Kaspersky OT CyberSecurity

Unified solution purpose-built
for cyber-physical systems resilience

kaspersky cybersecurity
true to business

Kaspersky OT CyberSecurity

Where experience delivers resilience

Industrial technologies
Robust industrial security solutions – tested, compliant and approved

Actionable knowledge
Trusted threat analytics and comprehensive industrial cybersecurity trainings

Field-tested expertise
A full range of professional services for robust and holistic cybersecurity

IT XDR

Kaspersky Next XDR Expert

IT — OT Convergence

Technologies

Specialized Solutions

- Kaspersky Antidrone
- Kaspersky Machine Learning for Anomaly Detection
- Kaspersky SD-WAN

Kaspersky Industrial CyberSecurity

Native OT XDR

for Nodes
Endpoint protection, detection and response

for Networks
Network traffic analysis, detection and response

Kaspersky OS Solutions

- Kaspersky Thin Client
- Kaspersky Automotive Secure Gateway

Knowledge

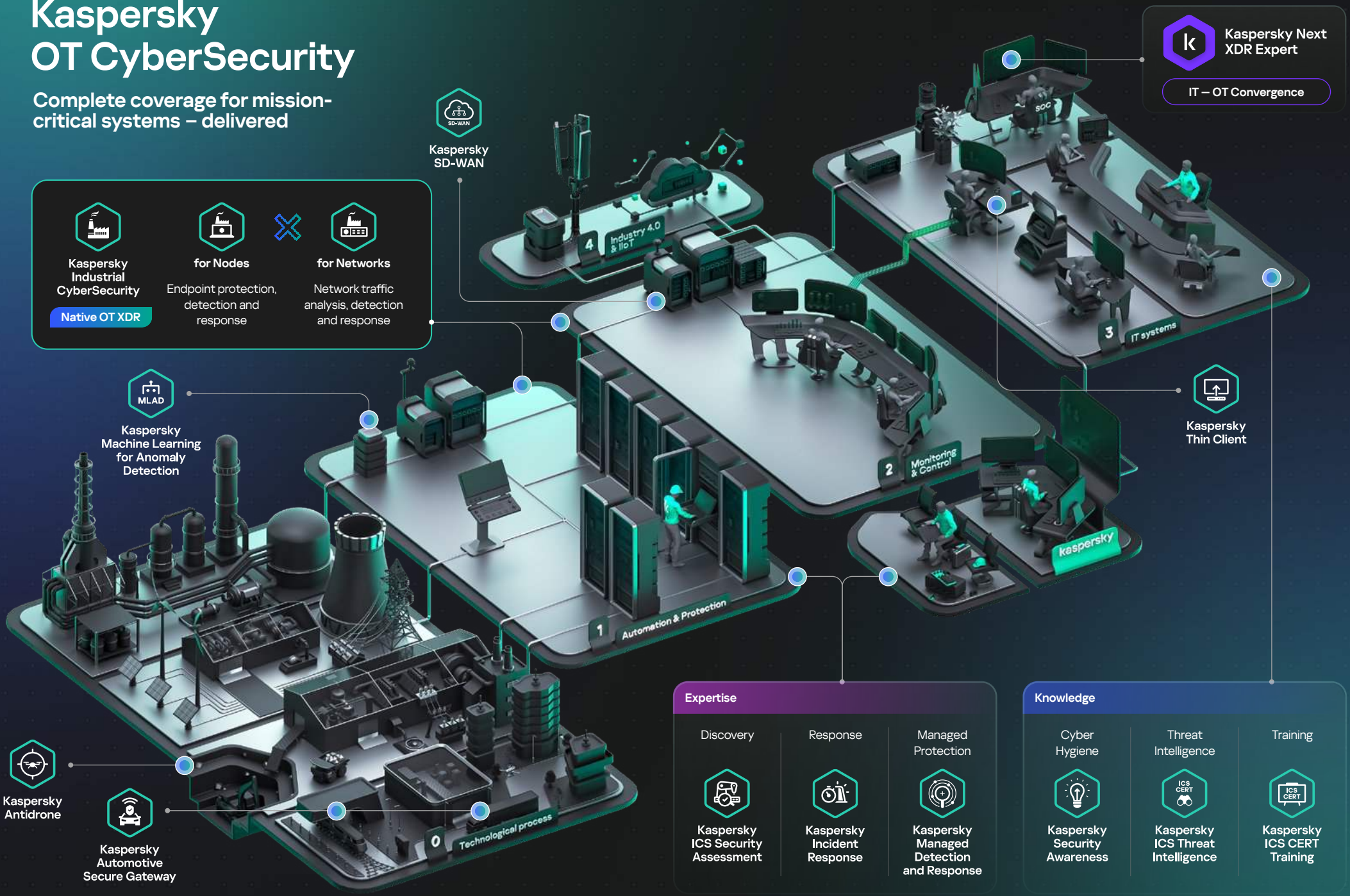
Cyber Hygiene	Threat Intelligence	Training
Kaspersky Security Awareness	Kaspersky ICS Threat Intelligence	Kaspersky ICS CERT Training

Expertise

Discovery	Response	Managed Protection
Kaspersky ICS Security Assessment	Kaspersky Incident Response	Kaspersky Managed Detection and Response

Kaspersky OT CyberSecurity

Complete coverage for mission-critical systems – delivered



Kaspersky Industrial CyberSecurity

360° situational awareness and risk exposure control

- **Asset inventory and network visibility.** Track all connected devices and their configurations. Build a network graph and analyze data flows.
- **Threat elimination.** Identify and mitigate threats across hosts and networks, with insights into root causes and safe response measures.
- **Risk assessment.** Assess vulnerabilities and monitor security settings changes for hosts, network devices and controllers.

Key advantages

- Tested and proven compatibility with 200+ industrial automation systems and devices
- Seamlessly integrated OT XDR platform that solves multiple challenges, purpose-built for critical infrastructure
- Low footprint solution that does not impact system performance or process continuity

KICS and its core technologies are subject to industry-leading audits

ISA/IEC 62443-4-1 | SOC 2 Type 2 | ISO/IEC 27001 | GB 42250-2022

Kaspersky Next XDR Expert

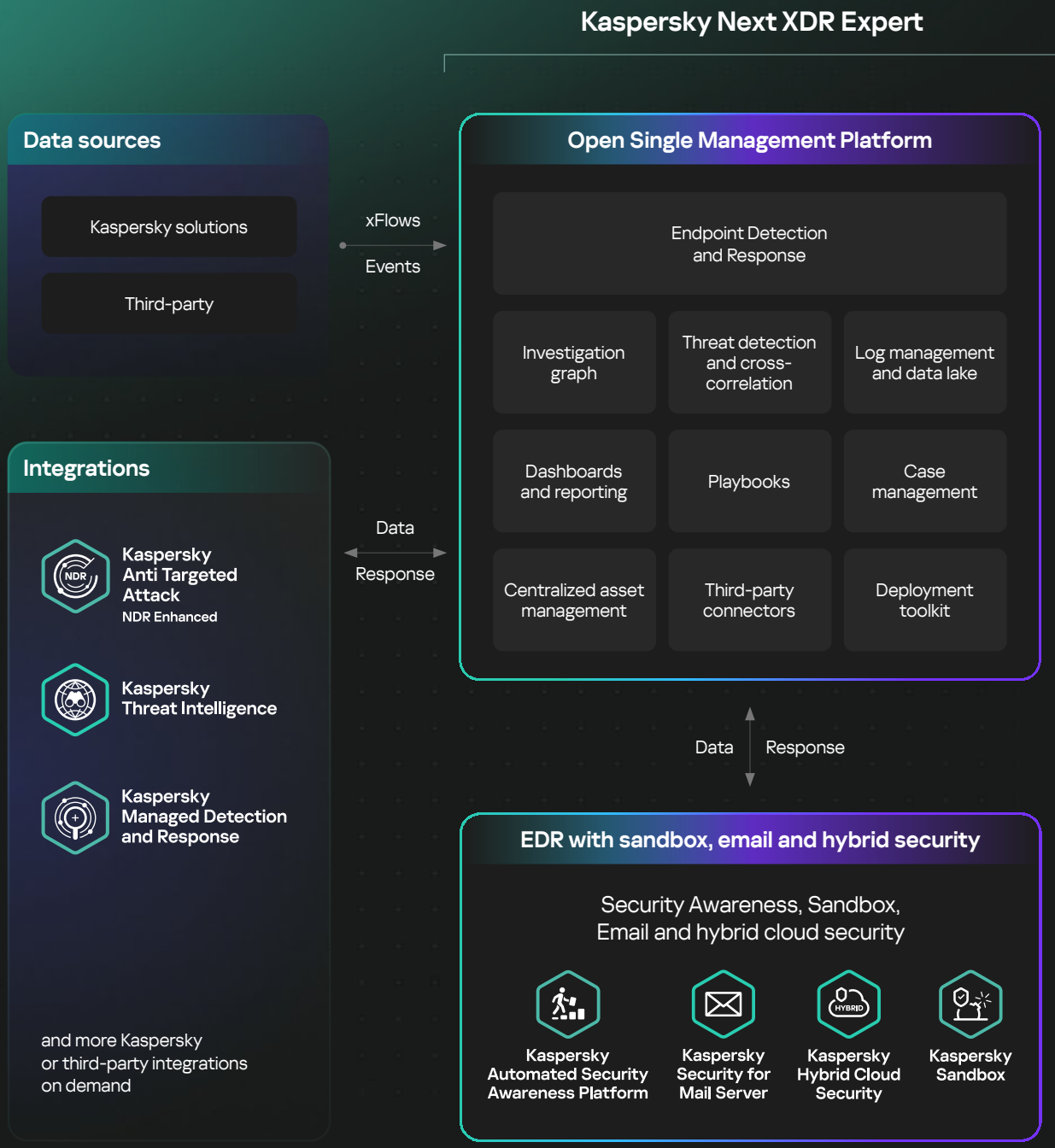
End-to-end protection across the industrial and corporate segments of your enterprise

Through close integration with Kaspersky Next XDR Expert, the Kaspersky Industrial CyberSecurity platform enables new scenarios including interactions with third-party solutions and enhanced investigative and response capabilities. The integration helps protect your business where industrial and corporate environments intersect.

Security teams gain a unified view of an incident's development and identify its root causes to prevent similar incidents in the future.

Key advantages

- Security and data sovereignty for converged, asset-intensive IT/OT/IoT infrastructures
- Native interoperability across Kaspersky products portfolio provides flawless and unparalleled integration



Kaspersky Machine Learning for Anomaly Detection

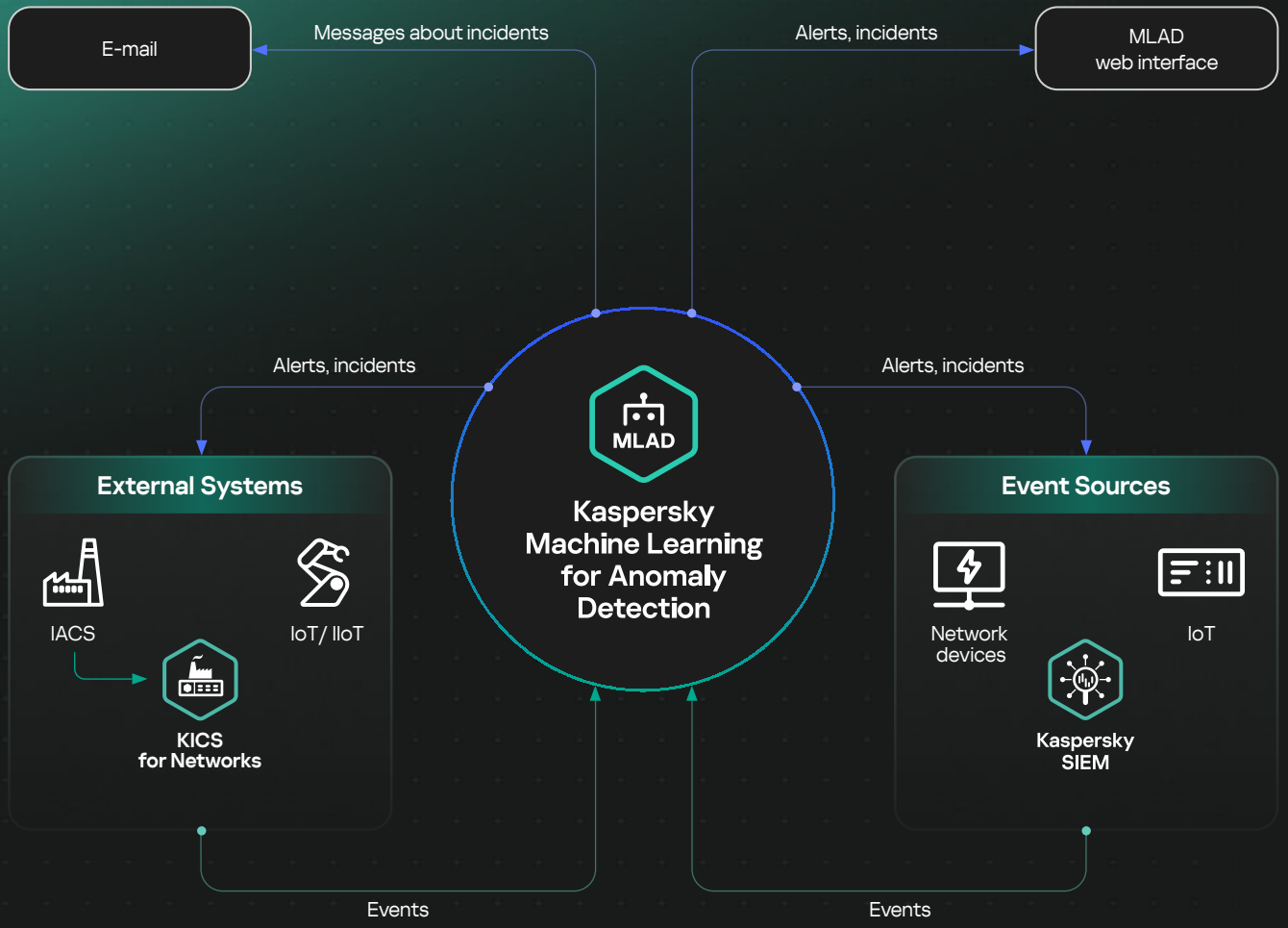
Early anomaly detection and predictive analytics

- Detects equipment faults and human error long before they become critical, helping to prevent failures and accidents.
- Identifies atypical employee actions or equipment operations that may indicate a specialized attack or sabotage.
- Identifies hard-to-detect anomalies in the operation of cyber-physical systems, caused by small deviations across multiple process parameters.

Integration with external systems

Kaspersky MLAD receives process telemetry from KICS for Networks, industrial automation systems and IoT/IIoT devices

MLAD event processor exchanges CEF messages with external sources: SIEM systems, IIoT and network devices



IACS – Industrial Automation and Control Systems

SIEM – Security Information and Events Management

IIoT – Industrial Internet of Things

IoT – Internet of Things

Kaspersky SD-WAN

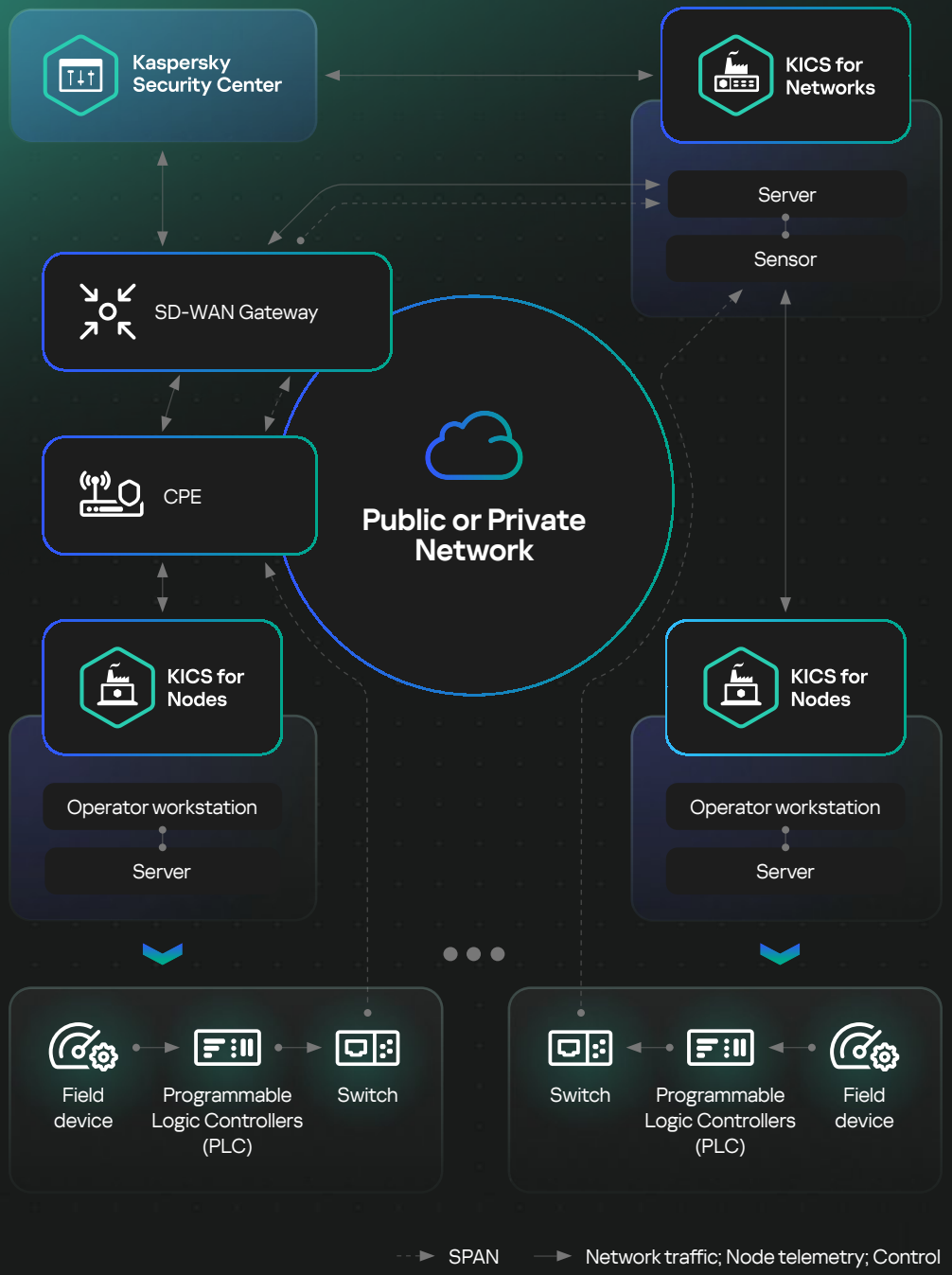
A unified solution that ensures the reliability of distributed industrial networks

Kaspersky SD-WAN enables industrial enterprises to build resilient, geographically distributed networks with centralized management, safeguarding the continuity of industrial processes.

Kaspersky Industrial CyberSecurity supports the use of SD-WAN infrastructure to collect industrial traffic, provide centralized monitoring and protect distributed industrial objects and systems.

Key advantages

- Easy scalability
- Cost optimization
- Convenient management
- Centralized security



Kaspersky Antidrone

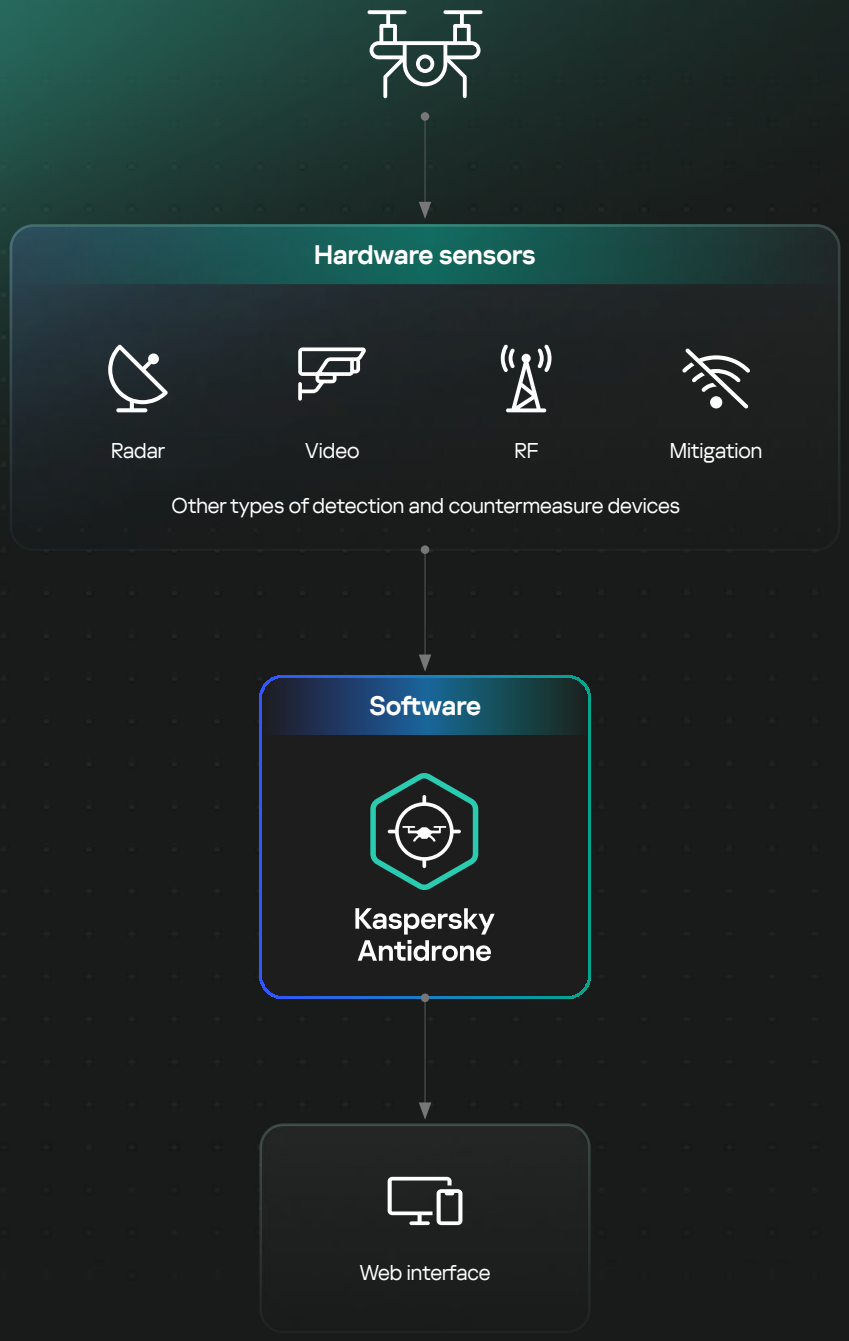
Drone monitoring and defense solution

Kaspersky Antidrone helps reduce the risk of process stoppages in industrial enterprises by preventing unauthorized drones from entering their territory. The system automatically scans the airspace, detecting and classifying drones. Information about what's happening is displayed in the web interface. In the event of a threat, and where permitted, operators can neutralize the drone.

Kaspersky Antidrone is a modular solution that can be deployed across industrial sites of any size. It also supports a "friend or foe" mode, allowing organizations to operate their own drones without interference while preventing unauthorized unmanned aerial vehicles from entering the area.

Key advantages

- Kaspersky Antidrone allows radar, RF scanners, cameras and jammers from different vendors to be combined and orchestrated in a single unified system.
- Multi-sensor fusion significantly improves detection reliability in cluttered, noisy or low-visibility conditions.



Kaspersky Thin Client

Secure remote and virtual desktop infrastructure

Risk

User workstations are among the most common targets for cyberattacks

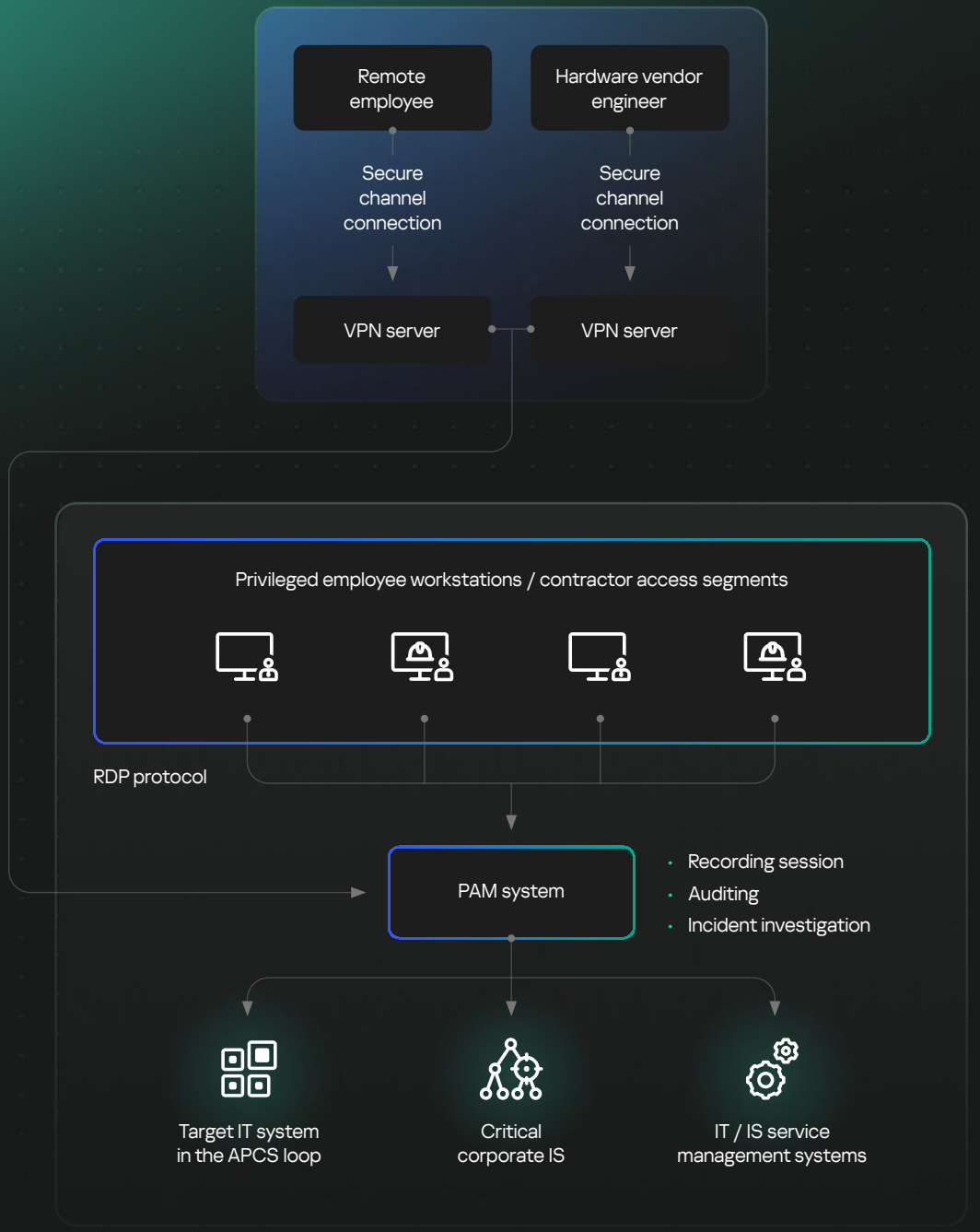
Solution

Kaspersky Thin Client is a solution for building a managed and functional infrastructure of thin clients based on Kaspersky's own microkernel KasperskyOS operating system.

With no active cooling or moving parts, thin clients deliver highly reliable performance in production environments.

Key advantages

- Secure by Design
- A single management platform for IS and IT
- Infrastructure integration in just two minutes



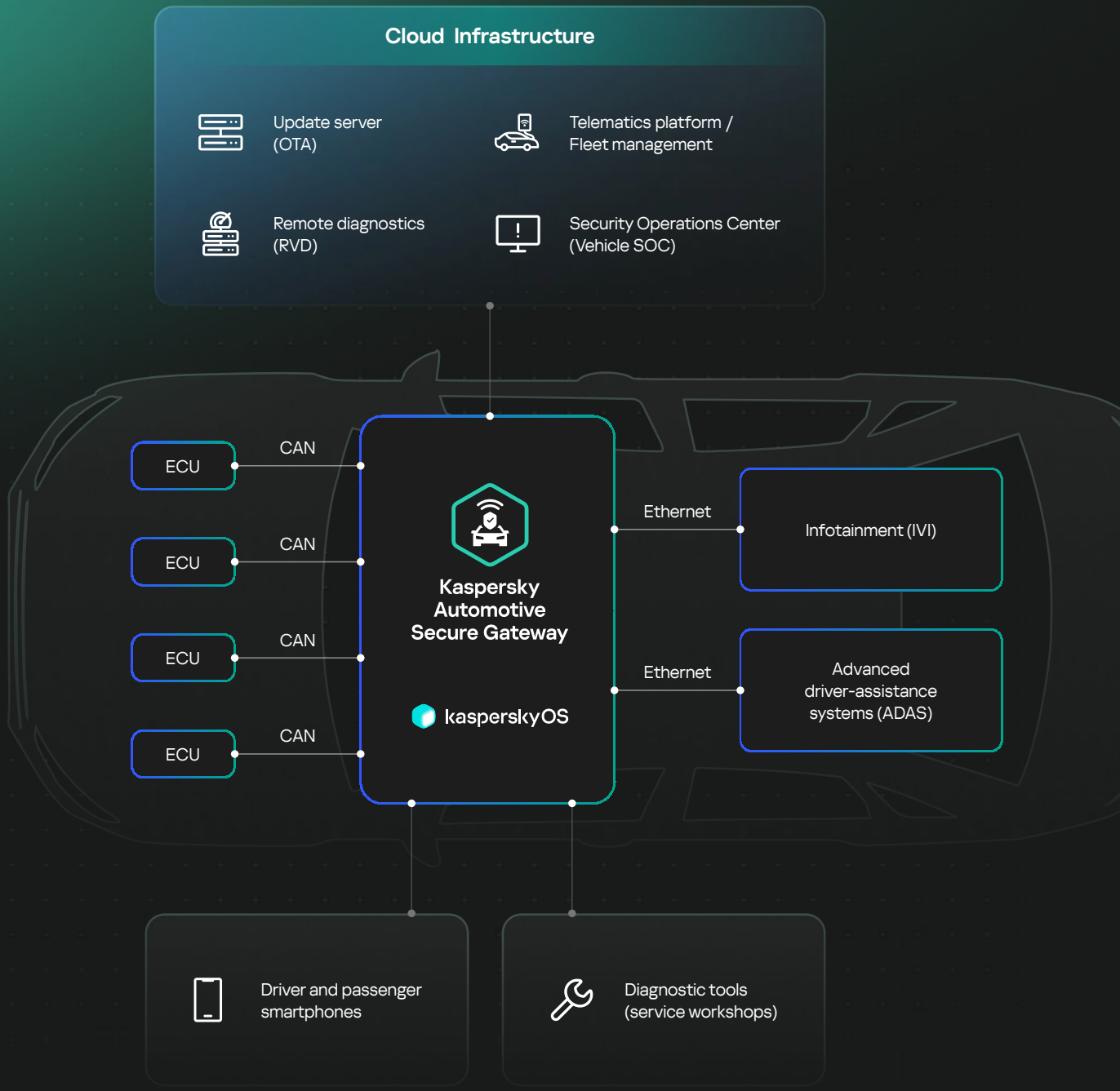
Kaspersky Automotive Secure Gateway

Building reliable IT systems for connected vehicles

- Secure software gateway for connected vehicles that also delivers the functions of a telematics control unit (TCU)
- Security from the operating system level
- Compliance with the latest requirements for ensuring vehicle cybersecurity and safety (ISO 26262, ISO/SAE 21434, UN R155, UN R156, Uptane)
- Secure and reliable communication between electronic units of the E/E architecture as well as between these units and the connected vehicle cloud and diagnostic devices
- Implementation of remote diagnostics, secure over-the-air ECU updates and other telematics services

Key advantages

- Unparalleled security and Cyber Immunity for industries with high information security requirements
- Integration of a secure gateway and telematics control unit in a single solution helps reduce costs
- Specialized protocols help optimize cellular traffic expenses



Knowledge

Kaspersky ICS Threat Intelligence

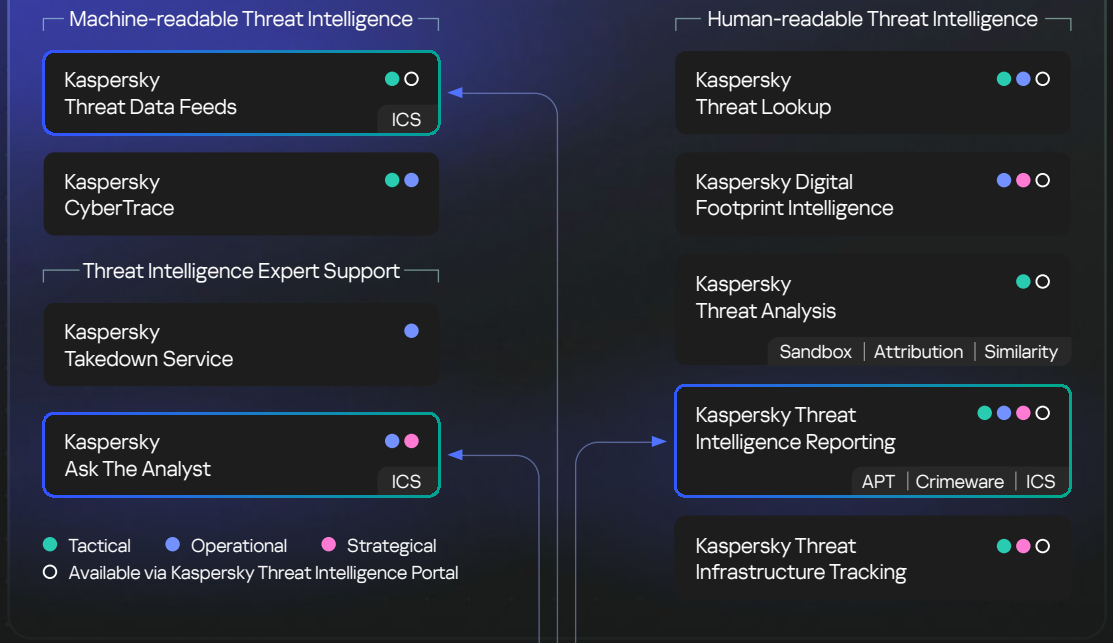
Deep insight into industrial cybersecurity threats and vulnerabilities to support effective risk assessment, attack detection, incident investigation and response.

Backed by the unparalleled expertise and experience of Kaspersky ICS CERT, the first private CERT in industrial cybersecurity.

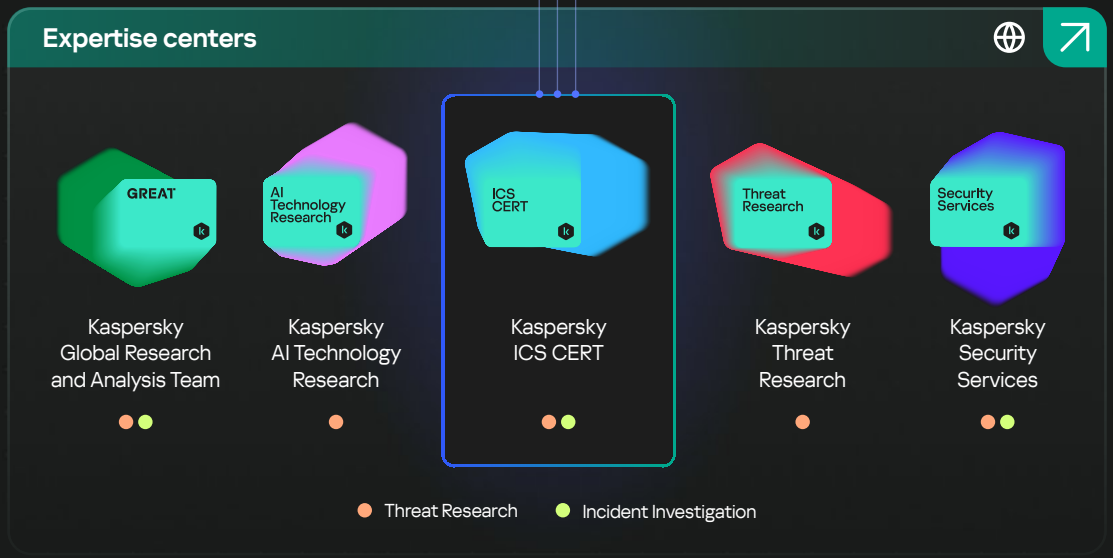
Key advantages

- Fast threat detection and extensive analytical capabilities
- Greater effectiveness in investigations and proactive threat hunting
- Comprehensive threat and vulnerability information for informed decision-making

Kaspersky Threat Intelligence products and services



Expertise centers



Kaspersky Threat Data Feeds

The Kaspersky Threat Data Feed service delivers near real-time threat intelligence to help industrial organizations protect their networks and systems from cyberthreats. The ICS data feeds include information on known malicious files and the latest known vulnerabilities, proven to be exploitable in industrial control systems. When placed in context, this data helps reveal the bigger picture and answer the “who, what, where, when” questions to identify adversaries, make faster decisions and respond effectively.

Key advantages

- Improved, accelerated incident response and forensic capabilities
- Reinforced security solutions
- Prevents exfiltration of sensitive data and intellectual property

What you get:

Kaspersky ICS Hashes Data Feed

Up-to-date threat intelligence for ICS and other systems used in OT to simplify and automate timely attack detection and investigation

prevention # detection # investigation

Kaspersky ICS Vulnerability Data Feed

Verified and refined data on vulnerabilities discovered in software and hardware of ICS systems and other systems used in industrial environments, provided in a machine-readable format

prevention # detection # investigation

ICS Vulnerability Data Feed in OVAL format

A regularly updated feed containing OVAL definitions for automated detection of known vulnerabilities in SCADA systems and other industrial software

detection

Kaspersky ICS Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting provides in-depth intelligence and greater awareness of malicious campaigns targeting industrial organizations, as well as information on vulnerabilities found in the most widely used industrial control systems and underlying technologies. Detailed information tailored for industrial organizations helps customers to safeguard critical assets, including software and hardware components and ensure the safety and continuity of technological processes.

Reports are delivered through **Kaspersky Threat Intelligence Portal** and are also available via API.

Key advantages

- Detect and prevent reported threats to safeguard critical assets and ensure the safety and continuity of technological process
- Correlate detected malicious or suspicious activity with Kaspersky research to attribute incidents to specific campaigns and identify threats

What you get:

APT reports

Reports on new APT and high-volume attack campaigns targeting industrial organizations, and updates on active threats

Vulnerabilities found

Reports on vulnerabilities identified by Kaspersky in the most popular products used in industrial control systems, the industrial internet of things, and infrastructures in various industries

The threat landscape

Reports on significant changes to the threat landscape for industrial control systems, newly discovered critical factors affecting ICS security levels and ICS exposure to threats, including regional, country and industry-specific information

Vulnerability analysis and mitigation

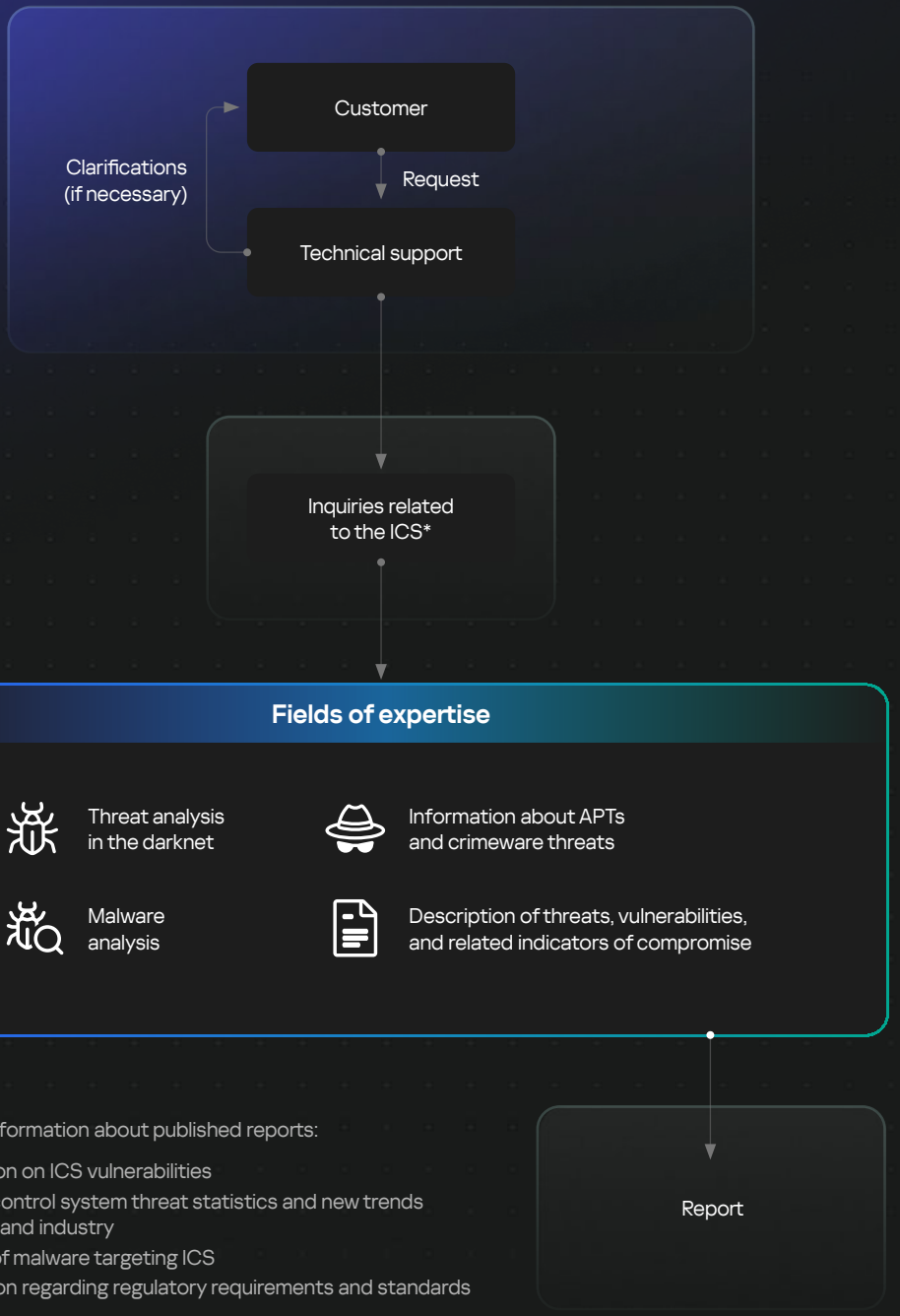
Our advisories provide actionable recommendations from Kaspersky experts to help identify and mitigate threats

Kaspersky Ask the Analyst

Kaspersky Ask the Analyst complements the Kaspersky Threat Intelligence portfolio. With this service, you can contact experts for support and useful information on specific threats and vulnerabilities that you face or are interested in. Using this data, you can improve your defenses against threats that target both your organization as a whole and your industrial infrastructure.

Key advantages

- Access to leading threat intelligence experts, including industrial security experts from Kaspersky ICS CERT
- Personalized and detailed contextual information for effective investigations
- Detailed instructions from our experts on how to respond to threats and vulnerabilities quickly and effectively



* Additional information about published reports:

- Information on ICS vulnerabilities
- Process control system threat statistics and new trends by region and industry
- Analysis of malware targeting ICS
- Information regarding regulatory requirements and standards

Knowledge

Contact us
Try now
Learn more

Kaspersky Security Awareness

Transform employees into a human firewall

Kaspersky's Security Awareness portfolio helps build a strong culture of cybersecurity across all levels of your organization:

- **Kaspersky Interactive Protection Simulation (KIPS)** – game-based simulation tailored to industrial scenarios (power generation, oil and gas, petrochemicals, etc.). It demonstrates how cybersecurity affects business performance, allowing managers to experience the impact of strategic decisions.
- **Kaspersky Automated Security Awareness Platform (ASAP)** – develops secure behavior across the workforce through interactive training and simulated phishing attacks, equipping employees with essential industrial cybersecurity knowledge and skills.
- **Kaspersky Executives Training** – a practical course that gives decision-makers and functional leaders a clear understanding of the cybersecurity landscape.

Major topics covered

- Email
- Websites and the internet
- Passwords and accounts
- Social media and messengers
- Industrial cybersecurity
- PC Security
- Mobile devices
- Confidential data
- GDPR
- Physical data security
- Bank card security and PCI DSS
- Artificial intelligence and neural networks
- Personal data

Knowledge

Contact us
Training Catalogue

Kaspersky ICS CERT Training

Applied learning

Our ICS training program is designed to help IT, OT and information security professionals, as well as managers and other employees, expand their knowledge of industrial cybersecurity and develop specialized hands-on skills.

Practical skills from Kaspersky experts

- Digital forensics and incident response
- Exploring vulnerabilities in OT/IoT devices and industrial software
- Cross-functional training programs for IT, OT and IS experts

Kaspersky ICS Security Assessment

Ensuring cyber resilience in OT environments

Risk

A single vulnerability is all it takes for cybercriminals to take control of an entire industrial system

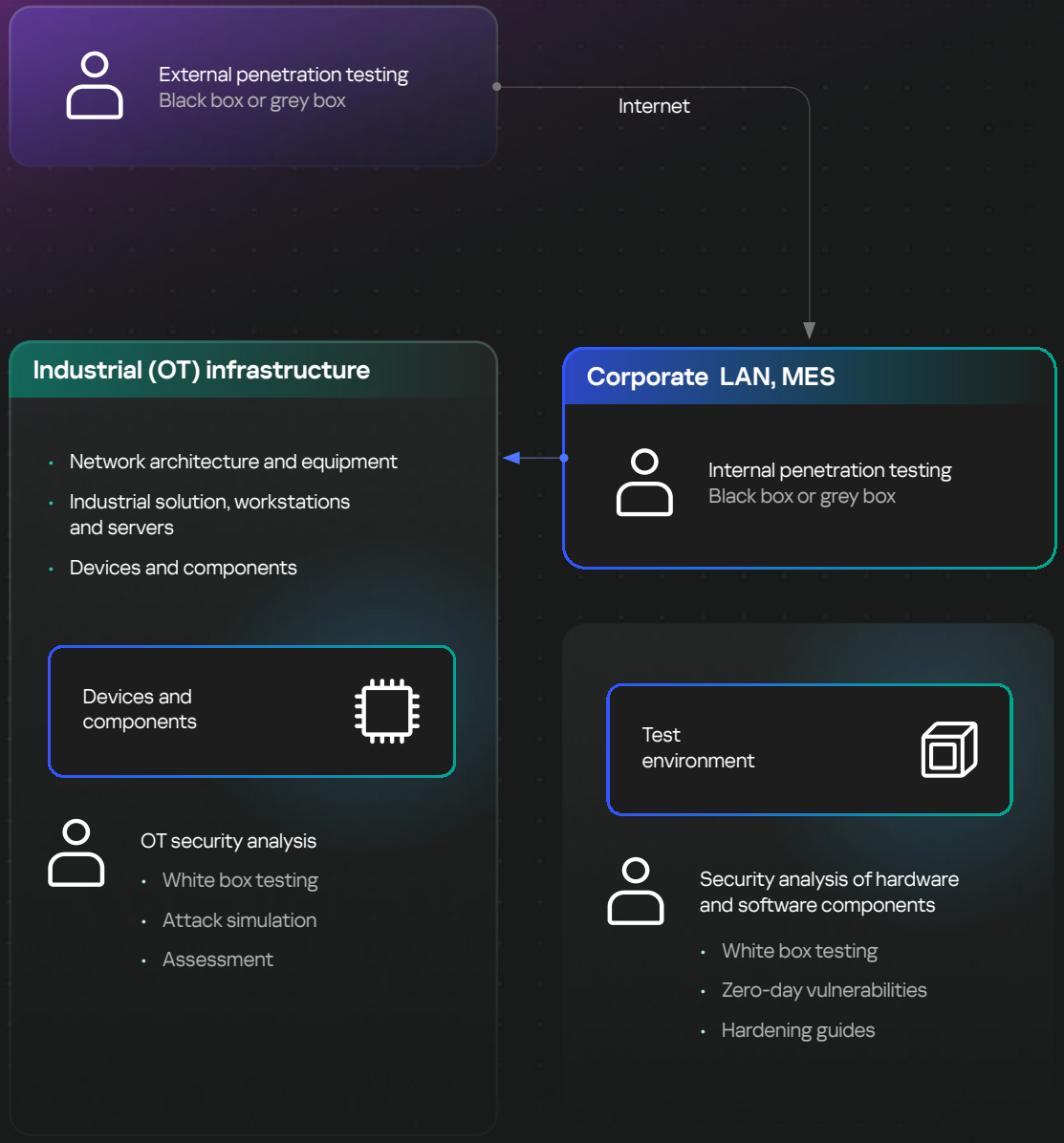
Solution

A comprehensive approach to identifying security vulnerabilities and weaknesses in industrial infrastructures

Key advantages

- Strengthen security controls to protect operators, engineers and other staff
- Identify vulnerabilities that hackers could exploit to disrupt assembly lines, manufacturing equipment or robotic systems
- Protect manufacturing designs, projects, and programs from theft
- Prevent breaches that could compromise product quality or safety

Kaspersky's approach to Industrial Security Assessment



Kaspersky Managed Detection and Response

AI-powered. Human perfected.

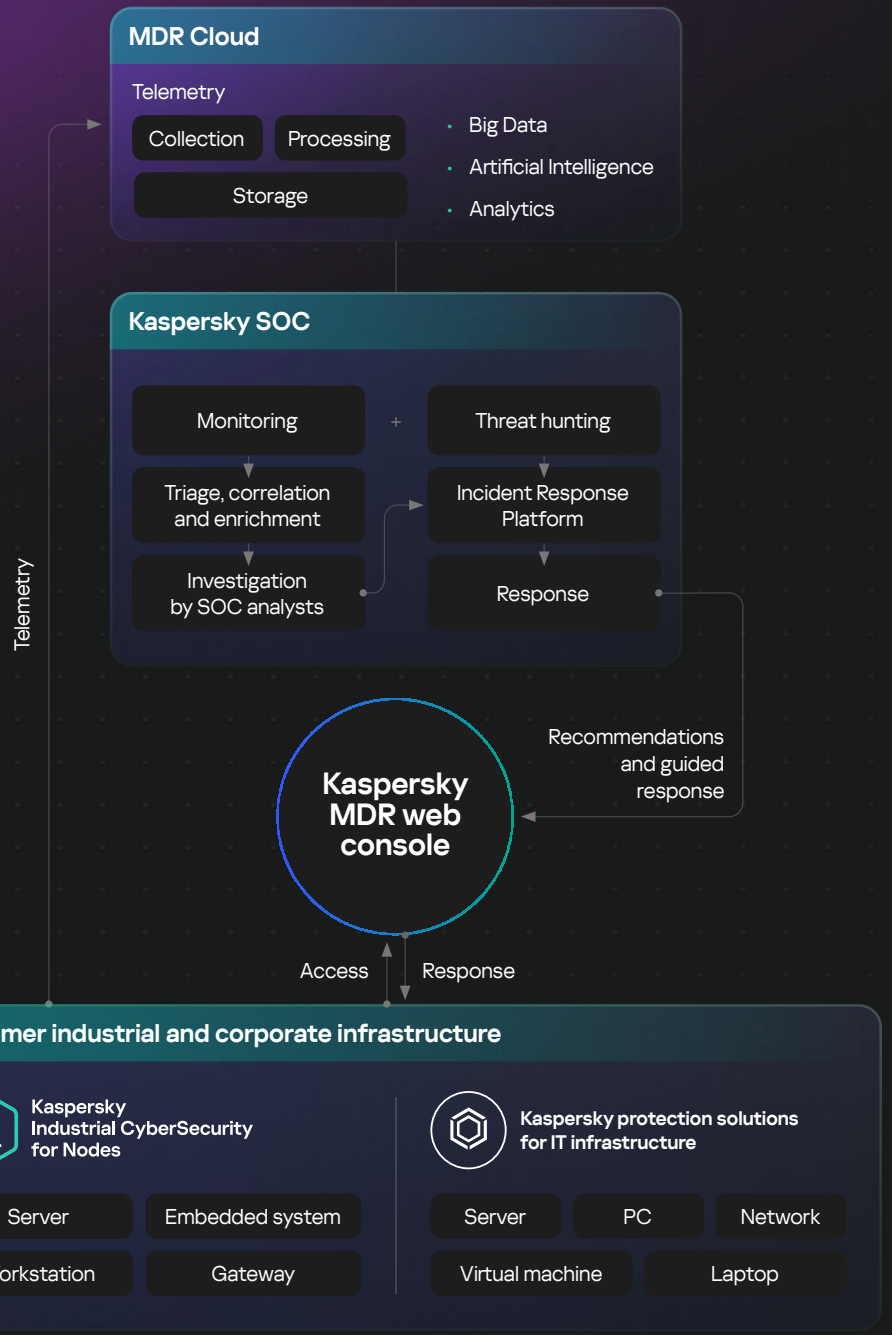
- Continuous hunting, detection, and elimination of threats targeting your industrial enterprise
- Reduced security costs by eliminating the need to hire new cybersecurity specialists
- Gain all the key benefits of a SOC without having to build one in-house

22% of our customers are from the Industrial sector

See the MDR analyst report to learn more

Key advantages

- Proactive threat detection: patented attack indicators help identify hidden threats within the control system
- Automated and guided response (with complete forensic investigation and malware analysis available on-demand)
- ICS cybersecurity expertise backed by one of the industry's most successful and experienced proactive threat detection teams



Kaspersky Incident Response

Managing the aftermath of a security breach

Risk

Incidents affecting critical infrastructure require the appropriate expertise in conducting a response at industrial facilities. Incorrect and untimely actions can significantly increase the damage from an attack.

Solution

- Rapid elimination of the consequences of an incident by Kaspersky's Global Emergency Response Team
- Support across the full incident investigation and response cycle
- Intelligence, collection, and remediation based on our own innovative tools
- On-demand expertise and knowledge sharing with your teams

Service composition

Incident response
Investigation and elimination of threats

Digital forensics
Analysis of digital evidence

Malware analysis
Get a detailed view of the files used in an attack

Explore the anatomy of a cyber world with the global report by Kaspersky Security Services

The partner you can trust

- ~30 years of world-class experience and petabytes of threat data
- ICS CERT – our own international OT/IoT security research division
- Proven expertise in the IT/OT security industry with numerous awards and achievements
- More than 200 interoperability certificates with automation vendors' solutions
- Proven technology effectiveness and compliance with industry standards and requirements

More about OT solutions

More about IT solutions

Contact us