

Kaspersky Industrial CyberSecurity: solution overview

kaspersky BRING ON
THE FUTURE



**Kaspersky
Industrial
CyberSecurity**

Kaspersky Industrial CyberSecurity: solution overview

Introduction

Historically, industrial companies all over the world have approached cybersecurity in their IT and OT (operational technology) networks differently. Most companies already have mature breach detection and incident response measures in their corporate infrastructure, but when it comes to OT they usually rely on an out of date air-gap approach. Industrial companies are becoming increasingly 'digital', investing more and more in smart technologies, new automation systems, and the adoption of digital transformation. That actually erases the gap between IT and OT environments that is used to prevent cyberthreats from reaching industrial control systems. According to Kaspersky ICS CERT, in the first half of 2021 the percentage of ICS computers on which malicious objects were detected reached 33.8%¹.

What are these threats?

First of all, they include the risk of accidental infection by conventional malware. You don't have to be a target to become a victim. A single flash drive or phishing email with a banking Trojan or ransomware brought unintentionally into the ICS environment can seriously affect the core business of a company. Even if accidental infections do not occur that often, it is obvious that a motivated hacker can also penetrate OT networks and cause considerable damage to expensive equipment or production, or steal valuable information.

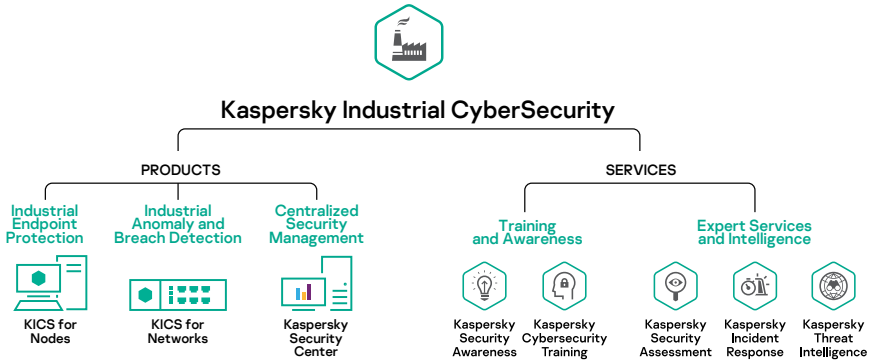
What are the proper OT cybersecurity measures?

1. Industrial endpoint protection to prevent accidental infections and make motivated intrusion more difficult.
2. OT network monitoring and anomaly detection to identify malicious actions on the level of programmable logic controllers (PLCs).
3. Training programs for employees to reduce accidents and minimize the human factor.
4. Dedicated expert services to investigate the infrastructure, conduct expert analytics or mitigate the impact of an incident.

¹ Threat landscape for industrial automation systems, H1 2021, Kaspersky ICS CERT
<https://ics-cert.kaspersky.com/reports/2021/09/09/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2021/>

What does Kaspersky provide?

Kaspersky addresses all the cybersecurity needs of industrial organizations in its **Kaspersky Industrial CyberSecurity (KICS)** portfolio. KICS offers a holistic approach to industrial cybersecurity, bringing value to any stage of the customer's OT security process – from cybersecurity assessments and training to advanced technologies and incident response.



In 2020, Kaspersky was mentioned in Gartner report “Competitive Landscape: Operational Technology Security”² as a representative vendor in 4 product categories, including:

- OT Endpoint security;
- OT Network Monitoring and Visibility;
- Anomaly Detection, Incident Response and Reporting;
- OT Security Services².

Frost and Sullivan recognizes Kaspersky with the 2020 Global Company of the Year Award based on recent analysis of the Global Industrial (OT/ICS) Cyber Security market³. Kaspersky is also the top vendor in the industrial cybersecurity category, based on overall sentiment ratings by over 250 qualified professionals in the industrial automation community, in VDC’s annual global survey⁴.

Meanwhile, Forrester’s studies show an ROI of 368% for a company using Kaspersky Industrial CyberSecurity for Nodes⁵ and an ROI of 135% for a company using Kaspersky Industrial CyberSecurity for Networks⁶ as well as other benefits such as expert support and peace of mind.

² Gartner: Competitive Landscape: Operational Technology Security, March 2020.

<https://www.gartner.com/document/3892469> (Gartner subscription is required to access the full report)

³ Frost & Sullivan: Best Practices Awards. 2020 Global Industrial (OT/ICS) Cyber Security Company of the Year Award.

<https://www.prnewswire.com/news-releases/kaspersky-commended-by-frost--sullivan-for-delivering-customer-focused-holistic-cybersecurity-solutions-301168341.html>

⁴ VDC Research: Industrial IoT Vendor Awards. 2020. https://ics.kaspersky.com/media/KICS_award_VDC_2020.pdf

⁵ Forrester Study: The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, April 2019.

<https://www.kaspersky.com/forrester-tei-for-kics>

⁶ Forrester Study: The Total Economic Impact™ of Kaspersky Industrial CyberSecurity, May 2021.

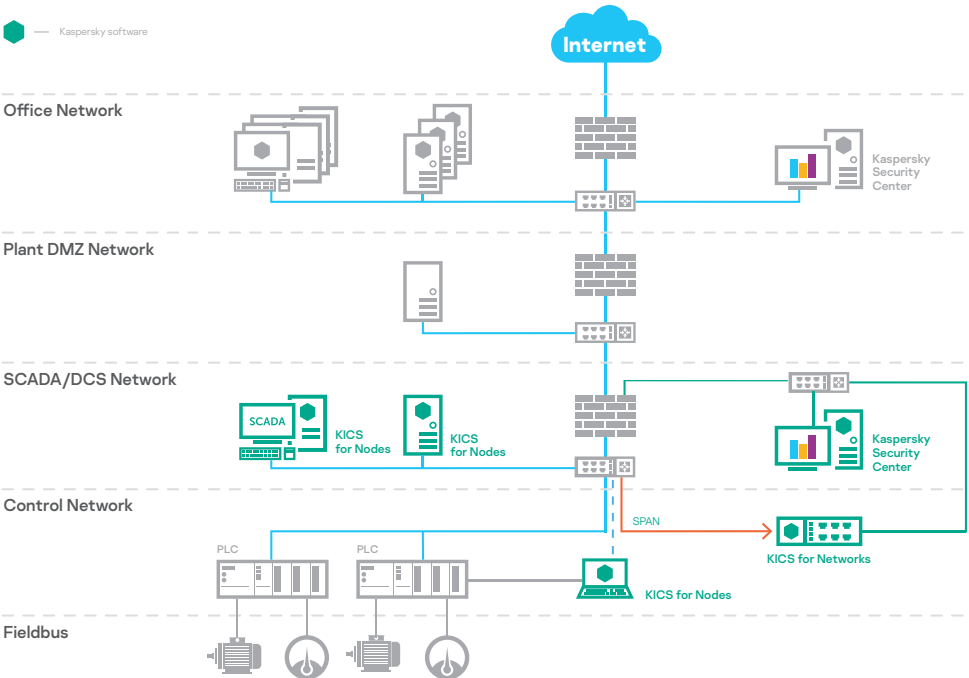
<https://go.kaspersky.com/Forrester-TEI-KICS-for-Networks>

Products

KICS products are designed to comprehensively secure the industrial elements of your organization: KICS for Nodes is aimed at industrial endpoints, while KICS for Networks monitors industrial network security.

KICS for Networks can retrieve important data from industrial endpoints protected with KICS for Nodes to improve customer experience, situational awareness and deployment flexibility. Security administrators can investigate accidents with a broad context: EPP-enriched incident details, precise asset parameters detection, and network communication maps from segments where traffic mirroring is not yet available.

Kaspersky Industrial CyberSecurity products deployment



KICS for Networks

KICS for Networks is an OT network monitoring and visibility solution, delivered as software or a virtual appliance, passively connected to the ICS network.

The benefits:

- ✓ **Asset discovery**
passive OT asset identification and inventory
- ✓ **Deep packet inspection**
almost real-time analysis of technical process telemetry
- ✓ **Network integrity control**
detection of unauthorized network hosts and flows
- ✓ **Intrusion detection system**
sends alerts about malicious network activities
- ✓ **Command control**
inspects commands over industrial protocols
- ✓ **External systems**
external detection capabilities by API integration
- ✓ **Machine learning for anomaly detection (MLAD)**
finds cyber or physical anomalies through real-time telemetry and historical data mining (recurrent neural network)
- ✓ **Vulnerability management:**
updatable database of vulnerabilities in industrial equipment, powered by Kaspersky ICS CERT

KICS for Networks detects anomalies and intrusions inside ICS networks in their early stages and ensures the necessary actions are taken to prevent any negative impact on industrial processes.

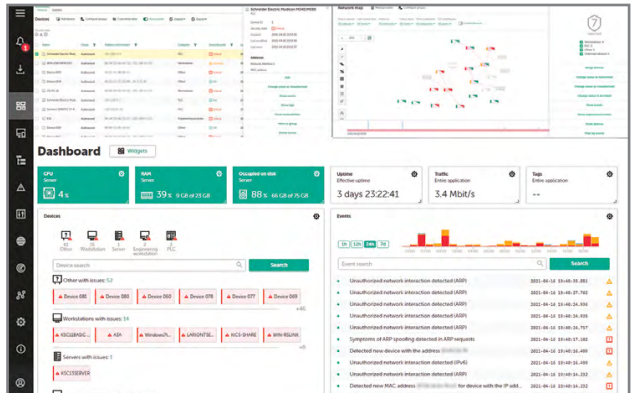
KICS for Networks is an appliance-agnostic solution that allows the customer to choose the industrial computing appliance vendor they trust the most.

The KICS for Networks interface displays a live dashboard and a network map, allowing working with assets and security events.

Example of KICS for Networks appliance



KICS for Networks interface



KICS for Nodes

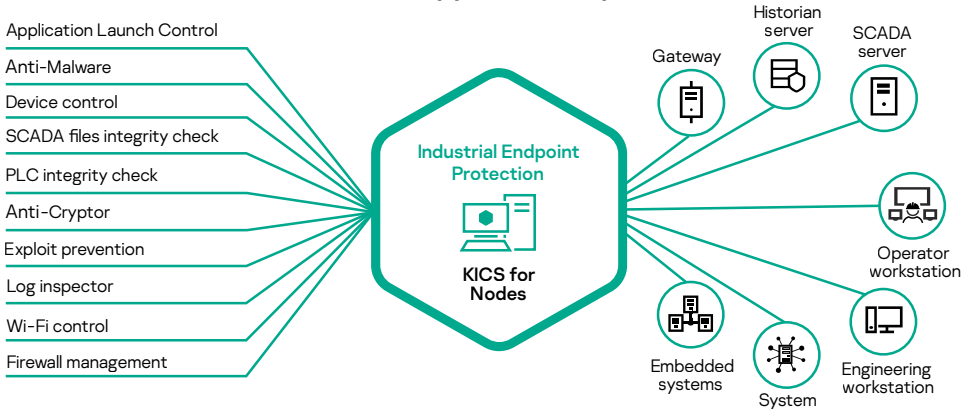
KICS for Nodes is an OT endpoint security product, delivered as software for Windows and Linux-based machines.

The benefits:

- ✓ Low impact on protected device
- ✓ Highest compatibility
- ✓ Advanced malware protection
- ✓ Control of environment

KICS for Nodes was specially designed to consume minimal resources. Built on security and embedded systems, its modular architecture means you only have to install the protective components you need. Protective components can be configured to the threat prevention mode or to detection-only mode. This approach is ideal for legacy, low-performance machines that require the maximum available computing power.

KICS for Nodes functions and supported endpoints



"We decided to partner with Kaspersky as Kaspersky Industrial CyberSecurity could be implemented whilst our operations were still running, and because the solution is compatible with the control systems we use"

Jan Houben, Plant Manager,
AGC Glass Germany GmbH

KICS for Nodes secures industrial nodes from the various types of cyberthreat that can result from human factors, generic malware, targeted attacks or sabotage. KICS for Nodes is compatible with the software and hardware components of industrial automation systems, such as SCADA, PLC and DCS.

Kaspersky Security Center

Kaspersky Security Center is a centralized security management solution for security orchestration of the entire OT infrastructure, with a map of all geographically distributed assets enriched with events, incident analytics and more.

The benefits:

- ✓ **Systems management**
 - Centralized system data collection
 - Centralized software deployment
 - Vulnerability detection and patch management
 - Extended client management capabilities
- ✓ **Policy management**
 - Centralized security policy management
 - Remote task scheduling and execution
- ✓ **Reporting and notification**
 - Event logging
 - Dashboards and reports
 - SMS/email notifications
- ✓ **SIEM integration**
 - Arcsight, Splunk, Qradar
 - Syslog server
- ✓ **HMI integration**
- ✓ **MES dashboard integration**
 - Security status and information delivery to IEC 104/OPC 2.0 compatible host

Kaspersky Industrial CyberSecurity: services

Our suite of services forms an important part of the KICS portfolio – we provide the full cycle of security services, from industrial cybersecurity assessment to incident response.

Expert services

“Their experience in the ICS cybersecurity domain, professionalism and the complexity of their solution, in comparison with other suppliers, has given us great value and ensured a bright future for our company’s security strategy”

Ondřej Sýkora, C&A manager, Plzeňský Prazdroj

- **Industrial Cybersecurity Assessment:** Kaspersky provides a minimally invasive industrial cybersecurity assessment, including external and internal penetration testing, OT security assessment and automation solution security assessment. Kaspersky experts provide significant insights into a company’s infrastructure and give recommendations on how to strengthen the ICS cybersecurity posture.
- **Threat Intelligence:** Up-to-date analytics collected by Kaspersky experts help enhance the customer’s protection from targeted industrial cyberattacks. Provided as TI feeds or tailored reports, they meet specific customer needs according to regional, industry and ICS software parameters.

“By undertaking the exercise and learning from the Kaspersky team’s knowledge, we have increased our protection against cyber security threats”

Yu Tat Ming, CEO,
PacificLight.

“Kaspersky was the best possible company to deliver professional industrial cybersecurity skills training for our ICS group”

Søren Egede Knudsen,
Chief Technical Officer,
Ezenta

- **Incident Response:** In the event of a cybersecurity incident, our experts will collect and analyze data, reconstruct the incident timeline, determine possible sources and motivation, and develop a remediation plan. In addition, Kaspersky offers a malware analysis service in which Kaspersky experts will categorize any malware sample provided, analyze its functions and behavior, and develop recommendations and a plan for its removal from your systems and for rolling back any malicious actions.

Training and awareness

- **Industrial Cybersecurity awareness training:** On-site and online interactive training modules and cybersafety games for employees interacting with industrial computerized systems and their managers. Participants gain a new insight into the current threat landscape and attack vectors specifically targeting the industrial environment, explore practical scenarios and acquire cybersafe working skills. The on-site course can be customized and adapted to run over one or two days.
- **Expert training programs:** The ICS Penetration Testing and ICS Digital Forensics training modules were created for cybersecurity professionals. Participants gain all the advanced skills needed to conduct comprehensive pentests or digital forensics in industrial environments. Certification included.

Learn more about KICS at
<https://ics.kaspersky.com>

#Kaspersky
#BringontheFuture

www.kaspersky.com

© 2021 AO Kaspersky Lab.
Registered trademarks and service marks are
the property of their respective owners.



Frost and Sullivan recognizes Kaspersky with the 2020 Global Company of the Year Award



Kaspersky is recognized as the 2020 Winner of VDC Research’s Platinum Award for Industrial IoT Vendors in the Industrial Cybersecurity category.