

Kaspersky OT CyberSecurity

A comprehensive solution
for cyber-physical systems security



kaspersky bring on
the future



Kaspersky
OT CyberSecurity



Kaspersky Next
XDR Expert

IT – OT
Convergence

Unified Industrial Safety Concept



Technologies

A robust selection of tested, compliant, and approved industrial security solutions



Knowledge

Reliable threat analytics and comprehensive industrial cybersecurity training



Expertise

A full range of professional services for comprehensive industrial cybersecurity

Technologies

Specialized
Solutions



Kaspersky
Antidrone



Kaspersky
Machine Learning
for Anomaly Detection



Kaspersky
SD-WAN



Kaspersky
Industrial
CyberSecurity

Native XDR



for Nodes

Endpoint protection,
detection and
response



for Networks

Network traffic
analysis, detection
and response

Kaspersky OS
Solutions



Kaspersky
IoT Secure Gateway



Kaspersky
Thin Client



Kaspersky
Automotive
Secure Gateway

Knowledge

Cyber
Hygiene



Kaspersky
Security
Awareness

Threat
Intelligence



Kaspersky
ICS Threat
Intelligence

Training



Kaspersky
ICS CERT
Training

Discovery



Kaspersky
ICS Security
Assessment

Response



Kaspersky
Incident
Response

Managed
Protection



Kaspersky
Managed
Detection
and Response



Kaspersky OT CyberSecurity

IT—OT Convergence

 Kaspersky Next
XDR Expert



Kaspersky
IoT Secure
Gateway



Kaspersky
SD-WAN



Kaspersky
Industrial
CyberSecurity

Native XDR



for Nodes

Endpoint protection,
detection and
response



for Networks

Network Traffic
Analysis, Detection
and Response



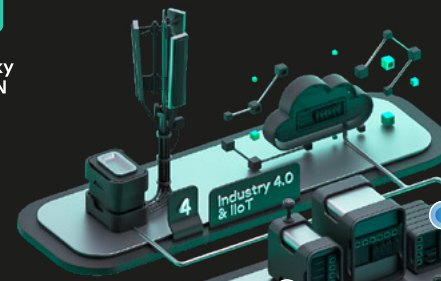
Kaspersky
Machine Learning
for Anomaly
Detection



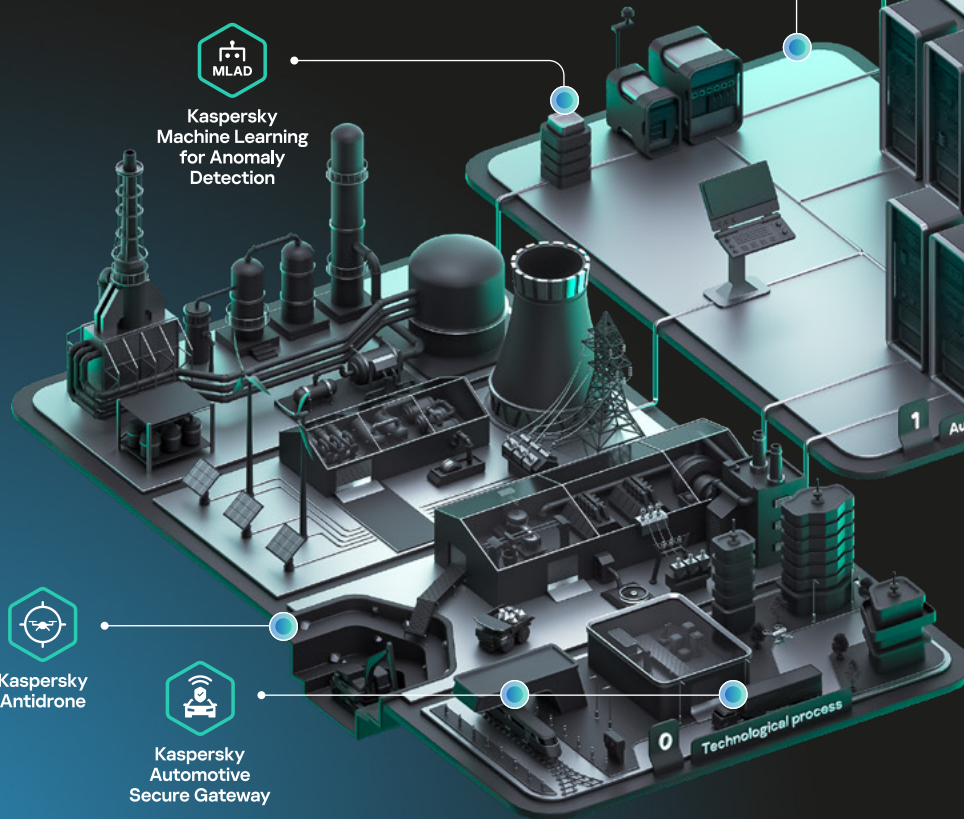
Kaspersky
Antidrone



Kaspersky
Automotive
Secure Gateway



Kaspersky
Thin Client



1 Automation & Protection

2 Monitoring & Control

3 IT systems

Expertise

Discovery



Kaspersky
ICS Security
Assessment

Response



Kaspersky
Incident
Response

Managed
Protection



Kaspersky
Managed
Detection
and Response

Knowledge

Cyber
Hygiene



Kaspersky
Security
Awareness

Threat
Intelligence



Kaspersky
ICS Threat
Intelligence

Training



Kaspersky
ICS CERT
Training

Visit website



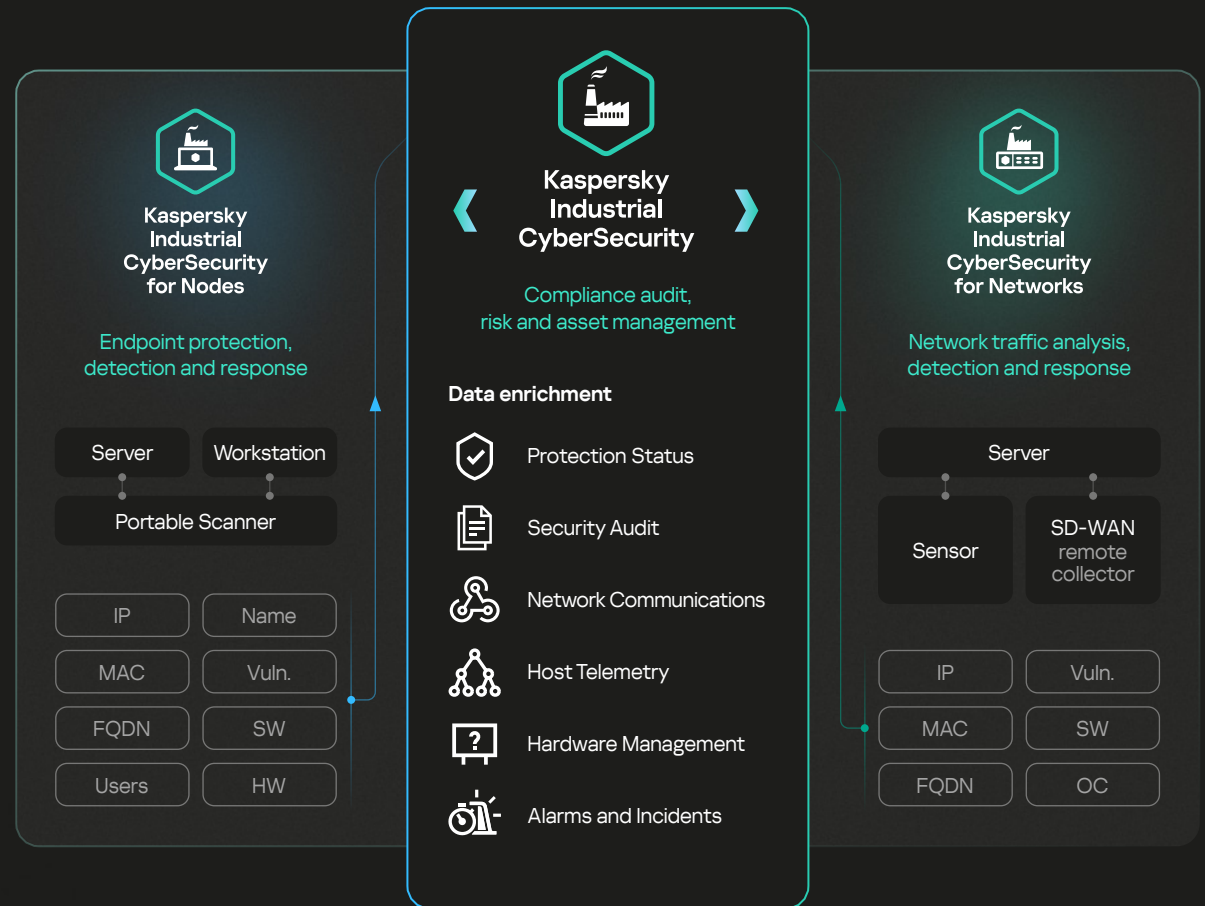
Kaspersky
Industrial
CyberSecurity

XDR

TECHNOLOGY

Native XDR platform to protect automation systems

- **Detection:** reveals hidden threats, anomalies, insecure communications, and intrusion attempts long before disruptions occur
- **Response:** safe site-wide response measures on hosts and networks
- **Asset management:** advanced automation system inventory and communications visibility
- **Security audit:** compliance management, safe vulnerability scanning and equipment configuration control



Advantages of the XDR platform



End-to-end coverage for Industrial Automation and Control Systems (IACS) tested with industrial vendors. Detection of network anomalies and threats. Endpoint protection for Linux and Windows, manual maintenance of isolated systems or bring-in computers.



Active and/or passive security audit of endpoints and networks. Centralized risk, security policy and asset management at all levels of IACS.



Outstanding systems and network visibility. Investigation and reconstruction of the entire kill chain. Visualization of incident progression across industrial networks and different nodes.

[Buy from a partner](#)

[Request a demo](#)

[Datasheet](#)

Audits: **IEC** 62443-4-1



SOC 2
Type 2



ISO/IEC
27001

Visit website



Kaspersky Next
XDR Expert

TECHNOLOGY

Unified cybersecurity 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 that include interactions with third-party solutions, with enhanced investigative and response capabilities. The platform also helps protect your business not just in industrial environments, but also where industrial and corporate environments overlap. This is achieved thanks to close cooperation with Kaspersky's best-in-class IT cybersecurity portfolio.

In this way, security teams can form a holistic picture of an incident's development and identify its root causes to prevent similar incidents in the future.

Data sources

Kaspersky solutions

Third party

xFlows

Events

Integrations



Kaspersky
Anti Targeted
Attack



Kaspersky
Threat Intelligence



Kaspersky
Industrial
CyberSecurity



Kaspersky
Automated Security
Awareness Platform

Third party

and more Kaspersky
or third-party integrations
on demand

Data

Response

Kaspersky Next XDR Expert

Kaspersky Next XDR Core

Investigation
graph

Log management
and data lake

Threat detection
and cross-correlation

Playbooks

Dashboards
and reporting

Centralized asset
management

Case
management

Deployment
toolkit

Third party
connectors

Data

Response

EDR with sandbox, email and hybrid security



Kaspersky
Hybrid Cloud
Security



Kaspersky Next
EDR Expert



Kaspersky
Security for
Mail Server

NB: Endpoints need to be activated via Kaspersky EDR Expert license

[Contact us](#)

[Datasheet](#)

Visit website



Kaspersky Machine Learning for Anomaly Detection

TECHNOLOGY

Early anomaly detection and predictive analytics

- Detects equipment faults and human error long before they become critical, helping to prevent failure and accidents
- Identifies atypical employee actions or equipment operations as signs of a specialized attack or sabotage
- Combines anomaly detection with predictive analysis of equipment condition and life cycle

Ecosystem and artificial intelligence



Standalone system or integration with KICS for Networks to receive telemetry/ events and send back alerts about detected anomalies



Applies diagnostic rules to the predefined symptoms of the problem, and machine learning to detect any deviations from normal equipment behavior



Uses AI to analyze process telemetry and events related to employee actions



[Contact us](#)

[Case studies](#)

[Implementation process](#)

mlad.kaspersky.com

[Visit website](#)



**Kaspersky
SD-WAN**

TECHNOLOGY

A unified solution that ensures the reliability of distributed industrial networks

Kaspersky SD-WAN enables industrial enterprises to build a resilient, geographically distributed network 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.

Kaspersky SD-WAN features:



Easy
scalability



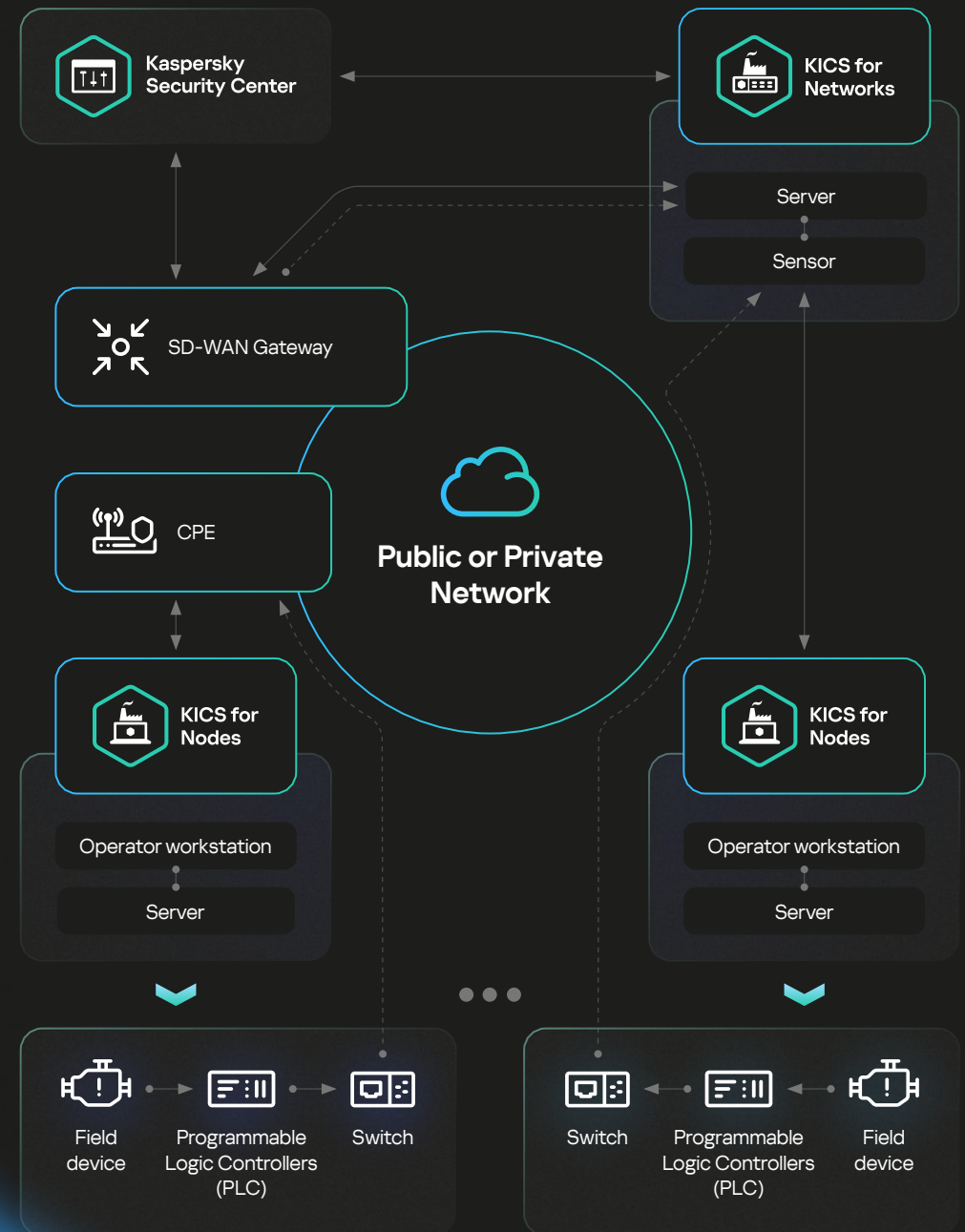
Convenient
management



Cost
optimization



Centralized
security



[Contact us](#)

---> SPAN --> Network traffic; Node telemetry; Control

Visit website



Kaspersky
Antidrone




TECHNOLOGY

Drone monitoring and defense solution

Kaspersky Antidrone reduces the likelihood of process stoppages at 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 with the appropriate permissions, the operator can neutralize the drone.

The Kaspersky Antidrone solution is modular and can be applied to industrial sites of any size. The solution also supports the "friend-or-foe" mode of operation, allowing customers to use their own drones and avoid intervention by illicit, unmanned air vehicles.

Key Features

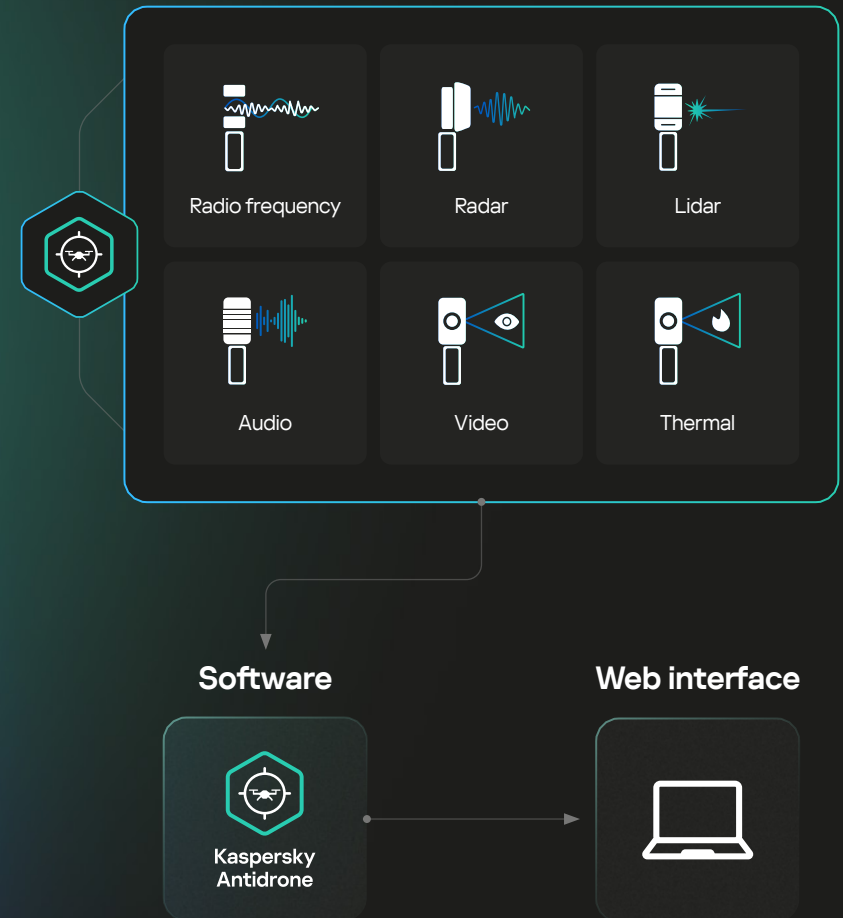
-  Drone detection and tracking
-  Drone classification using neural networks
-  Directional and omni-directional jamming

[Request a demo](#)

[Datasheet](#)



Hardware modules



antidrone.kaspersky.com/en

Visit website



Kaspersky
IoT Secure Gateway

TECHNOLOGY

Trusted data for business development in Industry 4.0

The solution consists of Kaspersky IoT Secure Gateways based on KasperskyOS, and the Kaspersky Security Center (KSC) management console. The gateways securely collect and transfer data from equipment to digital and cloud platforms, delivering high-quality business intelligence to optimize production and prevent incidents. The console enables mapping of events from different sources and managing of up to 100,000 physical, virtual and cloud workstations.

Key Features



Secure data transport

Reliable data transmission, traffic control and filtering



Integration with business systems

Support for cloud platforms and data transfer to corporate business systems



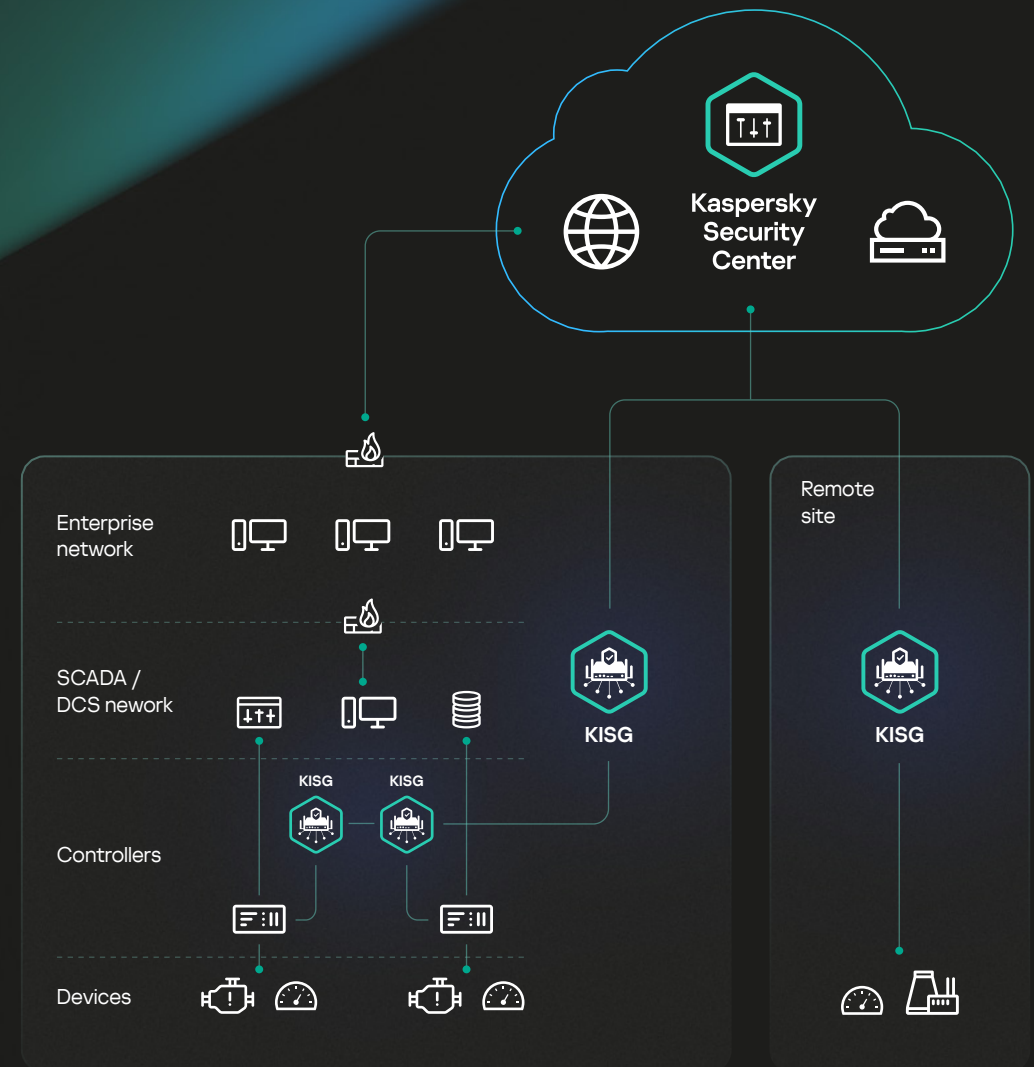
Third-party app support

Create your own applications for KasperskyOS and their secure delivery to devices



Cyber immune defense

Network infrastructure protection and innate resistance to most types of cyber attacks



[Contact us](#)

[Datasheet](#)

Visit website



Kaspersky
Thin Client

TECHNOLOGY

Product Application

Risk

Users' 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

Key Features



Secure
by Design



A single management
platform for IS and IT



User-friendly
interface

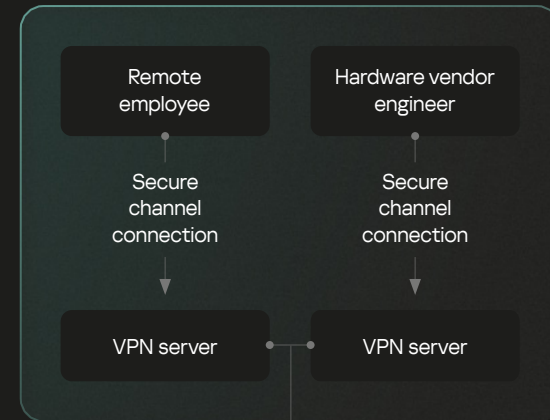


Integration in infrastructure
in just 2 minutes

[Feature List](#)

[Request a demo](#)

[Datasheet](#)



Visit website

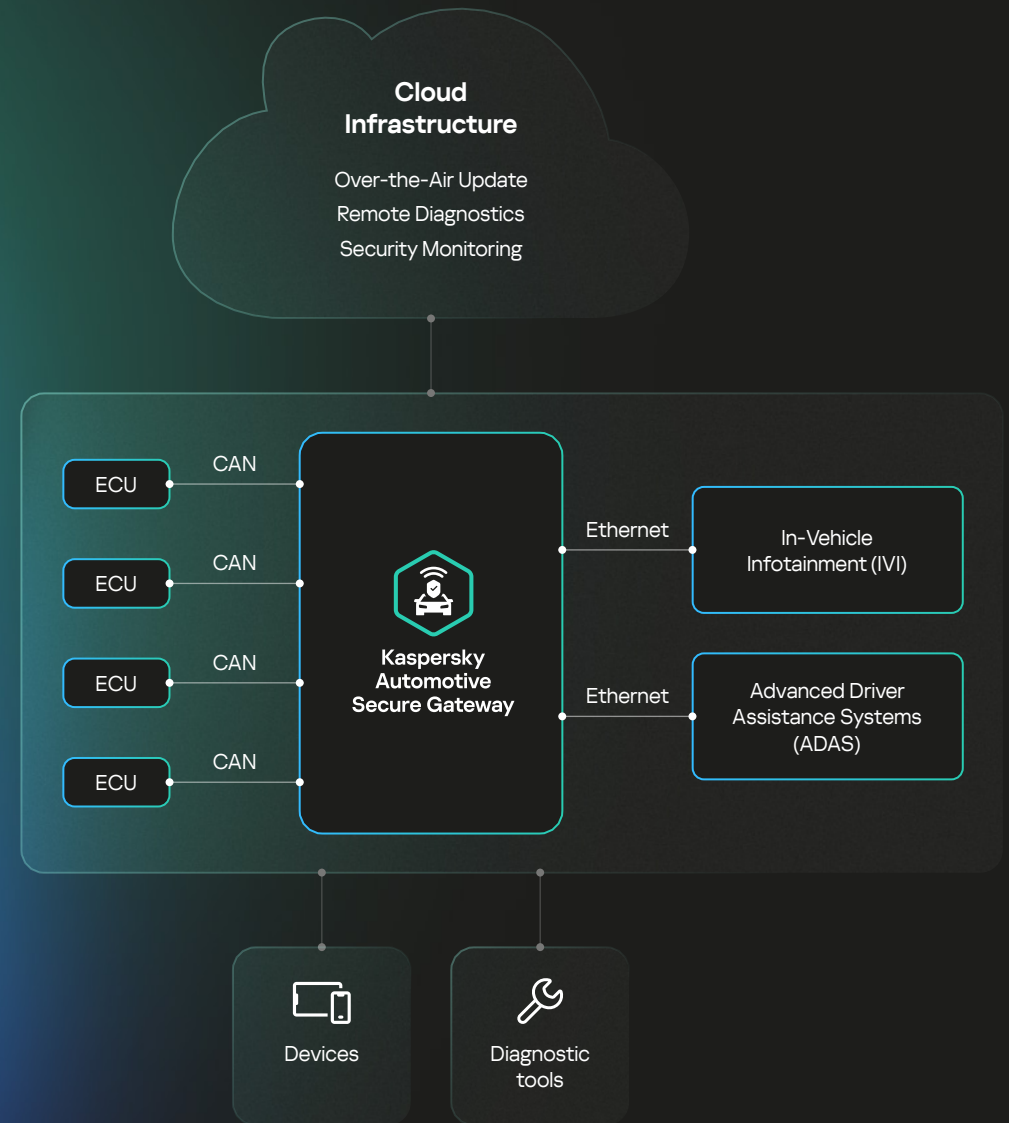


**Kaspersky
Automotive
Secure Gateway**

TECHNOLOGY

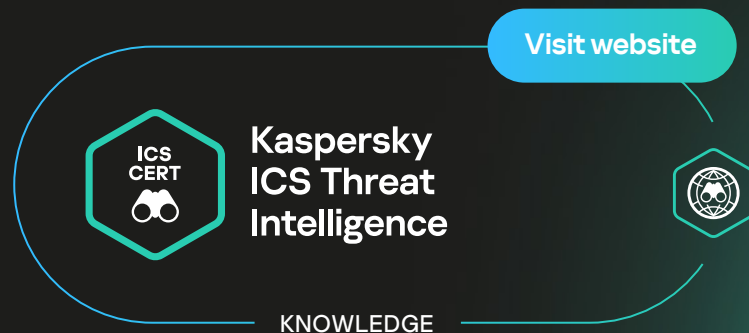
Building reliable IT systems for connected vehicles

- Software for high-performance controllers of connected cars that combines the functions of a telematics control unit (TCU) and a secure gateway
- 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 and 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
- Compatible with AUTOSAR Adaptive platform



[Contact us](#)

[Datasheet](#)



Deep understanding of industrial cybersecurity threats and vulnerabilities for efficient risk assessment, successful 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 Features

- Fast threat detection and extensive analytical capabilities
- Increases the effectiveness of investigations and active threat searches
- Comprehensive threat and vulnerability information for informed decision-making

[Request a demo](#)

[Solution overview](#)

[Contact us](#)

Kaspersky Threat Intelligence products and services

Machine-readable Threat Intelligence

Kaspersky Threat Data Feeds



ICS

Kaspersky CyberTrace



Threat Intelligence Expert Support

Kaspersky Takedown Service



Kaspersky Ask The Analyst



ICS

- Tactical
- Operational
- Strategic
- Available via Kaspersky Threat Intelligence Portal

Human-readable Threat Intelligence

Kaspersky Threat Lookup



Kaspersky Digital Footprint Intelligence



Kaspersky Threat Analysis



Sandbox | Attribution | Similarity

Kaspersky Threat Intelligence Reporting



APT | Crimeware | ICS

Kaspersky Threat Infrastructure Tracking



Expertise centers



Kaspersky Global Research and Analysis Team



Kaspersky Threat Research



Kaspersky AI Technology Research



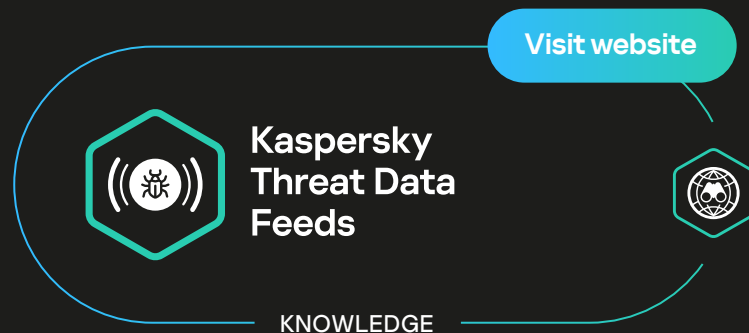
Kaspersky ICS CERT



Kaspersky Security Services



- Threat Research
- Incident Investigation



Kaspersky Threat Data Feed service delivers real-time threat intelligence information to help industrial organizations protect their networks and systems from cyber threats. The data feeds include information on known malware, phishing websites, latest known vulnerabilities and exploits, and other types of cyber threats. Set in context, the data can more readily reveal the 'bigger picture' and be used to answer the 'who, what, where, when' questions to identify your adversaries, make quick decisions and take action.

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

[Contact us](#)

[More about the service](#)

Visit website



Kaspersky ICS Intelligence Reporting



KNOWLEDGE

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 popular 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 via **Kaspersky Threat Intelligence Portal** or can be accessible by API.

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.

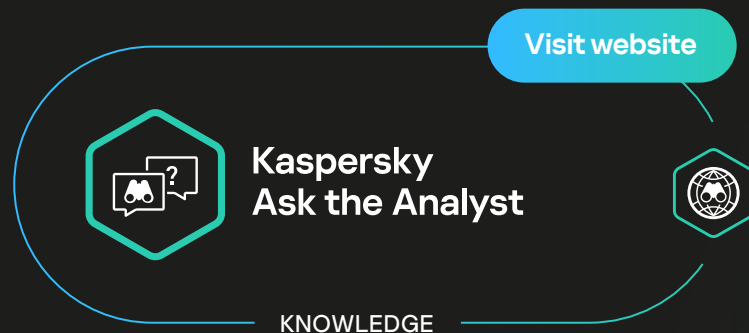


Vulnerability analysis and mitigation

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

[Contact us](#)




[More about the service](#)



What you get:

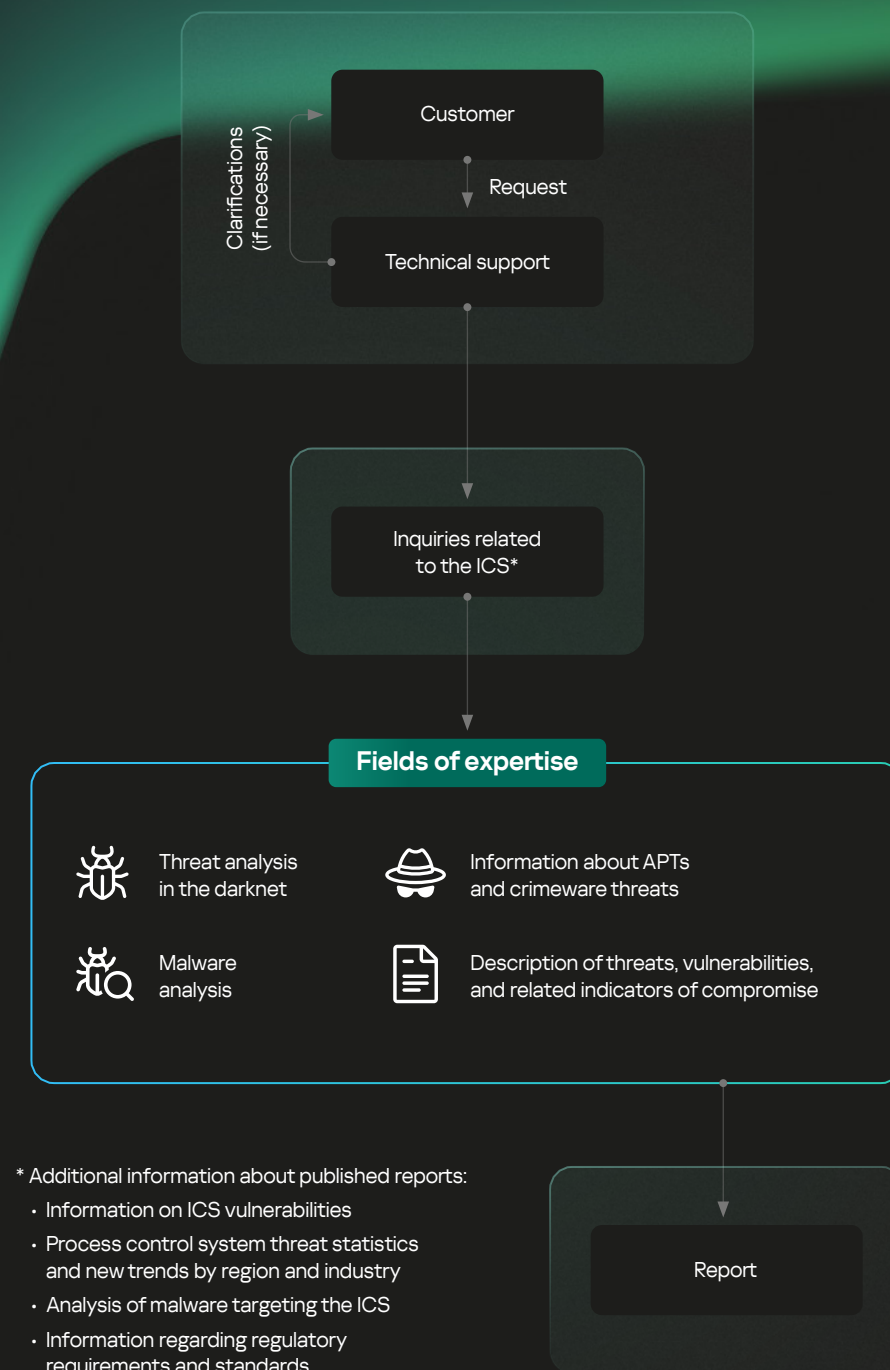
Kaspersky Ask the Analyst complements our Kaspersky Threat Intelligence portfolio. With this service, you can contact experts for support and useful information on specific threats and vulnerabilities that you face or are interested in. Using this data, you can improve your defenses against threats that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

Key Benefits

-  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 quickly to threats and vulnerabilities

[Contact us](#)

[More about the service](#)



[Visit website](#)

**Kaspersky
Security
Awareness**

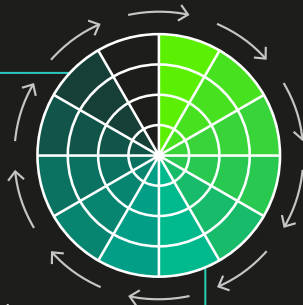
KNOWLEDGE

Transform employees into cyber defenders

- Training materials that arm your employees with the necessary knowledge about the most important aspects of industrial cybersecurity, increasing the level of awareness at all levels of the organization
- Kaspersky Interactive Protection Simulation – game-based training through business simulations featuring a multitude of scenarios across different industries: Power Station, Water plant, Oil & Gas, Petrochemical, Petroleum holdings, etc.
- The Kaspersky Automated Security Awareness Platform (ASAP) – interactive learning modules and simulated phishing attacks designed to foster cybersafe behavior

Major topics covered

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



[Contact us](#) [Try Now](#) [Training Catalogue](#)

[Visit website](#)

**Kaspersky
ICS CERT
Training**

KNOWLEDGE

Applied learning

Our ICS training program has been specially designed to ensure that information technology (IT), operations technology (OT), and information security (IS) professionals, as well as managers and other employees, can expand their knowledge of industrial cybersecurity and gain specialized hands-on skills.

Practical skills from Kaspersky experts



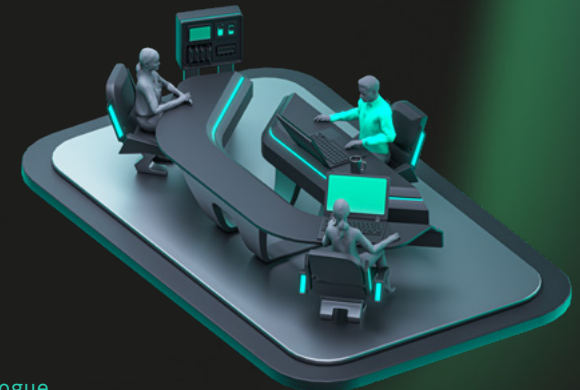
Digital forensics and incident response



Exploring vulnerabilities in OT/IoT devices and industrial software



Cross-functional training programs for IT, OT, and IS experts



[Contact us](#) [Training Catalogue](#)

[Visit website](#)



Kaspersky ICS Security Assessment

EXPERTISE

Risk

One vulnerability is enough for cybercriminals to gain control of entire industrial systems

Solution

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

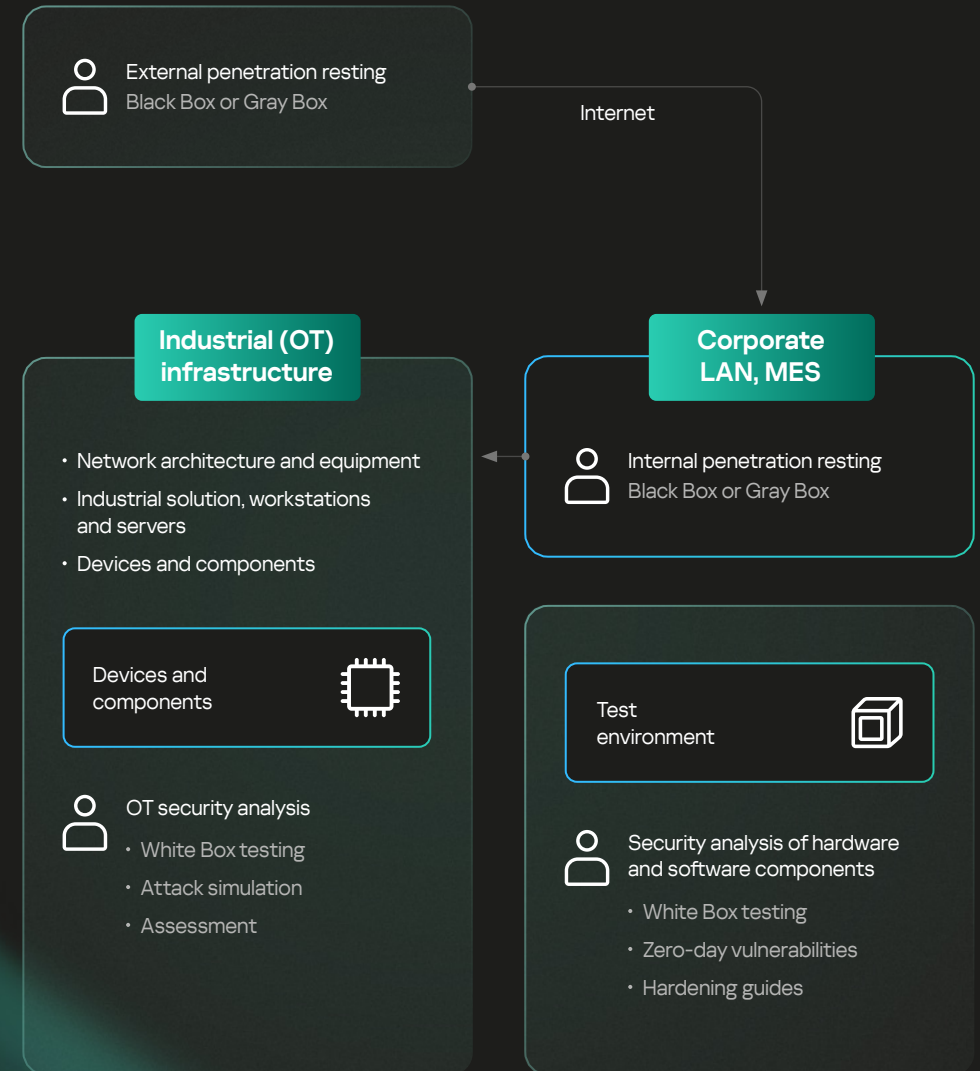
With Kaspersky ICS Security Assessment you can:

- Strengthen security controls to protect operators, engineers, and staff members
- Identify vulnerabilities that hackers could exploit to disrupt assembly lines, manufacturing machines, or robotic arms
- Protect your manufacturing schemes, projects, and programs from theft
- Avoid breaches in the production process that could lead to shortcomings in product quality or safety

[More about the service](#)

[Contact us](#)

Kaspersky's approach to Industrial Security Assessment








Kaspersky Managed Detection and Response

Visit website

EXPERTISE

Key Features

-  Proactive threat detection: patented attack indicators help track undetected 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

What you get:

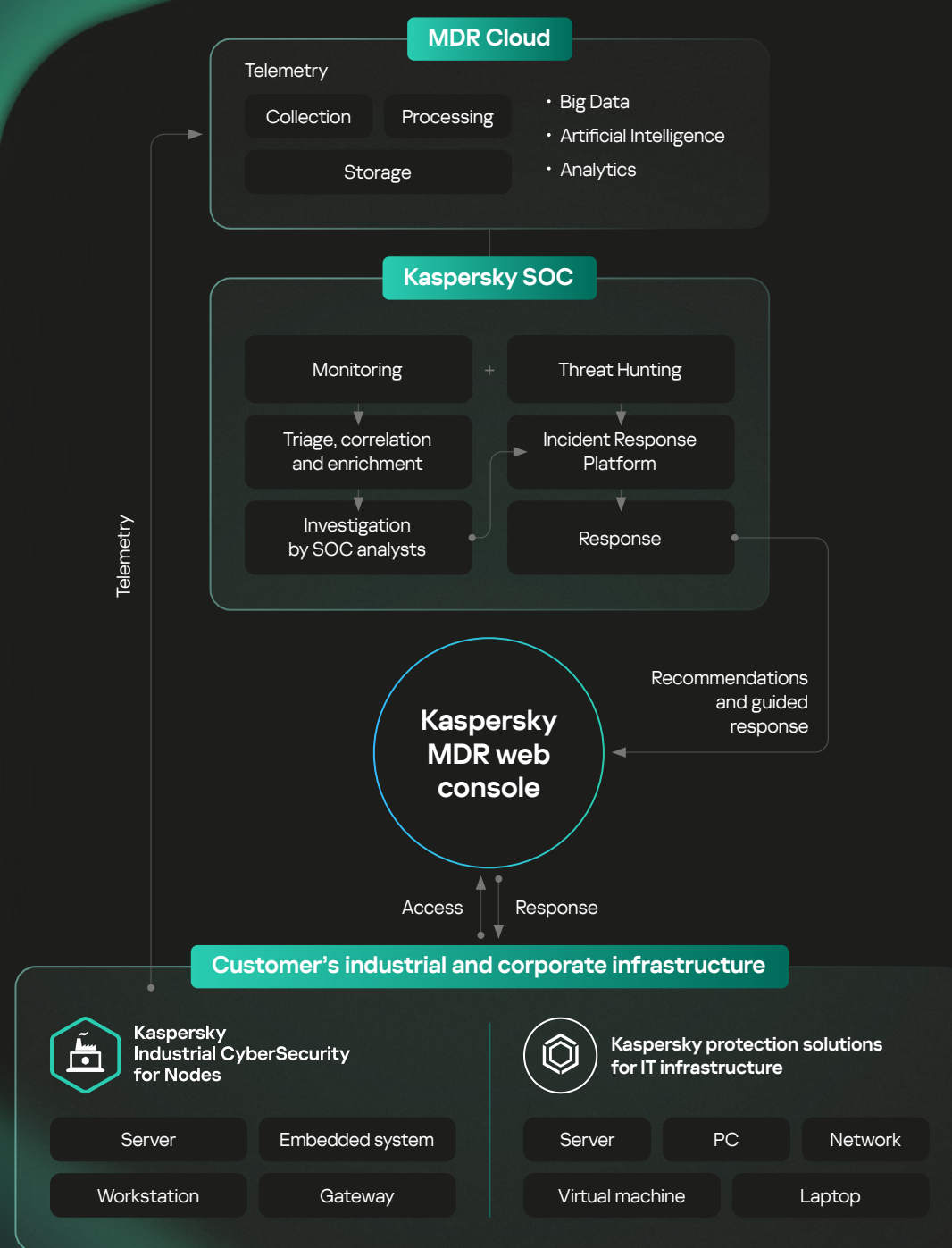
- Continuous hunting, detection, and elimination of threats targeting your industrial enterprise
- Reduced security costs by eliminating the need to hire new cybersecurity experts
- All the key benefits of a SOC, without having to establish one in-house

22% of our protected customers are from the Industrial sector

See the [MDR analyst report](#) to find out more

[Contact us](#)

[More about the service](#)



[Visit website](#)



**Kaspersky
Incident Response**

EXPERTISE

Responding to incidents

Risk

Critical infrastructure incidents 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
- Analysis of the causes, sources, and consequences of the incident
- Detailed view of the malware used

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

[Learn more](#)

[Contact us](#)



Discover Incident Response trends in Kaspersky Global Emergency Response Team [research](#).

The partner you can trust



27 years of world-class
experience and petabytes
of threat data



ICS CERT — own international
OT / IoT security research
division



Proven expertise in the IT/OT
security industry with numerous
awards and achievements



More than 100 certificates
of interoperability with
automation vendors' solutions



Proven technology effectiveness,
compliance with standards
and requirements

[More about
OT ecosystem](#)

[More about
IT ecosystem](#)

[Contact us](#)

