Kaspersky OT CyberSecurity

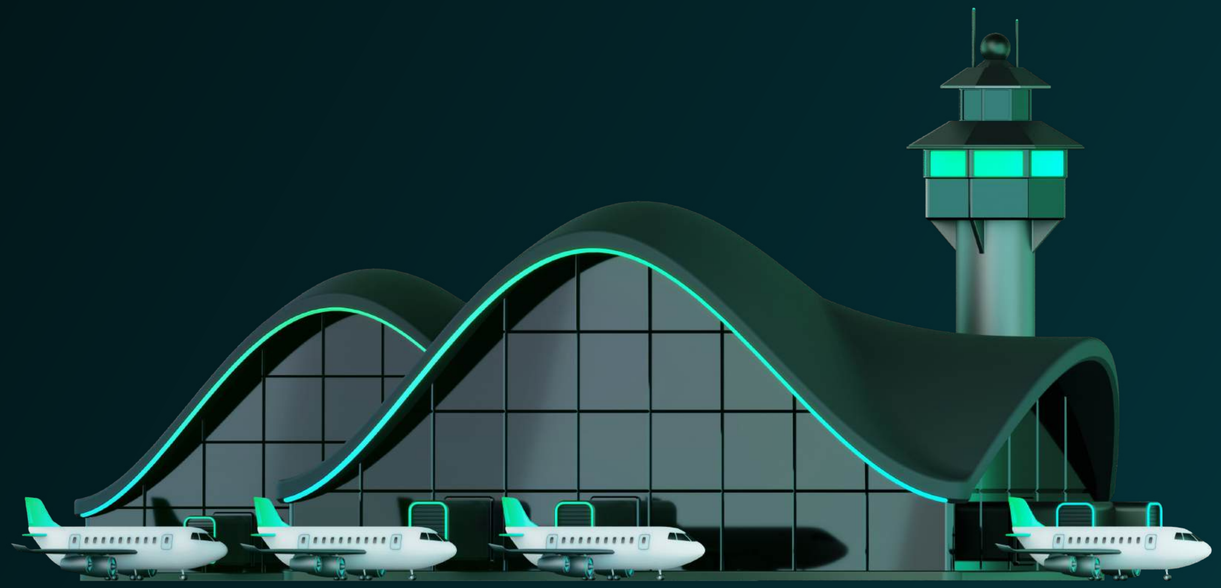
Vertical offering
for airport operators

kaspersky

Industry overview: Preparing for the future of civil aviation

12 billion travelers annually

According to projections by the International Civil Aviation Organization (ICAO), passenger volumes are expected to triple by 2050, potentially surpassing 12 billion travelers annually. This dramatic increase presents unprecedented commercial opportunities for airports, airlines, and aviation service providers.



However, with rapid growth comes heightened operational complexity across airport ecosystems, involving intricate coordination of **air traffic management (ATM), ground handling, passenger processing, cargo logistics, and facility management.** Concurrently, airports face an increasing number of threats due to expanding attack surface, elevating their exposure to cybersecurity risks that can disrupt critical aviation operations.

Key industry challenges impacting aviation cybersecurity

- Achieving net-zero carbon emissions targets through sustainable infrastructure upgrades compliant with international environmental and **ICAO** environmental protection guidance.
- Addressing acute cybersecurity skills shortages, especially in securing legacy OT systems alongside modern IoT-connected aviation technologies.

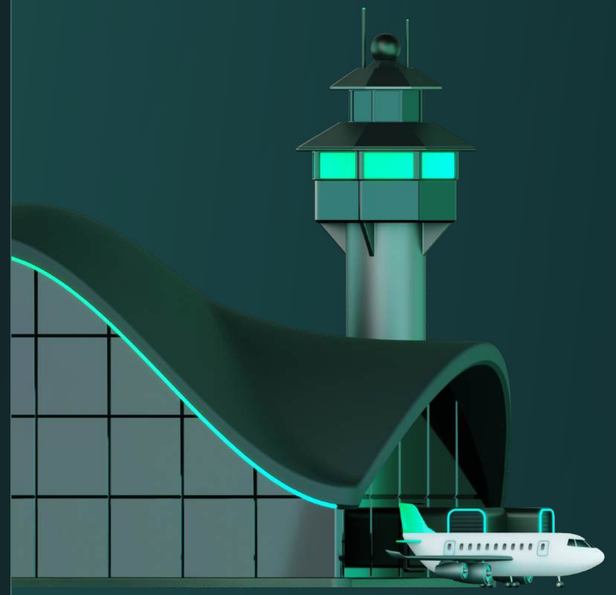
High stakes due to public visibility and regulatory oversight

Airport operations are subject to intense scrutiny from passengers, government agencies such as **FAA, EASA, TSA, and ICAO,** as well as cybersecurity regulators enforcing frameworks like **NIS2 and TSA Cybersecurity Directives.** Any operational disruption, system downtime, or data breach can result in rapid escalation of public concern, multi-agency investigations, regulatory sanctions, and significant financial penalties, in addition to damaging the airport's reputation.

Continued vigilance and proactive cybersecurity governance are essential for preserving safety, security, and passenger confidence throughout the aviation ecosystem.

Destination: Smart airport

The future of aviation lies in transforming airports into intelligent, interconnected hubs that deliver a comprehensive digital experience while ensuring operational safety and sustainability. Kaspersky supports this vision by enabling airports to embark on a comprehensive digital transformation journey that prioritizes a seamless passenger experience alongside robust cyber resilience.



Key elements of this smart airport vision include:

Zero-emission infrastructure designed to comply with international environmental standards and ICAO's environmental goals, reducing the airport's carbon footprint while maintaining operational efficiency.

Built **safe by design**, integrating cybersecurity into every layer of the airport's operational technology and IT systems, ensuring secure and resilient infrastructure from day one.

Seamless security checkpoints and screening processes, leveraging biometric identity verification and automated threat detection to accelerate passenger flow without compromising safety.

Deployment of **autonomous vehicles for airside and landside passenger transfers,** optimizing transit times and operational control with secure connected vehicle frameworks.

Implementation of **personalized, real-time flight information display systems (FIDS)** to enhance passenger communications and improve wayfinding throughout the airport.

Through these innovations and more, airports can achieve operational excellence, sustainability targets, and superior passenger satisfaction, all underpinned by a robust cybersecurity posture.

Threat landscape for airport systems

Impact	Consequences	Recent trends	Example
Ransomware Complete system lockdown affecting all airport operations	Flight cancellations, passenger stranding, financial losses	Targeting critical infrastructure with higher ransom demands, specifically designed to impact operational technology systems	**SamSam attack / $17 million* recovery cost (city-wide)** Atlanta Hartsfield–Jackson Airport *While not limited to the airport, the city of Atlanta's ransomware attack disrupted multiple services, including Wi-Fi at the world's busiest airport
DDoS attacks Service disruption of online systems and passenger services	Website downtime, booking system failures, passenger information delays	Coordinated attacks during peak travel periods to maximize disruption	**KillNet / Up to 12 hours downtime longest-known website outages** Simultaneous attack on 14 US airports' websites
Insider threats Data breaches and system compromise from authorized personnel	Passenger data exposure, operational disruption, regulatory penalties	Lateral movement attacks exploiting network vulnerabilities and privileged access abuse	**Pegasus Airlines / 23 mln files / 6.5 TB of data** Containing sensitive flight system data and personally identifiable information of crew and passengers was exposed. This happened because the company's system administrator made a mistake and didn't manage to properly configure the cloud environment, leaving sensitive data without password protection
Advanced persistent threats (APTs)	Compromised travel intelligence, operational disruptions, diplomatic tensions, and reduced public confidence in airport security infrastructure	Increasing attack sophistication, expanded targeting of interconnected systems, and escalation from pure espionage to hybrid intelligence disruption operations	APT groups establish long-term covert access to airport networks for intelligence gathering on passenger data, cargo information, and security protocols while maintaining disruptive capabilities
Supply chain attacks	Supply chain cyberattacks pose an existential threat to airport operations by completely bypassing traditional security perimeters and compromising critical aviation infrastructure beyond airport operators' direct control	These attacks represent one of the most dangerous cybersecurity threats for airports because the compromise originates from trusted partners, making detection nearly impossible until systems are already compromised and massive operational damage has occurred	Hundreds of cancelled and delayed flights at major EU airports were caused by a massive cyberattack on Collins Aerospace, a company specializing in the design, production, and maintenance of aviation systems. The hack disabled the vMUSE check-in and boarding software, which enables the shared use of counters for both check-in and boarding processes

Comprehensive protection for all airport systems

Boosting airport security within its core

- Ensuring critical business continuity*
  - Maintain operational continuity during security events
  - Provide protection without disrupting critical processes
  - Enable rapid recovery from security incidents
  - Support regulatory compliance requirements
- Legacy system protection
- Real-time monitoring of all critical systems, integrated into airport's existing AOC
- Automated threat detection and response capabilities
- Network segmentation to contain potential breaches
- Incident response coordination across all systems

* Proper protection should inherently guarantee the continuity of critical processes. Standard information security tools can themselves become causes of failures if not properly designed for operational environments.

Main challenges in airport cybersecurity

Integrating and securing legacy avionics support systems, SCADA, and Fieldbus networks alongside emerging IoT-enabled smart airport technologies.

Establishing network segmentation between critical operational segments such as air traffic control (ATC), baggage handling systems (BHS), and security screening systems to prevent cascading failures, while ensuring continued visibility and centralized management capabilities across all airport infrastructure.

Constantly evolving responses to regulatory mandates such as ICAO's Aviation Cybersecurity Strategy, EASA Part-IS, and TSA Cybersecurity Directive, which require flexible, scalable cybersecurity frameworks adaptable to dynamic airport operational needs and compliance audits.

Airports operate within highly complex and interconnected corporate and OT environments, where the malfunction or compromise of a single system can trigger cascading failures, severely affecting operational continuity. Moreover, many airports rely on legacy automation systems and specialized hardware that must be seamlessly integrated into modernized, digital ecosystems without compromising process integrity.

What we protect

Building management systems

HVAC, lighting, fire safety, and power distribution systems that maintain the airport environment

Back office

Airport operational database, airport management system, enterprise resource planning, passenger service system, integrated communication systems, business and financial systems

Autonomous electric vehicles for airside operations

Automated baggage tugs and loaders, autonomous passenger stairs and boarding ramps, smart electric utility vehicles

Ground support equipment

Telescopic passenger boarding bridge automation systems, programmable logic controllers for boarding bridges

Supply chain

Warehouses, fuel storages and stations, other third party systems

Air traffic control systems

Control tower and air traffic management systems, airfield control and monitoring systems

Airport management system and flight information display systems

Digital boards/displays

Internal transportation systems

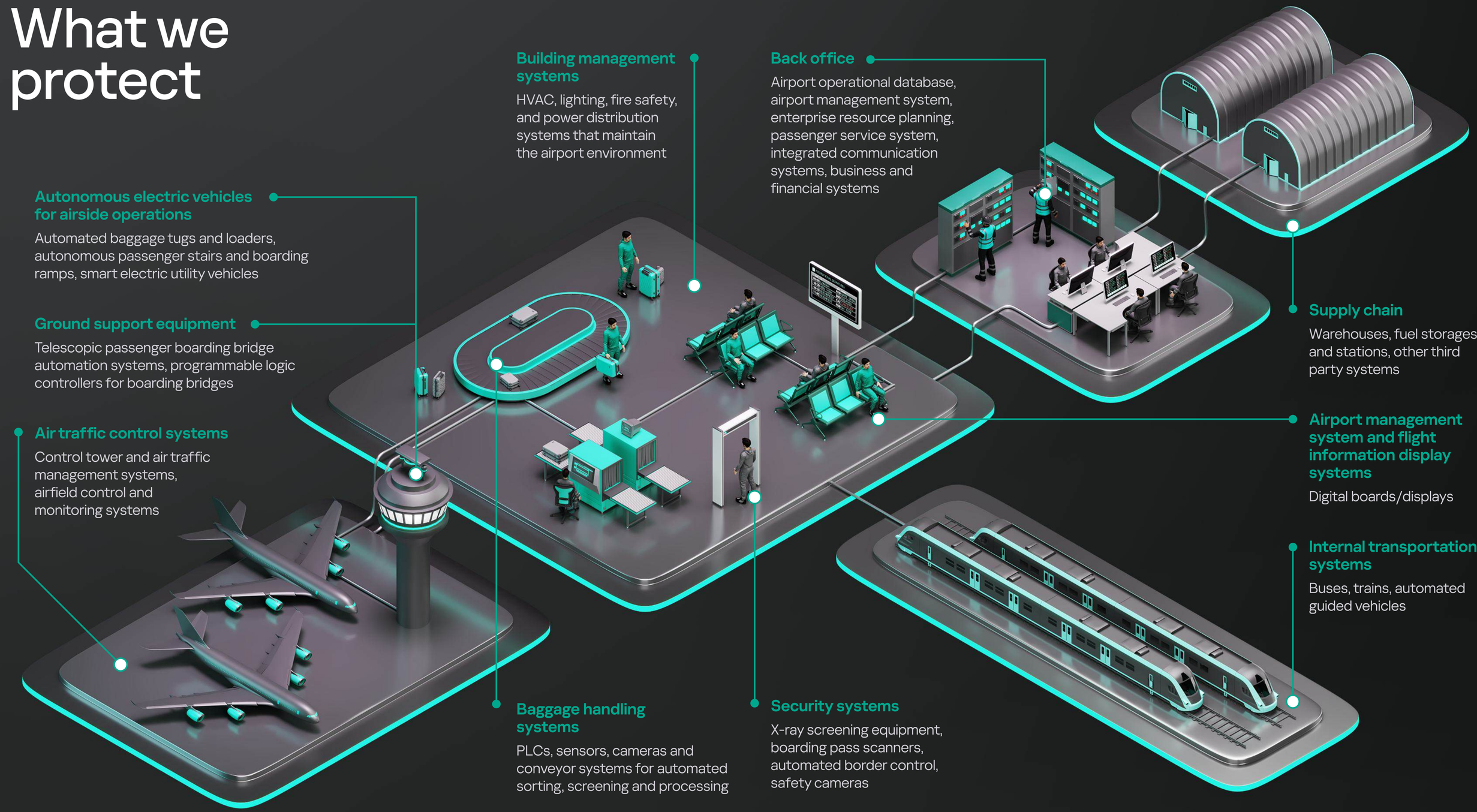
Buses, trains, automated guided vehicles

Baggage handling systems

PLCs, sensors, cameras and conveyor systems for automated sorting, screening and processing

Security systems

X-ray screening equipment, boarding pass scanners, automated border control, safety cameras



Comprehensive cybersecurity protection for airports

Protection for critical cyber-physical systems, automation and extended IoT

- Kaspersky Industrial CyberSecurity
- Kaspersky Industrial CyberSecurity for Nodes
- Kaspersky Industrial CyberSecurity for Networks

Airport network security

- Kaspersky SD-WAN
- Kaspersky Anti Targeted Attack

Managed or on-premise protection for classic Information systems and assets

- Kaspersky Next XDR Expert
- Kaspersky Hybrid Cloud Security
- Kaspersky Managed Detection and Response

Airport IT-OT SOC

- Kaspersky Unified Monitoring and Analysis Platform
- Kaspersky SOC Consulting
- Kaspersky Threat Intelligence

Maintenance, education, training and security awareness

- Kaspersky Security Awareness
- Kaspersky Professional Services

Managing supply chain and other risks

- Kaspersky Threat Intelligence
- Kaspersky Incident Response
- Kaspersky Security Assessment
- Kaspersky Compromise Assessment

Addressing key OT challenges with Kaspersky Cybersecurity

Domain	What are we protecting	Kaspersky capabilities	Product
Non-operational systems protection	Workloads in non-operational segments of airport (back office, supply chain, AMS, FIDS)	Combines strong endpoint protection and controls with the transparency and speed of EDR and the visibility and powerful tools of XDR, in straightforward product tiers	Kaspersky Next XDR Expert
		The solution mitigates security risks inherent in cloud environments, including malware, phishing and network threats, and reduces virtualization resource consumption	Kaspersky Hybrid Cloud Security
Operational technologies protection	Critical cyber-physical systems, controllers and IoT (air traffic control and airfield systems, BHS, BMS, security)	• Comprehensive asset inventory • Real-time monitoring and threat detection • OT XDR platform • Automated vulnerability management • Compliance audit	Kaspersky Industrial CyberSecurity
Network protection	Network protection and segmentation between IT and OT networks of airport	A comprehensive solution that protects against sophisticated cyberthreats with network sandboxing and advanced NDR	Kaspersky Anti Targeted Attack
		Kaspersky SD-WAN builds fault-tolerant, scalable and secure networks with unified management. The solution allows you to use diverse communication channels, rapidly connect new locations with a zero-touch experience, optimize costs and cloud connections	Kaspersky SD-WAN
Access control and security for supply chain	Securing and preventing unauthorized access to critical systems	Cyber immune thin client to secure remote access to airport systems	Kaspersky Thin Client
Security operation center	Unified solution to implement the ISMS policies by monitoring, detecting, and reporting on security events	High-performance next-generation SIEM solution for centralized collection, analysis and correlation of information security events from multiple sources — enabling fast detection and response to cyber incidents. It's a critical technology for any organization building its own SOC	Kaspersky Unified Monitoring and Analysis Platform Kaspersky Threat Intelligence
Bridging the workforce gap	Solving airport staff shortage	Round-the-clock managed protection against cyberthreats and sophisticated attacks that traditional automated security measures miss	Kaspersky Managed Detection and Response
		Kaspersky experts deliver tailored support to enhance infrastructure protection and build resilience against sophisticated cyberthreats	Kaspersky Professional Services
Education and awareness	Employee training and awareness	Comprehensive set of training programs designed to strengthen your IT security team's skills, enabling them to mitigate your organization's risk and respond effectively to incidents	Kaspersky Cybersecurity Training

Cyber resilience with the Kaspersky OT CyberSecurity

Learn more about Kaspersky's comprehensive cybersecurity approach

Inventory and assets

EXPERTISE

Network Asset Discovery

- Identify all hardware and software assets within the OT infrastructure
- Create a detailed inventory to plan your cybersecurity strategy

Endpoint Inventory

- Catalog hardware and software components
- Identify critical assets and vulnerabilities with an up-to-date inventory

Policy Development

- Develop comprehensive policies and procedures
- Establish cybersecurity levels and identify required controls with hazard and impact analysis

Essential security

EXPERTISE

OS Hardening

- Configure systems securely; apply patches and updates regularly
- Implement additional controls
- Prevent exploits and check removable devices

Application Control

- Maintain system integrity by restricting unauthorized applications

Endpoint Protection

- Implement anti-malware to protect devices across ICS and OT environments

Advanced threat detection, audits and compliance

KNOWLEDGE+TECHNOLOGY+EXPERTISE

Network Visibility

- Monitor network traffic to detect anomalies and understand attack patterns

Threat and Anomaly Detection

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

Security Audits

- Conduct regular vulnerability scans and compliance audits
- Maintain detailed system audits and control configurations

Compliance Management

- Ensure compliance with regulatory requirements and industry standards

Network segmentation

KNOWLEDGE+TECHNOLOGY+EXPERTISE

Intrusion Prevention

- Boost threat detection and prevention through integration with existing network infrastructure

Restricted Data Flow

- Optimize segmentation and data flow with SD-WAN and VLANs
- Enforce security controls even in remote or smaller locations

IoT Controls

- Implement security controls visibility with advanced secure-by-design gateways and protocols for IoT devices

Remote Access

- Control remote access with thin clients and secure gateways

Mature security operations

KNOWLEDGE+TECHNOLOGY+EXPERTISE

Industrial SOC Threat Intelligence

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

SOC Consulting

- Engage experts to strengthen 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

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

Fault tolerance and readiness

TECHNOLOGY

Expert Training

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

Awareness Training

- Conduct regular training sessions to increase organization-wide awareness and readiness

Asset Performance Analysis

- Apply tools and methodologies to analyze asset performance, ensure reliability and detect potential failures

Key capabilities of Kaspersky solutions

Continuous monitoring and asset inventory

24/7 situational awareness with real-time monitoring integrated into the airport operations center (AOC) and security operations center (SOC)

Comprehensive threat protection

Automated detection and response to cyber threats both in operational and non-operational IT networks of airport

IT-OT network segmentation

Network micro-segmentation and zone-based architecture aligned with IEC 62443 standards to contain lateral threat propagation between IT and OT domains

Employee training and awareness

Particular attention is given to training internal security teams through specialized courses in incident response, malware analysis, and digital forensics. This approach enables organizations not only to receive expert assessment of their security systems but also to develop internal competencies for independently countering modern cyber threats

Incident response

Incident response orchestration tools for cross-system coordination ensuring swift mitigation of potential cascading incidents

Cyber-physical security

Robust protection measures for cyber-physical systems including legacy and modern PLCs and IoT that remain critical to airport safety and reliability, respecting strict uptime and availability SLAs

Risk-based vulnerability management

Risk-based approach to vulnerability assessment and patch management

www.kaspersky.com

Secure critical airport operations with Kaspersky

Contact us for product information, demos or answers to your questions

Contact us

#kaspersky
#bringonthefuture