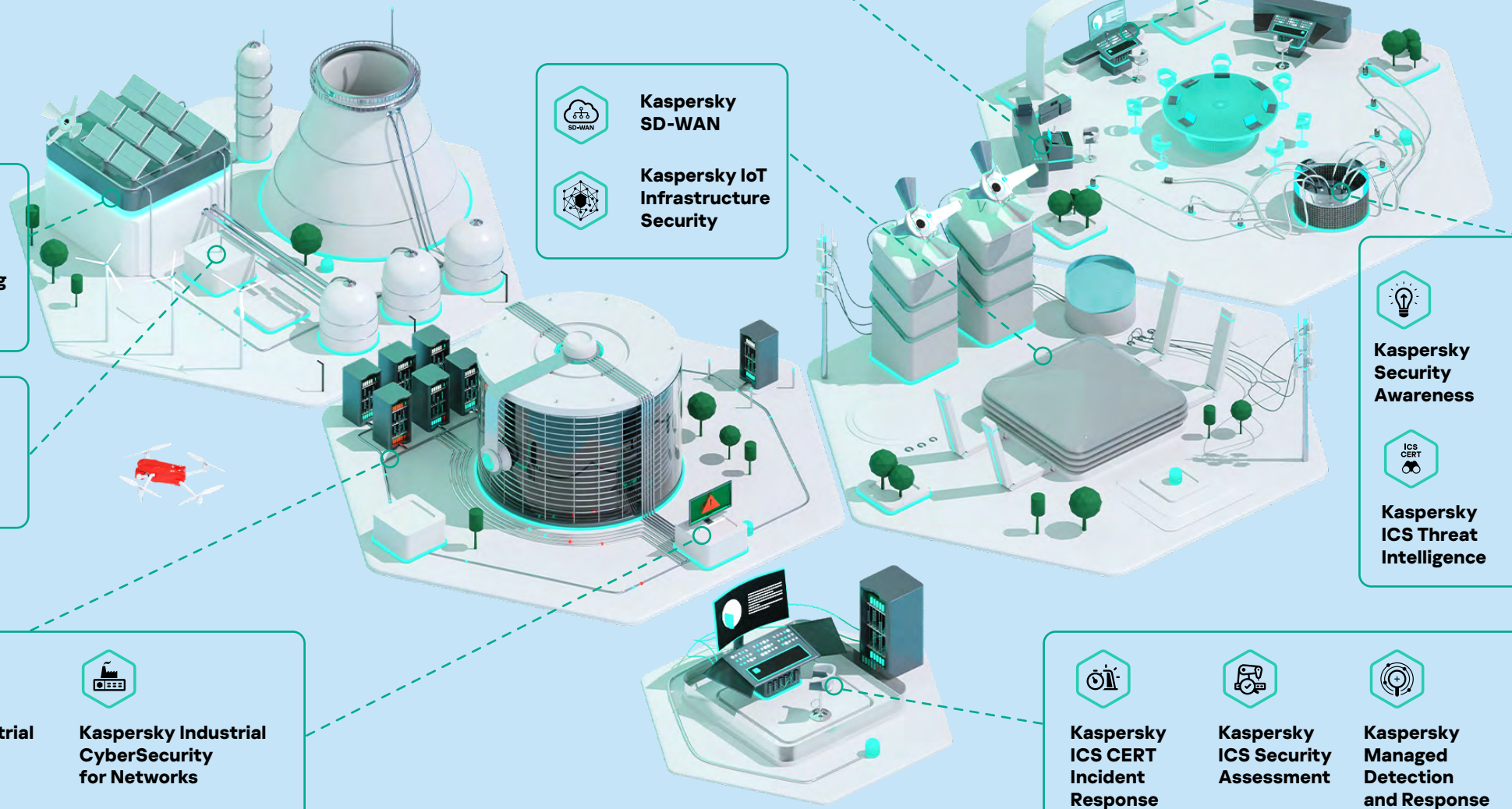
Industrial security ecosystem



Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Secure Remote Workspace

Kaspersky SD-WAN

Kaspersky IoT Infrastructure Security

Kaspersky Machine Learning for Anomaly Detection

Kaspersky Antidrone

Kaspersky Security Awareness

Kaspersky Ask the Analyst

Kaspersky ICS Threat Intelligence

Kaspersky ICS CERT Training

XDR platform

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Kaspersky ICS CERT Incident Response

Kaspersky ICS Security Assessment

Kaspersky Managed Detection and Response

Kaspersky Industrial Emergency Kit

Kaspersky Industrial CyberSecurity

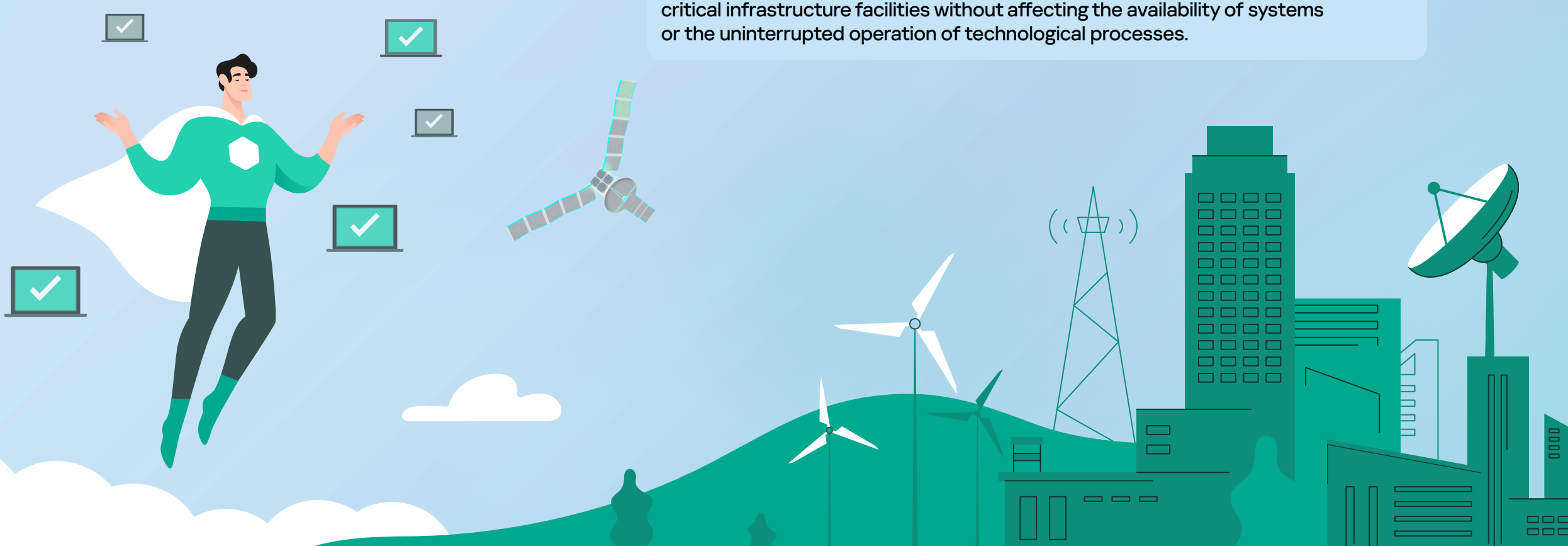
Key industries using the ecosystem

- Oil, gas and chemical industries
- Energy, including the nuclear sector
- Metallurgy and mining
- Industrial production

Future areas for the use of KOTCS

- Pharmaceuticals and medical equipment
- Transport and logistics
- Telecommunications

The key component of the KOTCS ecosystem is the Kaspersky Industrial CyberSecurity (KICS) platform, designed to protect industrial enterprises and critical infrastructure facilities without affecting the availability of systems or the uninterrupted operation of technological processes.



KICS

The native XDR platform KICS is a vital part of the automated process control system, conducts in-depth analysis of traffic and telemetry of components, actively responds to threats, or simply informs users about them. It helps protect modern digital and connected industrial automation systems against attacks of any complexity and also monitor the safe operation of software and hardware systems of previous generations.

KICS ensures the total visibility of what is happening at all levels of the technological process: physical devices, controllers, SCADA[1] servers and production management systems. The platform has been tested for compatibility with products from leading industrial automation system vendors, including Siemens, Honeywell, B&R (ABB Group), Yokogawa, Emerson, Schneider Electric, Baker Hughes, GE and others.

The KICS platform is compatible with numerous process control systems from 50+ vendors

The platform features two closely interrelated and complementary components: KICS for Nodes to protect industrial operator panels, workstations and servers, and KICS for Networks to monitor industrial network security.

KICS today

~230,000
KICS for Nodes licenses sold

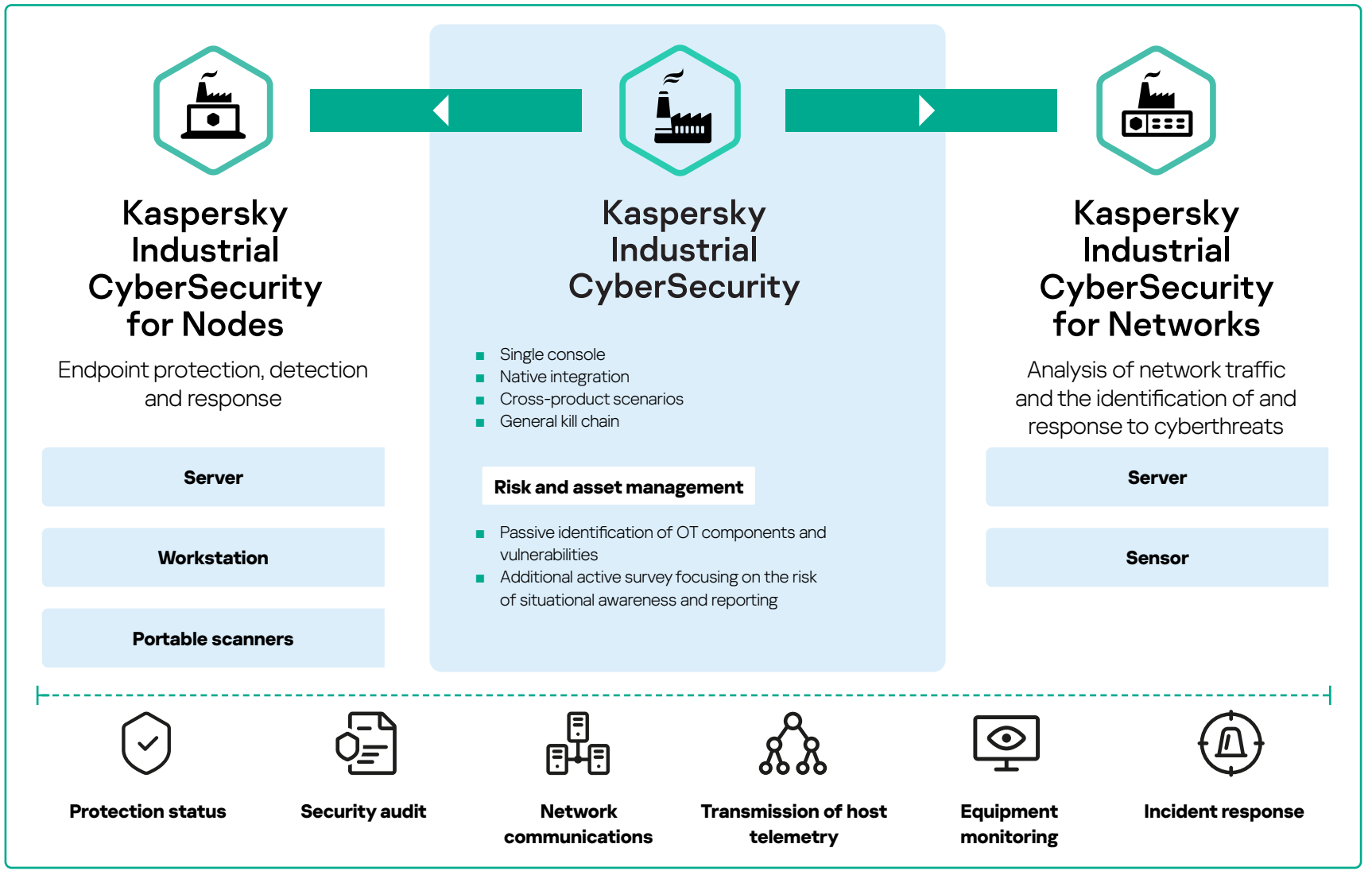
>1,000
industrial customers use KICS solutions

430
industrial networks of major customers protected worldwide

+20%
average income per customer

[1] Supervisory Control and Data Acquisition.

XDR platform for industry



KICS protects all automated process control systems that are currently in operation:

- Brown field (more than 90%) – systems created from 2005 to the 2020s, that generally consist of distributed control systems (DCS) with various types of microprocessor controllers (PLC[1], IED[2] and RPA[3]), computer human-machine interfaces (HMI) on old Windows OS and industrial Ethernet-based networks
- Promising projects and popular areas (5–10%) – various types of digitalization, connected sites, cloud technologies, the IIoT, digital twins, virtualization of industrial systems, AI/computer vision, DSS[4] and additive technologies

The KICS platform provides full visibility and control over what is happening in the control systems of an industrial enterprise's key technological processes. It detects and blocks network threats as well as traffic and process anomalies, prevents malware from infecting computer equipment and detects violations of safety policies by personnel. In addition, it helps conduct inventories of industrial assets, perform security audits, detect vulnerabilities and manage risks.

1 Programmable logic controllers.
2 Intelligent electronic devices.
3 Relay protection and automation.
4 Decision support systems.

Our contribution to the safe production of clean energy

We protect energy facilities with modern information and operational technologies and services

The Ust-Kamenogorsk and Shulbinskaya hydroelectric power plants are major strategic facilities that supply clean energy from renewable sources to residents and enterprises in Eastern Kazakhstan. The power plant managers were looking for the best solution to ensure their safe and seamless operation.

The project to protect hydroelectric power plant infrastructure was a complex one because the following key criteria had to be taken into account when selecting a suitable solution:

- Architectural requirements
- Requirements for compatibility with other solutions
- Requirements for automated process control systems

The KICS platform ultimately proved to be the most suitable solution for protecting the production processes of the hydroelectric power plants. It was incorporated into the technological systems of power plants that are located in different cities and only connected by a VPN channel.

What was the result?

Our KICS solution ensures the industrial infrastructure of the two hydroelectric power plants operates securely at all levels – from process control system servers and automated workstations to programmable logic controllers and network equipment – without disrupting the interaction of information systems and industrial equipment. KICS can effectively identify different types of threats at the hydroelectric power plants: human errors, disruption of communications between devices, employees performing work without approval, attacks and malware.

Creating Cyber Immunity

Objective

Ensure the reliable and predictable operation of industrial systems and reduce the risk of incidents and related accidents

The number of internet-connected devices is growing with each passing day, which also entails an increase in cybercrime. Cyberthreats can cause substantial physical damage to industrial enterprises, energy facilities, cars and smart city systems, among other things.
The information security industry is constantly creating new technologies and products, but they are often only just catching up with hackers. It is crucial to find a way to stay ahead of them and protect ourselves against cyberthreats.

Solutions

Prevent cyberattacks with KasperskyOS

Cyber Immunity makes it possible to create hardware and software IT systems with built-in protection against cyberattacks. It is a critical factor for the development of industrial automation, wearable industrial devices, the Internet of Things (IoT) and remote access to critical facilities. We already have access to such Cyber Immune devices as gateways for the Industrial IoT, thin clients, smart city controllers and gateways for cars.

As part of our Cyber Immune approach, we have developed our own operating system, KasperskyOS, a platform for creating products and solutions that are protected at the architectural level.

We achieve Cyber Immunity by splitting the system into isolated components and controlling interaction between them. With this approach, most attacks on the system will be futile, since it will continue to perform critical functions even in an aggressive environment and prevent hackers from pulling off successful attacks.

Two key features of KasperskyOS are its own microkernel and security monitor – the Kaspersky Security System subsystem – which provides a higher level of security and meets Cyber Immunity requirements right out of the box. Such solutions are virtually impossible to compromise, and the number of possible vulnerabilities in them is minimized.

Helping industrial companies implement their ESG strategies

Objective

Monitor and analyze sustainability indicators

Major industrial companies operate on the principles of sustainable development and develop their own ESG strategies. They set climate change targets and plan to gradually minimize their carbon footprint. To track their progress in this regard, companies monitor and analyze greenhouse gas emissions and pollutants in real time and retrospectively. Companies with significant greenhouse gas emissions from their operations, including transport and mining companies, are particularly interested in such a reporting system.

Industrial and occupational safety is another key aspect of sustainability. Industrial companies are incorporating injury reduction goals into their ESG strategies. They collect and analyze data on working conditions and injuries to track their progress in achieving these goals, identify vulnerabilities, and take action to prevent workplace accidents. IT solutions are used for this purpose to automatically monitor compliance with safety regulations, record violations and transfer this data to the reporting system.

Solutions

Create products that can track ESG targets

In an effort to not only help our customers protect their cars against hacking, but also control fuel consumption, build optimal logistics routes and take into account emissions from vehicles, we created the Kaspersky Automotive Secure Gateway solution. It runs on the KasperskyOS, collects all the essential digital data about a vehicle's operation, makes such data visible, transparent and understandable, and sends it to servers for analysis with an assessment of how to improve performance in the future. Our solution enables customers to achieve their sustainability goals in reality, not just on paper. In addition, it securely updates the gateway, helps update other electronics in the vehicle, collects information about other internal network events in the vehicle and sends it to the security monitoring center, thereby ensuring that there is a single point of control and response, and minimizing maintenance costs.

Helping customers comply with requirements to protect critical infrastructure

Objective

Ensure that users of our solutions comply with the laws of different countries

Industrial enterprises and operators of critical infrastructure must comply with local legal and industry requirements for risk management and reporting incidents. Kaspersky guarantees that its products comply with standards and legal requirements for industrial cybersecurity in different countries around the world.

For more about the legal and industry requirements we consider when developing our products and solutions, please see Appendix 4 on p. 149

Solutions

Consider requirements and standards when developing products for industrial enterprises

KICS is the world's first XDR platform certified to IEC 62443–4-1

Both products of the KICS platform – KICS for Nodes and KICS for Network – are certified in accordance with major international cybersecurity standards and also consider or help meet the requirements of other international laws and the following industry standards:

- ISO/IEC 27 001 IEC 27 002 (DIN 2008 in Germany) – a standard that establishes the requirements for the creation, introduction, maintenance and continuous improvement of an information security management system at an organization
- ISO/IEC 27 019 (DIN 2011 in Germany) – a standard used to ensure information security in the energy sector
- ISO/IEC 27 032 – a standard adressing Internet security issues and contains recommendations for eliminating the most common threats in this regard (social engineering, zero-day attacks[1], spyware, etc.)
- ISO/IEC 15 408 – a standard with the historical name "Common Criteria" that describes the accumulated experience of various countries in the development and practical use of criteria for assessing the security of information technologies
- IEC 62 443 (ANSI/ISA99) – a series of these standards that contains requirements for the design of cybersecurity management systems for automated process control systems and SCADA
- IEC 62 351 – a standard that encompasses information security issues in energy systems
- NIST CSF – recommendations for ensuring the security of industrial control systems that were developed by the U.S. National Institute of Standards and Technology
- NERC CIP – a set of cybersecurity standards for critical infrastructure and the protection of the U.S. power grid that is also used by some Latin American countries
- NIS 2 Directive (EU) 2022/2555) – a new EU directive on cybersecurity[1]
- IMO MSC.428(98) – a Maritime Safety Committee resolution that regulates the management of cyber-risks in the maritime industry as part of safety management systems
- ICAO – a cybersecurity strategy in aviation[2]
- IAEA Nuclear Security Series No. 17-T (Rev. 1) – methods to ensure computer security for nuclear installations

Starting from February 8, 2022, the scope of certification extends to Kaspersky's data processing services (KSN). Many KICS customers enable KSN during installation. It is crucial for them that we use the best global practices at its data centers in Zurich, Frankfurt, Toronto, Moscow and Beijing. Find out more about this here.

Our KICS platform is fully certified by TUV Austria for compliance with the international standard for the software development life cycle to ensure the cybersecurity of industrial enterprises. The trust level is three out of four.

Kaspersky undergoes audits by Service Organization Controls (SOC 2). As part of Type 2 certification, the Company's solutions were tested for the effectiveness of controls used to protect the development and release of anti-virus databases against unauthorized intervention. The performance of Kaspersky's control mechanisms was not assessed on a specific date, as it is in the Type 1 audit, but over the course of six months.

1 EU member states must adopt and publish the cybersecurity measures required to comply with the new directive by October 17, 2024.
2 FAA Advisory Circular 119-1 – Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP).

Our results

KICS

Sales of the KICS platform have increased significantly on all major industrial cybersecurity markets. In 2023, Kaspersky's industrial cybersecurity business demonstrated the following results:

- The KICS platform firmly moved into the top five of all the Company's B2B products in terms of revenue
- Industrial Cybersecurity once again had triple-digit revenue growth as a percentage compared with last year
- The sales plan was exceeded by 128%
- The gross EBITDA margin, operating EBITDA margin and EBITDA margin range from 20% to 40%

Main drivers in the development of the Kaspersky Industrial CyberSecurity platform

- Growing threats and emerging information security incidents that industrial companies increasingly encounter in their operations
- The need for a solution that is capable of protecting heterogeneous infrastructure that consists of technological processes that are simultaneously controlled by both legacy automation systems and modern solutions based on networks with advanced architecture, current operating systems and industrial software versions
- The active introduction of connected smart devices and devices of the Industrial Internet of Things as part of the digitalization process, as well as the widespread use of IT, software, hardware and network technology stacks at industrial facilities

We expect two-fold growth in this business segment over the next four years. To achieve this goal, we will continue to invest in the development of KICS technological capabilities and promote it in key regions.

KasperskyOS

During the reporting period, we started developing a regional business to protect virtual workplaces, which have become particularly important in the post-pandemic period, when many companies have switched to a hybrid workplace model.

In August 2023, we signed an agreement with Centerm, to deliver specialized workstations (thin client on KasperskyOS) based on orders from any country. We have already received the first orders from Switzerland and Malaysia.

In 2023, our specialists conducted an in-depth study on how to expand hardware platforms with unique solutions built on Cyber Immunity principles, and commenced expert work to obtain the required opinions and regulatory approvals.

Our plans for 2024

Industrial cybersecurity

We offer advanced and comprehensive protection

across every segment of our customers' infrastructure using the technology, knowledge and expertise within our OT ecosystem. We develop cross-product scenarios to use our natively-integrated technologies in response to new customer demands and also include our partners in our open ecosystem of solutions.

- Investments in Linux functions and the development of the KICS platform's technological capabilities
- Expansion of supported hardware platforms and industrial communication protocols, and development of an expert database of industrial devices
- Elaboration of scenarios for the use of wearable devices and secure data exchange, as well as creation of information security audit tools and routine checks even for isolated systems and networks

Expansion

to new vertical markets in which companies need to clearly monitor ESG indicators

- Collaboration with clients from such industries as transportation, logistics, semiconductors, as well as automotive and component manufacturing
- Partnerships with leaders in OT integration and creation of technology alliances with regional champions among vendors of industrial automation systems[1]

Geo-expansion

into regions where Kaspersky has a smaller presence. To accomplish this, we are adapting the ecosystem to the specific features of each region

- Continued investments in historical markets: Russia, the CIS and Europe
- Expanded cooperation with regional partners to protect critical infrastructure: Brazil, China, India, Indonesia, Saudi Arabia, UAE, Algeria and South Africa

KasperskyOS

Development

of the business community of partners, whose members use Cyber Immune products in vertical industry solutions

Launch

of pilot projects with key customers in various industries to develop a scenario with the effective use of Cyber Immune solutions

Analysis

of regulatory requirements to create a description of a new class of devices with built-in (Cyber Immune) protection

[1] Regional leaders and manufacturers of industrial equipment and automation systems.