Potenziate la vostra attività in crescita con una sicurezza estesa, efficace, intuitiva e conveniente

Kaspersky Next XDR Optimum

kaspersky bring on the future

Per le piccole e medie imprese

Kaspersky Next XDR Optimum è destinato alle piccole e medie imprese con un'infrastruttura IT consolidata e un budget ragionevole per la cybersecurity. Indipendentemente dal fatto che la sicurezza sia gestita da un team IT più ampio o da un piccolo gruppo dedicato, la soluzione fornisce strumenti facili da gestire che assicurano una protezione completa e affidabile senza sovraccaricare le risorse esistenti.

Ottenete il massimo dalle vostre risorse e aumentate l'efficacia della risposta agli incidenti

Le minacce informatiche che colpiscono le piccole e medie imprese stanno diventando sempre più sofisticate e attive. Sempre più spesso gli autori degli attacchi sfruttano strumenti di sistema legittimi e tecniche avanzate per eludere il rilevamento. Nel frattempo, i dipendenti che non sono consapevoli dei rischi per la cybersecurity sono vulnerabili ad attacchi di phishing e di social engineering, che causano danni finanziari e reputazionali.

Allo stesso tempo, le risorse limitate, tra cui budget ridotti e carenza di personale qualificato, rendono ancora più difficile la difesa contro queste minacce. Ecco perché è fondamentale disporre di strumenti avanzati ma semplici da usare, che garantiscano un adeguato livello di protezione per la vostra azienda.

Estendete la sicurezza con Kaspersky Next XDR Optimum

Progettata per i team di sicurezza più piccoli, la soluzione rafforza la risposta agli incidenti e consente lo sviluppo di competenze senza aggiungere attività di routine che richiedono molto tempo. Grazie all'automazione di diversi processi, il vostro team può concentrarsi su ciò che conta.

Kaspersky Next XDR Optimum si integra facilmente nell'infrastruttura esistente, senza bisogno di aggiungere nuovi componenti di sistema.

Rilevamento, analisi e risposta

- Rilevamento comportamentale
- Aggregazione degli avvisi
- Cloud Sandbox
- Individuazione delle prove delle minacce (IoC) e IoC personalizzati
- Analisi delle root cause
- Gamma di azioni di risposta

Funzionalità di protezione endpoint

- Anti-malware avanzato
- Hardening esteso
- Valutazionevul-nerabilità
- Controlli degli endpoint
- Protezione dei dati
- Gestione patch

Da un livello eccezionale di protezione endpoint e sicurezza cloud all'automazione delle attività IT e alle funzionalità XDR essenziali:

Affidatevi a una protezione **endpoint straordinaria**

Evitate interruzioni delle attività aziendali con la protezione automatica tramite strumenti anti-ransomware e anti-malware basati su machine learning, che prevengono le infezioni causate da minacce note e sconosciute.

Correggete le vulnerabilità attraverso l'hardening dei sistemi e la formazione

Riducete la superficie di attacco con l'hardening dei sistemi basato sul comportamento dell'utente e risparmiate tempo con la gestione centralizzata delle vulnerabilità, delle patch e del criptaggio. Inoltre, forniamo la formazione di cui il vostro team ha bisogno per sfruttare al meglio le vostre nuove funzionalità di sicurezza.

Estendete le funzionalità di **rilevamento e risposta**

Ottenete informazioni approfondite sulle minacce e sul loro movimento all'interno e all'esterno degli endpoint. Utilizzate l'automazione e la risposta guidata per contrastare gli attacchi, nonché strumenti di indagine essenziali per tracciarne le attività.

Formate l'intero team affinché svolga un ruolo attivo nella sicurezza

Fornite al personale IT e ai dipendenti non tecnici le conoscenze e le competenze necessarie per garantire la sicurezza. Rafforzate il vostro team di sicurezza IT e create una cultura aziendale solida e attenta alla sicurezza tra i dipendenti.

Sfruttate il nostro sistema basato sul cloud per **l'elaborazione dei file**

Esaminate facilmente i file dannosi e ottenete più contesto e dettagli con la nostra integrazione Cloud Sandbox: fate l'upload dei sample potenzialmente dannosi per verificarne la reputazione in pochi secondi direttamente dall'interfaccia del prodotto e utilizzate i dati generati per le future scansioni IoC.

Controllate lo Shadow IT con una sicurezza cloud su cui potete contare

Riducete le vulnerabilità e salvaguardate i dati e i dipendenti controllando lo Shadow IT. Scoprite quali servizi cloud vengono utilizzati, bloccate gli accessi non autorizzati e identificate i dati sensibili archiviati nelle app Microsoft 365.

Approfittate di **diverse opzioni di distribuzione**

Riducete il costo totale di proprietà con strumenti di automazione e distribuzione basati sul cloud oppure eseguite l'installazione on-premises per un controllo completo[1].

[1] La console di gestione on-premises è basata su Linux. Kaspersky Next XDR Optimum supporta tutti i sistemi operativi attraverso i suoi agenti endpoint e la console cloud. Un'opzione di distribuzione su cloud sarà disponibile nel quarto trimestre del 2025

Kaspersky Next XDR Optimum: incluso nella product line Kaspersky Next

Kaspersky Next è una linea di prodotti con diversi livelli per le aziende di qualsiasi dimensione. Kaspersky Next Optimum è pensato per le piccole e medie imprese con team di cybersecurity snelli che desiderano ampliare la protezione senza aggiungere complessità. Inizia con una solida protezione endpoint, potenziata da funzionalità Endpoint Detection and Response e consente un aggiornamento graduale a capacità XDR o MXDR essenziali per un livello sofisticato di cybersecurity.

PerchéKaspersky Next Optimum?

Basato sulla nostra soluzione endpoint più avanzata

Da oltre un decennio i prodotti Kaspersky si classificano costantemente nelle prime posizioni nei test e nelle recensioni indipendenti. 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

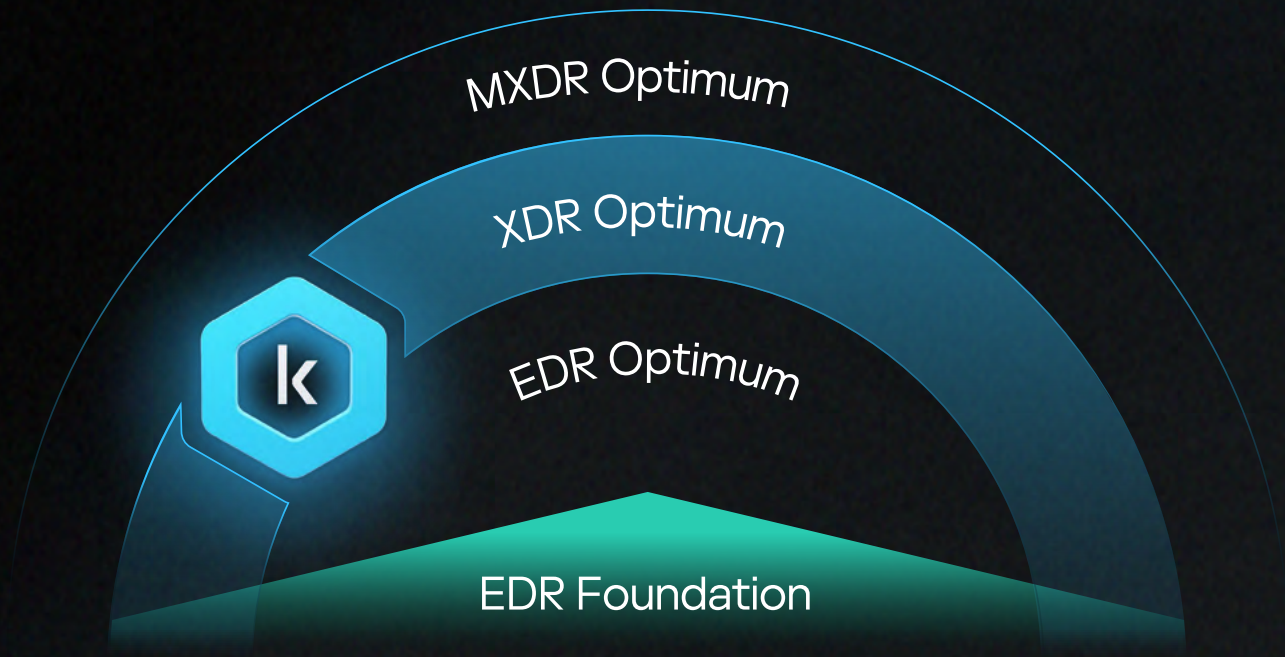
Kaspersky Next si basa su decenni di esperienza accumulata e sulle approfondite competenze dei nostri team di sicurezza globali. I nostri specialisti collaborano per affrontare le minacce informatiche complesse, perfezionando costantemente le tecnologie alla base dei nostri prodotti. Questo approccio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

Difesa multilivello basata sulla tecnologia AI

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.



www.kaspersky.it

Per saperne di più

#kaspersky
#bringonthefuture