Kaspersky Next MXDR Optimum

Proteggi in modo più intelligente, risparmia di più: potenzia la tua attività in crescita con una potente cybersecurity supportata dall'intelligenza artificiale e da competenze leader a livello mondiale

kaspersky bring on the future

Sommario

01

01 Linea di prodotti Kaspersky Next

02 Panoramica MXDR Optimum

03 Panoramica delle funzionalità

04 Ulteriori informazioni

Perché scegliere Kaspersky Next?

Basato sulla nostra soluzione endpoint più avanzata

Per oltre un decennio, i prodotti Kaspersky si sono classificati costantemente ai primi posti nei test e nelle recensioni indipendenti, guadagnando premi per il primo posto e podi.

La nostra comprovata protezione endpoint automatizzata riduce il numero di avvisi che i team di sicurezza devono analizzare, migliorando la loro efficienza.

Supportato da conoscenze approfondite, competenze ed esperienza

Kaspersky Next si basa su decenni di esperienza accumulata e sulle approfondite competenze dei nostri team di sicurezza globali. I nostri specialisti collaborano per affrontare le minacce informatiche complesse, perfezionando costantemente le tecnologie alla base dei nostri prodotti. Questo approccio gestito da esperti garantisce che le nostre soluzioni siano affidabili, innovative e in linea con le reali esigenze di sicurezza.

Prevenzione multilivello basata sulla tecnologia IA

Kaspersky utilizza algoritmi predittivi, clustering, reti neurali, modelli statistici e algoritmi avanzati per aumentare la velocità del rilevamento e migliorarne la precisione.

La cybersecurity che cresce con voi

Kaspersky Next protegge le aziende di qualsiasi dimensione. Man mano che le vostre esigenze aumentano, potete facilmente passare dalla protezione endpoint essenziale alle soluzioni avanzate e specializzate disponibili nei livelli superiori.

Fonti di dati supportate

- Desktop e server Windows
- Computer Mac OS
- Computer Linux
- Piattaforme di virtualizzazione
- Rete

Sommario

02

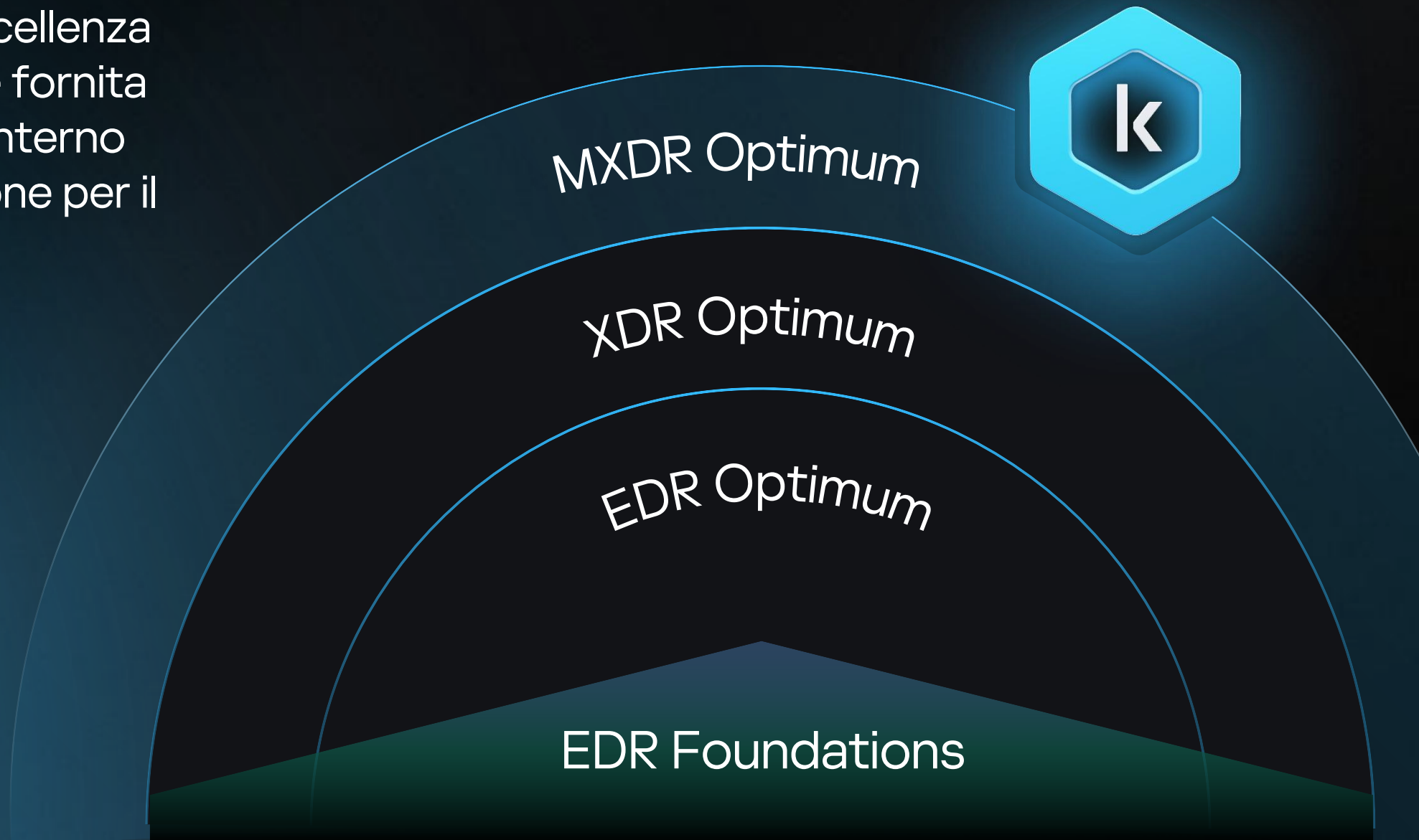
01 Linea di prodotti Kaspersky Next

02 Panoramica MXDR Optimum

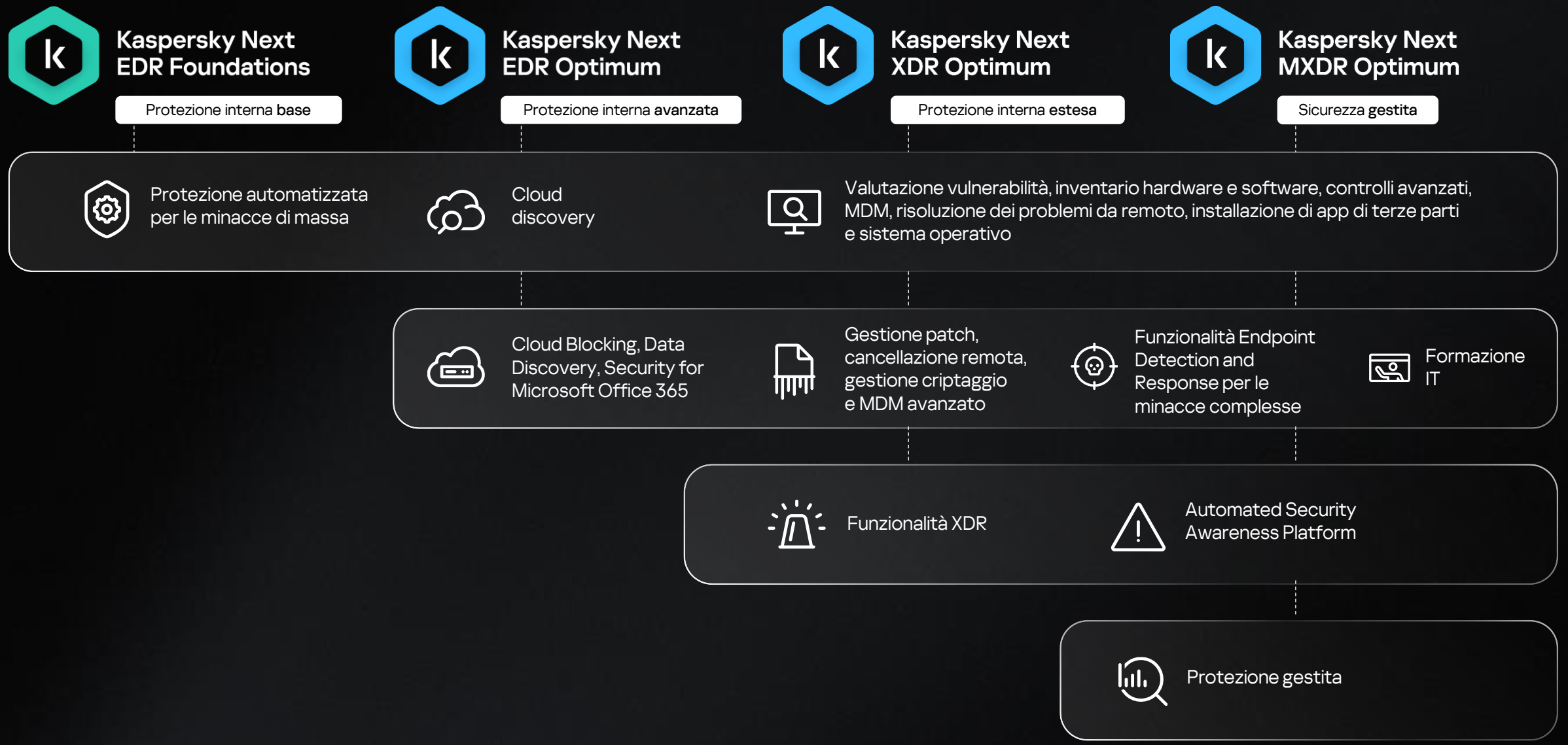
03 Panoramica delle funzionalità

04 Ulteriori informazioni

Il massimo dell'eccellenza e della protezione fornita da Kaspersky, all'interno di un'unica soluzione per il mondo SMB



Protezione scalabile



Offerta ottimale per le medie imprese

Kaspersky Next EDR Foundations

Protezione automatizzata per le minacce di massa

- Multi-layered Anti-Malware
- Motore comportamentale
- Prevenzione degli exploit
- Remediation engine
- Protezione dalle minacce tramite file, Web, rete ed e-mail a livello di endpoint
- Firewall
- Host Intrusion Prevention
- Protezione AMSI
- Prevenzione degli attacchi BadUSB
- Root-cause analysis con una scheda di avvisi
- Threat Intelligence globale tramite Kaspersky Security Network
- Difesa dalle minacce mobile

Hardening dei sistemi

- Vulnerability assessment
- Inventario hardware e software
- Controllo applicazioni, Web e dispositivi
- Mobile Device Management (MDM)
- Risoluzione dei problemi da remoto
- Installazione di sistemi operativi e app di terze parti

Cloud security

- Cloud discovery

+

Kaspersky Next EDR Optimum

Funzionalità Endpoint Detection and Response per le minacce complesse

- Ricerca degli indicatori di compromissione (IoC) con risposta automatica trasversale tra più endpoint
- Controllo adattivo delle anomalie
- Risposta guidata e "single-click"
- Controllo degli oggetti critici di sistema
- Spostamento dei file in quarantena/ripristino dei file dalla quarantena
- Isolamento della rete/rimozione dell'isolamento della rete
- Acquisizione/Eliminazione file
- Avvio/Completamento dei processi
- Scansione delle aree critiche
- Prevenzione dell'esecuzione
- Esecuzione dei comandi

Hardening dei sistemi

- Patch management
- Cancellazione remota
- Gestione della crittografia
- MDM avanzato

Cloud security

- Blocco delle attività sul cloud
- Data Discovery
- Security for Microsoft Office 365: Exchange, OneDrive, SharePoint, Teams

Formazione IT

- Cybersecurity training per amministratori IT

+

NOVITÀ

Kaspersky Next XDR Optimum

Funzionalità Extended Detection and Response per le minacce complesse

- Aggregazione degli avvisi
- Risposta di Active Directory dalla scheda dell'avviso

Automated Security Awareness Platform

- Formazione flessibile sulla Security Awareness per i dipendenti
- Corsi personalizzabili disponibili in 25 lingue
- Dashboard e report sulla Security Awareness
- Campagne di phishing simulate
- Formazione in formato video e audio
- Risposta di Automated Security Awareness Platform dalla scheda dell'avviso

Kaspersky Cloud Sandbox

- Caricamento ed esecuzione di un file in Cloud Sandbox
- Caricamento di un file da un indirizzo Web e successiva esecuzione in Cloud Sandbox
- Funzionalità anti-evasione per contrastare i malware progettati per evitare le sandbox
- Esecuzione del file estratto dal report Cloud Sandbox
- Esportazione dei risultati dell'analisi
- Rilevamento automatico dei tipi di file
- Gestione delle attività obsolete per l'esecuzione

+

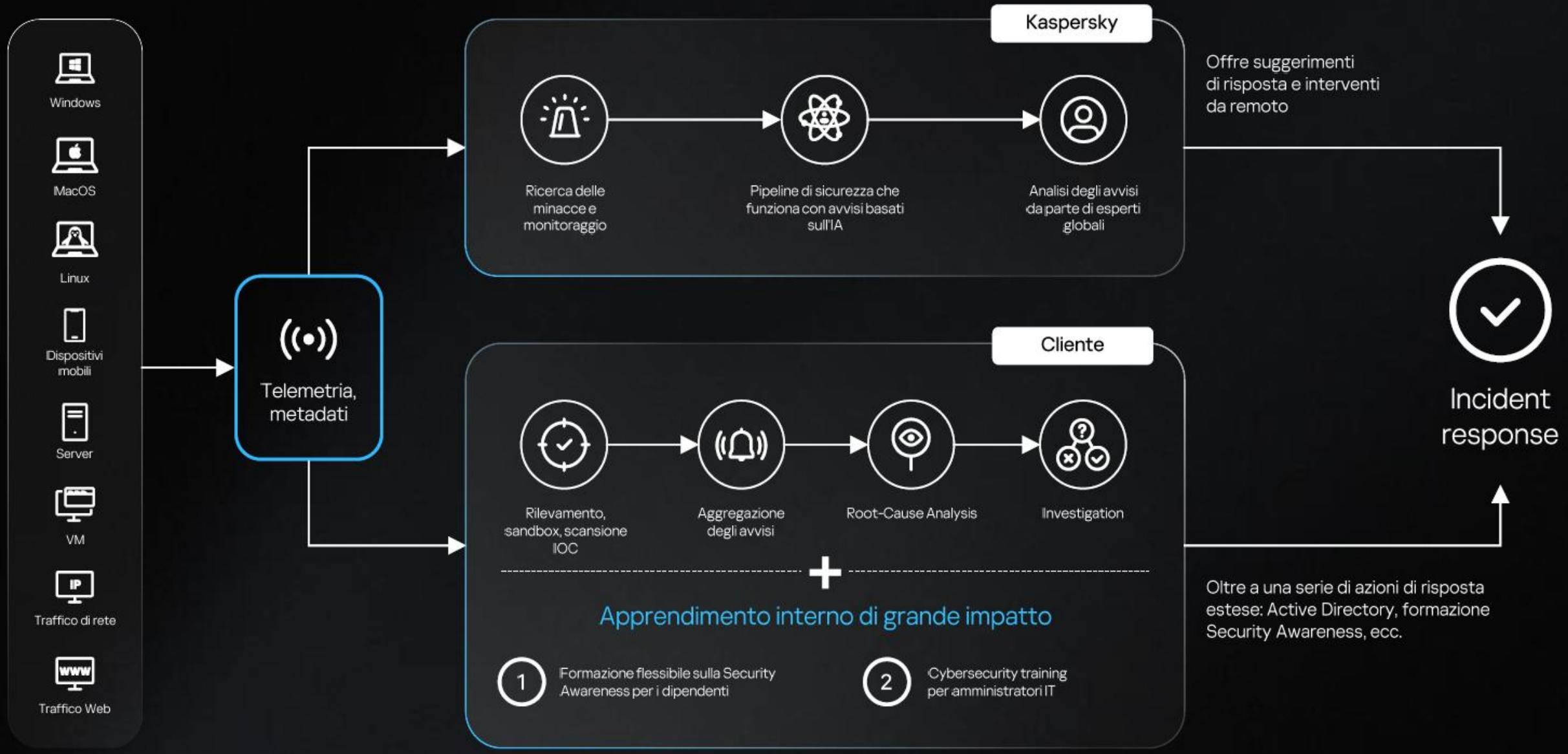
NOVITÀ

Kaspersky Next MXDR Optimum

Managed protection

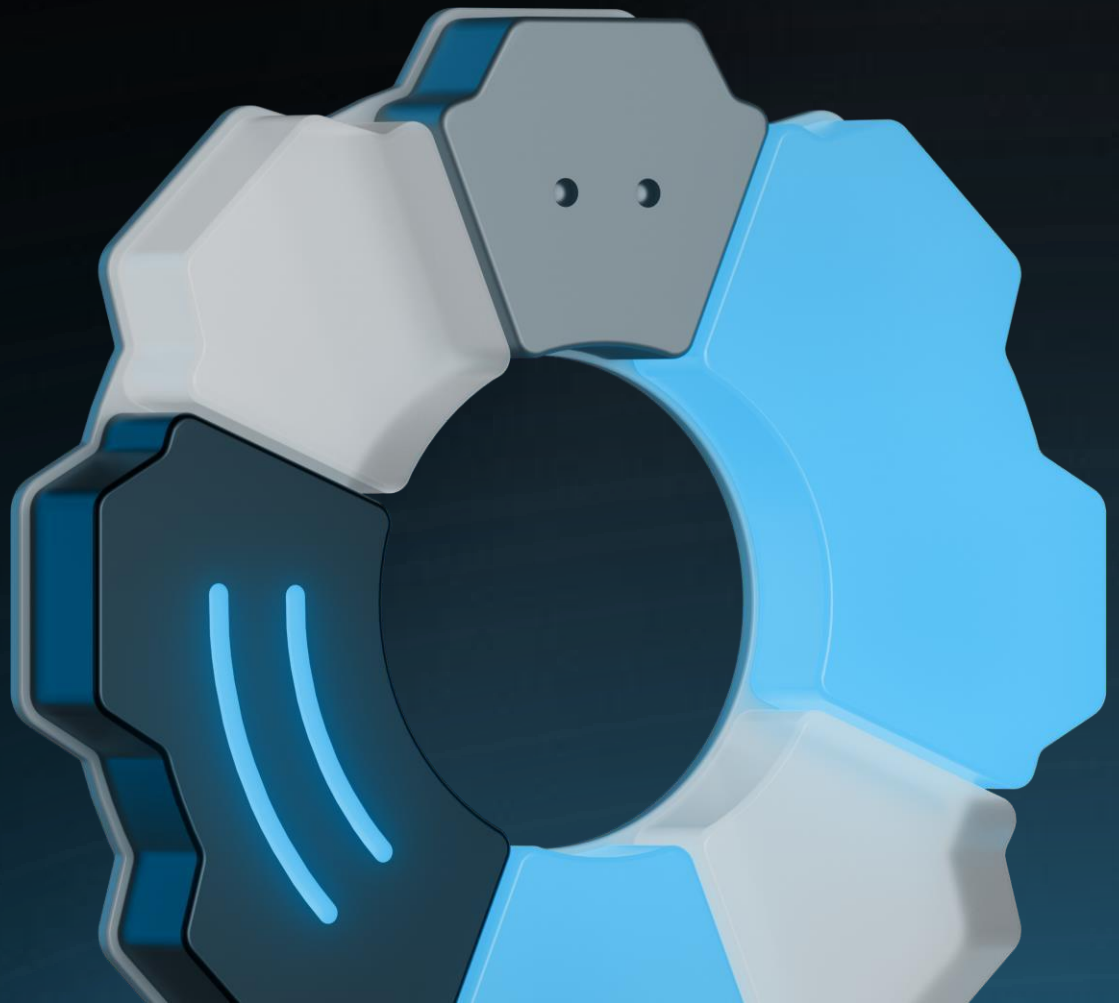
- Ricerca delle minacce e monitoraggio continuo 24 ore su 24, 7 giorni su 7
- Invio dell'incidente per ulteriori indagini da parte del SOC di Kaspersky
- Comunicazione diretta con il team SOC in merito agli incidenti
- Notifiche sugli incidenti tramite e-mail/Telegram
- Scenari di risposta guidata e automatizzata
- API REST per l'integrazione con IRP/SOAR
- Meccanismi di intelligenza artificiale che accelerano le indagini sugli incidenti
- Visibilità degli asset con gli stati attuali
- Compatibilità con applicazioni EPP di terze parti
- Dashboard intuitive nel portale MDR
- Rapporti periodici
- Archiviazione dei dati di telemetria non elaborati per 3 mesi

Come funziona



Sommario

03



01 Linea di prodotti Kaspersky Next

02 Panoramica MXDR Optimum

03 Panoramica delle funzionalità

04 Ulteriori informazioni

Protezione endpoint

Protezione automatizzata per le minacce di massa

Protezione endpoint

Monitoraggio dei dati in entrata e in uscita sul dispositivo, esegui una scansione per rilevare minacce e fermarle prima che causino danni.

Protezione multilivello

Protezione basata su firma, analisi euristica e comportamentale con tecnologia di rilevamento basata su modelli.

Protezione avanzata

Con l'analisi ML dei modelli dannosi e i dati anonimizzati da Kaspersky Security Network (KSN) sulle minacce attuali.

Protezione aggiuntiva

Prevenzione intrusioni, controllo dell'accesso ai file di sistema e blocco delle connessioni sospette ai dispositivi, inclusi Android e iOS.

Riduzione della superficie di attacco

Hardening del sistema

Diversi componenti di controllo, come Adaptive Anomaly Control e gli algoritmi di machine learning, aiutano ad adattare automaticamente l'hardening dei sistemi e la configurazione dei criteri di sicurezza al comportamento dell'utente.

Gestione delle vulnerabilità e delle patch

Il Vulnerability e patch management semplifica gli aggiornamenti e ottimizza le operazioni IT e di sicurezza, supportando l'installazione del sistema operativo e del software di terze parti sugli host.

Rilevamento e risposta degli endpoint

Funzionalità Endpoint Detection and Response

Indicatori di compromissione

Ricerca degli indicatori di compromissione (IoC) con risposta automatica trasversale tra più endpoint

Analisi delle root cause

Strumenti per i dati e di visualizzazione per accertare la root cause della minaccia e se sono necessarie ulteriori azioni di risposta

Response automatizzata

Automazione e guida integrata per la risposta

Enrichment

Accesso al Threat Intelligence Portal

Extended Detection and Response

Funzionalità Extended Detection and Response

Combinazione dei segnali più piccoli e deboli in un quadro più ampio e utile, aggregando gli avvisi di Kaspersky Security Center e offrendo ai clienti un vantaggio XDR essenziale.

Aumento dell'efficacia della risposta agli incidenti e delle indagini sulle minacce consentendo agli utenti di inviare i file potenzialmente dannosi a Cloud Sandbox dalla scheda dell'avviso.

Possibilità di rispondere tramite l'integrazione con Kaspersky Security Awareness Platform.

Per ridurre il lavoro ripetitivo e liberare tempo per attività più importanti, gli utenti possono configurare incarichi di formazione automatici direttamente dalla scheda dell'avviso.

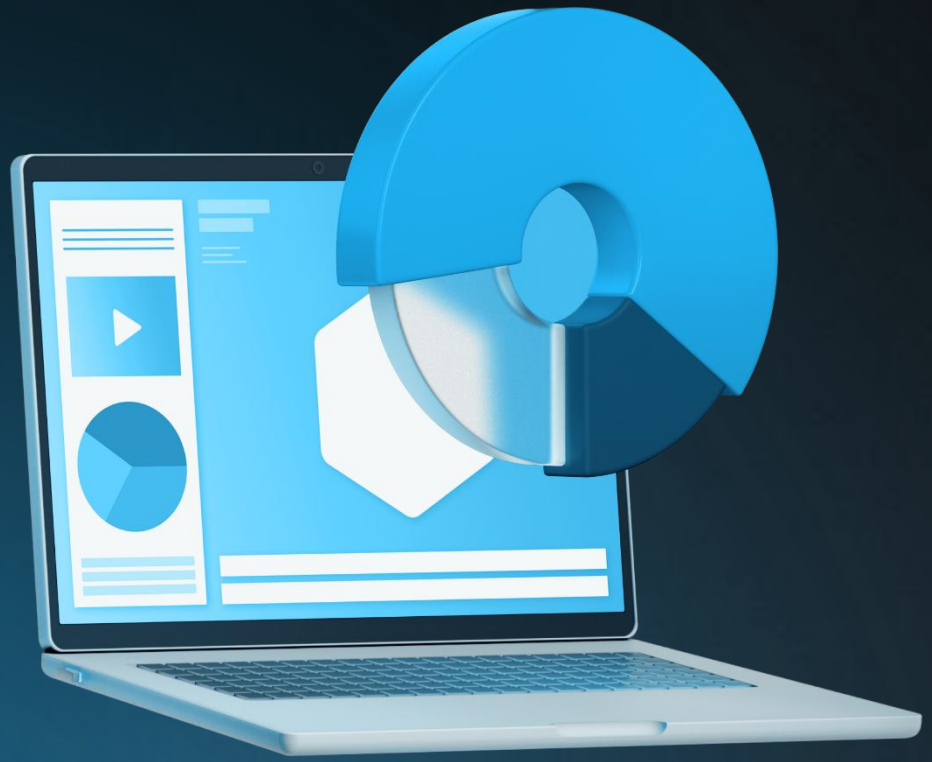
Utilizzo della risposta di terze parti e possibilità di bloccare gli utenti.

Integrazione diretta con la piattaforma di Awareness K-ASAP

Kaspersky Security Awareness

Sviluppa competenze di sicurezza diffuse nell'organizzazione, riducendo l'esposizione al rischio e rafforzando la continuità operativa.

La soluzione include corsi di formazione per gli utenti con accesso alla nostra piattaforma di apprendimento online che consente di sviluppare la Cybersecurity Awareness



Corsi di formazione

- Facilità di utilizzo ed efficienza di apprendimento per i dipendenti
- Gestione di programmi che fanno risparmiare tempo alle aziende
- Avviate i programmi di formazione sulla cybersecurity in pochi, semplici passaggi

Quattro semplici passaggi per configurare la piattaforma e avviare la formazione

Al resto ci pensa la piattaforma!

https://support.kaspersky.it/kasap/1.0

4 Imposta una data di inizio per la formazione (può essere diversa per ciascun gruppo)

3 Imposta un livello obiettivo per ciascun gruppo: seleziona il tipo di corso, gli argomenti e i livelli

2 Suddividili in gruppi in base al livello di rischio

1 Aggiungi gli utenti alla piattaforma

Portale Threat Intelligence

Gli utenti possono usare il nostro Kaspersky Threat Intelligence Portal per verificare qualsiasi file sospetto, hash dei file, indirizzi IP e indirizzi Web, per convalidare e assegnare la priorità agli alert di sicurezza associati, garantendo una reponse tempestiva alle minacce

- La reputazione di un file dal Kaspersky Threat Intelligence Portal è integrata nella scheda degli avvisi per un'analisi della root cause ancora più rapida e precisa
- Rilevamento delle minacce avanzate presenti nei file, facendoli passare attraverso l'intera serie di tecnologie che vi offriamo
- Arricchimento e assegnazione di priorità agli avvisi analizzando IP, hash di file, domini e indirizzi Web sospetti
- Esecuzione degli indirizzi Web sospetti nella nostra sandbox URL e ricezione di un report completo sulla minaccia

Extended Detection and Response

Query cloud sandbox

L'integrazione con Kaspersky Cloud Sandbox consente di eseguire varie azioni utilizzando Kaspersky Threat Intelligence Portal

- Rilevamento automatico dei tipi di file
- Gestione delle attività obsolete per l'esecuzione
- Caricamento ed esecuzione di un file in Cloud Sandbox
- Caricamento di un file da un indirizzo Web e successiva esecuzione in Cloud Sandbox
- Funzionalità anti-evasione per contrastare i malware progettati per evitare le sandbox
- Esecuzione di un file estratto dal report di Cloud Sandbox
- Esportazione dei risultati dell'analisi

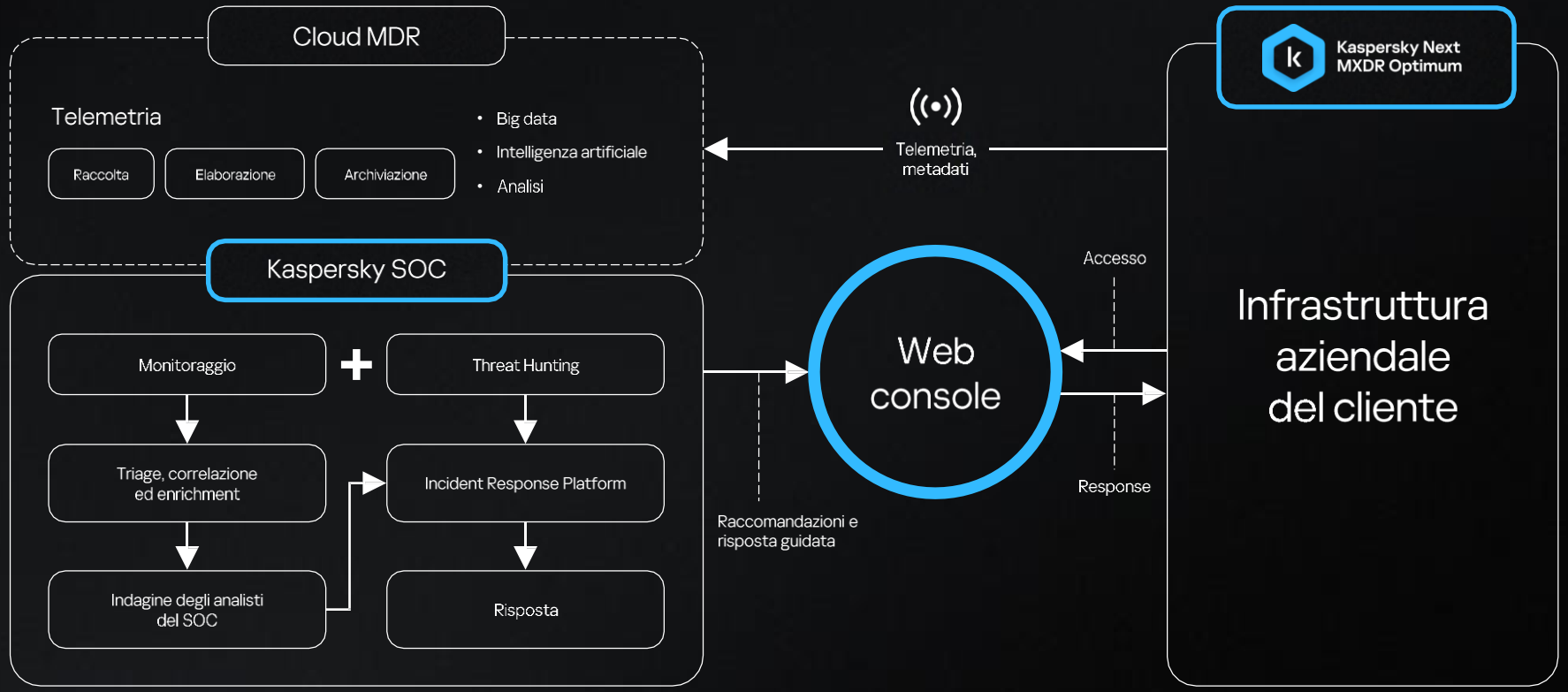
Managed Detection and Response: Servizio gestito 24/24, 7 giorni su 7 dal SOC Kaspersky

1 Kaspersky Next MXDR Optimum cattura e inoltra i dati al SOC di Kaspersky.

2 La telemetria, i metadati e la priorità degli avvisi sono analizzati da strumenti di ML/IA, con il coinvolgimento attivo degli esperti del SOC di Kaspersky.

3

Il team SOC di Kaspersky indaga sugli avvisi e ti segnala le attività dannose, fornendo raccomandazioni e risposte guidate dettagliate.



Motori di intelligenza artificiale (IA)

I meccanismi di intelligenza artificiale filtrano automaticamente i falsi positivi, migliorando notevolmente la produttività degli analisti e riducendo i tempi medi di assegnazione delle priorità, rilevamento e risposta (MTTD/MTTR)

Eventi

Alert

Correlazione dei dati

Analisi IA

Assegnazione delle priorità degli avvisi

Analisi degli avvisi

Incidenti

Conferma dello stato di attivazione: Vero/Falso

Capacità delle tecnologie IA

1

Rilevamento più rapido

L'IA analizza gli oggetti sospetti proprio nel momento in cui i dati arrivano

2

Risolve il 35-40% degli avvisi

Aumenta significativamente la produttività degli analisti, consentendo SLA con tempi di reazione ridotti

3

Assegnazione delle priorità degli avvisi

Consente ai nostri analisti di concentrarsi sugli avvisi più importanti

4

Risoluzione automatica degli avvisi

Non è necessario coinvolgere analisti umani

Managed Detection & Response

Key Benefits

- Consolidata esperienza dal **2014**
- Soluzione **All-in-One**
- Analisi **Proattiva** delle minacce 24/7
- Componente **Umana**
- **Response** guidata e automatizzata
- **Threat Intelligence** strategica
- Integrazione **SOC** o **Acquistabile come modulo a parte**
- Modalità **MSP** e **MSSP**
- Servizio non solo IT ma anche **OT**

Scenari di risposta

Il nostro team esamina gli episodi e crea risposte che è possibile accettare o rifiutare, tra cui:

Tipo di risposta	Descrizione
Recupero di un file	Copia di un file dall'infrastruttura locale al SOC di Kaspersky
Isolamento	Isolamento dalla rete della risorsa specificata
Disabilitazione dell'isolamento	Disabilitazione dell'isolamento della rete della risorsa specificata
Eliminazione di una chiave di registro	Eliminazione di una chiave o un ramo di registro per la risorsa specificata
Dump della memoria	Creazione di un dump della memoria e invio al SOC di Kaspersky
Terminazione di un processo	Terminazione di un processo sulla risorsa specificata con Kaspersky Endpoint Security for Windows

SLA

Livello di priorità	Tempo di reazione
Alto (esempio: attacco mirato)	1 ora
Medio (esempio: malware comune)	4 ore
Basso (esempio: adware, riskware, ecc.)	24 ore

Ulteriori informazioni, tra cui i criteri relativi agli incidenti, sono disponibili nei Termini e condizioni

Protezione aggiuntiva

Cloud security

Cloud security

Cloud discovery

Monitorate l'utilizzo di oltre 2.700 servizi per scoprire l'utilizzo non autorizzato del cloud

Blocco delle attività sul cloud

Potete bloccare l'accesso degli utenti alle risorse cloud, ai social network o agli strumenti di messaggistica inappropriati o non autorizzati

Data Discovery

Ottenete visibilità e controllo dei dati sensibili in MS SharePoint Online, OneDrive e Teams

Sicurezza di Office 365

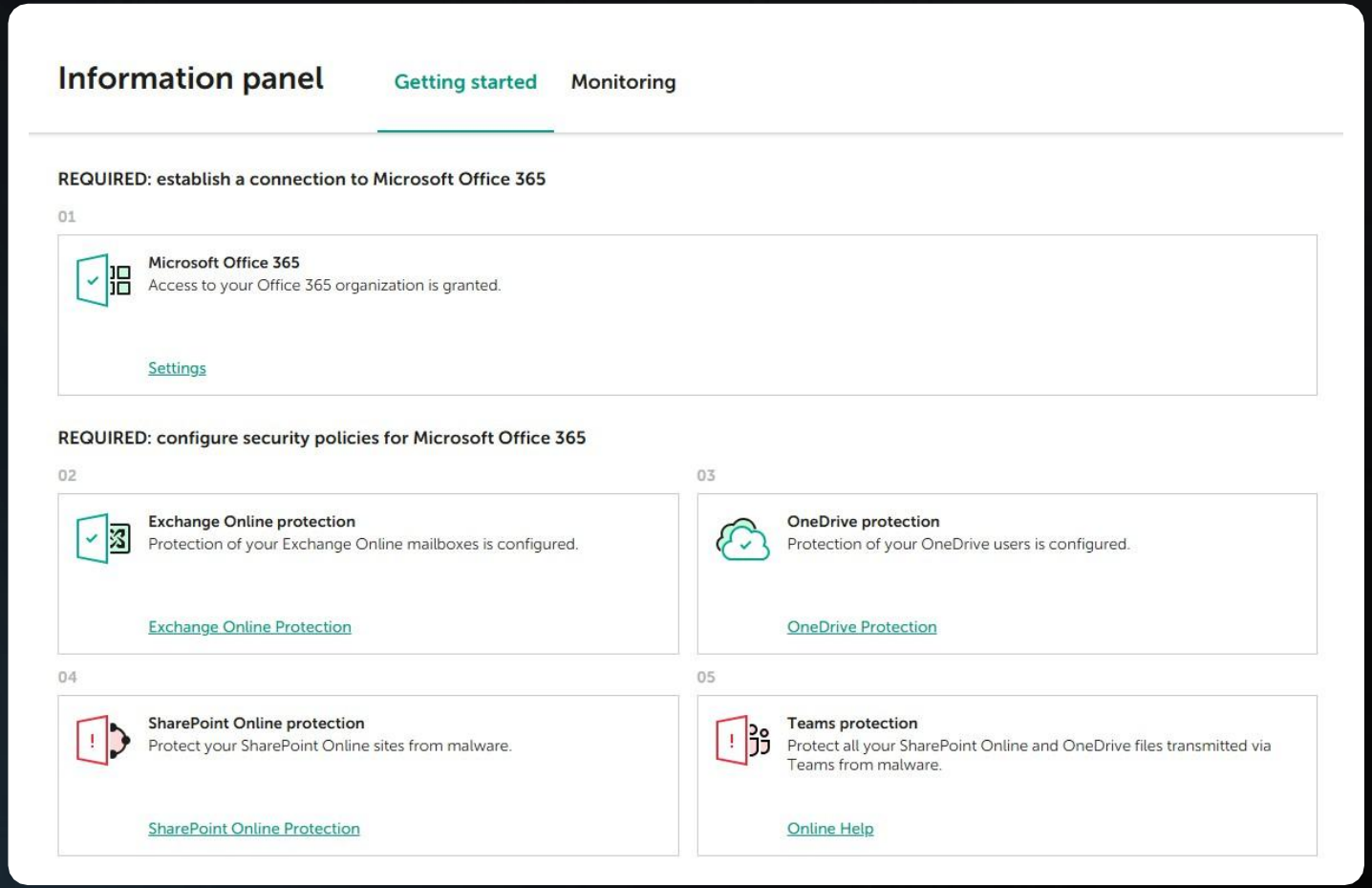
Anti-phishing, anti-malware, anti-spam, rimozione degli allegati indesiderati

Scoprite quali dati sensibili sono archiviati nelle app Microsoft 365.

Sicurezza di Office 365

Cloud security

- Protezione avanzata dalle minacce
- Anti-phishing, anti-malware, anti-spam, rimozione degli allegati dannosi
- Per tutte le principali applicazioni MS Office 365

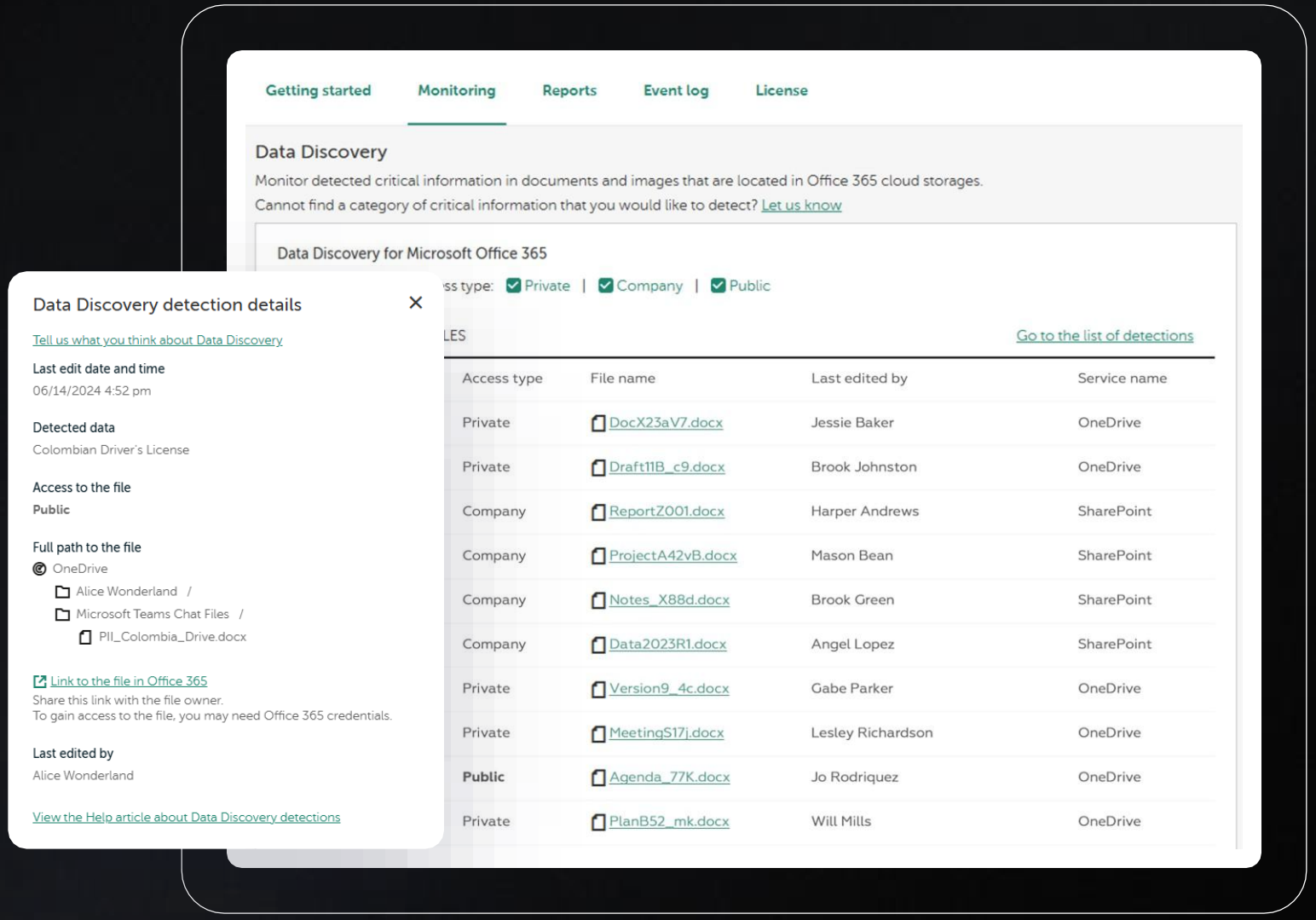


Data Discovery

Cloud security

Ottenete visibilità e controllate i dati sensibili nelle app Office 365.

I risultati sono disponibili in report e nell'elenco dei rilevamenti eseguiti, oltre che nei widget della dashboard.



Kaspersky

kaspersky