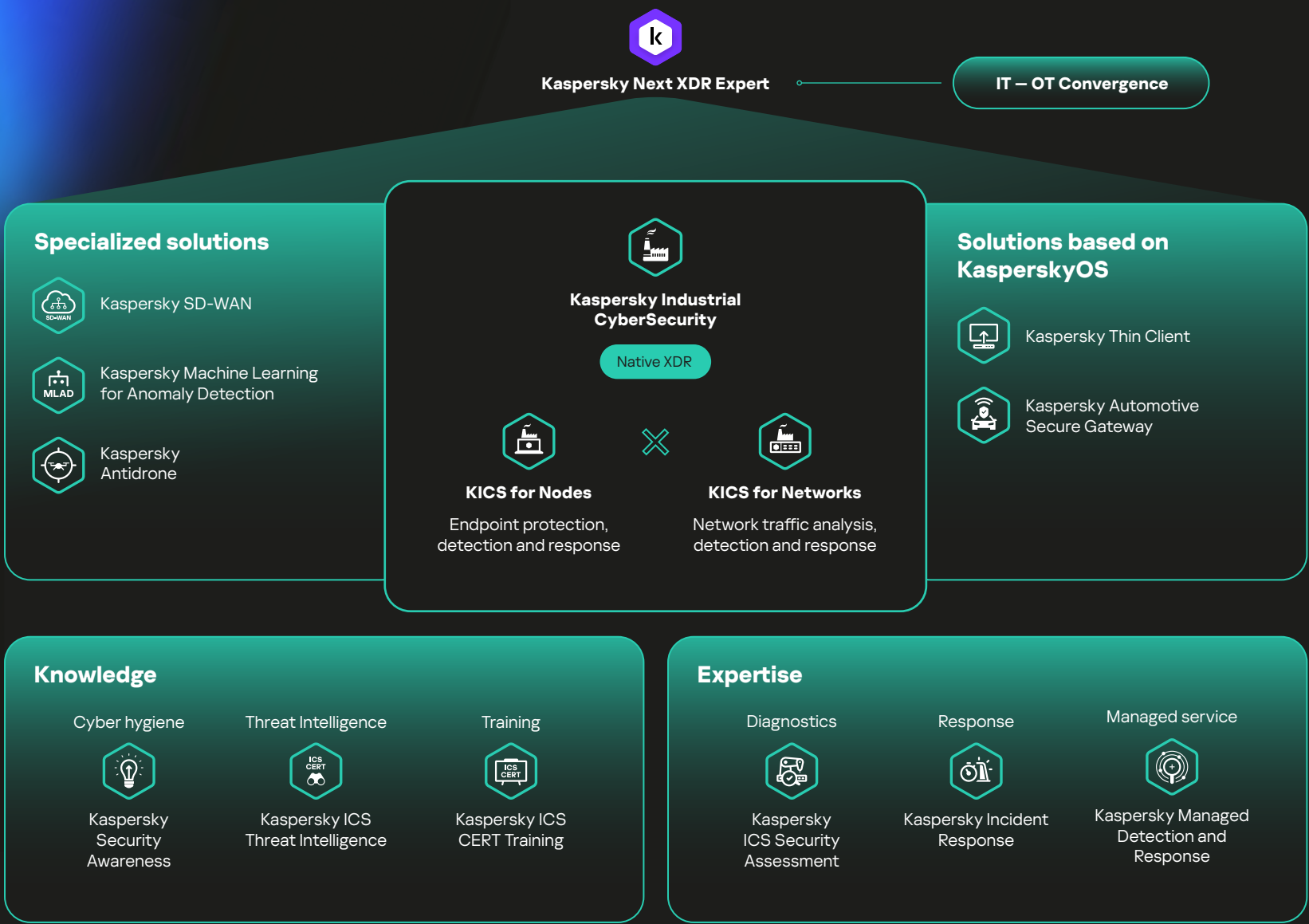
¹ The Industrial Internet of Things (IIoT) is a multi-level system that includes sensors and controllers installed on components and assemblies at an industrial facility, data transmission and visualization tools, powerful analytical tools for interpreting received information, and many other components.

Key areas of application

- Oil, gas and chemical industries
- Electric power industry, including nuclear power, and housing and communal services
- Metallurgy and mining
- Industrial production, including microelectronics

Promising areas of application of Kaspersky OT CyberSecurity

- Pharmaceuticals and medical equipment
- Transport and logistics, including airports
- Telecommunications
- Large infrastructure facilities (stadiums, business centers, shopping centers, residential complexes)



Kaspersky Industrial CyberSecurity (KICS) is the foundation of the Kaspersky OT CyberSecurity ecosystem

Today, KICS protects

12%

of global oil and gas production

10%

of petrochemical production

Up to 15–25%

of the extraction and processing of various metals

15%

of commercial nuclear generation

20%

of nitrogen and phosphorus fertilizer production

The core of the cyber-physical industrial security ecosystem is Kaspersky Industrial CyberSecurity (KICS). This native OT XDR platform provides situational awareness, cyber resilience, visibility into industrial network events, and powerful protection for core automation systems without affecting the availability of industrial processes.

KICS helps prevent costly downtime, security incidents, data theft, and sabotage caused by mass threats, targeted attacks, ransomware, or insider activity, while also protecting legacy equipment, extending its service life, and supporting compliance with national and international standards and information security best practices.

The platform consists of:

- KICS for Nodes — protection of servers, workstations, and operator panels running Linux and Windows
- KICS for Networks — network traffic analysis, asset inventory, anomaly and intrusion detection, and network threat response.

Geographic distribution of KICS

During the reporting period, we significantly strengthened our relationships with companies specializing in energy storage systems and the manufacture of electric vehicles and solar panels. Our clients include five manufacturing companies, each of which is among the top 5 global leaders in their industries, according to independent sources.

In 2025, these relationships gave the business a boost that led to the organization of [KICS Con China 2025](#) in Shenzhen, an innovative region known for its technology cluster. This conference brought together more than 100 participants. Industry roundtables for the oil and gas sector in the META¹ region were also held.

We consistently expand our technology partnership program. The KICS platform has been tested for interoperability with industrial automation vendors in Latin America, East Asia, and China, including Altus, Chint, Consen, Supcon and HollySys, helping customers build resilient supply chains and make responsible technology choices.

Our new KICS-protected clients:

- Nuevo Hospital de Toledo (Spain) — the largest hospital in the Iberia region
- [Birla Sugar Group](#) — India's largest sugar producer
- [Holy Stone](#) — a leader in China's cement industry
- [Atlas Tapes](#) (Greece) — the largest manufacturer of electrical tape in the European Union
- OLED — China's largest OLED display manufacturer

The KICS platform is compatible with a wide range of process control systems from

70+ vendors

>50

successful cases implementing KICS

¹ Middle East, Turkey, Africa.

Native OT XDR platform



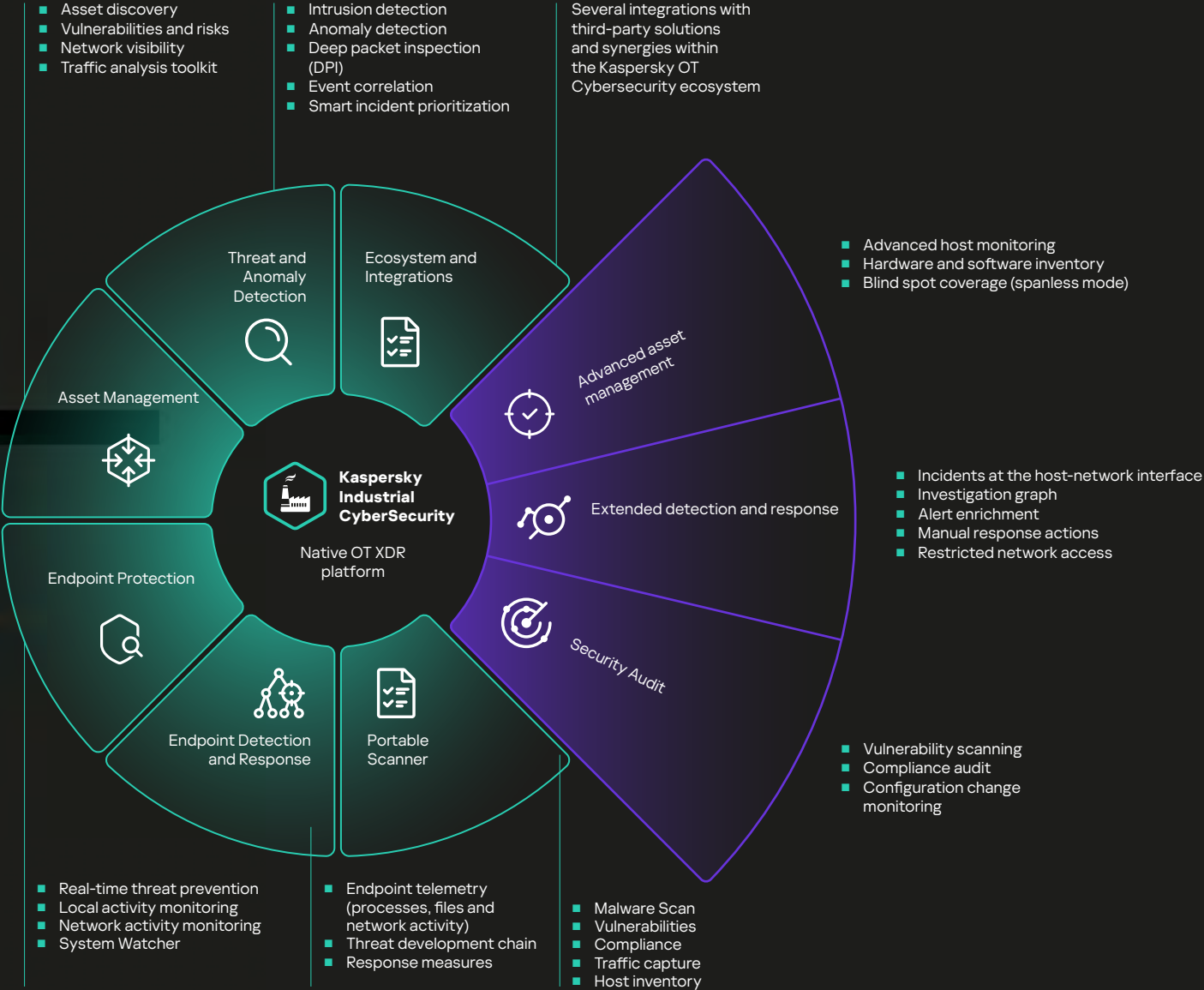
Kaspersky Industrial CyberSecurity for Networks

Network traffic analysis, detection and response



Kaspersky Industrial CyberSecurity for Nodes

Endpoint protection, detection and response



We build Cyber Immunity

Why this matters

A Cyber Immune system is an approach to building IT systems with innate protection against cyberattacks. We believe that such systems can be created using KasperskyOS. To achieve this, KasperskyOS combines best practices in information system development with a focus on secure architecture, secure system design principles and patterns, quality control, secure software development methodology, industry standards, and mandatory penetration testing. This is how we draw closer to a wonderful future where systems solve security problems out of the box.

We propose to build systems so they are secure-by-design by separating them into isolated parts and controlling the interactions between those parts.

As a result, even if an attacker manages to penetrate one line of defense, the rest of the system continues to operate securely. This is especially important for industrial automation, wearable devices, the Internet of Things (IoT), and remote access to critical infrastructure.

KasperskyOS

The KasperskyOS operating system, consisting of a microkernel and the Kaspersky Security System subsystem, provides standard security and enables the development of Cyber Immune solutions.

By combining a microkernel architecture with concepts of MILS (Multiple Independent Levels of Security) and FLASK (Flux Advanced Security Kernel), KasperskyOS creates a fundamentally new level of cybersecurity, significantly increasing a system's resilience to cyberattacks.

In 2024–2025, we took a significant step in our development of KasperskyOS: we adjusted our strategy and began expanding the scope of its use as a full-fledged general-purpose operating system.



Flagship release: Kaspersky Thin Client 2.3

During the reporting period, the key product was the new commercial version of [Kaspersky Thin Client 2.3](#), which combined the achievements of 2024 with new features from 2025:

- extended support for peripherals (webcams, headsets, scanners)
- centralized management of monitor settings via Kaspersky Security Center
- Technical support through remote administration
- Secure Boot mode.

This is the first release certified on the Dell Wyse 3040 platform, marking a significant step in expanding hardware compatibility.

Examples of successful deployment of Kaspersky Thin Client

- Aswant Distribution, an international partner, became the exclusive distributor of Kaspersky Thin Client in Malaysia and Indonesia. Between 2024 and 2025, it delivered cyberimmune thin clients to government bodies, industrial enterprises, and financial and educational institutions in the region.
- The Kulim Municipal Council's deployment of the system reduced operating costs by 20% and increased the cyber resilience of infrastructure.



We create products that help track ESG indicators



Kaspersky Automotive Secure Gateway is a [solution](#) for protecting connected vehicles, including a security gateway, an intrusion detection and prevention system (in-vehicle IDPS), telemetry services, remote control, and a navigation system.

Care for the environment

Our solution can continuously monitor vehicle systems (battery, electronics, driving parameters, etc.), enabling, for example, optimized charging and extended battery life, as well as fewer service vehicle trips and, consequently, reduced CO₂ emissions, thanks to predictive diagnostic data.

Human safety

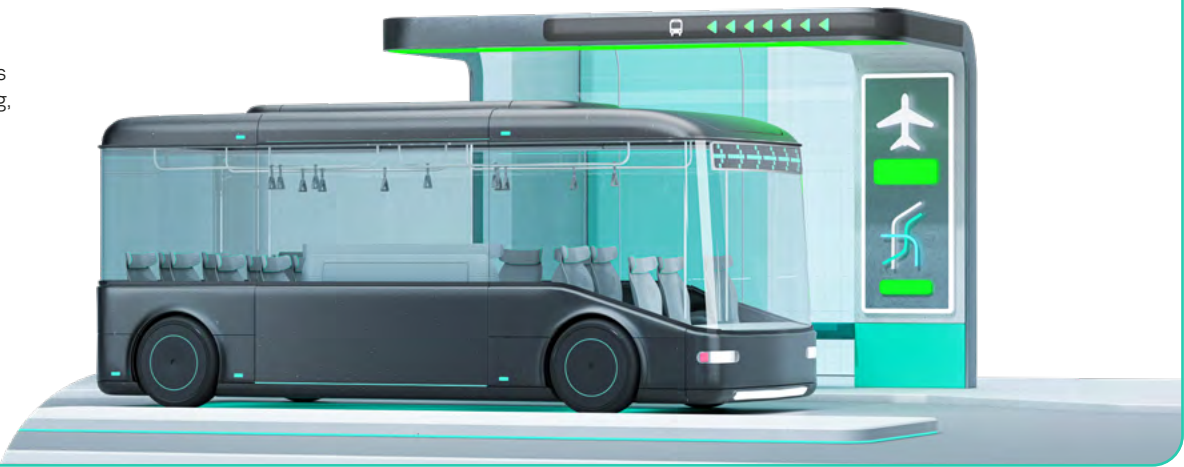
Our solution and its development processes and individual software components are certified as compliant with ISO 26262 (ASIL B). This functional safety standard for the automotive industry minimizes the risk of harm to human life and health resulting from vehicle system failures.

Accounting for data security and functional safety requirements opens the way to remote business scenarios (remote maintenance, autonomous transportation, flexible operating models for access to vehicles) without compromising on human safety and cyber risks.

Management quality

Kaspersky Automotive Secure Gateway helps automakers comply with international vehicle cybersecurity standards, including by monitoring information security events and sending them to the Vehicle Security Operations Center (VSOC) for a prompt response and incident investigation.

These features of Kaspersky Automotive Secure Gateway facilitate the implementation of ESG principles in the transportation industry.



We comply with requirements and standards when developing solutions

Kaspersky guarantees that its products comply with industrial cybersecurity standards and legal requirements worldwide.

For more information about the legal and industry requirements we account for when developing our products and solutions, please see [Appendix 5](#) on page 135

KICS is the world's first XDR platform certified as compliant with the IEC 62443-4-1 industrial standard.

Both products within the KICS platform—KICS for Nodes and KICS for Network—have been certified as compliant with key international cybersecurity standards and also address or help meet the requirements of other international laws and industry standards.

Our results

Kaspersky OT CyberSecurity in 2024–2025

The Kaspersky OT CyberSecurity platform and Kaspersky Industrial CyberSecurity, one of the solutions included in the platform, showed strong sales growth in the reporting period. Interest in these solutions increased due to:

- market factors, including increased attacks on industrial enterprises, tighter regional regulations, import substitution, a focus on cyber sovereignty and diversification of security suppliers, and increased customer maturity
- Kaspersky's long-term strategy to strengthen its position in domestic markets and expand geographically
- a strategic approach to cross-product ecosystem sales for public sector and critical infrastructure customers

2nd place

in Kaspersky's portfolio in terms of total sales of all ecosystem products

KICS in 2025

The KICS platform has demonstrated 25% annual business growth, demonstrating strong momentum in all key markets, including regions affected by geopolitical issues. International sales are growing by more than 50% year-on-year thanks to Kaspersky's strategy to expand its geographic reach.

+25%

growth in sales compared to 2024

Top 5

domains among Kaspersky's B2B products

+20%

CAGR (compound annual growth rate) year-on-year

KasperskyOS

In 2024–2025, the KasperskyOS ecosystem demonstrated sustainable growth and expanded into new markets. The portfolio of KasperskyOS-based solutions has expanded, covering the corporate, transport, and embedded segments. During this period, the platform achieved double-digit growth in the number of installations worldwide and triple-digit growth rates in the Russian market (as percentages).

>540

protected networks of large customers with structural economic importance

+20%

increase in ARPC (average revenue per customer) due to cross-selling and up-selling solutions (cross-selling and increasing sales to existing customers)

16%

of Kaspersky's revenue comes from industrial customers (second place after the public sector)

>330,000

licenses sold

Our plans for 2026–2027

Industrial cybersecurity

Industrial companies around the world are moving from closed (proprietary) solutions to open architectures and software-defined automation.

Accordingly, our plans for industrial cybersecurity for 2026–2027 include:

- 1. Integrate and develop KICS.** Regarding the development of Kaspersky OT CyberSecurity, we plan to continue integrating KICS with Kaspersky Cloud Workload Security, our solution for protecting cloud and container environments, while simultaneously expanding its functionality and integration with other products. KICS already uses AI technologies for monitoring (device profiling, process analysis), and we are developing protections against future AI-based cyberattacks.
- 2. Develop cyberimmune devices and new technologies.** Another area of KOTCS development is the creation of Cyber Immune devices that run KasperskyOS: thin clients. We also plan to progress from connected car gateways to V2X¹ data control devices for highly automated vehicles.
- 3. Train specialists.** Together with Kaspersky Academy, we plan to develop collaboration with leading technical universities that have departments or academic laboratories that research automated process control systems or information security. By offering students the opportunity to gain relevant, hands-on experience, we are already building a pipeline of engineers who will protect mission-critical enterprises for decades to come.

Develop KasperskyOS

In the coming years, KasperskyOS will focus on moving beyond its niche as an embedded solution to become a fully-fledged technical foundation for secure, next-generation digital ecosystems.

Main areas for ecosystem development

- 1. Expand areas of application.** KasperskyOS will become a universal secure platform for the digital ecosystems of companies, government bodies, and industrial organizations.
- 2. Further the technological development of the kernel and SDK.** Improvements to the microkernel architecture, performance optimization, and expansion of developer tools (KasperskyOS SDK) will allow partners and developers to more quickly create new solutions based on the operating system.
- 3. Grow the ecosystem.** Build a community of integrators and developers who use KasperskyOS, expand educational programs and startup accelerators related to cyberimmune security.
- 4. Expand internationally.** Scale deployment of KasperskyOS in Asia, the Middle East, Turkey and Latin America, creating regional centers of excellence, and developing localized versions of products.
- 5. Gain regulatory and industry recognition.** Continue to collaborate with regulators and industry associations to develop standards for a new class of devices and systems whose built-in cyberimmunity is proven by architecture.
- 6. Contribute to the ESG agenda.** Use KasperskyOS as a foundation for building secure and energy-efficient solutions in transportation, industry, energy and IT to help reduce carbon footprints and improve equipment efficiency.

¹ Vehicle-to-everything — Real-time communication between a connected vehicle and any other object (other vehicles, road infrastructure objects: traffic lights, pedestrians, networks, etc.) via wireless communication technologies.

