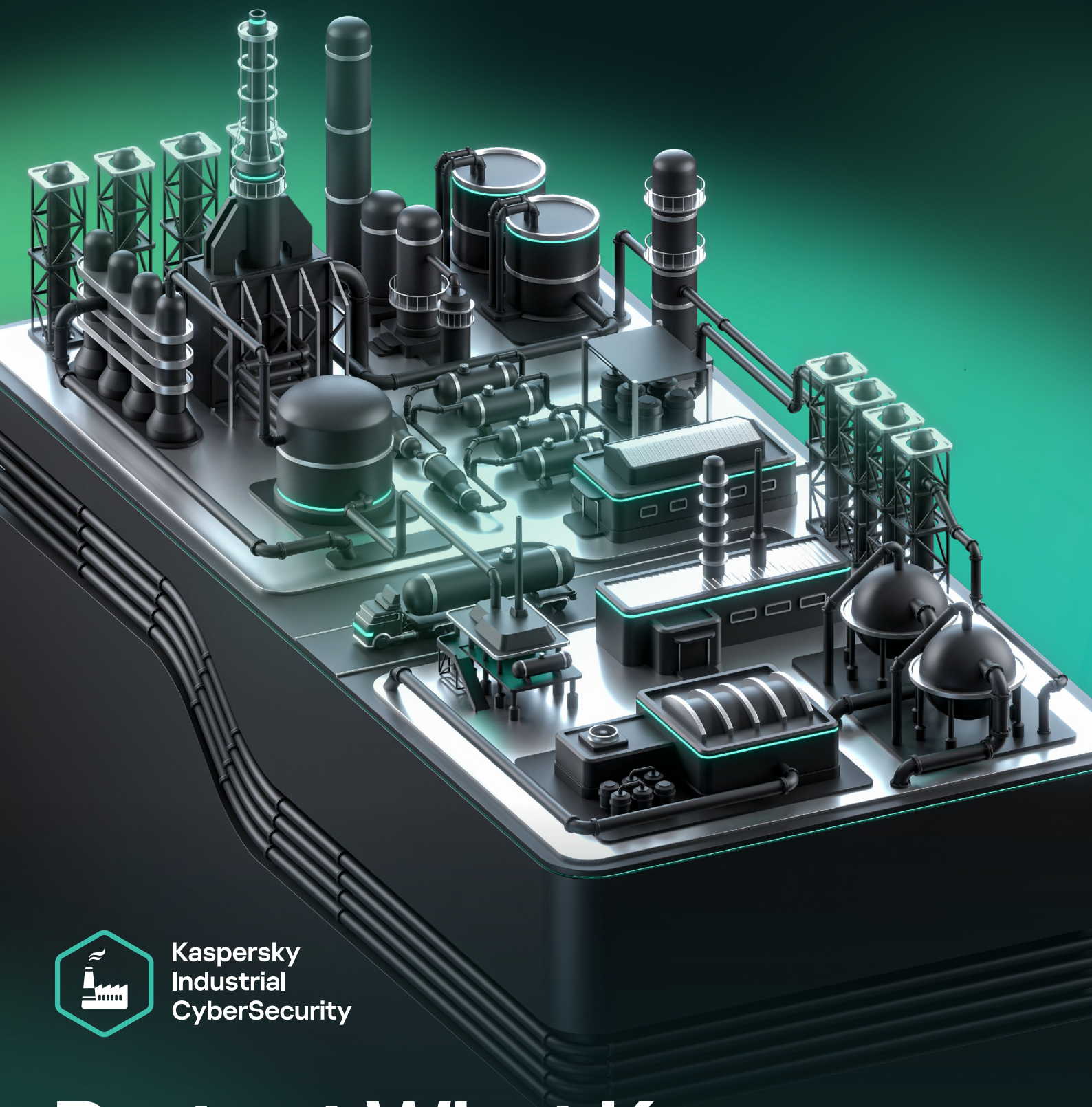


kaspersky



Kaspersky  
Industrial  
CyberSecurity

# Protect What Keeps the World Running

# 360° situational awareness and risk exposure control for critical infrastructure

Kaspersky Industrial CyberSecurity (KICS) is a purpose-built platform delivering multi-layered protection for operational technology (OT) environments. It ensures continuity of technological process and availability of control systems.



## Key business outcomes



Unify workflows and strengthen internal alignment across OT, SecOps, IT and business



Get ahead in digital transformation and embrace Industry 4.0 innovations securely, without exposing critical processes



Gain the advantages of data sovereignty and transparent ownership costs



Simplify internal, regulatory and industry-specific compliance journey



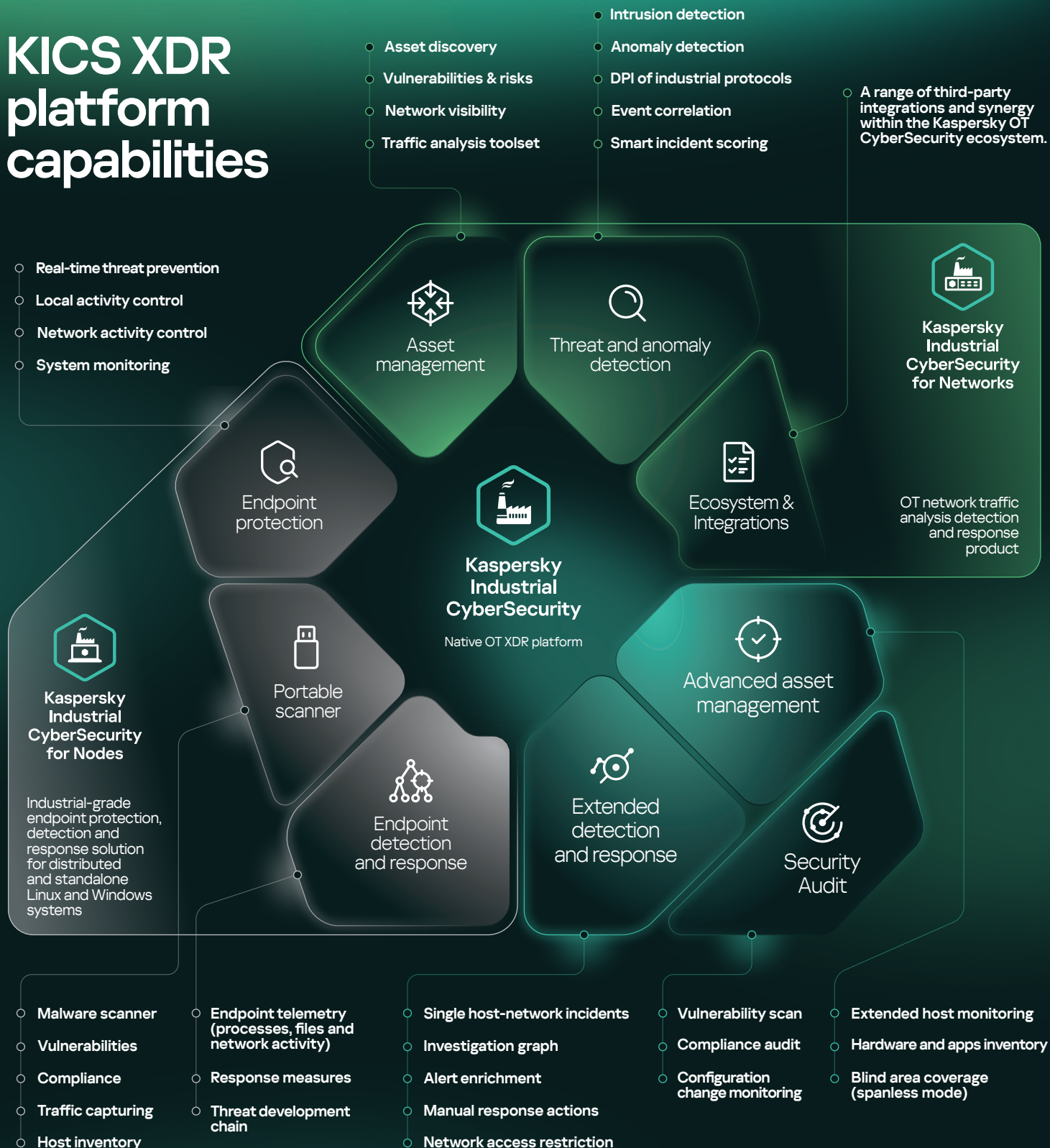
Adapt to evolving cyberthreats with a future-proof, scalable solution



Benefit from seamless integration with Kaspersky's best-in-class IT cybersecurity portfolio



# KICS XDR platform capabilities



## Operational benefits

### Low footprint

With modular deployment and tunable resource consumption, KICS does not impact system performance or process continuity, and also prevents software bloat.

### Compatibility

Over 125 versions of Windows and Linux supported and more than 200 IACS systems and devices tested guarantee compatibility with your existing infrastructure.

### Native integration

KICS for Nodes and KICS for Networks seamlessly work together to provide frictionless integration, centralized management and extended cross-product capabilities.

# Solution architecture and use cases

## Advanced asset management with AI profiling

Identify all connected devices and their interactions with asset discovery toolset and ultimate network visibility to take control over shadow infrastructure, leaving no unknown devices in your OT environment.

## Extended detection and response

Detect malicious or unsafe activity and contain threats before they impact process, with detects for 5000+ network attacks, DPI for 50+ industrial protocols and safe response options.

## Continuous security audit

Gain comprehensive security posture awareness across distributed, air-gapped and highly sensitive isolated environments with 3100+ pre-defined audit rules and 1300+ OVAL vulnerability tests.

### 3 Business & enterprise

Security operations center



Kaspersky Next XDR Expert

### 2 Monitoring & control



Kaspersky Industrial CyberSecurity for Nodes

Site supervisory control



agent-based asset inventory



hardware inventory

security audit

The unparalleled expertise powering our portfolio

Expertise Centers



[Learn more](#)

Installation-free KICS for Nodes portable scanner for isolated systems and bring-in devices

Standalone equipment



### 1 Automation & protection



Kaspersky Industrial CyberSecurity for Networks

KICS for Networks passively ingests network traffic from:

- Own network sensors
- SD-WAN collectors
- Endpoint agents
- Portable scanner

passive monitoring (SPAN)

network response

agentless polling of network devices

Substation automation system



active polling of OT assets

Main process control system



endpoint response



alerts from hosts and network



Secondary remote sites



OVAL-based configuration control

compliance audit via active polling or passive monitoring

### 0 Technological process



## Integration cases



Kaspersky Next XDR Expert

Used together, the KICS Platform and Kaspersky Next XDR Expert provide unified IT-OT XDR capabilities and complex protection for converged infrastructures.



Kaspersky Machine Learning for Anomaly Detection

Integration with the Machine Learning for Anomaly Detection (MLAD) solution enables KICS for Networks to send telemetry for analysis and receive alerts for detected anomalies.



Kaspersky SD-WAN

KICS can leverage the SD-WAN infrastructure to collect industrial traffic, provide centralized monitoring and protect distributed industrial objects and systems.



Kaspersky Industrial CyberSecurity

[Learn more](#)