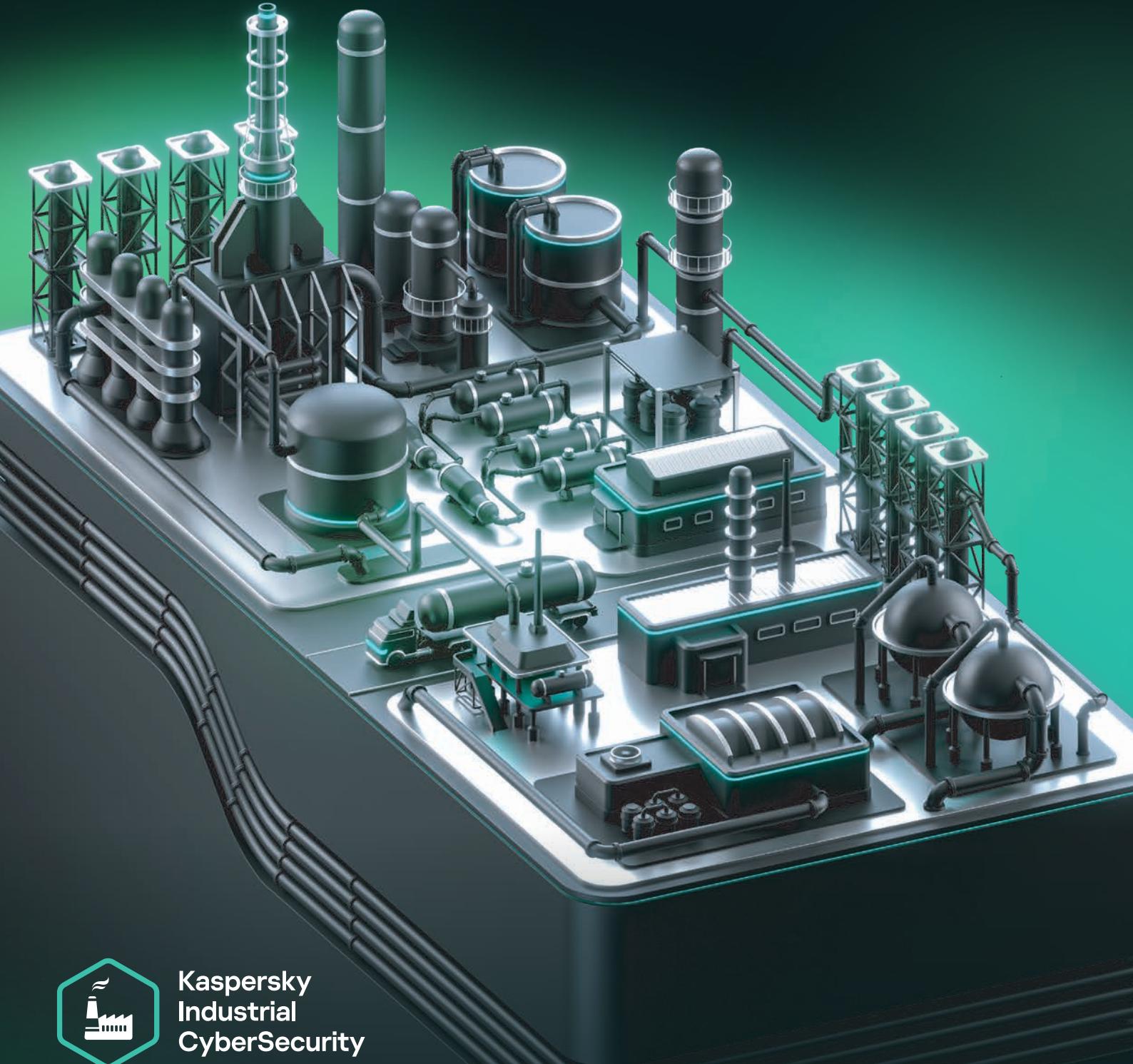


kaspersky



Kaspersky  
Industrial  
CyberSecurity

**Protezione per ciò che  
fa funzionare il mondo**

# Consapevolezza della situazione a 360° e controllo dell'esposizione al rischio per le infrastrutture critiche

Kaspersky Industrial CyberSecurity (KICS) è una piattaforma appositamente progettata per offrire protezione multilivello per gli ambienti OT (Operational Technology). Garantisce la continuità del processo tecnologico e la disponibilità dei sistemi di controllo.

The screenshot displays the Kaspersky Industrial CyberSecurity (KICS) platform interface. On the left, there's a navigation sidebar with options like Dashboard, Assets, Network Map, Topology Map, Sessions, Process Control, Security Audit, Events, Risks, Reports, and About. Below this is a circular 'Device by Security state' summary with values: Critical (416), Warning (121), and Normal (89). The main area features several dashboards:

- Dashboard:** Shows CPU (3%), RAM (50%), and Occupied on disk (80%) usage.
- Traffic by protocols:** A chart showing network traffic distribution across various protocols.
- Device by Status:** A circular summary showing 416 devices in total, broken down into Unauthorized (13), Authorized (353), and Archived (50).
- Top application by number of events:** A bar chart showing the top applications based on event count.
- Risk scores:** A donut chart showing risk levels: Low (259), Medium (822), and High (5120).
- GOOSE-communications statuses:** A circular summary showing 296 GOOSE communications, with counts for Online (234), Offline (12), and Unknown (50).
- Equipment:** A detailed view for PLC02-TM02 showing hardware and software specifications, uptime, traffic, and tags.
- Configurations:** A comparison of configurations for PLC02-TM02, showing changes over the last 35 days.
- Network Interaction Map:** A diagram showing the connections between PLC01-TM01 (174.42.2) and PLC02-TM02 (174.42.3).

## Vantaggi chiave per l'azienda



Unificare i flussi di lavoro e rafforzare l'allineamento interno tra OT, SecOps, IT e azienda



Avanzate nella trasformazione digitale e abbracciate le innovazioni del settore 4.0 in modo sicuro, senza esporre i processi critici



Ottenete i vantaggi della sovranità dei dati e dei costi di proprietà trasparenti



Semplificare il percorso di conformità interna, normativa e specifica del settore

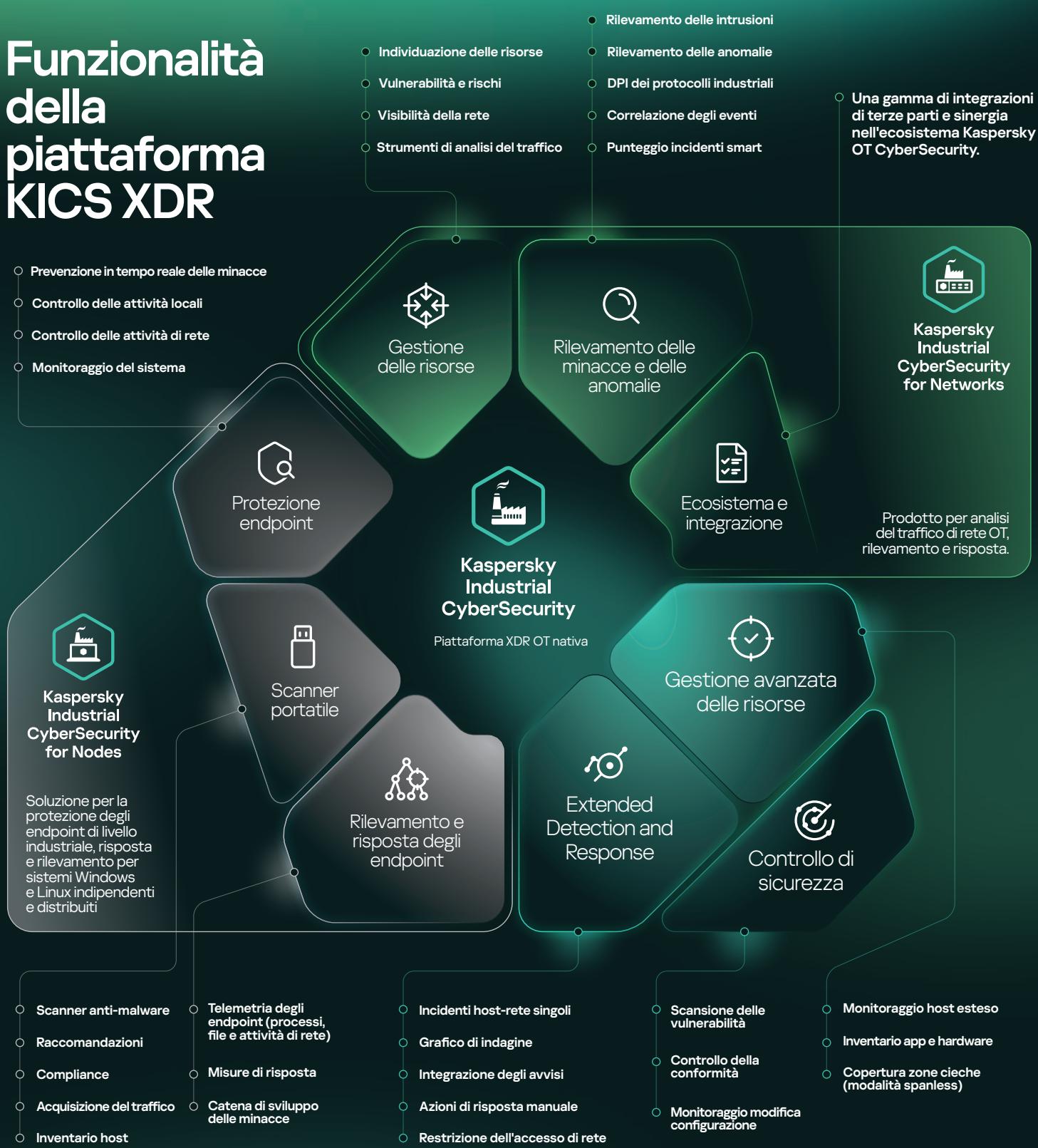


Adattatevi alle cyberminacce in continua evoluzione con una soluzione scalabile e a prova di futuro



Approfittate dell'integrazione perfetta con il portfolio di cybersecurity IT leader del settore di Kaspersky

# Funzionalità della piattaforma KICS XDR



## Vantaggi operativi

### Low footprint

Grazie all'implementazione modulare e al consumo di risorse regolabile, KICS non influisce sulle prestazioni del sistema o sulla continuità dei processi, con un impatto bassissimo sulle risorse del sistema su cui è installato.

### Compatibilità

Oltre 125 versioni di Windows e Linux supportate e più di 200 sistemi e dispositivi IACS testati garantiscono la compatibilità con la vostra infrastruttura esistente.

### Integrazione nativa

KICS for Nodes e KICS for Networks lavorano insieme per garantire un'integrazione fluida, una gestione centralizzata e funzionalità estese tra prodotti.

# Architettura della soluzione e casi d'uso

## Gestione avanzata delle risorse con profilazione AI

Identificate tutti i dispositivi connessi e le loro interazioni con il set di strumenti di individuazione delle risorse e la massima visibilità di rete per rilevare i dispositivi non censiti (shadow IT), senza lasciare dispositivi sconosciuti nell'ambiente OT.

## Extended Detection and Response

Rilevate attività dannose o pericolose e contenete le minacce prima che abbiano un impatto sui processi, con rilevamento di oltre 5000 attacchi di rete, DPI per oltre 50 protocolli industriali e opzioni di risposta sicura.

## Controlli di sicurezza continui

Ottenete una consapevolezza completa della posizione di sicurezza in ambienti distribuiti, di tipo "air-gap" e altamente sensibili con oltre 3100 regole di controllo predefinite e oltre 1300 test di vulnerabilità OVAL.

### 3 Business & Enterprise

#### Security Operations Center

Kaspersky Next XDR Expert

### 2 Monitoraggio e controllo



Kaspersky Industrial CyberSecurity for Nodes

#### Controllo di supervisione dell'impianto



inventario risorse basato su agenti



Kaspersky Next XDR Expert

### 1 Protezione e automazione



Kaspersky Industrial CyberSecurity for Networks

monitoraggio passivo (SPAN)

risposta di rete



polling dei dispositivi di rete senza agente

risposta endpoint



avvisi da host e rete



Kaspersky Industrial CyberSecurity for Networks

KICS for

Networks

acquisisce passivamente il traffico di rete da:

- Sensori di rete propri
- Collettore SD-WAN
- Endpoint agent
- Scanner portatile

Scanner portatile KICS for Nodes senza installazione per sistemi isolati e dispositivi bring-in

Apparati non connessi

Expertise Centers



L'esperienza senza pari che alimenta il nostro portfolio

Per saperne di più

### 0 Processo tecnologico



## Casi di integrazione



Kaspersky Next XDR Expert

Utilizzati insieme, la piattaforma KICS e Kaspersky Next XDR Expert forniscono funzionalità XDR IT-OT unificate e una protezione complessa per infrastrutture convergenti.



Kaspersky Machine Learning for Anomaly Detection

L'integrazione con la soluzione Machine Learning for Anomaly Detection (MLAD) consente a KICS for Networks di inviare dati di telemetria per l'analisi e di ricevere avvisi per le anomalie rilevate.



Kaspersky SD-WAN

KICS può sfruttare l'infrastruttura SD-WAN per raccogliere il traffico industriale, fornire un monitoraggio centralizzato e proteggere oggetti e sistemi industriali distribuiti.



Kaspersky Industrial CyberSecurity

Per saperne di più