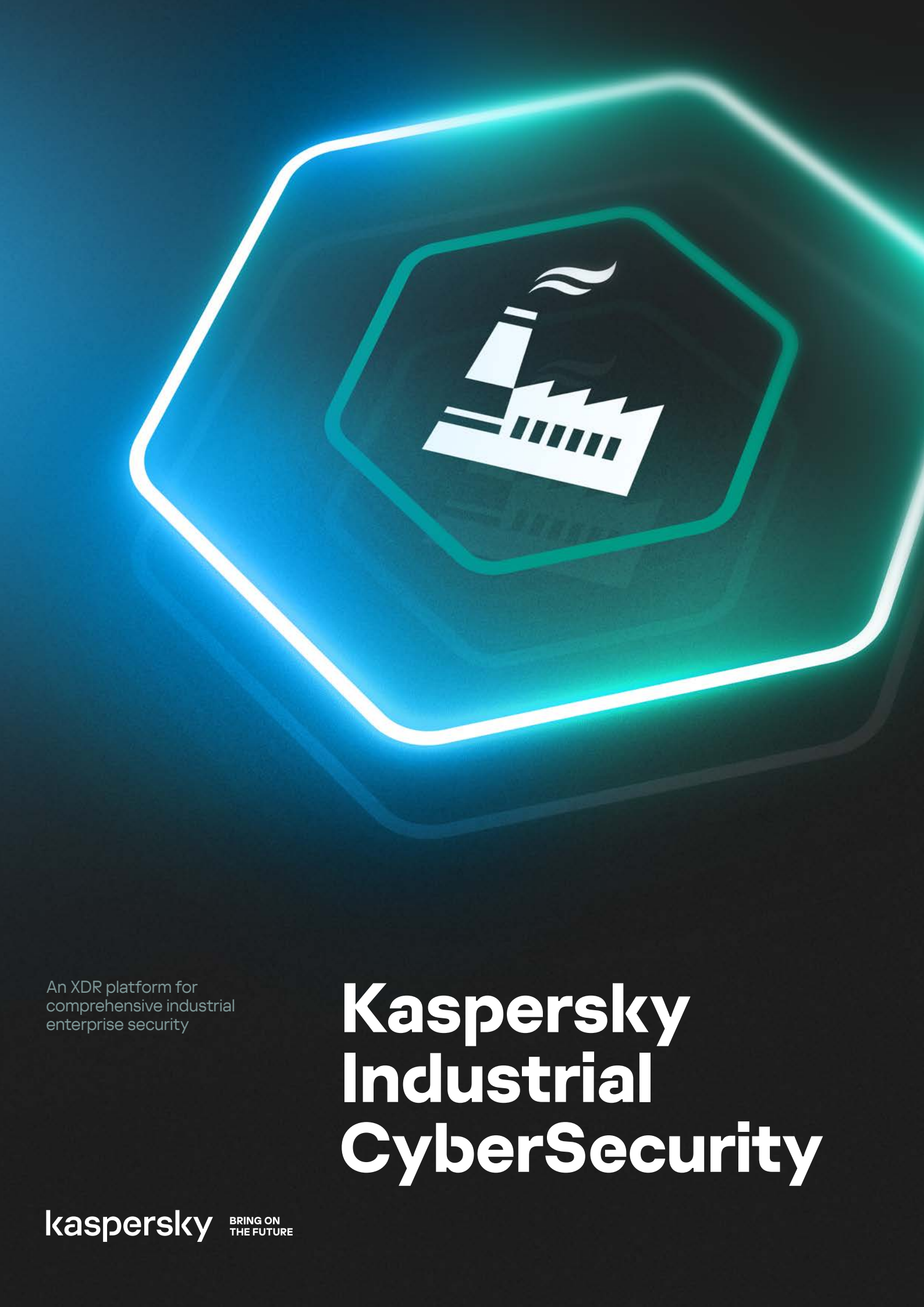


An XDR platform for comprehensive industrial enterprise security

Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

Attacked by malware

Since the beginning of 2023, about 35% of computers related to ICS have been attacked by malware – almost 5% less than the previous year.

Kaspersky ICS CERT, October 2023

Learn more

Cyber threats faced by ICS and industrial enterprises

The new reality for owners and operators of industrial infrastructures is shaped by hacktivists' growing interest in automation systems, high regulatory requirements, IT-OT convergence, and the rise of cyberattack variety in the industrial sector (an increase of almost 50% in H1 2023 compared to H2 2022, according to Kaspersky ICS CERT statistics).

The penetration of digital technologies, which is usually seen as a good thing, erases the gap between IT and OT environments that used to protect the latter from cybercriminals. While a single flash drive brought into the ICS environment can seriously affect a company's core business, a motivated hacking group can penetrate OT networks and cause considerable damage, and/or steal valuable information. Combined with the automation standards evolving from common recommendations to legislative requirements and the increasing need to share best practices as well as manage risks, this makes cybersecurity of industrial enterprises a formidable challenge.

Kaspersky ICS CERT expects organizations from the following industries to face cyberattacks with increasing frequency:

Oil, Gas and Chemical

The high value of data and systems these enterprises control makes them an attractive target for ransomware and malicious actors who seek to disrupt operations or manipulate prices.

High-Profile Industrial Manufacturing

These enterprises play critical societal roles and possess valuable data that can be exploited for financial gain, leading to massive economic and reputational damage.

Minerals, Metals & Mining

The minerals, metals and mining industry is targeted for its valuable resources, financial impact, and interconnected supply chains.

Power, Grid and Utilities

The key role power, grid and utilities play in our daily lives is the main reason for attacks aiming to create chaos or exert influence.

The primary targets of APT attacks will include:

Critical infrastructure owners and operators

Strategically important government or public organizations face considerably greater potential consequences from operational interference

High-profile Industrial players

From single plant to nationwide or international scale, these companies engage in high-risk operations, involving significant incident costs

Production and business process stability, as well as the protection of valuable assets, are directly related to the sustainable development of industrial enterprises and critical infrastructure facilities. Attacks on industrial systems, particularly ICS and SCADA, are on the rise. Meanwhile, modern cyberthreats aimed at industrial environments appear to be immune to conventional solutions.

Choosing a partner you can trust, with a deep knowledge of overlaps between industrial and corporate cybersecurity and the capacity to provide a full range of cutting-edge security technologies has never been more important.

Learn more about the common TTPs of attacks against industrial organizations

Learn more

KICS XDR Platform enables users to see the bigger picture and broader context: the chain of incidents on network and endpoint level, precise asset parameters, network communication and topology maps even from segments where traffic mirroring is not yet available, and more.

Endpoint sensor

- Protection Status
- Security Audit
- Network Communications
- Host Telemetry Transmission
- Equipment Monitoring
- Incident Response

Advanced ICS security technologies

Kaspersky Industrial CyberSecurity (KICS) is a native Extended Detection and Response (XDR) Platform for industrial enterprises, specially designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats. The platform comprises integrated technologies that secure core Industrial Automation and Control System components on every level. KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality. KICS for Networks is designed for OT network-traffic analysis, detection and response. Site-level centralized management function, essential for scaling OT Security Operations to a high volume of large, diverse and geo distributed industrial infrastructures, is integrated into the platform.

Seamless integration across platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering an improved customer experience, situational awareness and deployment flexibility. With Extended Detection and Response the KICS Platform enables IT-OT convergence and delivers numerous single-vendor benefits.

Kaspersky Industrial CyberSecurity for Nodes

EDR-enhanced Endpoint Protection

- Server
- Workstation
- Portable Scanners

Kaspersky Industrial CyberSecurity

- Unified Console
- Native Integration
- Cross-Product Scenarios
- Common Kill Chain
- Risk and Asset Management

Kaspersky Industrial CyberSecurity for Networks

Protecting Industrial Devices from Network Threats

- Server
- Sensor

Response Measures

- Host isolation
- Execution Prevention
- Quarantine

Platform Application Points

Convergence of OT and IT environments

DMZ / GTW

IT environment

OT environment

Kaspersky Industrial CyberSecurity for Nodes

- Operator Workstation
- SCADA Server
- Engineer Workstation
- ICS Gateway

Network equipment

SPAN

Kaspersky Industrial CyberSecurity for Networks

- Bay Control Unit (BCU)
- Intelligent Electronic Device (IED)
- Programmable Logic Controllers (PLC)
- Relay protection and safety instrumented system (SIS)
- Isolated Nodes (manual checking with KICS Portable Scanner)

Physical Level

Early anomaly detection and predictive analytics

Kaspersky Machine Learning for Anomaly Detection (Kaspersky MLAD) is an innovative system that uses a neural network to simultaneously monitor a wide range of telemetry data. It detects equipment faults and human error, helping to prevent failure and accidents, identifies atypical employee actions or equipment operations as signs of a specialized attack or sabotage, and combines anomaly detection with predictive analysis of equipment condition and life cycle.

Learn more

Protected by Kaspersky products

Kaspersky Industrial CyberSecurity for Networks

KICS for Networks

A proprietary protocol-level solution for industrial network monitoring and traffic analysis, shipped as software or as a virtual device.

KICS for Networks identifies anomalies and intrusions in the ICS at an early stage, shows how the attack develops over the network and in the nodes (EDR kill chain and telemetry), and ensures the necessary actions are taken to prevent any negative impact on industrial processes.

The solution helps to detect and rank risks based on data from vulnerabilities and network connections, as well as the role of various assets, to prevent incidents.

Benefits

Asset Inventory

Automatic asset inventory and data collection using passive and active methods of data gathering

Network Inventory and Visualization

- Network communications map
- Network topology diagram

Vulnerability and Risk Assessment

- OT-specific vulnerability and risk management
- Automatic scoring and prioritization
- Risk remediation recommendations

Network Anomaly Detection

Network integrity control with baseline deviation monitoring and detection of malicious and suspicious network activity

OT Process Control and Deep Packet Inspection (DPI)

- Industrial payload data extraction
- Real-time process control
- Industrial command control
- Advanced OT process monitoring by Kaspersky MLAD

Integration and Data Exchange

- Centralized information
- Integration with Kaspersky and third-party or Customer systems (IEC 104, OPC, CEF, Syslog, API-based connectors)

Centralized compliance audit of industrial network nodes

KICS for Networks offers centralized industrial network node auditing, including agent-based (via KICS for Nodes) and agentless auditing of networking hardware and endpoints for vulnerabilities and compliance with OVAL* and XCCDF** industry standards.

- Automated centralized security audit for Windows, Linux nodes, network devices
- Compliance audit. Full-functional editor for compliance checks and parameters
- All reports and asset data are available in one place – KICS for Networks asset base
- Protected vault for nodes credentials
- Support any third-party or customized OVAL databases
- Built-in SCADA vulnerabilities database by ICS CERT

* Open Vulnerability and Assessment Language (OVAL)
** The Extensible Configuration Checklist Description Format (XCCDF)

Kaspersky Industrial CyberSecurity for Nodes

KICS for Nodes

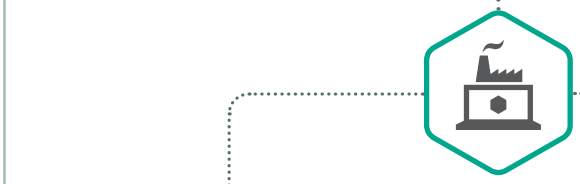
Industrial-grade, tested and certified Endpoint Protection, Detection and Response. A low-impact, compatible and stable solution for Linux, Windows and standalone systems.

KICS for Nodes protects every endpoint in a modern, digital, managed and distributed automation system. The solution collects telemetry to create a clear and detailed visual representation of an incident's progress on workstations, servers, gateways and other endpoints, reassuring automation system administrators that an incident has been fully dealt with and won't happen again.

KICS for Nodes Portable Scanner enforces a cybersecurity policy on standalone machinery, automation systems or equipment on which security software cannot be installed. With a very low operational footprint, it does not interfere with existing security solutions.

- Installation-free solution that provides ultimate situational awareness and OT-visibility even for a standalone infrastructure.
- Allows you to perform on-demand scans on multiple machines during maintenance windows simultaneously, and provides convenient reports.
- Conducts anti-malware compliance checks of equipment accessing an OT site, including third-party contractors' computers.

- Device Control
- File Integrity Control
- PLC Integrity Control
- Anti-Cryptor
- Exploit Prevention
- Network Threat Prevention
- Windows Log inspector
- Wi-Fi Control
- Firewall Management
- Registry Monitor
- Security Audit
- EDR Agent
- Endpoint Sensor (Integration with KICS for Networks)



- Windows Nodes
- Linux Nodes
- Portable Scanner
- Audit Agent

- Gateway
- Historian server
- SCADA server
- Operator workstation
- Engineering workstation
- System management workstation
- Embedded systems

Benefits

Low impact

- Low impact on protected devices for best system performance
- No reboot required for installation, update or upgrade
- Detection-only mode available
- Tunable system resource consumption

Compatibility

- Legacy OS support starting from Windows XP SP2 and Windows Server 2003 SP1
- Compatibility with industrial automation vendors
- Portable Scanner as an installation-free option

Extended protection

- Protection from malware, ransomware and exploits
- Log analysis
- Firewall control
- Built-in ICS EDR technology
- Air-gapped database updates

Modular deployment

- Flexible options and safe non-intrusive settings designed for OT
- Modular architecture allows selecting only the required protective components

PLC support

- Siemens SIMATIC S7-300, S7-400, S7-400H, S7-1500, S7-1200, SIPROTEC 4
- Schneider Electric Modicon M340, M580
- Devices based on CODESYS V3
- Fastwel CPM723-01

Audit

- OVAL open standard-based comprehensive security and compliance audit

Kaspersky XDR effectiveness factors

Contextual Understanding of unique characteristics, requirements, specialized systems, protocols, and operational considerations

Integration with ICS enables comprehensive visibility and analysis of industrial network traffic and system behavior

OT-specific Threat Intelligence to leverage Kaspersky's expertise in the area of industrial environment threat protection

Customization and configuration to tailor the solution to the specific risk tolerance, network architecture, and regulatory compliance needs

A **single vendor** to get the most out of vendor support and collaboration, including providing timely updates and patches

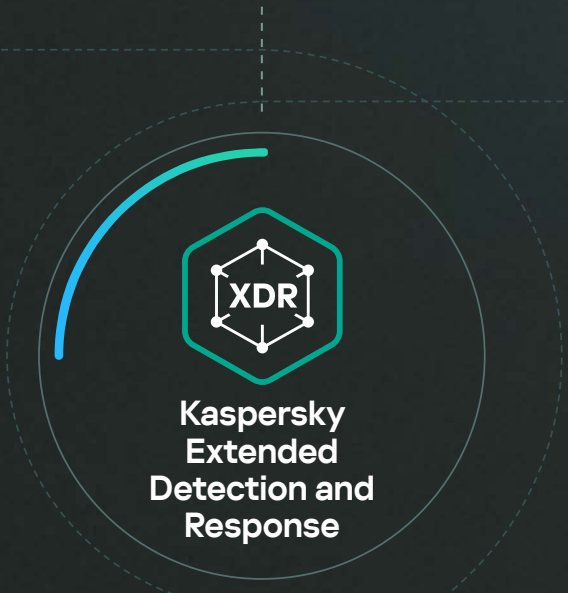
Unified cybersecurity across the industrial and corporate segments of your enterprise

Attacks on industrial systems, particularly ICS and SCADA, are on the rise. Choosing a partner you can trust, with a deep knowledge of overlaps between industrial and corporate cybersecurity and the capacity to provide a full range of cutting-edge industrial and corporate cybersecurity technologies has never been more important.

Kaspersky XDR is the perfect tool to create a safe, threat-free work environment. Its compatibility with a variety of security products facilitates the establishment of a secure cyberspace, providing industry-specific options for your business and protecting it from any threat, no matter how big or small. Kaspersky XDR's integration options allow it to provide a unified, all-encompassing view of threats, equipping your security team with all the tools and data they need to protect your business from current and potential threats.

Learn more

IT–OT convergence
with Kaspersky Hybrid XDR



IT Cybersecurity

Learn more

Kaspersky Extended Detection and Response

OT Cybersecurity

Learn more

Environment boundary

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

ICS CERT

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

Customers around the world

ROSATOM NORNICKEL EuroChem

NLMK TATNEFT ROSSETI Wintershine

alperia PacificLight КазМунайГаз AGC

Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity for Nodes

Kaspersky Industrial CyberSecurity for Networks

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture