

Kaspersky OT CyberSecurity

A cyber-physical security ecosystem
for industrial enterprises





**Kaspersky
OT CyberSecurity**

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

IT-OT Convergence

**Kaspersky
Extended Detection
and Response**

Technologies

Specialized Solutions



**Kaspersky
Antidrone**



**Kaspersky
Machine Learning for
Anomaly Detection**



**Kaspersky
SD-WAN**



**Kaspersky
Industrial
CyberSecurity**

KICS XDR



for Nodes
Endpoint protection,
detection and
response



for Networks
Network traffic
analysis, detection
and response

Kaspersky OS Solutions



**Kaspersky
IoT Secure
Gateway**



**Kaspersky
Secure Remote
Workspace**



**Kaspersky
Automotive
Secure Gateway**

Knowledge

Cyber Hygiene



**Kaspersky
Security
Awareness**

Threat Intelligence



**Kaspersky
ICS Threat
Intelligence**

Training



**Kaspersky
ICS CERT
Expert
Trainings**

Expertise

Discovery



**Kaspersky
ICS Security
Assessment**

Managed Service



**Kaspersky
Incident
Response**

Response



**Kaspersky
Managed
Detection
and Response**



Kaspersky OT CyberSecurity

IT-OT Convergence

Kaspersky Extended Detection and Response



Kaspersky Industrial CyberSecurity



for Nodes
Endpoint protection, detection and response



for Networks
Network traffic analysis, detection and response

KICS XDR



Kaspersky SD-WAN



Kaspersky IoT Secure Gateway



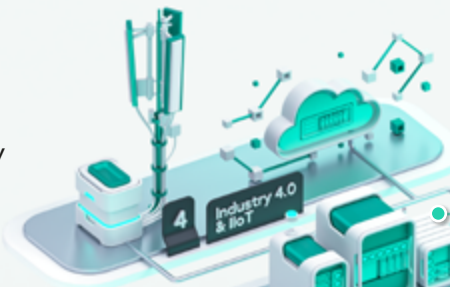
Kaspersky Machine Learning for Anomaly Detection



Kaspersky Antidrone



Kaspersky Automotive Secure Gateway



4 Industry 4.0 & IIoT



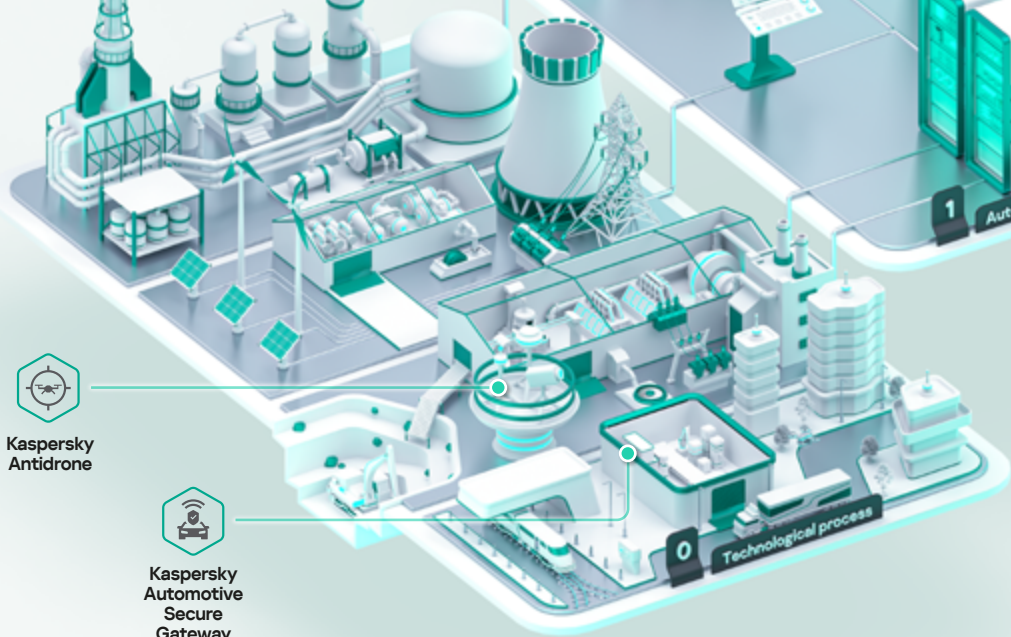
3 IT systems



2 Monitoring & Control



1 Automation & Protection



0 Technological process



Kaspersky Secure Remote Workspace

Expertise

Discovery



Kaspersky ICS Security Assessment

Managed Service



Kaspersky Incident Response

Response



Kaspersky Managed Detection and Response

Knowledge

Cyber Hygiene



Kaspersky Security Awareness

Threat Intelligence



Kaspersky ICS Threat Intelligence

Training



Kaspersky ICS CERT Expert Trainings

Visit website



Kaspersky
Industrial
CyberSecurity

XDR

TECHNOLOGY

Native XDR platform to protect automation systems

- Reveals hidden threats, anomalies, vulnerabilities, and intrusion attempts long before they become dangerous to your operations
- Certified by automation vendors and regulators
- No adverse effect on technological processes. Prevents unacceptable damage
- Facilitates the management of complex, distributed automation infrastructure and incident response
- Helps mitigate risks and maintain a record of violations

Advantages of the XDR platform



End-to-end coverage for Industrial Automation and Control Systems (IACS). Protection for Linux, Windows, isolated or third-party computers, as well as detection of network anomalies and threats.



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



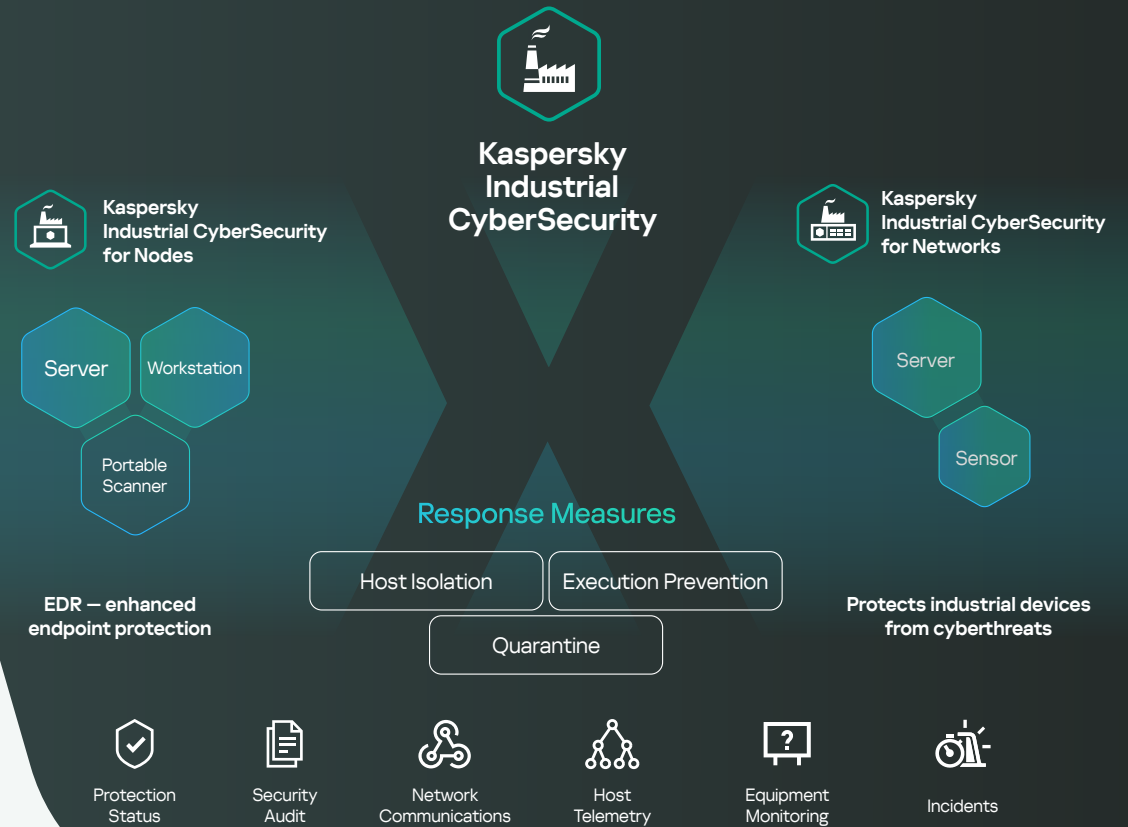
Outstanding systems and network visibility. Investigation and reconstruction of the entire killchain. Visualization of incident progression across industrial networks and different nodes.

[Buy from a partner](#)

[Request a demo](#)

[Datasheet](#)

ics.kaspersky.com



Visit website



Kaspersky Extended Detection and Response

TECHNOLOGY

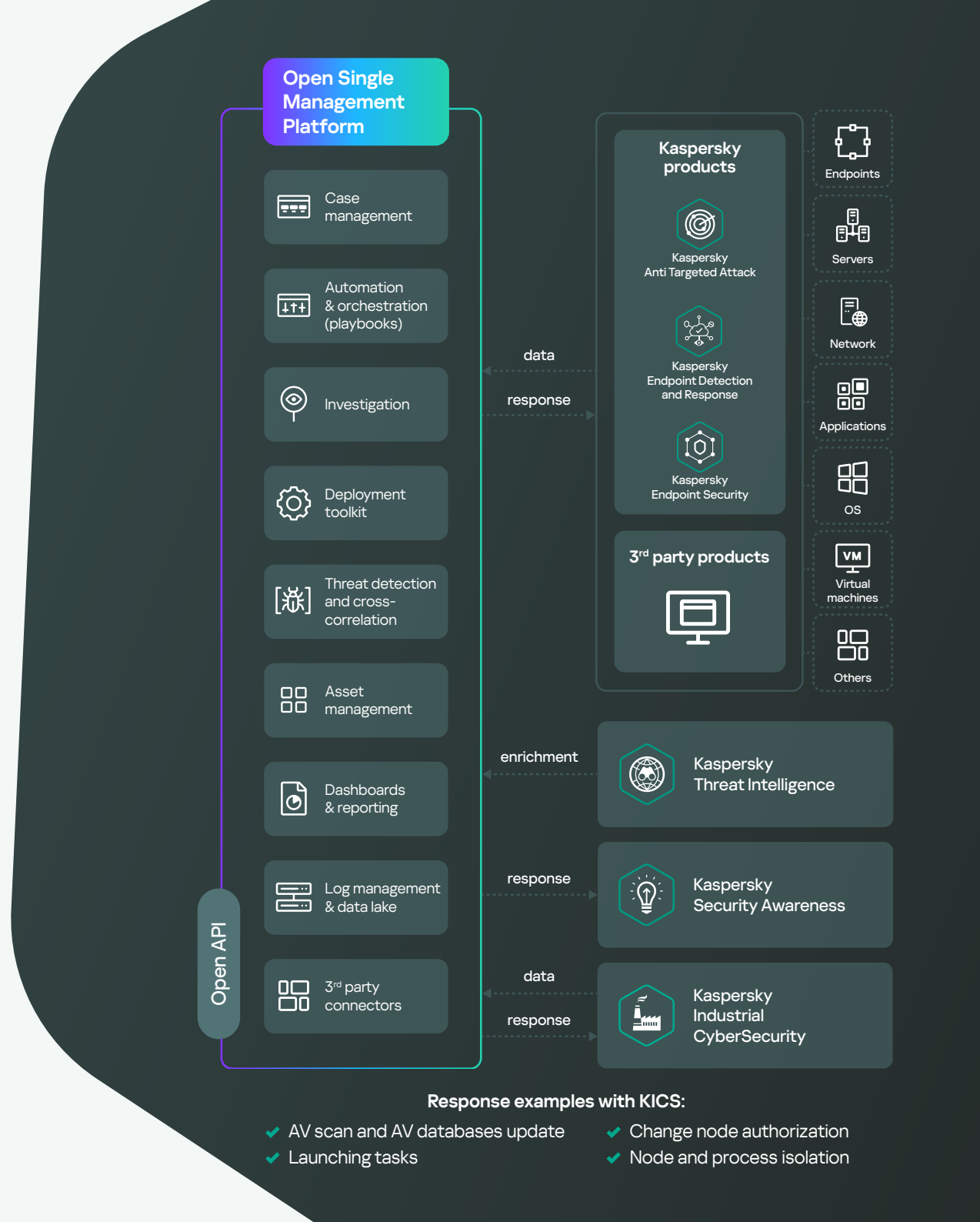
Unified cybersecurity across the industrial and corporate segments of your enterprise

Through close integration with Kaspersky Extended Detection & Response, 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 concert 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.

[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



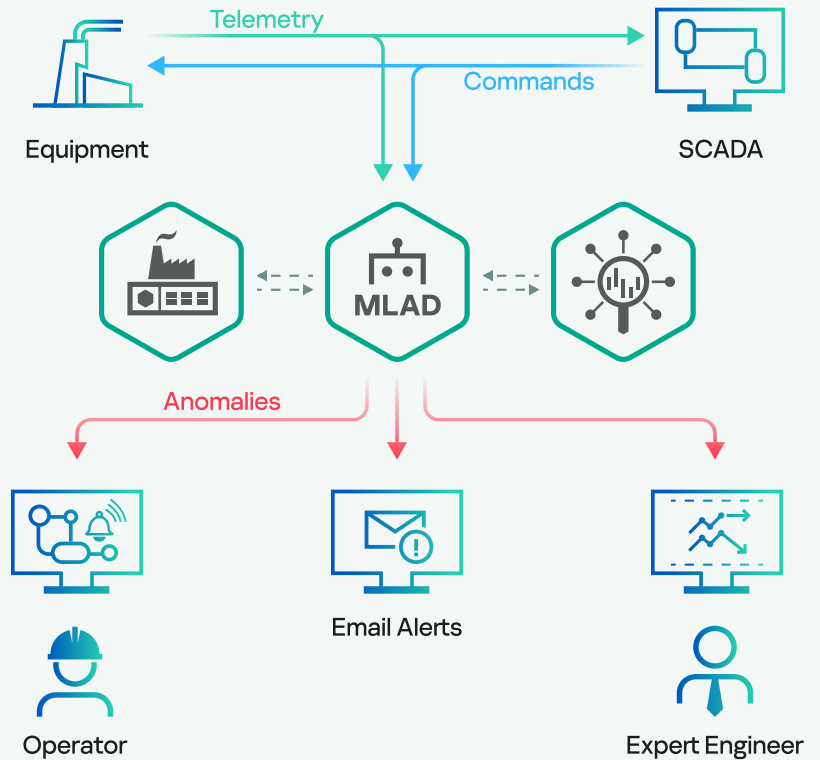
Integration with KICS for Networks and KUMA: receives telemetry and events from these systems and sends back alerts about detected anomalies



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



Visit website



Kaspersky
SD-WAN

TECHNOLOGY

Kaspersky SD-WAN features:



Easy
scalability



Convenient
management



Cost
optimization



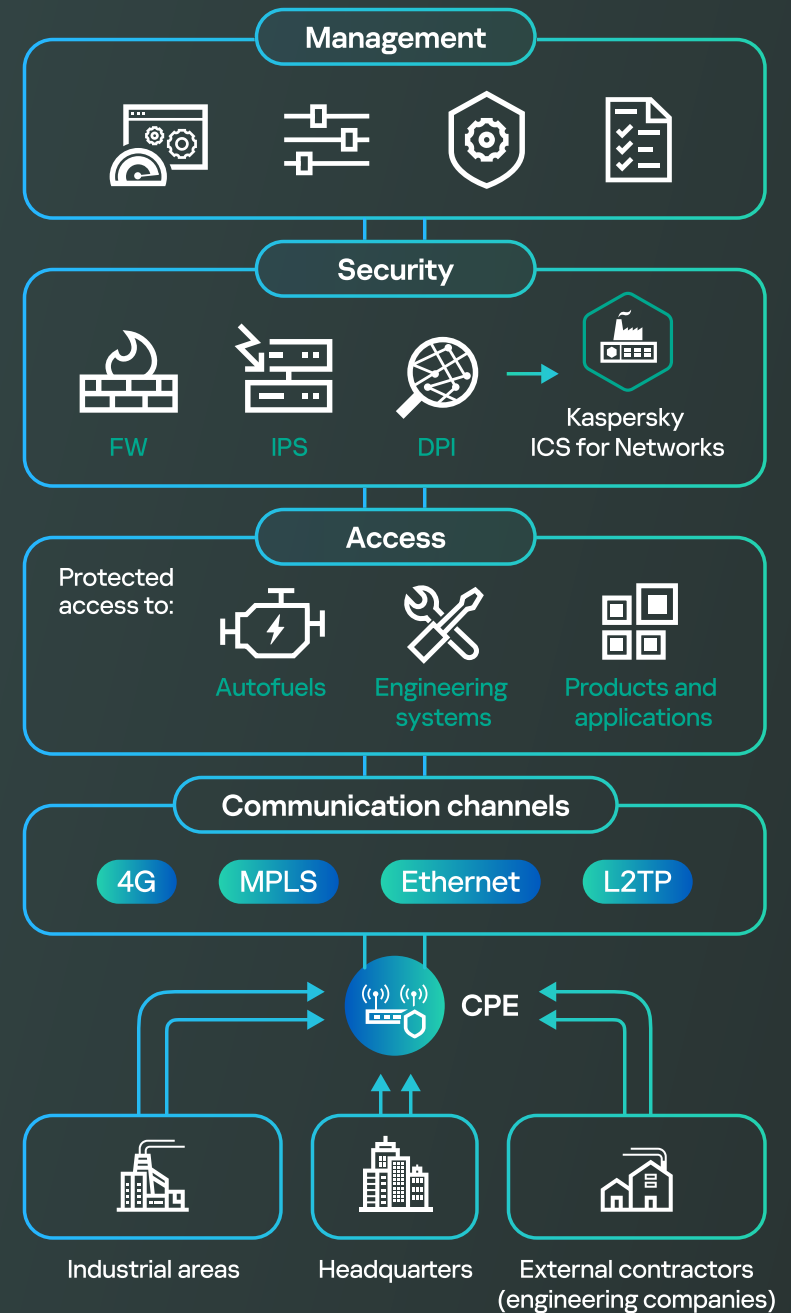
Centralized
security

A single solution for reliable industrial networks

Kaspersky SD-WAN allows enterprises to build a fault-tolerant, geographically distributed network with centralized management, while ensuring the continuity of production processes. The Kaspersky SD-WAN architecture allows you to easily integrate Kaspersky and third-party security tools through Virtual Network Functions (VNFs) manager.

Using the SD-WAN infrastructure with Kaspersky ICS for Networks, you can organize a centralized monitoring and protection system for numerous distributed industrial sites.

[Contact us](#)



Visit website



Kaspersky
Antidrone

TECHNOLOGY

Key Features

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

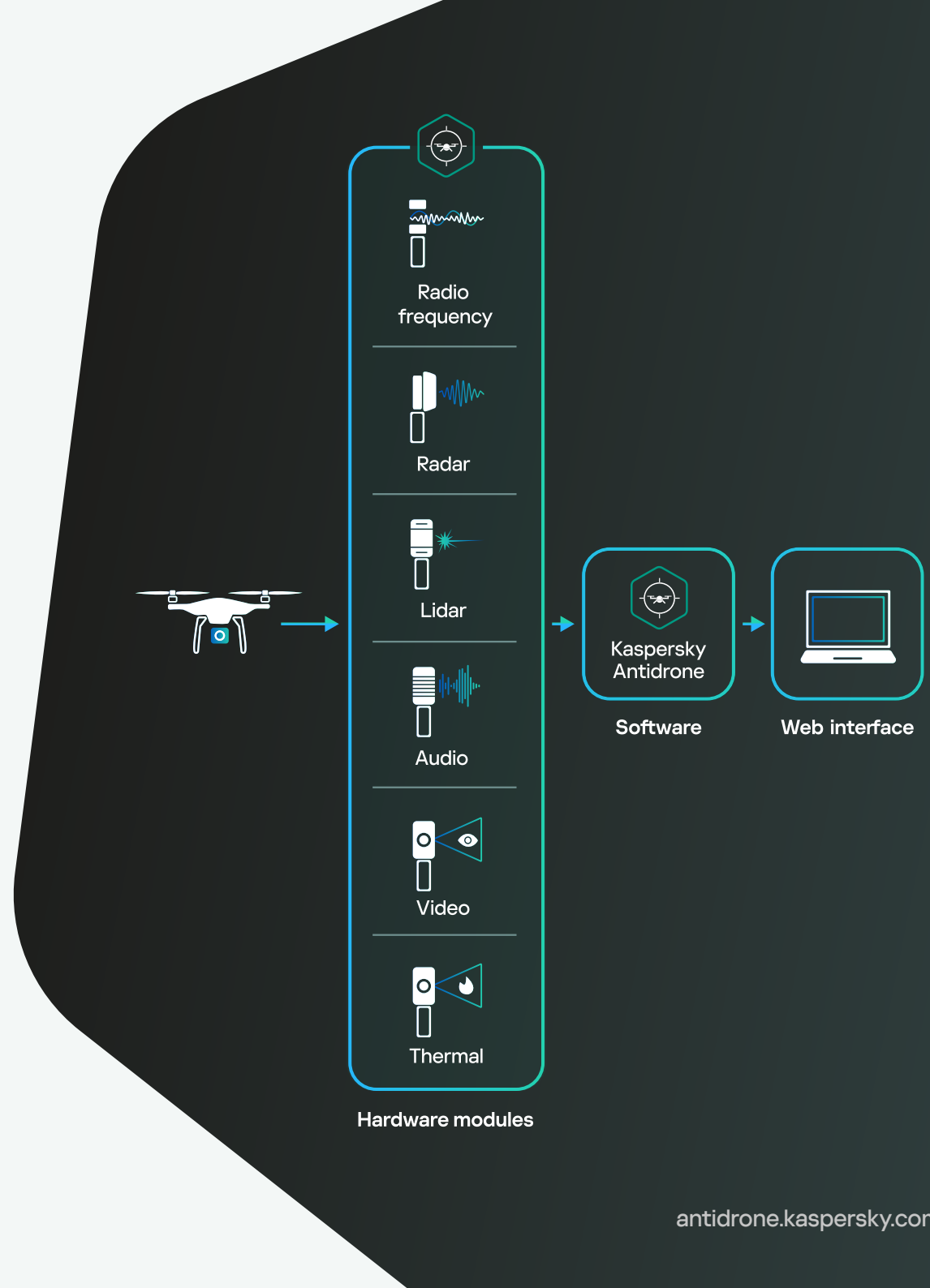
Drone monitoring and defense solution

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.

[Request a demo](#)

[Datasheet](#)

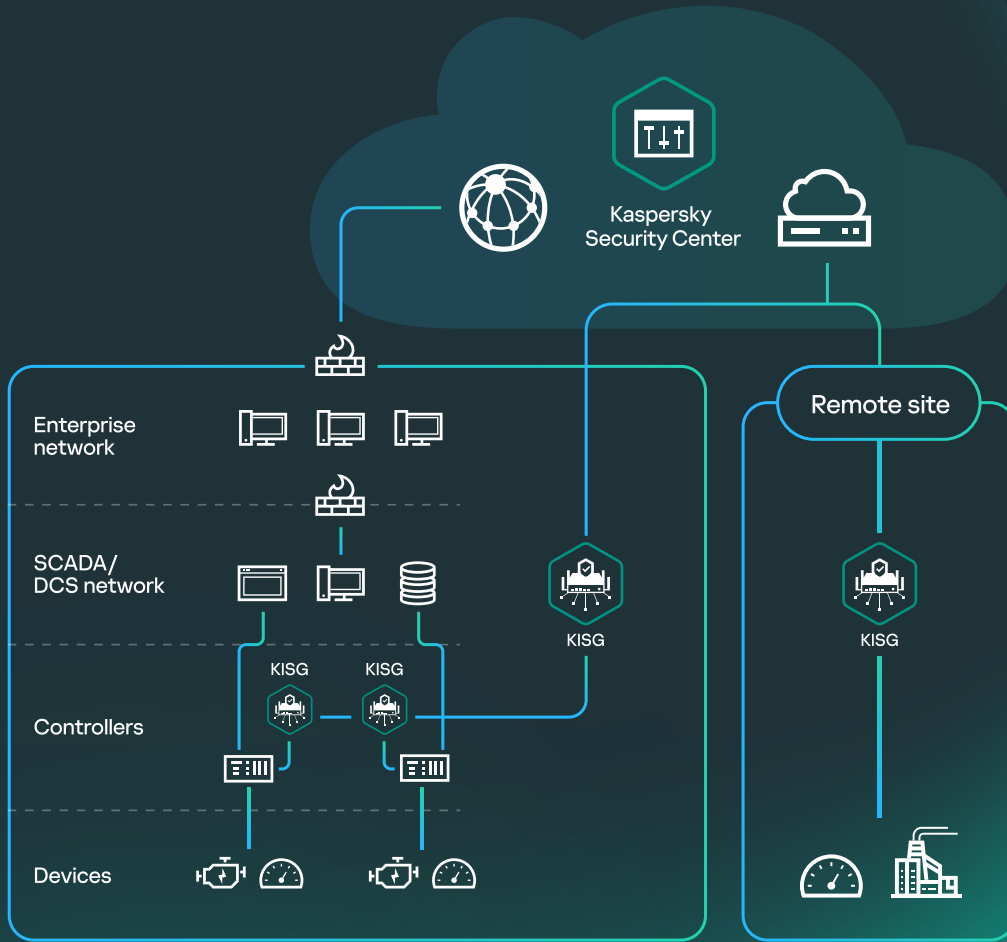


[Visit website](#)



Kaspersky IoT Secure Gateway

TECHNOLOGY



Key Features

- Secure data collection and transport from IoT devices to digital and cloud platforms
- Kaspersky Cyber Immunity based on KasperskyOS provides the «innate» resistance to the vast majority of types of cyberattacks without additional security tools
- Infrastructure transparency, centralized event management, and production optimization

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.



The technical and commercial development of this solution is handled by Adaptive Production Technologies LLC (Aprotech, a subsidiary of Kaspersky)

[Contact us](#) [Request a demo](#) [Datasheet](#)

[Visit website](#)



**Kaspersky
Secure Remote
Workspace**

TECHNOLOGY

Product Application

Risk

Users' workstations are among the most common targets for cyberattacks

Solution

Kaspersky Secure Remote Workspace (KSRW) is a solution for building a managed and functional infrastructure of thin clients based on Kaspersky's own microkernel KasperskyOS operating system

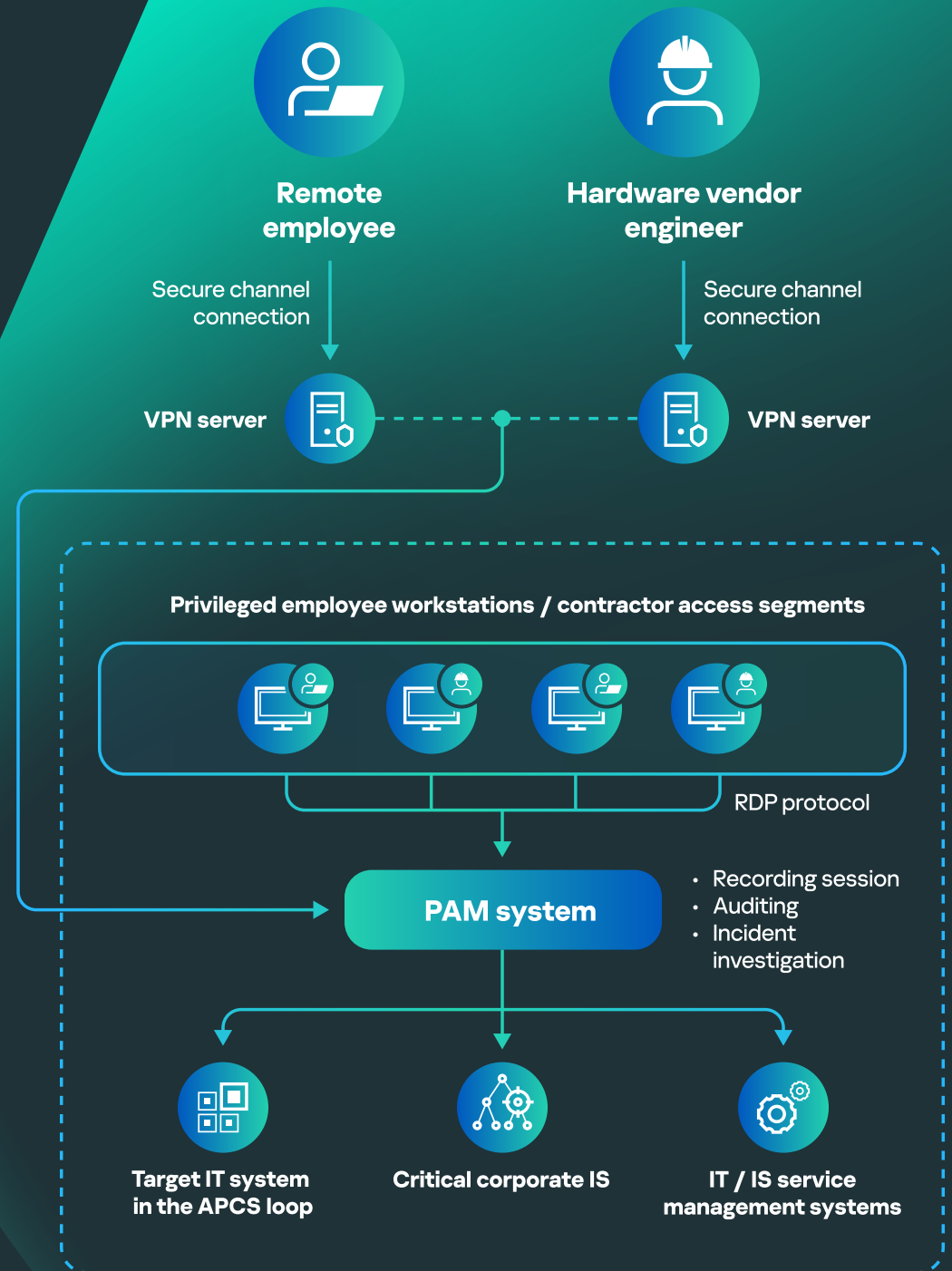
Cyber Immune Thin Client infrastructure

Cyber Immune Thin Clients as part of Kaspersky Secure Remote Workspace provide a secure connection to virtual desktops, including a trusted zone for connecting users to the industrial infrastructure.

[Solution Overview](#)

[Request a demo](#)

[Datasheet](#)

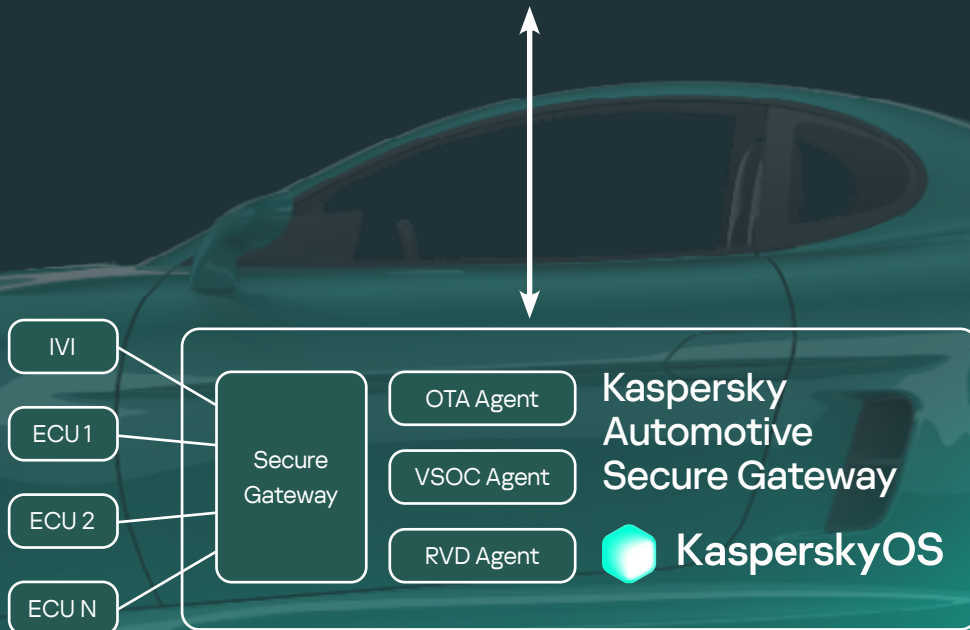
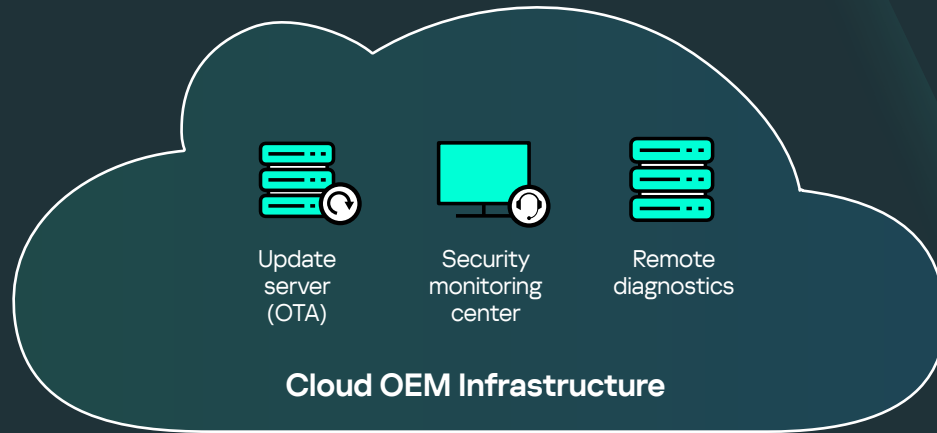


[Visit website](#)



Kaspersky
Automotive
Secure Gateway

TECHNOLOGY



Vehicle protection

- Unauthorized access
- ECU targeted attacks
- Attacks via vehicle infotainment systems (IVI)
- Malicious diagnostics
- Compromise of update system
- Uncontrolled connections and data flows, communication disruption

Key Benefits

- Secure-by-design solution
- Helps comply with cybersecurity regulations
- 4-in-1: Connected gateway, security gateway, OTA-master and VSOC agent
- Compliance with ISO21434, ISO26262, AUTOSAR Adaptive, Uptane

AUTOSAR

[Contact us](#) [Datasheet](#)

[Visit website](#)



**Kaspersky
ICS Threat
Intelligence**



KNOWLEDGE

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

Stay ahead of your adversaries with in-depth visibility into cyberthreats targeting your organization



**Kaspersky
ICS Threat
Data Feeds**

A set of regularly updated threat intelligence data feeds tailored to the specific needs of industrial cybersecurity

Threat Intelligence
Automatic data streams



**Kaspersky ICS
Threat Intelligence
Reporting**

Provides greater awareness of malicious campaigns targeting industrial organizations as well as information on vulnerabilities found in the most popular industrial control systems



**Kaspersky
Ask the
Analyst**

A service for customers to request expert guidance and insights into specific threats they're facing or are interested in.

[Request a demo](#)

[Solution overview](#)

[Contact us](#)

[Visit website](#)



Kaspersky ICS Threat Data Feeds



KNOWLEDGE

Kaspersky Threat Data Feed service delivers real-time threat intelligence information to help industrial organizations to protect their networks and systems from cyberthreats. The data feeds include information on known malware, phishing websites, latest vulnerabilities and exploits, and other types of cyberthreats. 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 Threat 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 process.

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.



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.



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.

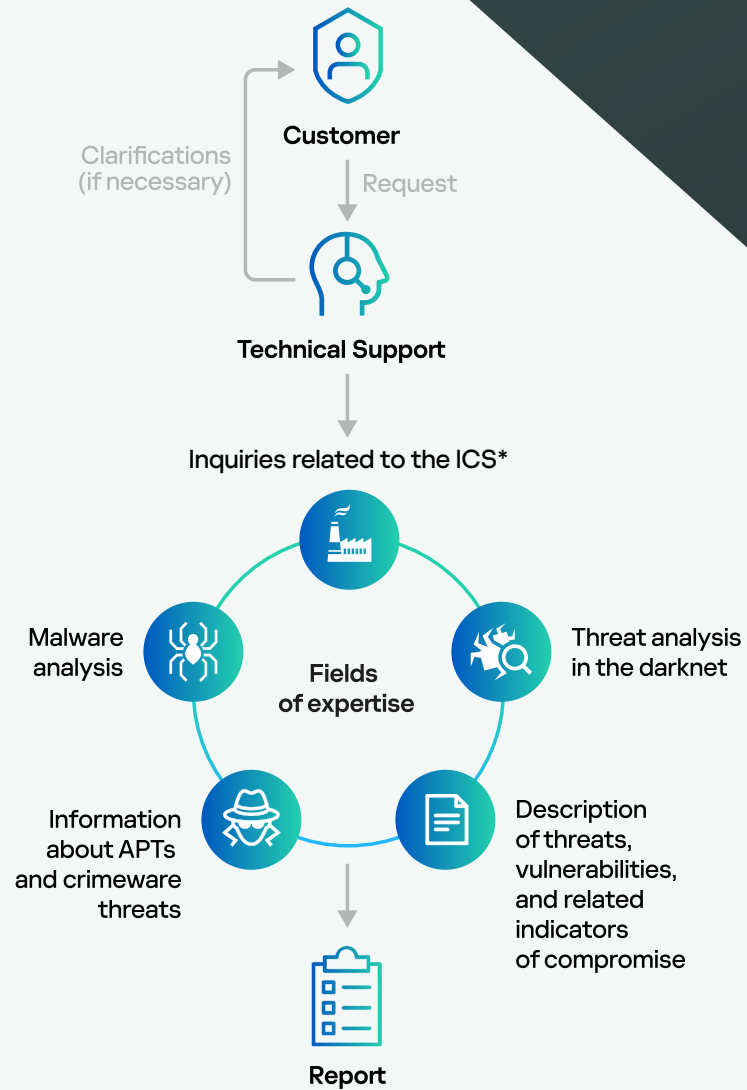


Vulnerability analysis and mitigation

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

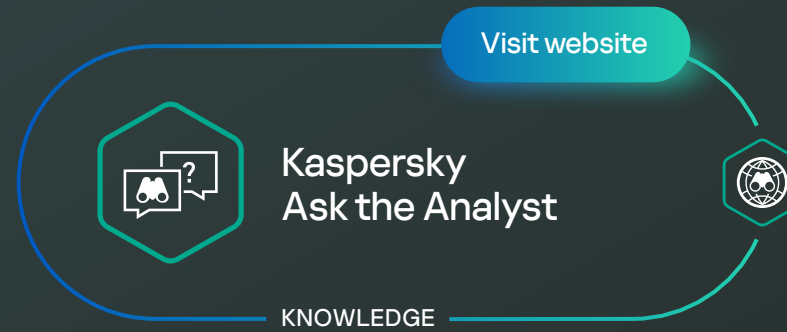
[Contact us](#)

[More about service](#)



*** 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 the ICS
- Information regarding regulatory requirements and standards



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

Visit website



Kaspersky ICS CERT Expert Trainings

KNOWLEDGE

Increase employee cyber-literacy

- 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: Thermal Power, Hydroelectric Power, 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

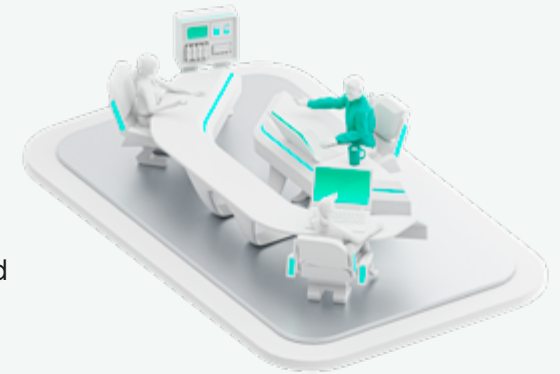
- Email
- Websites and the internet
- Passwords and accounts
- Social media and messengers
- Industrial cybersecurity
- PC Security
- Mobile devices
- Confidential data
- Bank card security and PCI DSS
- GDPR



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

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

Analysis of your industrial infrastructure's security

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

- Attack surface
- The security level of the industrial network infrastructure, DCS, and industrial devices
- Risks of critical systems compromise

Checking critical components

- Network traffic, including industrial protocols
- Process control components: SCADA, PLC, smart meters, etc.
- Physical elements of the automated process control system
- Network architecture, including ACS networks

[More about the service](#)

[Contact us](#)

INTERNET

 **External penetration testing**

 Black Box or Gray Box

**Corporate
LAN, MES**

 **Internal penetration testing**

 Black Box
or Gray Box

**Industrial (OT)
infrastructure**



**Devices and
components**



 **OT security analysis**

 White Box testing


 Interview


 Audit

**Test
environment**



 **Security analysis
of hardware and
software components**

 White Box testing

 Zero-day vulnerabilities

 Standards

Visit website



Kaspersky Managed Detection and Response

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:

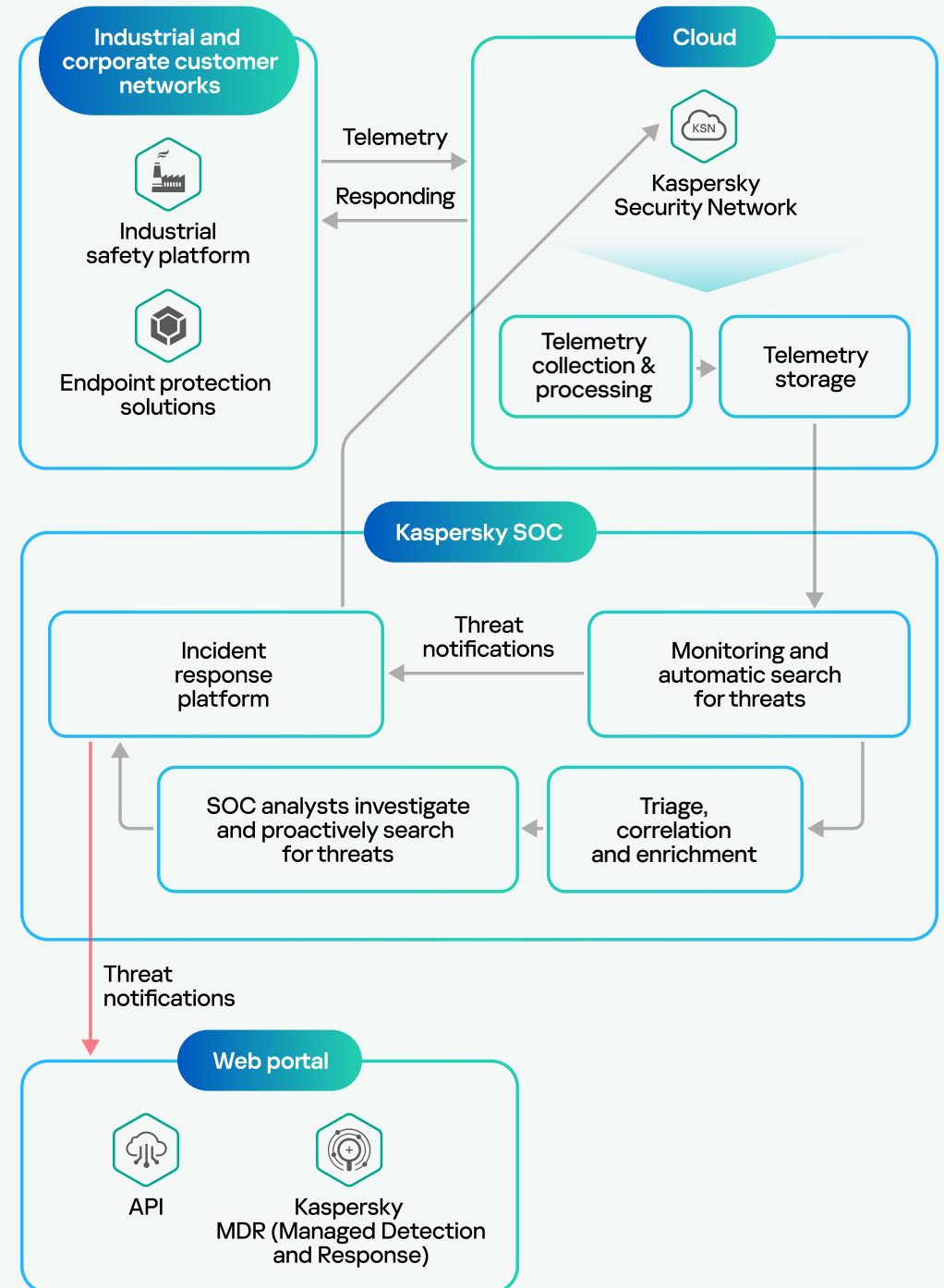
- Continuous hunting, detection, and elimination of threats targeting your industrial enterprise
- Reduced security costs by eliminating the need to hire new cybersecurity experts
- All the key benefits of a SOC, without having to establish one in-house

25% of our protected customers are from the Industrial sector

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

[Contact us](#)

[More about the service](#)



Visit website



Kaspersky
Incident Response

EXPERTISE

Responding to incidents

Risk

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

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
- Additional support by Kaspersky ICS-CERT

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

[Order the IR Handbook at Kaspersky ICS-CERT](#)

[Learn more](#)

[Contact us](#)



Discover IR trends in Kaspersky Global Emergency Response Team (GERT)' [research](#).

The partner you can trust



26 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](#)