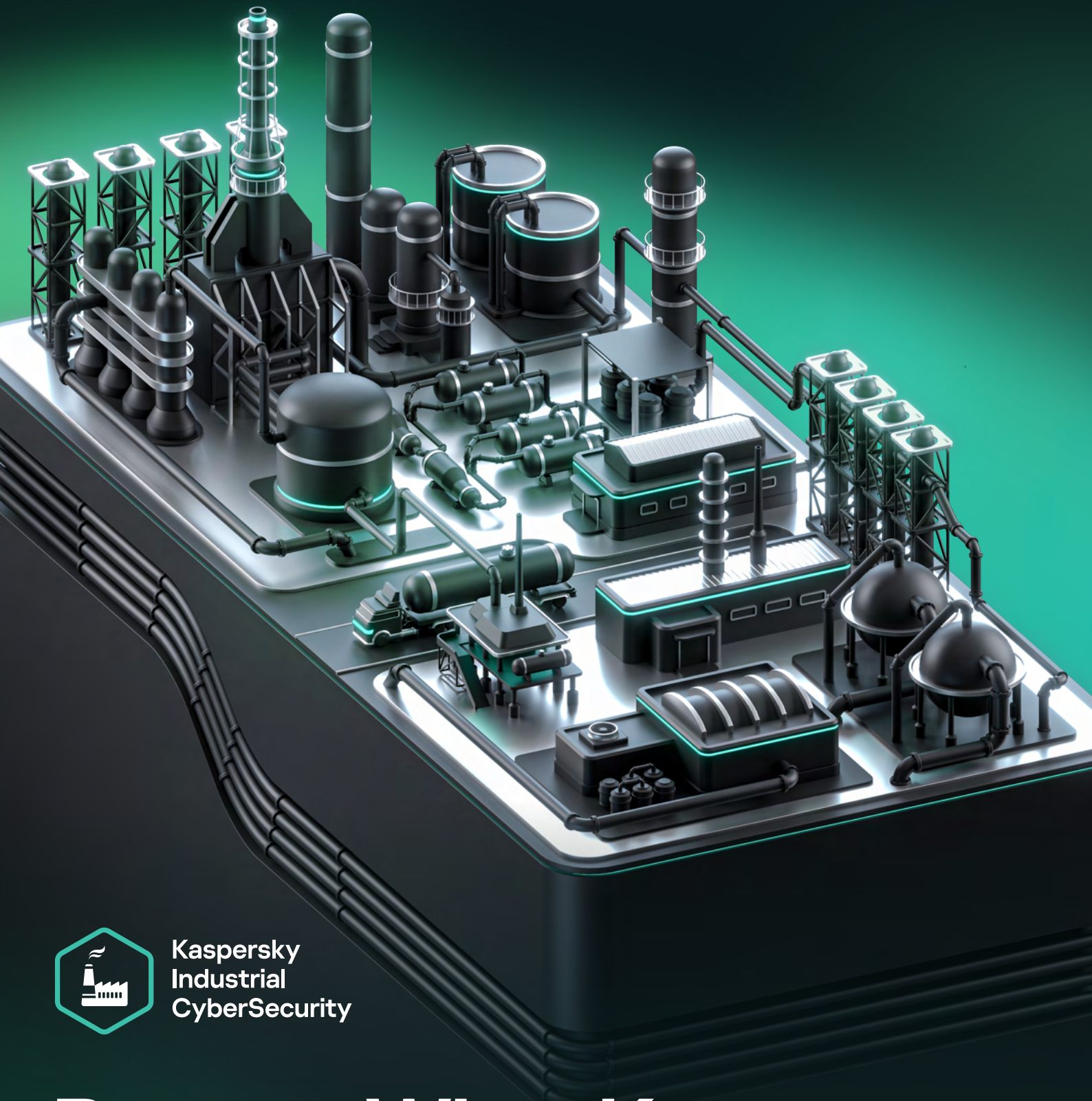
kaspersky



Kaspersky
Industrial
CyberSecurity

Protect What Keeps the World Running

kaspersky

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

kaspersky

KICS XDR platform capabilities

- Asset discovery
- Vulnerabilities & risks
- Network visibility
- Traffic analysis toolset

- Intrusion detection
- Anomaly detection
- DPI of industrial protocols
- Event correlation
- Smart incident scoring

- A range of third-party integrations and synergy within the Kaspersky OT CyberSecurity ecosystem.

- Real-time threat prevention
- Local activity control
- Network activity control
- System monitoring

- Malware scanner
- Vulnerabilities
- Compliance
- Traffic capturing
- Host inventory

- Endpoint telemetry (processes, files and network activity)
- Response measures
- Threat development chain

- Single host-network incidents
- Investigation graph
- Alert enrichment
- Manual response actions
- Network access restriction

- Vulnerability scan
- Compliance audit
- Configuration change monitoring

- Extended host monitoring
- Hardware and apps inventory
- Blind area coverage (spanless mode)

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.

kaspersky

Solution architecture and use cases

Advanced asset management with AI profiling

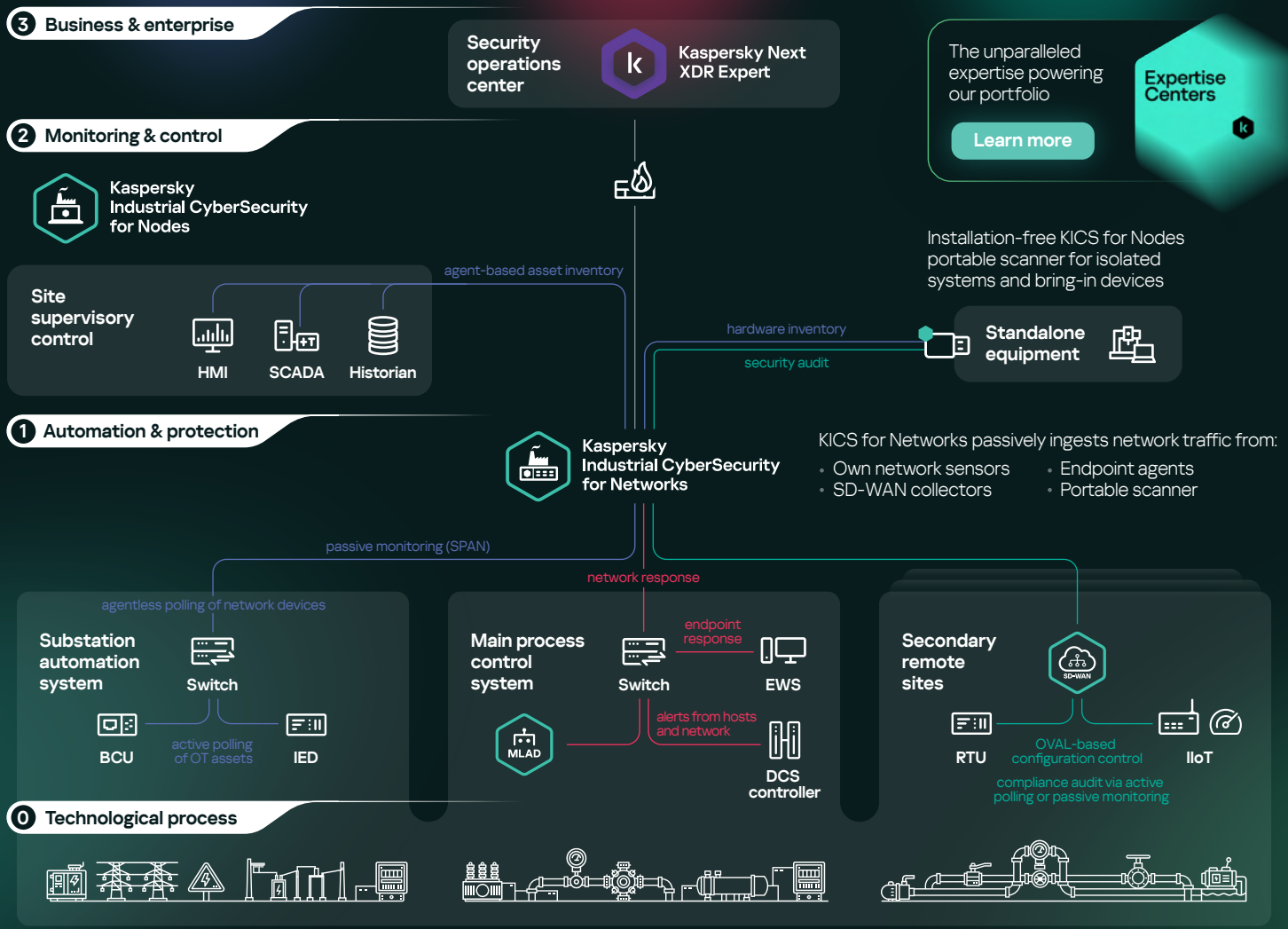
Identify all connected devices and their interactions with asset discovery toolset and ultimate network visibility to take control over shadow infrastructure, leaving no unknown devices in your OT environment.

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.



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.com

Discover more on Kaspersky technologies, knowledge and expertise for protection against cyber-physical threats at all levels of OT systems and networks

Kaspersky Industrial CyberSecurity

Learn more