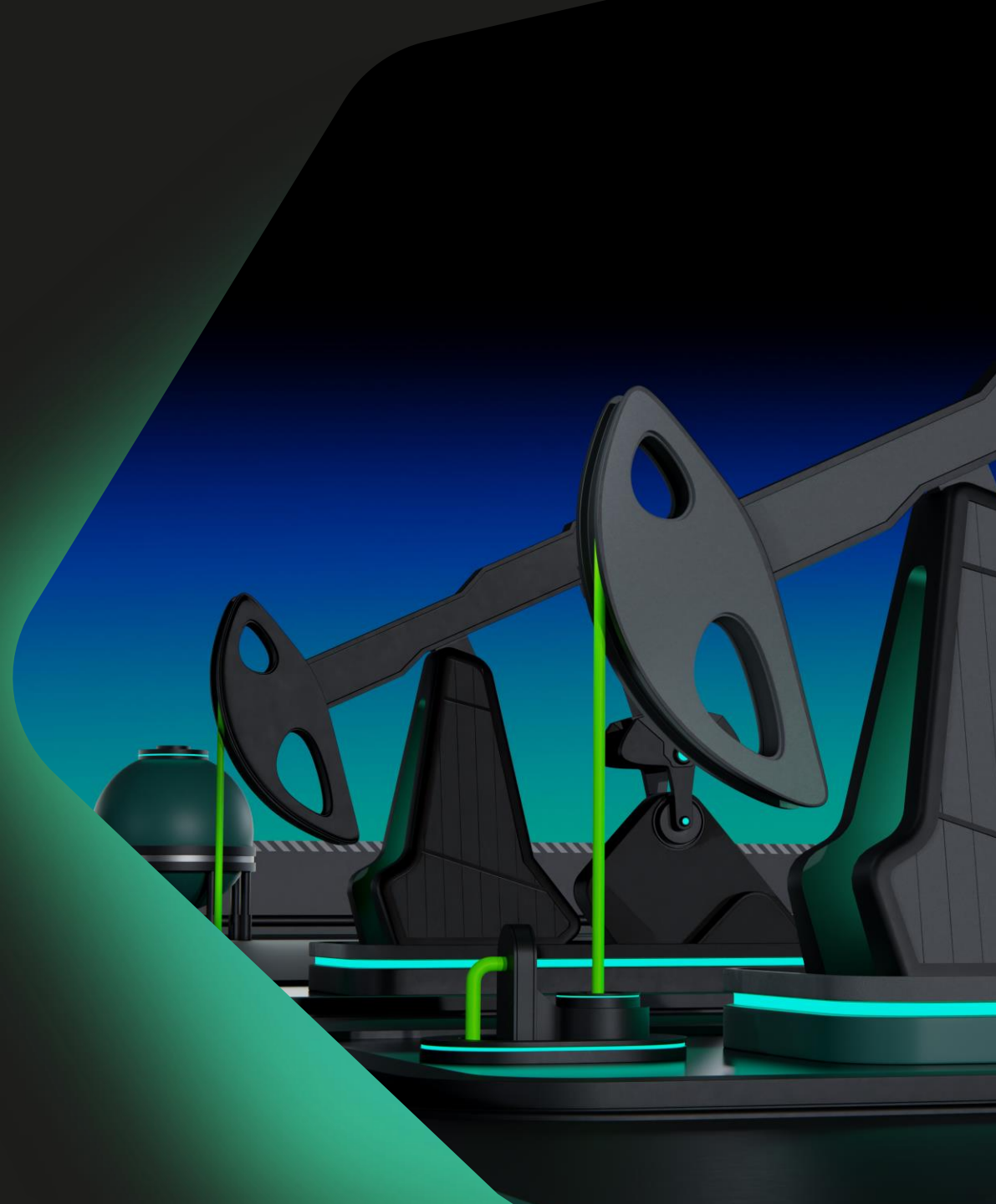



Kaspersky OT Cybersecurity

Vertical offering
for Oil and Gas companies




Industry summary


The oil and gas industry dominates the energy market and has major impact on the global economy. High demand in workforce and ever-growing consumption for heating and electricity highlight the importance of this industry. Aside from the energy, petroleum, gas and LNG are crucial in:




Construction and high-tech materials



Chemicals and fertilizers



Life science and pharmaceuticals



Many other vital spheres

In recent years, oil and gas companies have also played an important role in the transition to sustainability, leveraging their extensive resources, expertise, and infrastructure to facilitate this shift.

Strategies are focusing on:



ESG-transformation



The UN's 17 Sustainable Development Goals (SDGs)¹

Actions and enabling technologies supporting a sustainability strategy

Digitalization trends

- Machine learning and artificial intelligence solutions used in predictive maintenance and for increased reliability
- Convergence of IT and OT systems
- IIoT and sensors for monitoring
- Digital twins for process optimization simulation
- AR and VR technologies for employee training
- Robotization and automation to handle dangerous tasks

Additional actions

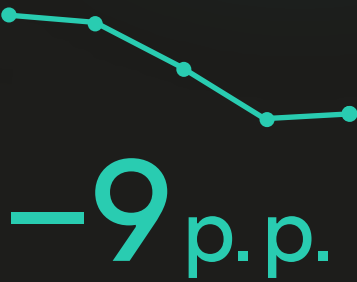
- Compliance with initiatives and directives
- Increasing cybersecurity
- Electrification, solarization and energy efficiency
- Renewing equipment

Following the sustainability strategy by implementing instruments of digitalization is impossible without stable cybersecurity, so that risk resulting in production downtime is minimized.

Increased investment in cybersecurity has resulted in a recent decrease in the number of attacks.

Sustainability initiatives of O&G companies

- Low carbon energy
- Net-zero emissions
- Preserving water resources (prevent spills)
- Reducing waste (circularity of products)
- Securing biodiversity
- Ensuring people's safety (zero fatal accident and decreasing TRIR²)
- Respect for human rights
- Fighting corruption
- Engaging stakeholders



Decrease of attacked ICS computers in the oil and gas industry in H2 2023 (compared to H2 2021)³

(1) — Sustainable Development Goals were adopted by the United Nations in as a call to action to ensure global peace and prosperity by 2030.
(2) — Total recordable injury rate. (3) — According to Kaspersky threat landscape for industrial automation systems statistics for H2 2023.

Digitalization in the oil and gas industry

Digital transformation trends application

IIoT & Cloud

- 1 Seismic data acquisition and processing
- 2 Drilling optimization
- 3 Pipeline leak detection
- 4 Refineries monitoring
- 5 Routing optimization and warehouse monitoring

Robotization and 5G

- 1 Unmanned aerial and underwater robots and drones for drilling inspection and work
- 2 Monitoring of pipeline condition in hard-to-reach places, and data acquisition
- 3 Plants inspection and capability for quick shut down in case of an issue

Hyper automation, AI, ML, RPA

- 1 Locate and define drilling spots
- 2 Pump failures predictions
- 3 Data analytics of pipelines and transport
- 4 Refineries failure prediction
- 5 Customer demand forecasting

Industrial metaverse: AR, VR

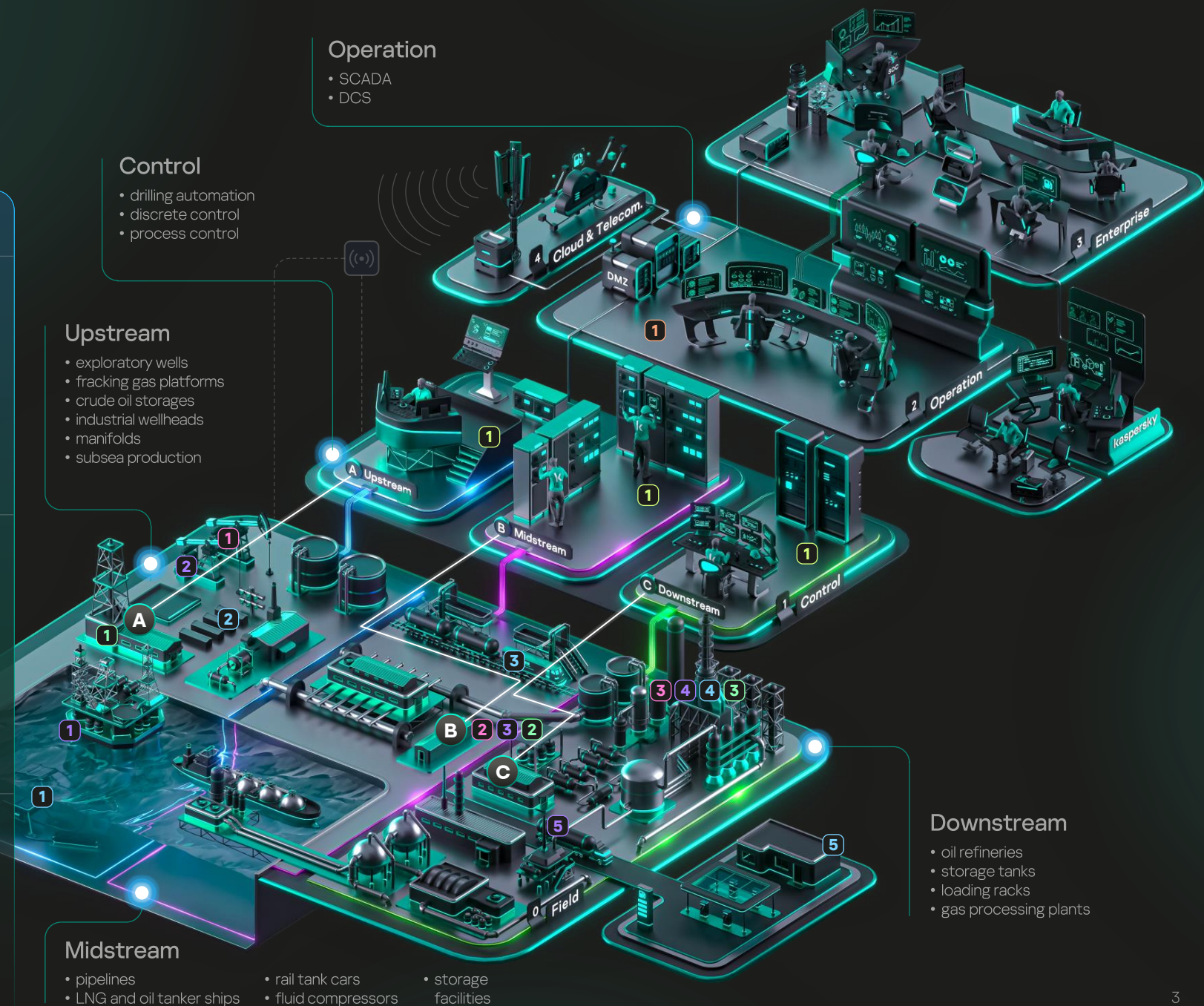
- 1 Personnel training, collaboration, maintenance in virtual environments

Digital twins

- 1 Modelling of drilling scenarios
- 2 Replicas of pipeline system for monitoring
- 3 Modelling oil refineries processes to expose bottlenecks




IT/OT convergence



- 1 Analyzing real-time data from sensors and equipment

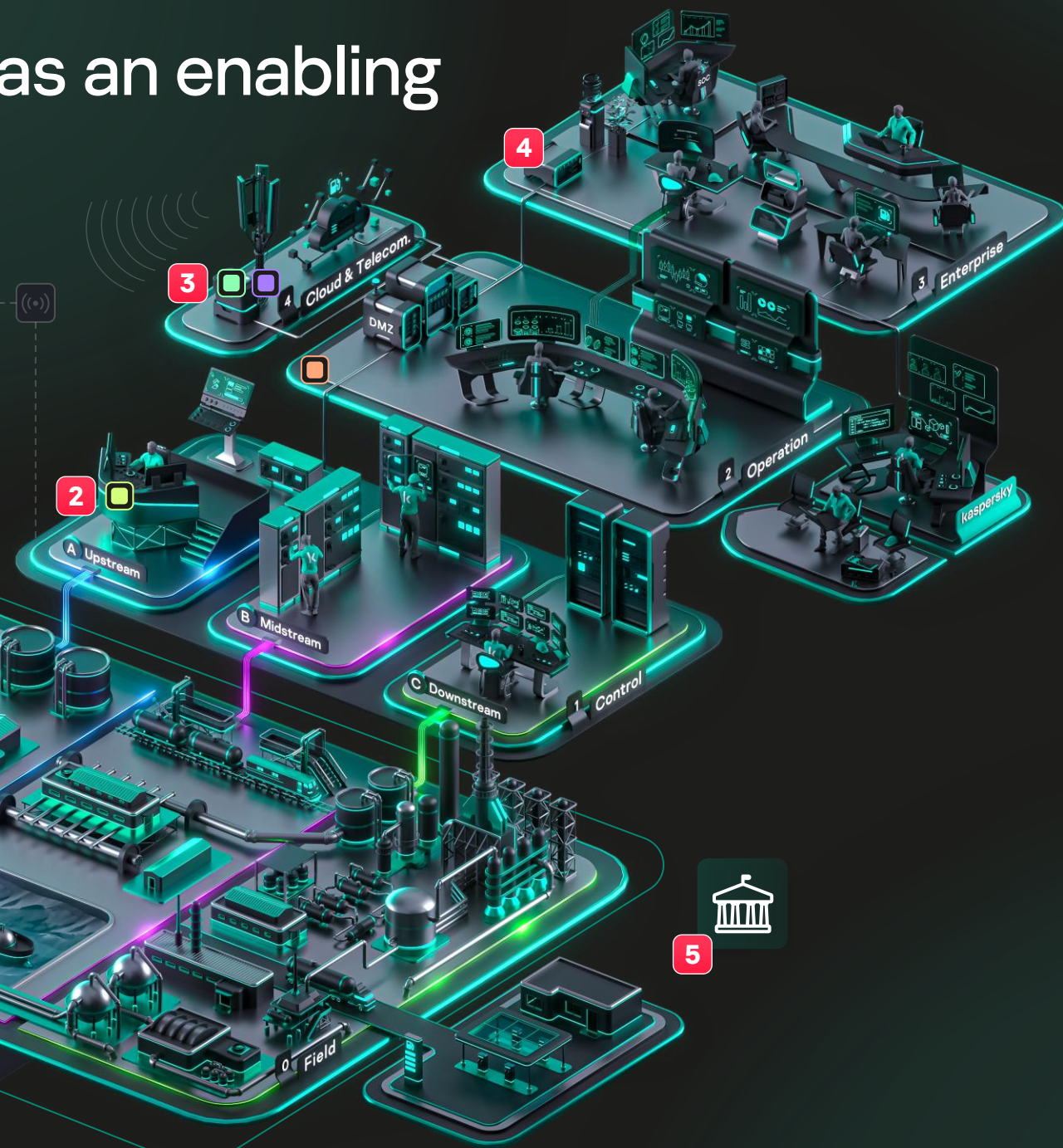


Cybersecurity as an enabling technology

Color legend
of digitalization trends

-  IIoT & Cloud
-  Digital twins
-  Robotization and 5G
-  Industrial metaverse: AR, VR
-  Hyper automation, AI, ML, RPA
-  IT/OT convergence

1    



At the same time, digital transformation in O&G industry goes hand in hand with security issues and challenges...

- 1 Attack surface expansion
- 2 Legacy infrastructure and out-of-control IT/OT convergence
- 3 External access to OT infrastructure
- 4 Personnel deficit
- 5 Critical infrastructure protection regulations

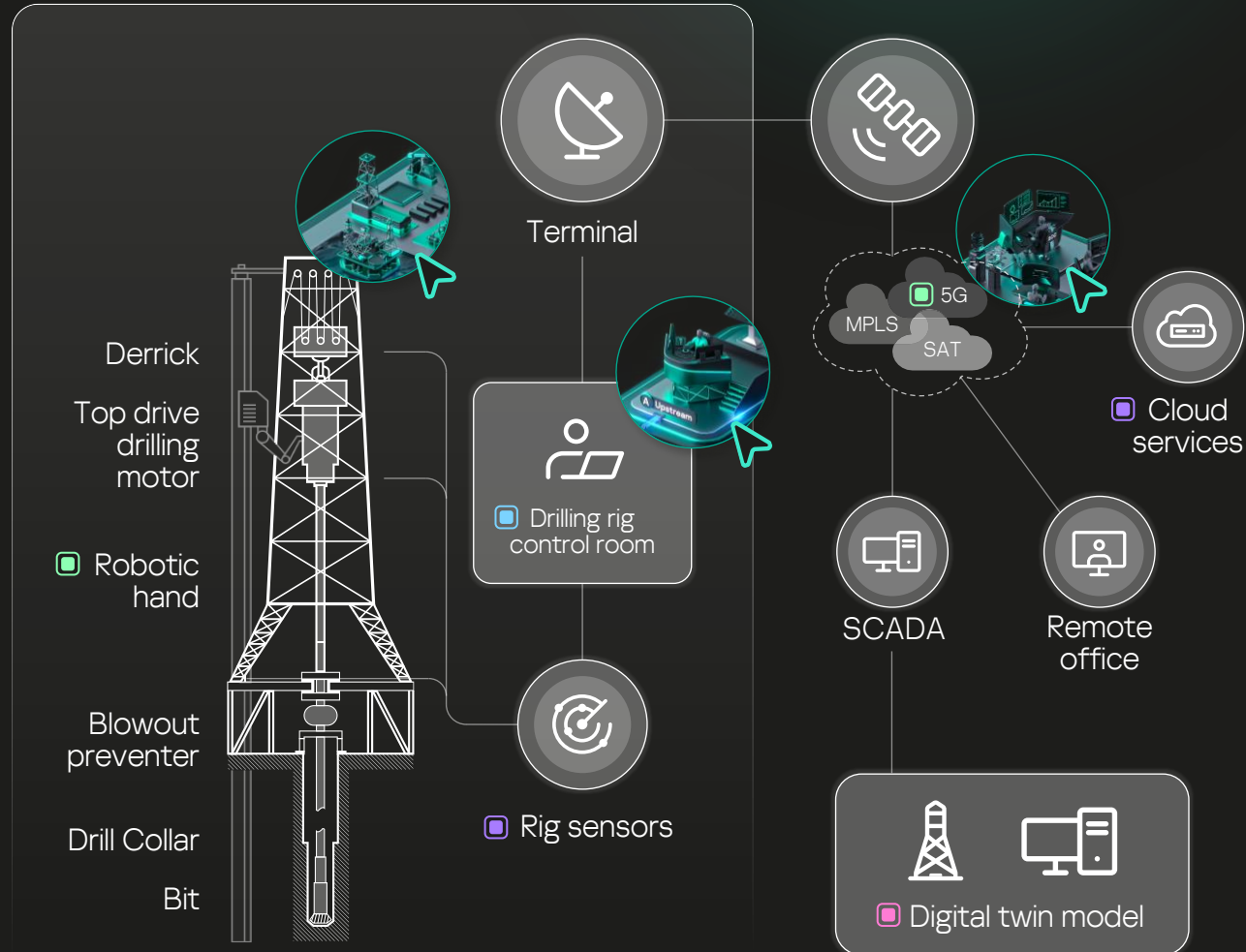
 Click on item to continue



1. Attack Surface Expansion

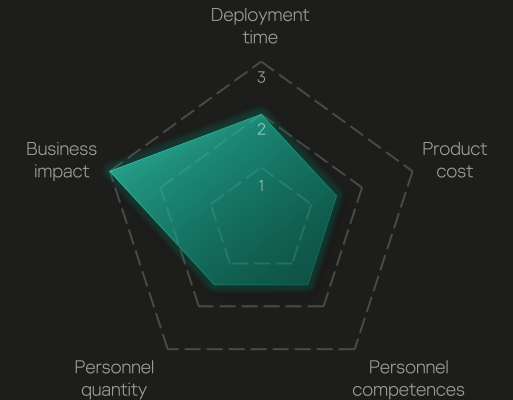
■ IIoT & Cloud ■ Digital twins ■ Hyper automation ■ Robotization and 5G

Upstream process example



ICS run and monitor drilling sites, pipelines and refineries creating complex process environment. Such an interconnected system becomes vulnerable to cyberattacks as connection to one computer or terminal gives access to wider surface of infrastructure

Solution characteristics



How Kaspersky can help



- End-to-end OT/IIoT infrastructure coverage
- Systems and network visibility
- Regular in-depth security audits

Ecosystem of supporting services

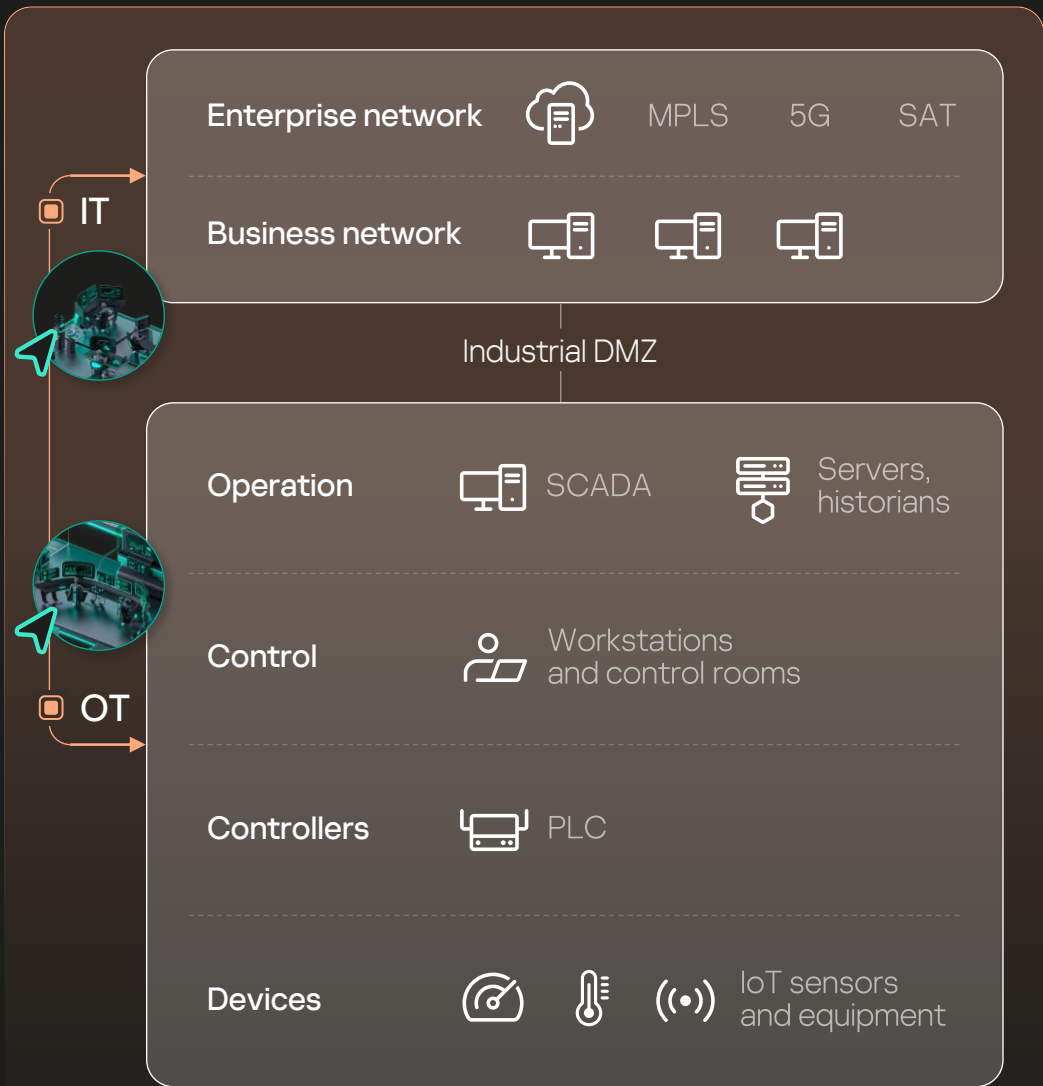


- Identifying security flaws in ICS infrastructures
- Checking critical components



- Proactive threat detection
- Automated and guided response
- ICS cybersecurity expertise

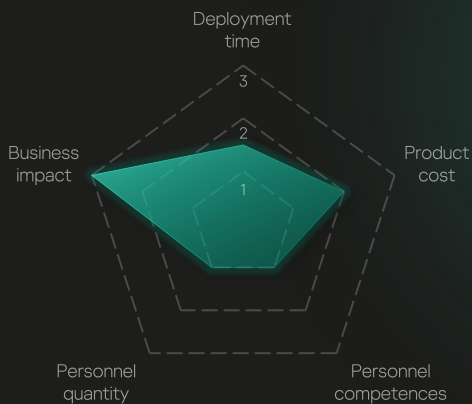
2. Legacy infrastructure and out-of-control IT/OT convergence



The integration of IT and OT has become key element of O&G process architecture, but its implementation can face security risks

- Unsecured legacy infrastructure with outdated technology
- Disparity in priorities between systems' cybersecurity which can result in contradictory protection mechanisms
 - IT's focus is on confidentiality and data integrity
 - OT's focus lies in real-time operations and availability

Solution characteristics



How Kaspersky can help



- Detection of threats and anomalies, safe response measures on hosts and networks
- Centralized risk, security policy and asset management at all levels of IACS



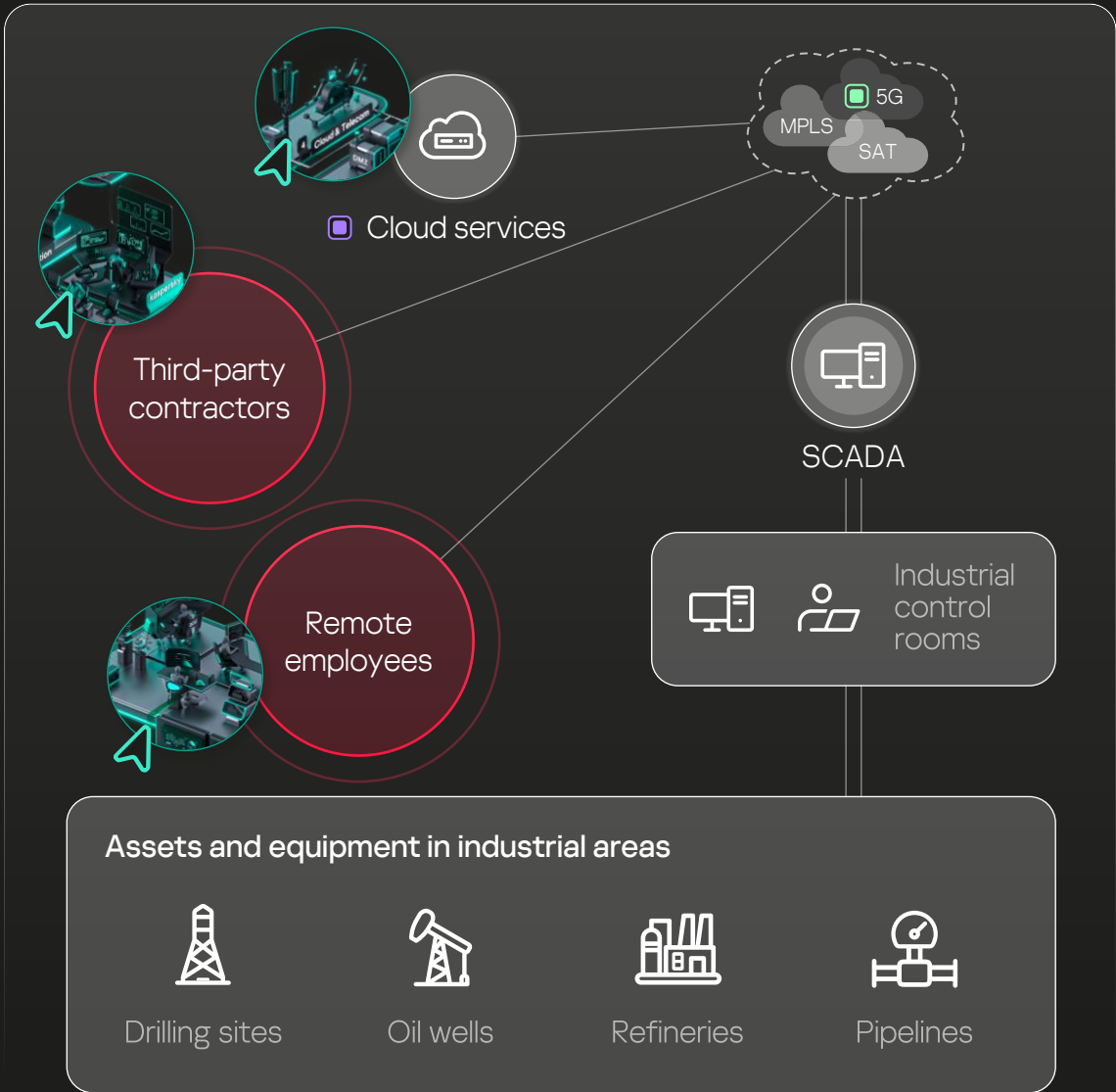
- Robust endpoint protection against ransomware, malware, fileless attacks and APTs
- Comprehensive visibility and superior defenses across all the organization's endpoints

Ecosystem of supporting services



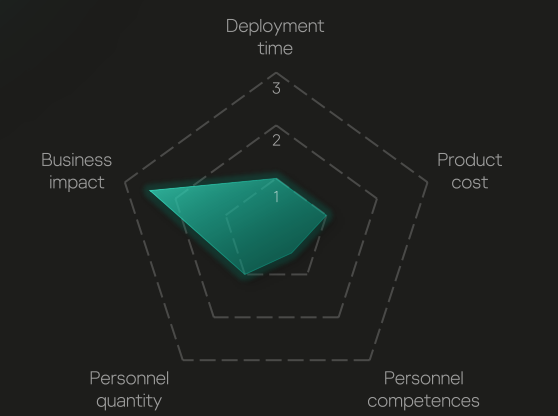
- Threat detection
- Investigations and active threat searches
- Comprehensive threat and vulnerability information

3. External access to OT infrastructure



Granting remote access to pipelines, refineries and other O&G systems allows to monitor, guide, and analyze data of industrial processes for work-from-home employees and vendors, grace to IT/OT convergence. This optimization requires the securing of external connection as users with wider access to OT infrastructure could expose it to major risk of cyberattacks

Solution characteristics



How Kaspersky can help

Kaspersky SD-WAN

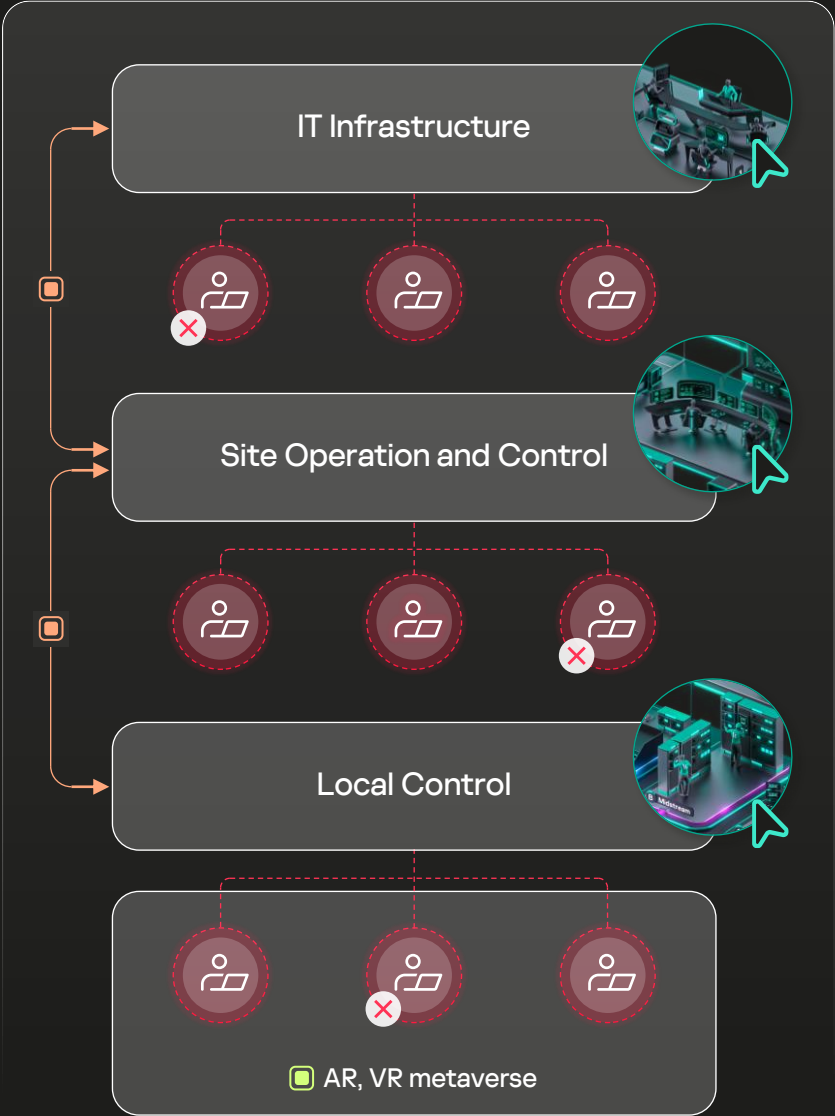
Rapid deployment of distributed network

- Easy scalability
- Convenient management
- Centralized security

Kaspersky Thin Client

- Cyber immune thin clients for secure remote access
- Centralized management tool to simplify administration of the thin client infrastructure

4. Personnel deficit

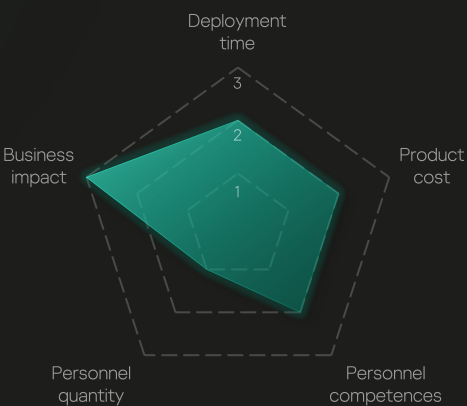


For more than a decade, the O&G industry has faced challenge in recruiting and retaining skilled professionals. This problem is escalating with digital transformation and the high demand for workers with hybrid technical and digital expertise.

43%
of workers surveyed globally in 2020 wanted to leave the energy sector in the next five years¹

(1) – [Spring 2022 outlook](#)

Solution characteristics



How Kaspersky can help

Kaspersky Industrial CyberSecurity

- Reduced workload for personnel responsible for cybersecurity
- Faster threat response

Kaspersky Extended Detection and Response

- Open single management platform
- Unified cybersecurity across the industrial and corporate segments

Ecosystem of supporting services

Kaspersky Security Awareness

- Training materials
- Game-based training through business simulations
- Interactive learning modules and simulated phishing attacks

Kaspersky ICS CERT

Practical skills from experts

- Digital forensics and incident response
- Exploring vulnerabilities
- Cross-functional training programs

Click on product to learn more

8

5. CIP regulations

Cybersecurity regulations for the energy - and particularly the oil and gas - sector address emerging threats and vulnerabilities, and set the industry benchmark for securing OT systems. Countries across the globe implement particular standards and directives which commonly include:

- Risk management and assessment
- Policies and procedures
- Systems security
- Incident response and reporting
- Workforce training



- ISA / IEC 62433
- ISO / IEC 27001
- ISA99



- NIS2 Directive
- ENISA Guidelines on Cybersecurity for OT and ICS
- EU Cybersecurity Strategy
- EU Cybersecurity Act
- EU Cyber Resilience Act



- NIST CSF
- NIST SP 800-82
- TSA Pipeline Security Directive
- API Standard 1164
- DOE Cybersecurity Capability Maturity Model



- Government Cyber Security Strategy
- NCSC's Cyber Assessment Framework



- IT Security Act 2.0
- BSI KritisV
- BSI ICS Security Compendium
- DVGW
- VDMA 66418



- National Cybersecurity Strategy
- ANSSI Cybersecurity Framework for ICS
- Critical Information Infrastructure Protection Law



- The Netherlands Cybersecurity Strategy (NLCS)
- Network and Information Systems Security Act (WBNl)
- NSCS Guide to Cyber Security Measures



- The National Security Framework
- CNPI Royal Decree 704/2011
- CCN-STIC Security Guides




- Swedish Cybersecurity Act
- Swedish Protective Security Act
- MSB Guidance



- National Cybersecurity Strategy
- Romanian Cybersecurity Law No. 362/2018
- National Energy Regulatory Authority Regulations



- National Cybersecurity Strategy and Action Plan
- BTK CIPR
- EPDK Cybersecurity Regulation



- Estratégia Nacional de Cibersegurança
- PNSI Framework
- ANP Regulations



- NCIIPC Guidelines
- Information Technology (IT) Act, 2000



- GB/T 44462.1-2024
- GB/T 22239-2019
- GB/T 32919-2016
- GB/T 25070-2019



- BSSN National Cybersecurity Strategy
- BSSN Regulation No. 4/2021
- Presidential Regulation No. 82/2022



- UAE Information Assurance Standards
- UAE Cybersecurity Council Framework
- UAE IoT Security Standard
- UAE CIIP Policy




- NCA OTCC-1:2022
- NCA ECC-2-2024
- NCA CGIoT-1:2024




Contact us for more about your regional standards and regulations

How Kaspersky can help





Kaspersky provides services and solutions based on a “defense in depth”, as recommended by industrial security solution providers as well as regulatory bodies in different countries







The products are designed to make oil and gas companies stay compliant with **IEC 62443**, **NIS2**, **NERC CIP**, **SOC 2 Type2**, **ISO/IEC 27001**



Compatibility tested with:





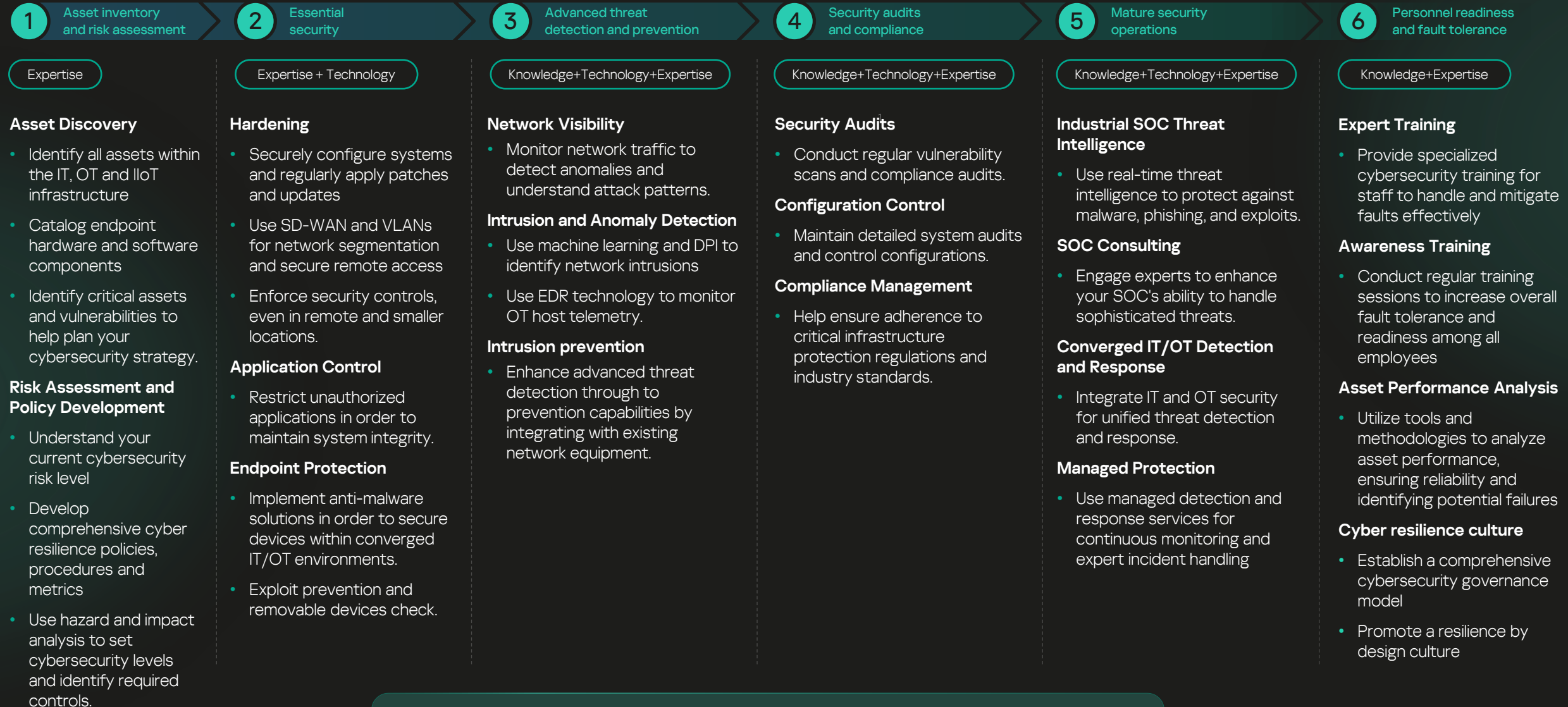
>130 systems from 50+ vendors

Kaspersky Security Awareness and Expert Trainings

Solution designed to empower employees with essential cybersafety skills, promoting compliance with the requirements of the NIS 2 Directive

Read more about NIS 2 Directive and our products' compliance

Cyber Resilience with Kaspersky OT Ecosystem



Learn more about Kaspersky comprehensive approach to cybersecurity at all levels



Kaspersky experience in O&G

10+ years

of experience in O&G sector

138 projects

completed

12%

Protecting O&G companies with 12% of a total world production

60 companies

already under protection

Kaspersky OT CyberSecurity Ecosystem provides comprehensive industrial infrastructure protection for oil and gas enterprise. The platform is capable of detecting and responding to complex attacks centrally across the entire industrial network.

Typical customer case studies

- Helping to integrate corporate and industrial sectors into a unified, secure infrastructure with end-to-end security
- Centralizing all information security functions in geographically distributed networks to improve visibility of infrastructure activities and more effective use of human resources
- Assisting in the protection of systems built on outdated and unsupported operating systems with obsolete and scan-sensitive security system equipment
- Ensuring stable operation of the information security system under high availability requirements and resource consumption constraints

Why oil and gas companies choose Kaspersky

- Deep expertise in cyberthreats with constant monitoring of the threat landscape
- Information security systems built with consideration for the latest digital trends
- Assistance in meeting regulatory requirements
- No impact on the industrial workflow and device operation
- Product offerings which regularly participate in tests by international research institutes and win a record number of first places
- Solutions tested for compatibility with the products of the leading vendors



>80%

of all IEC 62443-3 security requirements covered by Kaspersky



242

systems from 57 ICS suppliers have been certified

Successful case studies from O&G Industry

Over the past 10 years of experience Kaspersky has:



Protected major integrated holding with **80 fields** located thousands of kilometers apart



Ensured the security of a region-unique terminal with a capacity of **205,000 tons** of petrochemical products, providing transportation control from rail to sea



Implemented a cybersecurity system at large gas transportation enterprise, which is part of the critical infrastructure and supplies gas to more than **20 million** people



TOP-5 largest O&G companies in Russia

- APCS protection using Kaspersky Industrial CyberSecurity solution
- Completed special "Industrial Cybersecurity Awareness" training based on real experience in investigating industrial cyber incidents

12 years
working
with Kaspersky

[Learn more](#)



RN-BashNIPIneft
Major upstream R&D center

The centralized information security system is built on the entire ecosystem of Kaspersky products, ensuring strong protection against cyber threats and the optimized workload for cybersecurity personnel.

[Learn more](#)



One of the largest oil refineries in the world

Opting for Kaspersky Industrial CyberSecurity (KICS) XDR resulted in:

- Stronger refinery information security
- Better cybersecurity and production process monitoring and analytics
- Rapid detection of, and response to, potential threats

[Learn more](#)

SIA VARS

The only petrochemical terminal in the Baltic region

Using Kaspersky Industrial CyberSecurity solution to ensure reliable protection of automatic line control systems for the transshipment and storage of chemical products

[Learn more](#)

www.kaspersky.com

© 2024 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.

Manage your security with Kaspersky
and become a partner

Contact us and take part in our global customer conference

[Learn more](#)



#kaspersky
#bringonthefuture