Una piattaforma di sicurezza per la sostenibilità e la trasformazione digitale delle realtà industriali

Kaspersky Industrial CyberSecurity Platform

kaspersky BRING ON THE FUTURE

Attacchi malware

Dall'inizio del 2022 quasi il 30% dei computer associati ai sistemi ICS ha subito attacchi malware, quasi il 10% in meno rispetto all'anno precedente

Kaspersky ICS-CERT, giugno 2022

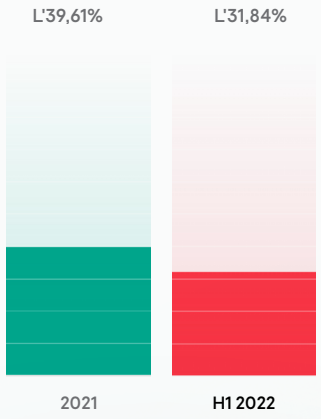
Per saperne di più

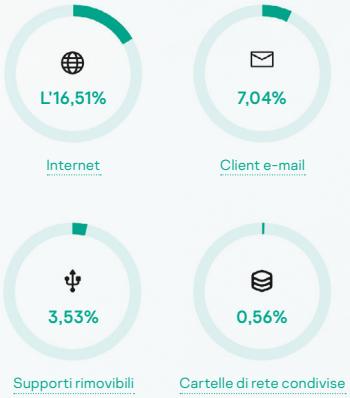
Le aziende industriali si approcciano alla cybersicurezza nelle proprie infrastrutture IT e OT (Operational Technology) in modo diverso. La maggior parte delle aziende adotta già misure di rilevamento e risposta di livello avanzato nelle reti aziendali, ma per l'OT fa in genere affidamento su un approccio di tipo "air gap" obsoleto. Le industrie stanno diventando sempre più "digitali" e continuano a investire in tecnologie smart, in nuovi sistemi di automazione e nell'adozione della trasformazione digitale. Questo tuttavia non fa altro che annullare la tradizionale distanza tra ambienti IT e OT necessaria a impedire alle minacce informatiche di colpire i sistemi di controllo e automazione industriali.

Essere l'obiettivo di un attacco non vuol dire per forza esserne vittima

Per essere soggetti a violazioni air gap accidentali o infezioni malware non serve necessariamente essere presi di mira da un attacco. Basta una sola unità flash, un cellulare, un messaggio e-mail di phishing o un ransomware introdotto nell'ambiente ICS per compromettere in modo drastico le attività principali di un'azienda. Allo stesso tempo, un gruppo di hacker motivato può insinuarsi nelle reti OT e causare ingenti danni alle apparecchiature, ai processi, alla produzione, alla sicurezza e alla qualità o rubare informazioni preziose.

Percentuale di computer ICS in cui sono stati bloccati oggetti dannosi dall'inizio del 2022





Cybersicurezza essenziale per OT

Protezione endpoint

per sistemi connessi e standalone. Una soluzione sicura e testata dovrebbe agevolare l'applicazione dei criteri di sicurezza, il supporto della conformità, l'esecuzione dei controlli di sicurezza, la gestione dell'inventario, le attività di applicazione delle patch e la raccolta di dati di telemetria precisi come un sensore endpoint

Protezione della rete

per la visibilità delle comunicazioni, il rilevamento delle minacce e la gestione delle risorse. Oltre a offrire una risposta manuale sicura, il sistema di analisi del traffico di rete e di rilevamento delle intrusioni controlla l'efficacia delle impostazioni del firewall, la segmentazione della rete e la conformità dell'utilizzo della rete.

Programmi di formazione

per consentire al personale di contenere il numero degli incidenti e ridurre al minimo l'impatto del fattore umano (errore umano)

Servizi offerti da esperti

per esaminare l'infrastruttura, condurre analisi di livello avanzato o mitigare l'impatto di un incidente

Riconoscimento globale

Nel 2020 Kaspersky ha ricevuto da Frost and Sullivan il Global Company of the Year Award in base all'analisi del mercato Global Industrial (OT/ICS) Cyber Security

Nel sondaggio globale annuale di **VDC** Kaspersky si è collocato al primo posto tra i fornitori nella categoria della sicurezza informatica industriale, sulla base delle valutazioni complessive di oltre 250 professionisti qualificati nella comunità dell'automazione industriale

Cosa offre Kaspersky

La piattaforma KICS (Kaspersky Industrial CyberSecurity) delle tecnologie integrate native e il nostro portfolio di servizi e formazione avanzata rispondono a tutte le esigenze di cybersicurezza delle aziende industriali e degli operatori delle infrastrutture critiche.

La piattaforma è un elemento chiave in un ecosistema esclusivo per le imprese industriali che include:

- Le migliori soluzioni aziendali di Kaspersky, che offrono un'autentica convergenza IT-OT e i molteplici vantaggi di un approccio basato su un unico fornitore
- Varie soluzioni specializzate per la cybersicurezza fisica, la sicurezza IOT industriale, il machine learning e l'area di lavoro sicura da remoto contribuiscono a offrire una scalabilità agile e illimitata

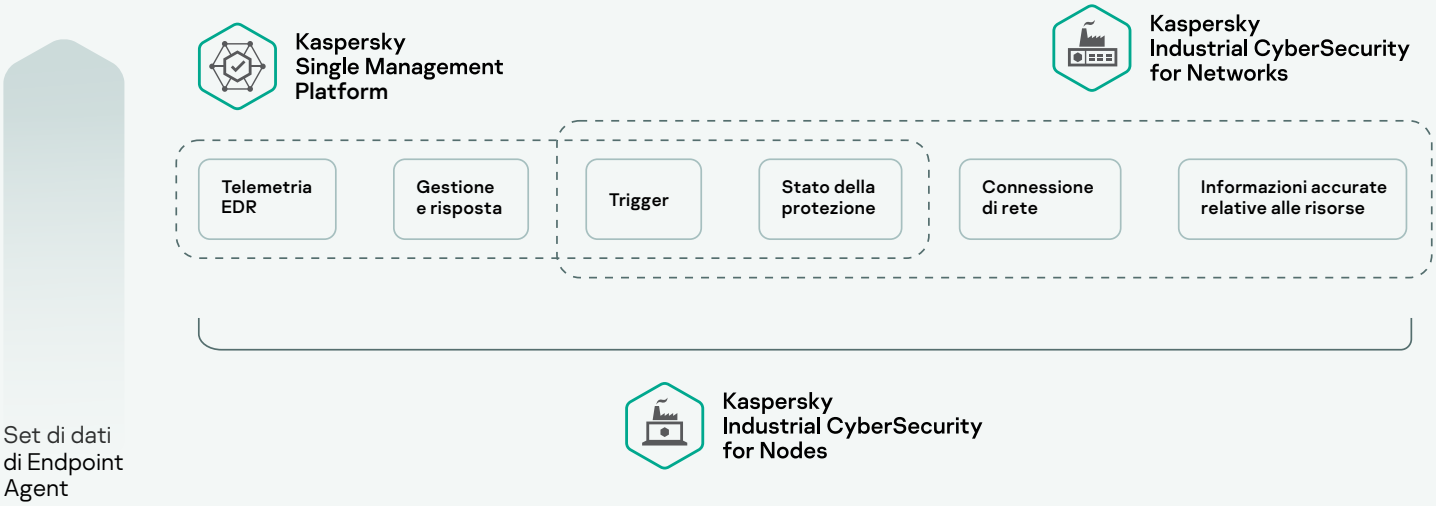
La piattaforma Kaspersky Industrial CyberSecurity è leader nelle seguenti categorie:

- OT Endpoint Security
- OT Network Monitoring and Visibility
- Anomaly Detection, Incident Response and Reporting
- OT Security Services

L'utilizzo integrato consente all'utente di avere una panoramica e un contesto più ampi ad esempio su: catena di incidenti a livello di rete ed endpoint, parametri precisi delle risorse, comunicazione di rete e mappe topologiche anche da segmenti in cui il mirroring del traffico non è ancora disponibile.

Prodotti

KICS è una piattaforma di cybersicurezza OT progettata per la protezione completa dei principali componenti Industrial Automation and Control System a ogni livello. La perfetta integrazione tra i componenti della piattaforma offre la piena visibilità di più reti OT distribuite in diverse posizioni e sistemi di automazione, offrendo una migliore esperienza del cliente, consapevolezza situazionale e flessibilità della distribuzione.



KICS for Nodes è un software di protezione degli endpoint, rilevamento e riposta con funzionalità di controllo conformità e sensore endpoint.

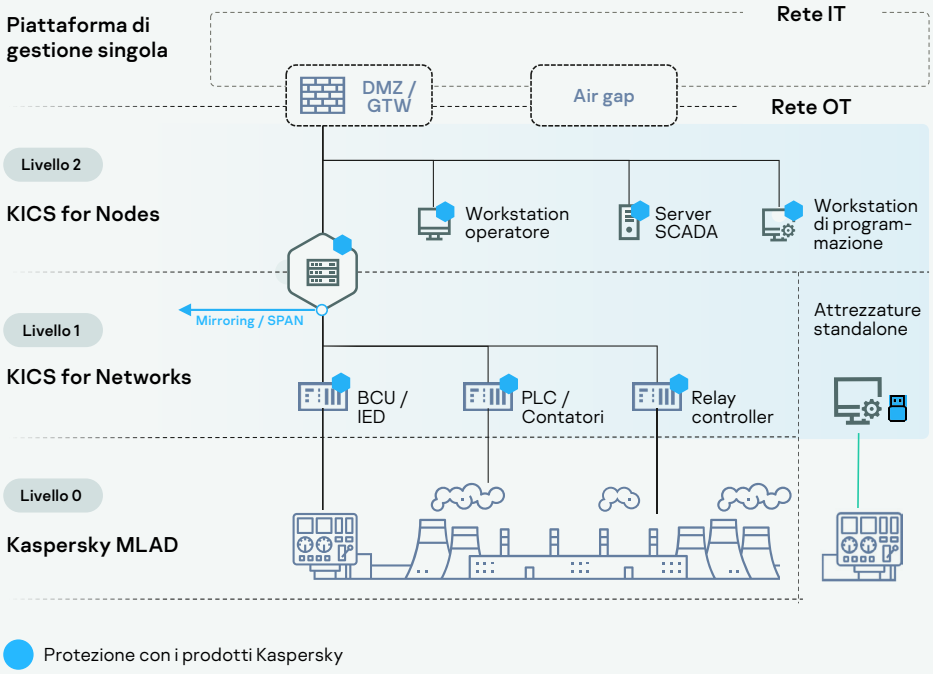
KICS for Networks è progettato per l'analisi del traffico di rete OT, per il rilevamento e la risposta.

La piattaforma di gestione singola fornisce un'interfaccia EDR avanzata e una rapida scalabilità in numerose posizioni.

Funzionalità aggiuntive

La soluzione offre numerose funzionalità aggiuntive. La tecnologia Network **Active Polling** consente la raccolta rapida e precisa della topologia di rete e delle impostazioni delle risorse. La funzionalità **Controllo endpoint** assicura la conformità ai criteri di sicurezza, inclusa la sicurezza delle impostazioni correnti e il controllo delle vulnerabilità. Il metodo di distribuzione **Portable Scanner** di KICS for Nodes aiuta a stabilire le best practice dei controlli di sicurezza per le attrezzature air gap standalone. **Il machine learning per il rilevamento delle anomalie** è un sistema di rilevamento precoce delle anomalie integrato nel processo tecnologico.

Architettura della soluzione



Funzionalità

Individuazione delle risorse
Inventario e identificazione delle risorse OT passive

Analisi approfondita dei pacchetti
Analisi quasi in tempo reale della telemetria dei processi tecnici

Controllo dell'integrità di rete
Rileva i flussi e gli host di rete non autorizzati

Sistema di rilevamento delle intrusioni
Invia avvisi relativi alle attività di rete dannose

Command control
Ispeziona i comandi in base ai protocolli industriali

Integrazione esterna
L'integrazione API flessibile aggiunge funzionalità di prevenzione e rilevamento

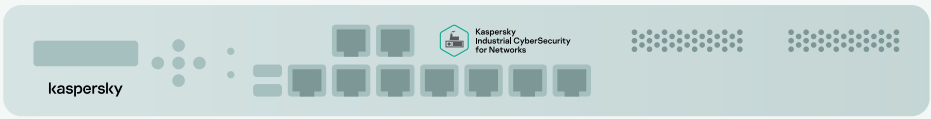
Machine learning per il rilevamento delle anomalie (MLAD)
Rileva anomalie informatiche o fisiche tramite mining in tempo reale dei dati storici e di telemetria (rete neurale ricorrente)

Gestione delle vulnerabilità
Database aggiornabile delle vulnerabilità nelle attrezzature industriali, fornito da Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

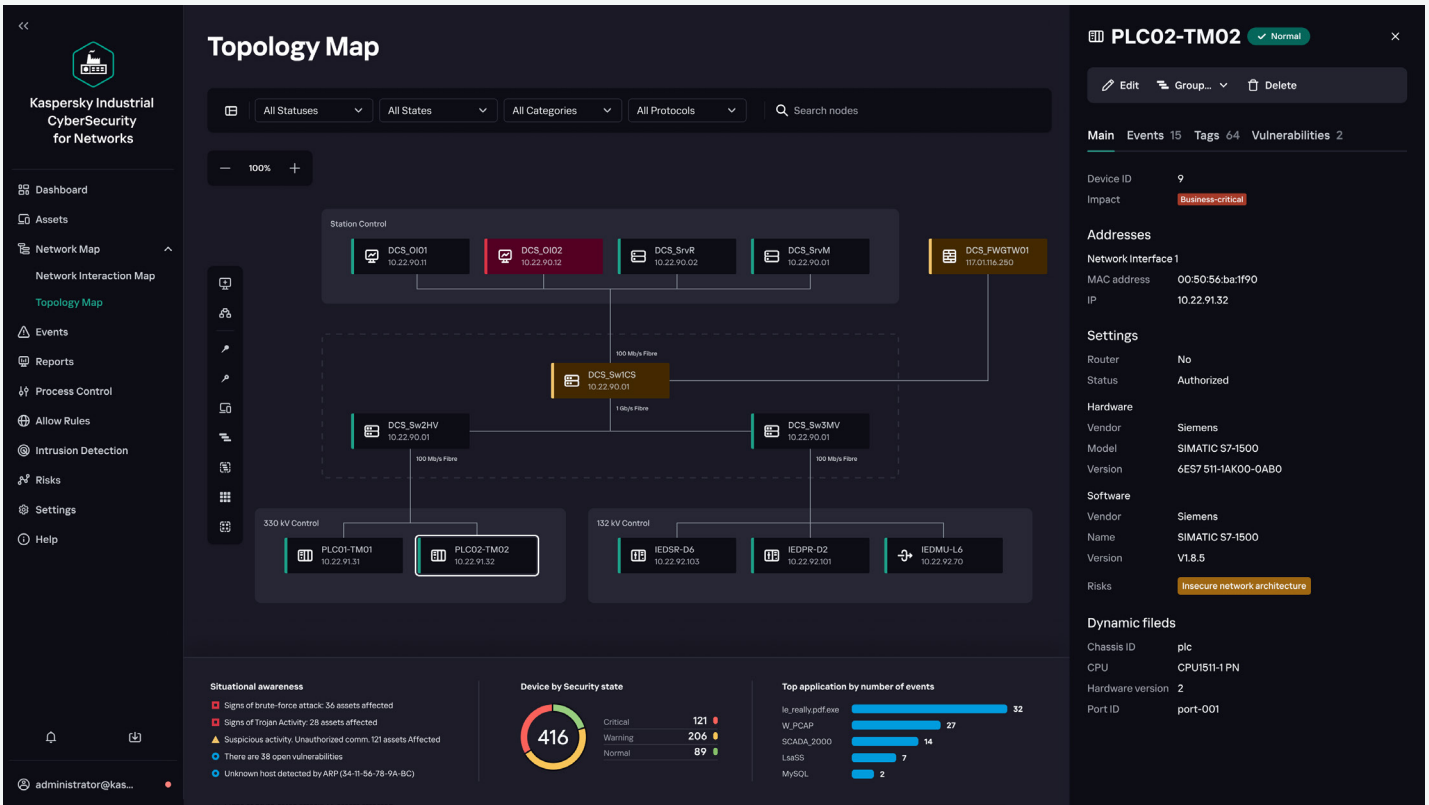
Analisi del traffico di rete OT, rilevamento e risposta. Visibilità chiara dei rischi con monitoraggio del traffico passivo, polling attivo e sensori endpoint.

Rileva anomalie e intrusioni all'interno delle reti ICS fin dalle fasi iniziali e garantisce che vengano presi i provvedimenti necessari per evitare qualsiasi impatto negativo sui processi industriali.



Soluzione indipendente dalle applicazioni che può essere integrata in modo rapido e ottimale nelle pratiche consolidate di sourcing, integrazione e garanzia dei nostri clienti.

Interface



KICS for Nodes è stato appositamente progettato per i requisiti più rigorosi dei sistemi di automazione distribuiti: ambienti complicati e misti, tempi di funzionamento estesi, use case connessi e standalone, istanze gestite e senza manutenzione e priorità della disponibilità del controllo a tutti i costi

Kaspersky Industrial CyberSecurity for Nodes

Rilevamento e risposta, protezione degli endpoint certificata e testata, di livello industriale. Una soluzione stabile e compatibile a basso impatto per sistemi Linux, Windows e standalone.

Protezione degli endpoint industriali, rilevamento e risposta

Protegge tutti gli endpoint di un sistema di automazione moderno, digitale, gestito e distribuito. Rivela nuovi livelli di visibilità degli incidenti nel processo di Root-Cause Analysis. L'agente raccoglie la telemetria dell'endpoint per creare una rappresentazione visiva chiara e dettagliata dell'avanzamento di un incidente su workstation, server, gateway e altri endpoint, garantendo agli amministratori dei sistemi di automazione che un incidente sia stato completamente gestito e che non si verificherà più.

Vantaggi

Basso impatto
sul dispositivo protetto per prestazioni superiori del sistema

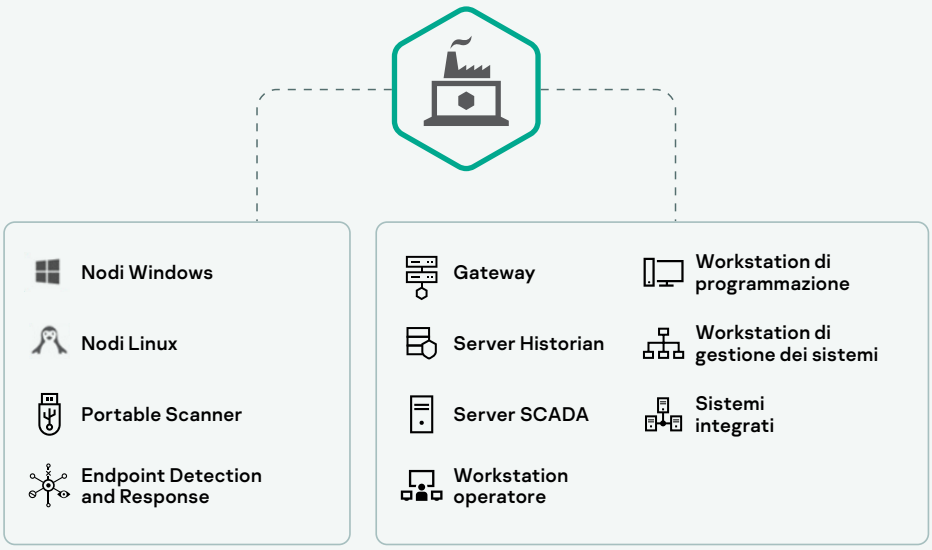
Compatibilità
con i computer a basse prestazioni di generazioni precedenti e con i sistemi Windows XP SP2 e Windows Server 2003 SP1 e versioni successive

Ciclo di vita esteso
con supporto esteso e licenze fino a 5 anni

Funzionalità complete
per tutti i sistemi Microsoft Windows desktop, server ed Embedded

Distribuzione modulare
Opzioni flessibili e impostazioni sicure non intrusive

Applicabilità alle infrastrutture miste
varianti Windows, Linux e Portable



KICS for Nodes Portable Scanner
Applica un criterio di cybersicurezza su macchinari standalone, sistemi di automazione o apparecchiature in cui non è possibile installare software di sicurezza. Massima consapevolezza situazionale e visibilità OT anche da un'infrastruttura standalone.

Soluzione senza installazione
KICS for Nodes può essere attivato su una serie di unità flash Portable Scanner aggiuntive. Consente di eseguire scansioni su richiesta simultanee su più macchine durante le finestre di manutenzione, di raccogliere i dati degli endpoint e di organizzarli in un comodo report di riepilogo.

Conformità alle normative e ai criteri interni
KICS for Nodes Portable Scanner effettua controlli di conformità anti-malware delle attrezzature che accedono a un sito OT, inclusi computer o fornitori di terze parti. Ha un impatto operativo molto basso e non interferisce con le soluzioni di sicurezza esistenti.

Vantaggi

Consapevolezza situazionale

Gestione di criteri/sistemi

Risposta e kill-chain

Creazione di report e notifiche

Integrazione SIEM

Integrazione HMI/MES

Kaspersky Single Management Platform

La Single Management Platform è una soluzione di gestione centralizzata della sicurezza per l'orchestrazione della sicurezza dell'intera infrastruttura OT, con una mappa di tutte le risorse distribuite geograficamente arricchita con eventi, analisi degli incidenti e altro ancora. Ottimizza l'efficienza dei team di sicurezza IT e OT misti. Una soluzione in cui tutti i controlli di sicurezza funzionano in armonia, consentendo una risposta rapida e precisa.

Servizi offerti da esperti

La nostra suite di servizi rappresenta una parte importante del portfolio KICS. Offriamo il ciclo completo dei servizi di sicurezza: dalle valutazioni della cybersicurezza industriale alla risposta agli incidenti.

> Rispetto ad altri fornitori, l'esperienza nel settore della sicurezza informatica ICS, la professionalità del team e la completezza della soluzione proposta da Kaspersky hanno rappresentato un innegabile valore aggiunto e garantiscono un futuro di successo per la strategia di protezione della nostra azienda.
>
> Ondřej Sýkora,
> Manager C&A,
> Plzeňský Prazdroj

Valutazione della cybersicurezza industriale

Valutazione della cybersicurezza industriale: Kaspersky offre un sistema di valutazione della cybersicurezza industriale poco invasivo che comprende penetration test interno ed esterno, valutazione della sicurezza OT e valutazione della sicurezza delle soluzioni di automazione. Gli esperti di Kaspersky offrono informazioni di rilievo sull'infrastruttura di un'azienda e suggerimenti su come potenziare la strategia di sicurezza informatica ICS.

> Grazie alla guida e alle competenze del team Kaspersky abbiamo potuto rafforzare la nostra protezione contro le minacce alla sicurezza informatica.
>
> Yu Tat Ming,
> CEO, PacificLight.

Threat intelligence

I dati analitici aggiornati raccolti dagli esperti di Kaspersky consentono di potenziare la protezione del cliente dagli attacchi mirati al settore industriale. Sotto forma di feed di threat intelligence o di report personalizzati, le analisi rispondono alle specifiche esigenze del cliente in base a parametri regionali, di settore e del software ICS.

INCIDENT RESPONSE

In caso di incidente, gli esperti di Kaspersky raccolgono e analizzano dati e malware, ricostruiscono la sequenza temporale dell'incidente, determinano le possibili origini e motivazioni e sviluppano un piano di remediation dettagliato. Il piano include suggerimenti sulla rimozione del malware dai sistemi dei clienti e sul rollback delle relative azioni dannose.

Formazione e consapevolezza

> La formazione offerta da Kaspersky per lo sviluppo di competenze professionali per la sicurezza informatica industriale del nostro gruppo ICS è stata la migliore.
>
> Søren Egede Knudsen,
> Chief Technical Officer

Industrial cybersecurity awareness training

Formazione interattiva in loco e online e cybersafety games per i dipendenti che utilizzano sistemi computerizzati industriali e i relativi responsabili. I partecipanti acquisiscono nuove prospettive sull'attuale panorama delle minacce e sui vettori di attacco mirati negli specifici ambienti industriali, esplorano scenari pratici e acquisiscono competenze sulla sicurezza informatica.

Programmi di formazione avanzati

I corsi di formazione ICS Penetration Testing e ICS Digital Forensics sono rivolti ai professionisti della cybersicurezza. I partecipanti acquisiscono tutte le competenze avanzate necessarie per eseguire test approfonditi o analisi digitali negli ambienti industriali.

Ecosistema di soluzioni specializzate

Kaspersky IoT Infrastructure Security

Protegge l'IoT a livello di gateway in base all'approccio Cyber Immunity di Kaspersky

Per saperne di più

Kaspersky Antidrone

Protegge lo spazio aereo dai droni in strutture di qualsiasi dimensione

Per saperne di più

Kaspersky Secure Remote Workspace

Infrastruttura thin client funzionale con Cyber Immunity

Per saperne di più

Kaspersky Security CAD

Modellazione digitale dei sistemi di sicurezza delle informazioni per le fasi di progettazione e funzionamento

Per saperne di più

Kaspersky Machine Learning for Anomaly Detection

Sistema di rilevamento precoce delle anomalie nei processi tecnologici industriali

Per saperne di più

Kaspersky Industrial CyberSecurity

Per saperne di più

www.kaspersky.it