Kaspersky OT Cybersecurity

Vertical offering
for next-gen stadiums,
smart venues and commercial buildings

Industry overview

68%

of the world's population will live in urban areas by 2050[1]

78%

of the world's energy is consumed by cities[2]

CAGR 30.4%

The global smart buildings market is expected to grow at a CAGR of 30.4% between 2025 and 2030[3]

Demographic shifts, rising urban density and migration patterns demand more efficient infrastructure and optimized spaces for concentrated populations.

Next-gen urban facilities such as connected venues and smart commercial buildings are emerging as solutions that address this complex web of demographic, economic and social trends and challenges.

Key objectives of digital transformation

- Improved asset performance and cost reduction
- Decarbonization and efficient energy usage
- Better safety and reduced security risk
- Outstanding visitor experience and well-being

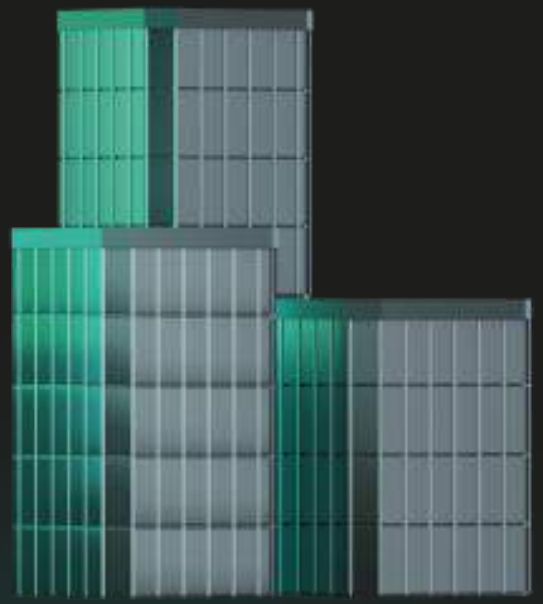
Builders, owners and operators of connected venues and buildings are accelerating digital transformation to enhance efficiency, reliability and sustainability. Expanding next-gen infrastructure demands ongoing cyber resilience to ensure operational continuity and customer trust.

Key digital transformation trends and technologies

- Increased connectivity across multiple sites
- IoT-enabled engineering systems (lighting, HVAC, elevators & escalators)
- Precise, ML-based microclimate control
- Digital twin technologies for crowd management
- High-density Wi-Fi and 5G infrastructures
- Drones and robotics for maintenance and proactive event management
- Motion control for transformable playing surfaces and retractable roofs
- Convergence of cloud, IT and OT systems
- Virtual/augmented/extended reality for enriched visitor and tenant experiences

(1) According to the UN Department of Economic and Social Affairs
(2) According to the UN Climate Action
(3) According to "Smart Building Market" report by Grand View Research

Digital transformation



From concrete and steel to controllers and sensors

Next-gen venues and connected buildings are no longer just physical structures made of concrete and steel – they're highly networked, asset-intensive, intelligent systems. Cloud-based command and control centers now oversee everything from HVAC and lighting to smart grids and ML-enabled operations across multiple sites.

Efficiency brings exposure

As venues and buildings evolve to technologically-enhanced environments, they become more exposed to cyber risks. For owners and operators, this underscores a stark reality: robust cybersecurity is a prerequisite for achieving strategic business goals.

According to Kaspersky ICS CERT, the building automation sector is the second most frequently targeted by cyberattacks worldwide.

1.35
times higher

The number of attacked ICS endpoints in building automation and construction industries, compared to global averages[2]

Highlight: FIFA World Cup 2022

The digitalization shift was on full display during the FIFA World Cup in Qatar in 2022. The tournament introduced the world's first 'connected stadium' concept where all eight stadiums, each housing hundreds of controllers, thousands of edge devices and a digital twin, were integrated into a single cloud management platform and SOC.

8
connected stadiums

>5 billion
people engaged worldwide[1]

500
controllers

50,000
edge devices

(1) According to "FIFA World Cup Qatar 2022™ in numbers" report
(2) According to "Threat landscape for industrial automation systems. Regions" Q1-Q2 2025 report by Kaspersky ICS CERT

Digital transformation

Trends and technologies

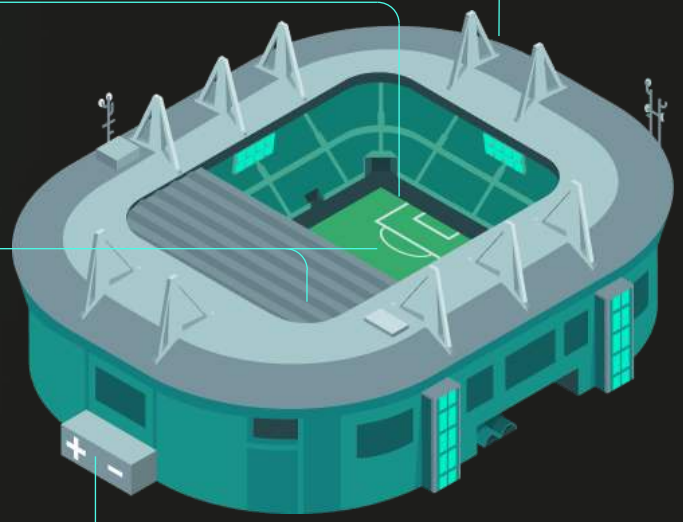
Network-centric stadium

DALI-2/D4i floodlight network
- Flicker-free IoT-ready luminaires
- Application controllers

ML-based pitch condition monitoring
- Vibration sensors and linear encoders
- Multispectral and hyperspectral cameras

Transformable surface and roof
- VFD-controlled bogies
- Laser alignment sensors
- Regenerative braking
- Growth chamber with precise microclimate control

Grid-tied BESS for peak-shaving
- Advanced thermal and state of charge management
- Solar to BESS converters
- LFP batteries



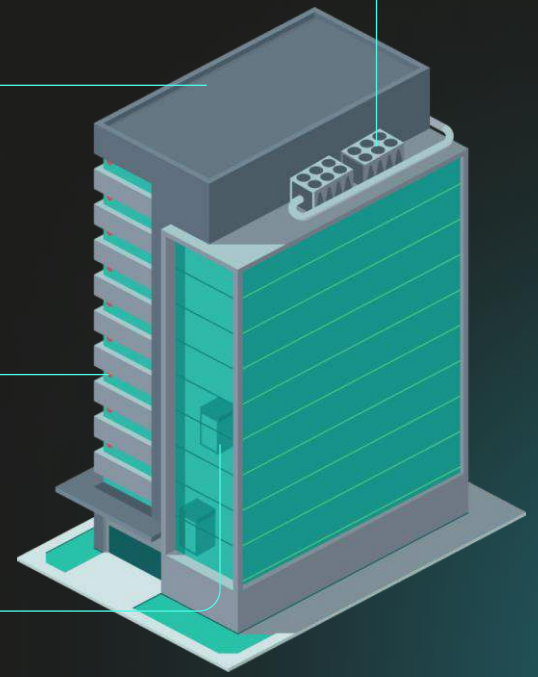
Smart and connected building

IoT-enabled smart HVAC
- DOAS
- VRF systems
- DDC controllers

Multi-operators 5G, Wi-Fi 6/6e/7
- High-performance APs for ultra-high density areas
- Location analytics & real-time positioning
- AI-driven self-optimizing Wi-Fi

DALI-2 emergency lighting network
- DALI/KNX gateways
- Application controllers
- Emergency lighting control gear

Internet of Elevators and Escalators
- IoEE cloud
- IoEE gateways
- Advanced destination dispatching



Convergence of physical-digital risks

Modern connected venues and stadiums are cyber-physical ecosystems: digital and physical systems are tightly integrated across HVAC, lighting, elevators, broadcast infrastructure, and even pitch management. This creates hybrid risks, where cyber incidents can trigger physical harm or disruption, and physical actions can undermine digital defenses.

How Kaspersky helps :

Kaspersky Industrial CyberSecurity

Protects heterogeneous OT and IoT environments of large venues against cyber risks and delivers extensive situational awareness.

Kaspersky Machine Learning for Anomaly Detection

Provides AI-driven detection of atypical employee actions or equipment operations to identify human errors, targeted attacks or sabotage.

Kaspersky Automotive Secure Gateway

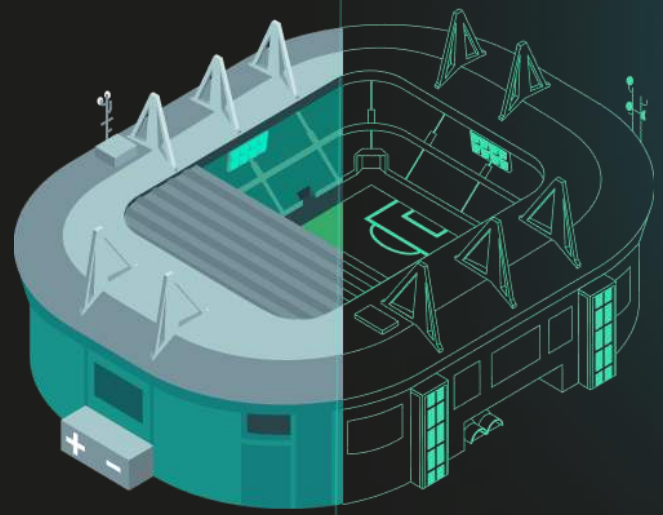
Enables secure and reliable communication between electronic units of a vehicle and between these units and the connected vehicle cloud.

Kaspersky Antidrone

Detects unauthorized drones entering the territory. “Friend-or-foe” mode allows your own or other approved drones to operate while ensuring intervention is directed only at illicit ones.

Physical safety risks

- HVAC equipment failure, health risks
- Blackout during a live event
  The Super Bowl blackout
- Elevator stoppage
- Connected rogue devices in the control room
- Physical drone payloads for cyber intrusion



Cybersecurity risks

- Altered HVAC settings
- Compromised lighting control system
- Tampering with motion-control system PLCs
- Malware introduced directly into the OT network
- Wireless signal spoofing

Converged threats

- Environmental manipulation
- Power sabotage
- Trapped people
- Physical intrusion
- Rogue signal injection

Exposure of OT/IoT infrastructures

In modern venues and commercial buildings, OT and IoT systems are no longer “behind the scenes”, so cybersecurity concerns shift focus to business continuity and safety risks. The top-down connectivity from enterprise cloud to physical machinery dramatically expands the attack surface and creates lateral movement paths to business-critical systems, necessitating proactive, multi-layered protection.

How Kaspersky helps:

Kaspersky Industrial CyberSecurity

Ensures network segmentation, detects threats and anomalies and offers safe response capabilities across OT endpoints and networks.

Kaspersky SD-WAN

Provides unified, centralized network security and management as well as real-time monitoring of distributed networks.

Kaspersky ICS Security Assessment

Helps identify security flaws in converged environments and provides actionable instructions for remediation

Enterprise / cloud layer

- Enterprise systems
- Cloud services

Building operations

- Event command and control
- AI-driven energy management
- Digital twin for crowd flow

Supervisory control

- Venue-level SCADA
- BMS/BAS
- EMS

Process control

- HVAC controllers,
- Elevator/escalator group PLCs
- DALI lighting control system

Physical equipment

- Central Utility Plant
- Generators
- LED boards

Supply chain compromise

Because smart buildings and venues today rely on complex ecosystems of vendors and third-party contractors, it's imperative to address external hazards. A supply chain attack can compromise trusted hardware before it even reaches the site, allowing adversaries to disrupt operations and compromise safety. Protecting against these attacks safeguards public trust, operational continuity, and the physical safety of thousands of people inside the venue.

How Kaspersky helps:

Kaspersky Industrial CyberSecurity

Detects network and process anomalies as well as unsafe activity to contain threats at an early stage. Enables continuous security audits.

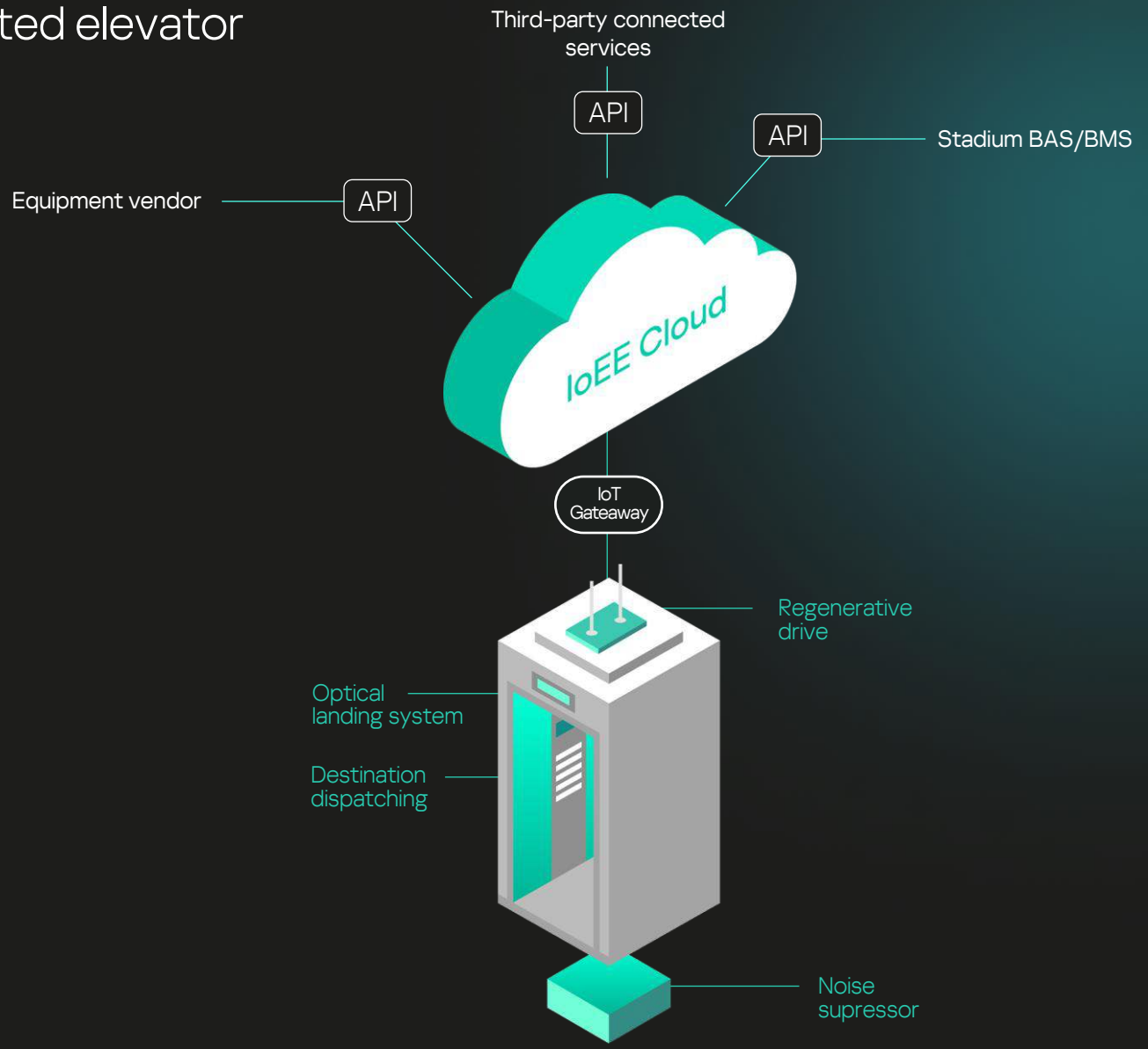
Kaspersky Next XDR Expert

Enables comprehensive visibility and robust protection for infrastructures where industrial and corporate segments overlap.

Kaspersky ICS Threat Intelligence

Delivers comprehensive understanding and evaluation of industrial cyberthreats and vulnerabilities targeting your organization.

Example of IoEE[1]-enabled connected elevator



(1) IoEE stands for "Internet of elevators and escalators", a networked ecosystem that includes sensors, controllers and gateways

Hybrid OT and cybersecurity skills gap

Modern connected buildings depend on deeply integrated OT, IoT and IT systems that require engineering and cybersecurity expertise. The shortage of professionals skilled in both domains may leave critical systems misconfigured, poorly monitored and vulnerable to cyber-physical threats. Without hybrid experts, organizations struggle to detect attacks that cross digital and physical boundaries, increasing risks to safety and operational resilience in smart facilities.

How Kaspersky helps:

Kaspersky Industrial CyberSecurity

Reduces staff workload by unifying operations and strengthening internal alignment across OT, SecOps and IT teams.

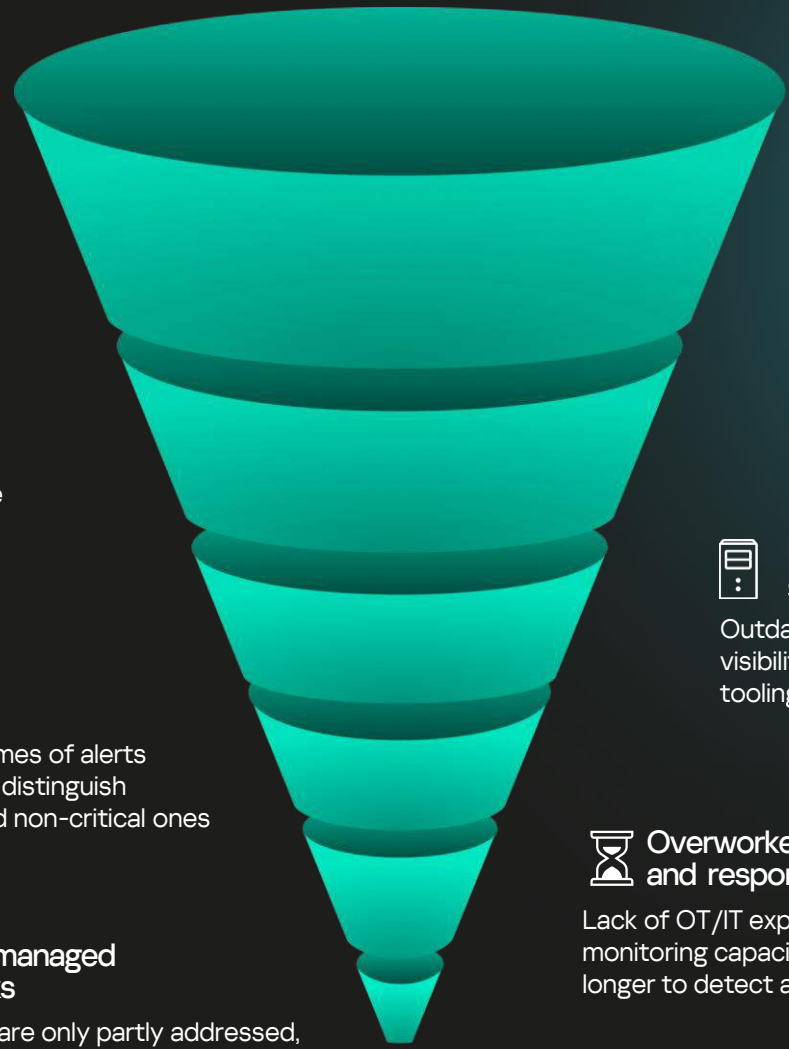
Kaspersky Security Awareness

Delivers the necessary OT cybersecurity knowledge and helps foster cybersafe behavior with interactive learning and attack simulations.

Kaspersky ICS CERT Training

Offers basic and advanced cross-functional training programs for staff, expanding their knowledge and empowering them with specialized hands-on skills.

1 in 5 confirmed cybersecurity incidents in industrial organizations took over a month to remediate[1]



Complex risk landscape

The evolving threat landscape and expansion of the attack surface across converged IT-OT environments increase risks

Fragmented vision and tool sprawl

Implementing separate tools to secure IT, OT and IoT environments results in more operational complexity

Legacy systems

Outdated platforms reduce visibility and control. Budget and tooling gaps slow coordination

Alert fatigue

Overwhelming volumes of alerts makes it difficult to distinguish between critical and non-critical ones

Overworked SOC teams and response delays

Lack of OT/IT experts limits monitoring capacity. Incidents take longer to detect and contain

Unmanaged risks

If threats are only partly addressed, hidden exposures remain unmonitored

(1) State of ICS/OT Security 2025, SANS

Advanced Persistent Threat (APT) groups

APT groups use long-term footholds to map process flows, maintenance habits and safety interlocks to craft precisely targeted, low-noise attacks that manipulate building automation, disrupt operations or compromise safety-critical systems. Comprehensive awareness of APT groups and their strategies is critical for cybersecurity professionals and business leaders, as not all high-profile threats are made known to the general public.

How Kaspersky helps:

Kaspersky Industrial CyberSecurity + Kaspersky Next XDR Expert

Used together, the KICS platform and Kaspersky Next XDR Expert provide unified IT-OT XDR capabilities and robust end-to-end protection against complex and persistent threats across modern converged, asset-intensive environments.

Kaspersky Managed Detection and Response

Continuously hunts, detects and eliminates threats – delivering all the key benefits of a SOC without having to establish one in-house

Kaspersky ICS Threat Intelligence

Increase the effectiveness of risk assessment, incident investigations and active threat searches with in-depth intelligence on APT tactics.

3/4 of BAS devices were locked out as a result of a cyberattack against a building automation engineering firm in Germany[1]

APT groups use a consistent, step-by-step approach to stay under the radar and make the attack hard to detect. The investigation data, threat actor profiles and technical data such as IoCs and custom detection rules are essential for fast and accurate threat response.

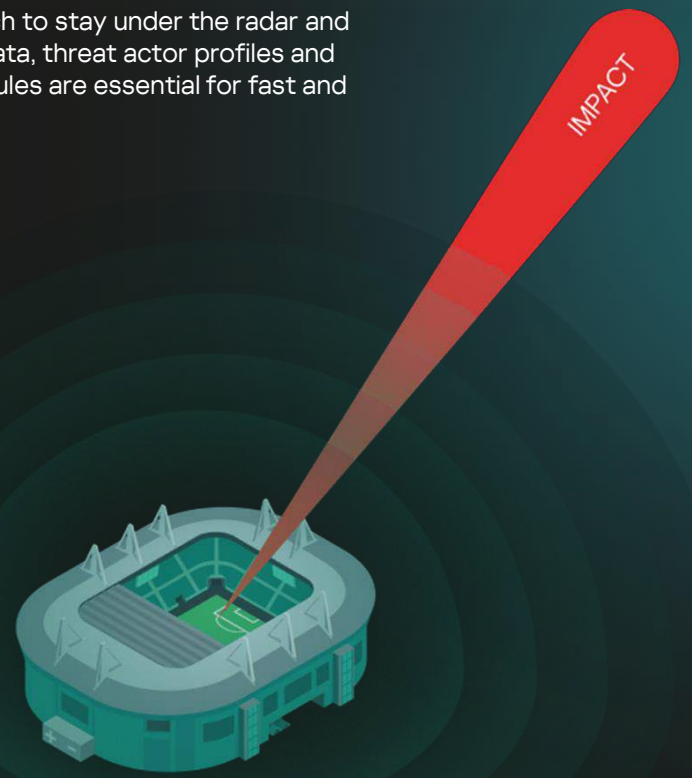
01 Establish initial access

02 Execute malicious code

03 Keep the footholds

04 Obtain contextual intelligence

05 Move laterally and hinder safeguards



(1) Lights Out: Cyberattacks Shut Down Building Automation Systems by Dark Reading

Cyber Resilience with Kaspersky OT Ecosystem

1 Asset inventory and risk assessment

Expertise

Asset Discovery

- Identify all assets within the IT, OT and IIoT infrastructure
- Catalog endpoint hardware and software components
- Identify critical assets and vulnerabilities to help plan your cybersecurity strategy

Risk Assessment and Policy Development

- Understand your current cybersecurity risk level
- Develop comprehensive cyber resilience policies, procedures and metrics
- Use hazard and impact analysis to set cybersecurity levels and identify required controls

2 Essential security

Expertise+Technology

Hardening

- Securely configure systems and regularly apply patches and updates
- Use SD-WAN and VLANs for network segmentation and secure remote access
- Enforce security controls, even in remote and smaller sites

Application Control

- Restrict unauthorized applications to maintain system integrity

Endpoint Protection

- Implement anti-malware solutions to secure devices within converged IT/OT environments
- Exploit prevention and removable devices check

3 Advanced threat detection and prevention

Knowledge+Technology+Expertise

Network Visibility

- Monitor network traffic to detect anomalies and understand attack patterns

Intrusion and Anomaly Detection

- Use machine learning and DPI to identify network intrusions
- Use EDR technology to monitor OT host telemetry

Intrusion Prevention

- Enhance advanced threat detection through prevention capabilities by integrating with existing network equipment

4 Security audits and compliance

Knowledge+Technology+Expertise

Security Audits

- Conduct regular vulnerability scans and compliance audits

Configuration Control

- Maintain detailed system audits and control configurations

Compliance Management

- To ensure adherence to critical infrastructure protection regulations and industry standards

5 Mature security operations

Knowledge+Technology+Expertise

Industrial SOC Threat Intelligence

- Use real-time threat intelligence to protect against malware, phishing, and exploits

SOC Consulting

- Engage experts to enhance your SOC's ability to handle sophisticated threats

Converged IT/OT Detection and Response

- Integrate IT and OT security for unified threat detection and response

Managed Protection

- Use managed detection and response services for continuous monitoring and expert incident handling

6 Personnel readiness and fault tolerance

Knowledge+Expertise

Expert Training

- Provide specialized cybersecurity training for staff to handle and mitigate faults effectively

Awareness Training

- Conduct regular training sessions to increase overall fault tolerance and readiness among all employees

Asset Performance Analysis

- Utilize tools and methodologies to analyze asset performance, ensuring reliability and identifying potential failures

Cyber Resilience Culture

- Establish a comprehensive cybersecurity governance model
- Promote a resilience by design culture

Learn more about Kaspersky's comprehensive approach to cybersecurity at every level

Cybersecurity Regulations

Cybersecurity regulations for public venues and connected buildings depend primarily on their designation as critical infrastructure. Those of national significance fall under some of the most robust regulatory regimes, requiring operators to blend governance, technical safeguards and rapid incident reporting.

- ISA/IEC 62433
- ISO/IEC 27001
- ISA99
- ISO 8102-20

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

- NCSC's Cyber Assessment Framework
- HSE OG86 (Cyber Security for IACS)

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

- UAE Cybersecurity Council Framework
- UAE IoT Security Standard
- DESC ICS/OT Security Standard

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

- National ICS Security Standard
- Qatar Cybersecurity Framework
- National Cyber Security Strategy

- CERT-In Directions
- NCIIPC Guidelines

- The Cybersecurity Act B.E. 2562
- NCSC notifications

- GB/T 30976.1-2014
- GB/T 22239-2019
- MLPS 2.0

- Cybersecurity Code of Practice for CII
- TR 111:2023
- TR 64:2018

- National Cybersecurity Policy
- ANATEL Act 77
- Decree No. 9573/2018

- Programa Nacional de ICIC
- Administrative Decision 641/2021

Kaspersky Industrial CyberSecurity

KICS and its core technologies are subject to industry-leading audits: IEC62443-4-1, ISO27001, SOC2 type 2.

Compatibility tested and proven with:

Schneider Electric · SIEMENS · EMERSON · Honeywell

200+ systems from 50+ vendors

Full list of compatibility statements

Validating a cybersecurity solution for compatibility with industrial automation and control systems (IACS) vendors is essential for ensuring security and operational continuity.

Without thorough compatibility assessment, cybersecurity products risk introducing latency, generating unsafe traffic, or disrupting IACS operations.

The testing ensures accurate parsing of proprietary protocols, reliable asset discovery, stable passive monitoring, and safe active response behaviors.

Looking for a technological alliance?

Our anti-malware technologies are integrated into products from over 150 leading vendors worldwide. Join our mission to build a safer future.

Discover the benefits of partnership

Kaspersky experience and case studies

The Nuevo Hospital de Toledo

The Nuevo Hospital de Toledo is the largest, most advanced healthcare facility in Castilla-La Mancha, Spain, serving over 435,000 residents. It manages all non-care services for the campus, including maintenance of the building and its ICT infrastructure.

Read the story

MODON

MODON is the Saudi Authority for Industrial Cities and Technology Zones. By integrating infrastructure, innovations and design, it fosters sustainable growth and creates smart, connected environments.

Read the story

Why choose Kaspersky

- Our unique team of experts work together across 5 Centers of Expertise, applying specialized knowledge and skills to tackle the most sophisticated and dangerous cyberthreats.
- Since 2013 Kaspersky products participated in 1022 independent tests and reviews. Our solutions were awarded 771 firsts and achieved 871 top-three finishes.
- We offer enterprise-grade customer support in over 200 countries, speaking your language and delivering world-class assistance from our team of certified engineers whenever and wherever you need it.

Don't miss the opportunity and join KICS Con

Lead the conversation or put your brand in the spotlight

Get together with hundreds of experts and industry players from around the world at the annual global Kaspersky Industrial Cybersecurity Conference to share insights and discuss cybersecurity insights and best practices .

Join KICS Con

www.kaspersky.com

MOST TESTED*
MOST AWARDED*
KASPERSKY PROTECTION
*kaspersky.com/top3

#kaspersky
#bringonthefuture