kaspersky 25 years

Kaspersky Optimum Security

State al passo con le minacce elusive: con funzionalità EDR[1]/MDR[2] complete che non graveranno sulle vostre risorse.

Kaspersky Optimum Security

Il 30% dei cyberattacchi andati a buon fine ha sfruttato strumenti di sistema legittimi

Kaspersky Incident Response Analyst Report, 2020

La sfida

Ransomware, malware e spyware finanziario sono diventati più abili nell'eludere il rilevamento, oltre a essere facili ed economici da acquistare attraverso il Dark Web, tutti elementi che oggi mettono in serie difficoltà molte organizzazioni.

Gli attacchi avanzati sono in aumento

Le minacce elusive odierne sono progettate per ignorare efficacemente la tradizionale protezione degli endpoint, introducendo rischi significativi per tutte le aziende. Se una minaccia non rilevata riesce a infiltrarsi nella vostra infrastruttura, potreste dover fronteggiare perdite significative con un impatto enorme sugli utili dell'azienda:

- interruzione dei processi business-critical e perdita dei dati
- ingenti danni alla reputazione e perdita di clienti
- multe e perdita di profitti.

La protezione degli endpoint va rafforzata

Questi ultimi attacchi **evitano il rilevamento** nascondendosi all'interno di strumenti di sistema legittimi e altri metodi e tecnologie prontamente accessibili, utilizzandoli per **ottenere l'accesso, persistere ed eseguire azioni dannose all'interno dell'infrastruttura, in modo rapido e inosservato**.

Il lavoro a distanza, dal canto suo, non fa altro che dare ulteriore risalto agli endpoint, che sono indiscutibilmente i punti di accesso all'infrastruttura più ambiti in assoluto.

Le risorse sono già sfruttate al massimo

Per garantire il vantaggio aggiuntivo di cui avete bisogno, la vostra organizzazione deve sviluppare capacità di risposta agli incidenti adeguate.

Ma un progetto come questo può avere costi elevati:

- software e hardware necessari possono essere molto costosi
- gli strumenti e i processi frammentati e divisi in silos abbassano l'efficienza della sicurezza
- si spreca tempo in attività di routine.

Il 45% degli attacchi è stato rilevato a causa di file sospetti o attività sospette degli endpoint, il cui rilevamento diventa quindi prioritario

Come sopra

La soluzione

Kaspersky Optimum Security rappresenta una soluzione efficiente di threat detection and response, supportata da un monitoraggio 24/7, risposte automatizzate e threat hunting, con l'assistenza e la guida degli esperti Kaspersky.

Protezione avanzata

I metodi di prevenzione automatica sono alla base di qualsiasi soluzione di protezione degli endpoint, ma devono essere corredati da strumenti avanzati, se si vogliono gestire le minacce elusive più pericolose.

Kaspersky Optimum Security fornisce un rilevamento avanzato basato su **machine learning** e capacità di risposta rapida, il tutto tramite il cloud. Il vostro team potrà affrontare anche le minacce prima considerate imbattibili con la massima rapidità e precisione.

Un investimento ottimale

Non ci sarà bisogno di assumere personale e formare lo staff esistente, né di impazzire per far funzionare una complicata distribuzione: Kaspersky Optimum Security semplifica e aiuta ad automatizzare i processi cruciali di risposta agli incidenti, adattandosi ai vostri requisiti specifici.

Le opzioni cloud e on-premises e un set di strumenti di sicurezza pronto e scalabile si adattano alle vostre esigenze, aiutandovi a ridurre la complessità del sistema IT, ad aumentare la produttività degli utenti e a rendere trasparenti i costi di implementazione.

Equilibrio ottimale

Raggiungete l'equilibrio ottimale fra semplificazione ed efficacia, intelligenza umana e automazione, efficienza e funzionalità, senza fare alcuna concessione alla vostra protezione!

Kaspersky Optimum Security vi aiuta a ridurre drasticamente il rischio di perdere denaro, clienti e reputazione, rafforzando le vostre difese contro le minacce nuove, sconosciute ed elusive. Con questa soluzione sarete pronti per affrontare il panorama odierno delle minacce in costante evoluzione.

Vantaggi chiave

- **Difendete la vostra azienda dal rischio reale di subire danni e interruzioni della produttività che possono essere causati** dalla più recente ondata di minacce elusive letali.
- **Sviluppate la vostra capacità interna** di risposta agli incidenti, sfruttando gli strumenti EDR (Endpoint Detection and Response) semplicissimi da usare.
- **Portate le vostre capacità di rilevamento al livello successivo con facilità,** grazie alle funzionalità MDR (Managed Detection and Response) potenti e immediate.
- Riducete notevolmente il rischio di attacco mediante **corsi di formazione per i vostri dipendenti, in grado di aumentare la loro consapevolezza della sicurezza.**
- Risparmiate preziose risorse sfruttando **l'automazione delle operazioni e la protezione gestita.**
- Risparmiate tempo e fatica con una soluzione che offre numerose funzionalità gestite **attraverso un'unica console, cloud oppure on-premises.**

Il 55% degli attacchi ha richiesto settimane o più per essere rilevato

Come sopra

Funzionalità principali

Kaspersky Optimum Security offre una vasta gamma di funzionalità essenziali per la protezione dalle minacce elusive. Tra le principali funzionalità sono inclusi rilevamento, analisi e risposta.

Advanced detection

- **Algoritmi di analisi del comportamento** basati su machine learning rilevano comportamenti sospetti in modo rapido e preciso.
- **Il threat hunting automatizzato**, basato su Indicatori di attacco proprietari (IoA, Indicators of Attack), rileva minacce complesse nascoste, il tutto con l'aiuto degli esperti Kaspersky.
- La funzionalità Controllo adattivo delle anomalie **gestisce automaticamente la configurazione degli strumenti per ridurre la superficie di attacco** in base ai profili degli utenti.
- Rilevamento cloud, inclusa una **sandbox cloud integrata**.

Analisi semplificata

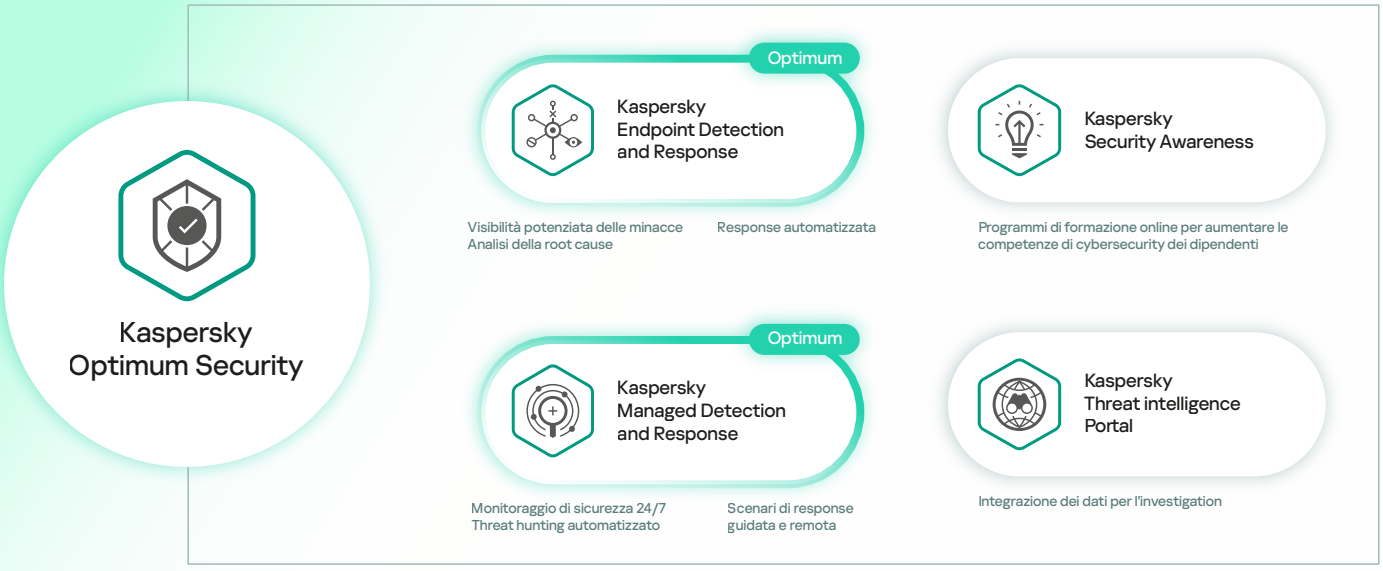
- Tutte le informazioni relative a un incidente vengono automaticamente raccolte in **un'unica scheda**.
- **La rappresentazione grafica e un processo di** indagine semplificato permettono di analizzare l'incidente in modo rapido ed efficiente, all'interno di un unico ambiente, per decidere come procedere al riguardo.
- Nel frattempo, tutti i rilevamenti ottenuti tramite gli IoC vengono esaminati da Kaspersky con **assoluta priorità per potervi fornire consigli personalizzati**.

Response automatizzata

- **La risposta rapida, con un solo clic**, permette di circoscrivere immediatamente un singolo incidente.
- **Grazie alla competenza** degli esperti Kaspersky, le risposte guidate permettono di affrontare anche le minacce più complesse e pericolose.
- **La risposta automatizzata su più endpoint** permette di individuare e gestire minacce analizzate o importate in qualsiasi punto della rete.

Sommario

Scegliete come usare Kaspersky Optimum Security: come soluzione gestita per avere una protezione ininterrotta, come set di strumenti EDR semplice da usare, oppure come un mix di entrambi, sfruttando l'esperienza e la competenza degli esperti Kaspersky, pur sviluppando internamente le vostre capacità di rilevamento e risposta. Kaspersky Optimum Security riunisce diversi prodotti in un'unica soluzione:



I messaggi e-mail dannosi costituivano il **31%** dei cyberattacchi andati a buon fine, quindi molti di essi avrebbero potuto essere evitati dai dipendenti stessi

Come sopra

E non è finita qui...

Potete potenziare ulteriormente le vostre difese con una serie di strumenti mirati ai vari aspetti della vostra sicurezza: rilevamento, indagine e consapevolezza.

Formazione degli utenti

Il segreto per ridurre la vostra superficie d'attacco e il numero degli incidenti di sicurezza è rendere i vostri dipendenti consapevoli delle minacce informatiche che per negligenza o semplice ignoranza potrebbero involontariamente introdurre nella vostra infrastruttura. **Kaspersky Security Awareness** aumenta la competenza e le abilità di tutti i dipendenti, permettendovi di proteggere la vostra infrastruttura mantenendo un ambiente virtuale sicuro grazie alla compartecipazione attiva di tutti gli utenti.

Leggete le ultime informazioni

Aiutate i vostri specialisti della cybersecurity ad analizzare e capire le minacce ancor più profondamente e rapidamente con le più recenti informazioni su file, hash, IP e URL associati ai threat. Ottenete una maggiore consapevolezza senza costi aggiuntivi, grazie al semplicissimo **Kaspersky Threat Intelligence Portal**.

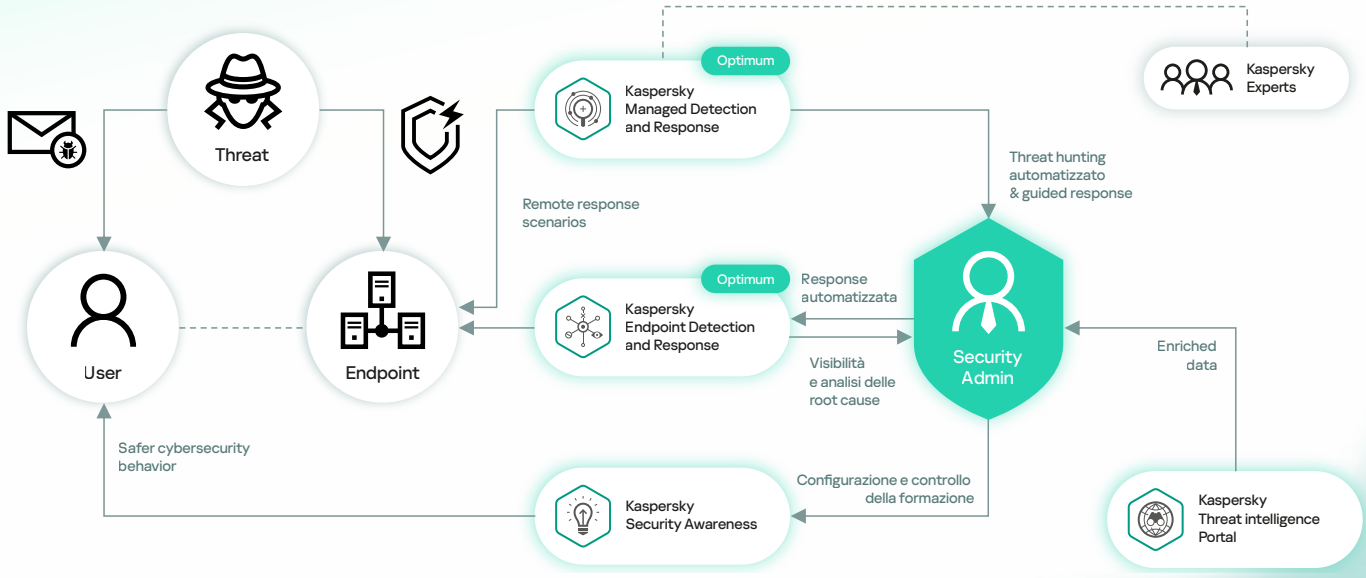
Consentiteci di aiutarvi

Per assicurarvi una protezione efficace della vostra infrastruttura IT, è necessario implementare e configurare i prodotti secondo le best practice e i vostri specifici requisiti di sicurezza.

Ottimizzate il ROI della vostra soluzione di sicurezza e assicuratevi che funzioni al 100% della capacità, consentendo ai nostri esperti dei **Kaspersky Professional Services** di aiutarvi a controllare, implementare, mantenere e ottimizzare la vostra soluzione di sicurezza.

Funzionamento generale

Prevenzione, rilevamento, analisi, risposta e formazione dei dipendenti sono tutti inclusi in Kaspersky Optimum Security. Ciascun componente apporta il proprio valore e può essere utilizzato separatamente, ma tutti contribuiscono a rispondere alle vostre esigenze di protezione degli endpoint elusivi in un'unica soluzione integrata.



Il 44% delle aziende considera il costo della protezione di ambienti sempre più complessi uno dei principali problemi

IT Security Economics 2021, Kaspersky

Funzionamento semplificato

Scoprirete che Kaspersky Optimum Security è semplice da gestire da un'unica console, permettendovi di sfruttare al massimo il tempo e le risorse a vostra disposizione.

Pacchetto completo

- Parte dell'ecosistema di sicurezza Kaspersky, potenzia le vostre difese partendo dalle basi della sicurezza fino a raggiungere funzionalità ottimizzate avanzate.
- Le varie funzionalità di Kaspersky Optimum Security possono essere gestite attraverso un'unica console cloud.
- Più livelli di protezione affrontano sia le minacce comuni che quelle elusive, nonché il rischio derivante dall'errore umano.

Facilità di gestione

- La console di gestione cloud offre un controllo rapido ed efficiente da qualsiasi postazione nel mondo.
- Le opzioni on-premises e SaaS garantiscono la stessa esperienza di gestione.
- La distribuzione è rapida e semplice, anche se non avete ancora familiarità con le soluzioni Kaspersky.
- Tutti gli strumenti possono essere controllati e gestiti in modo semplice e intuitivo dal vostro team, senza bisogno di un lungo processo di familiarizzazione o formazione.

Risparmiare tempo e risorse

- La protezione gestita vi aiuta a creare funzionalità di rilevamento e risposta senza i livelli associati di investimento nella sicurezza, anche se avete poca esperienza e poco personale addetto alla cybersicurezza.
- I processi fondamentali vengono automatizzati, rendendo la risposta agli incidenti veloce, precisa ed efficiente.
- Una migliore security awareness dei dipendenti riduce il numero di minacce che riusciranno a penetrare le vostre difese e, di conseguenza, gli incidenti da gestire!

In pratica

Parliamo di come funzionano in pratica tutti questi strumenti.

Penetration

L'utente riceve un'e -mail di phishing oppure accede a una risorsa web dannosa, infettando l'host

- Security awareness dei dipendenti
- Riduzione della superficie di attacco
- Prevenzione automatizzata delle minacce

Installazione

Il vettore iniziale d'infezione distribuisce i componenti necessari, comunica con un server C&C[1] ed esplora l'ambiente circostante

- Meccanismi di detection avanzati, tra cui analisi comportamentale basata su machine learning e sandbox cloud
- Threat hunting automatizzato con IoA[2]
- Scenari di response guidata e remota

Rooting

Viene impiegata una serie di strumenti per ottenere persistenza e iniziare i movimenti laterali, se necessario

- Analisi delle root cause e scansione IoC[3]

[1] Comando e controllo
[2] Indicatori d'Attacco
[3] Indicatori di Compromissione

L'approccio passo-passo di Kaspersky

Insieme possiamo costruire le vostre difese, partendo dall'affidabile protezione offerta da Kaspersky Security Foundations e salendo gradualmente fino alle capacità di risposta agli incidenti di Kaspersky Optimum Security, per raggiungere il massimo con l'applicazione dei potenti strumenti di Kaspersky Expert Security, volti a proteggervi dalle minacce più avanzate. Scegliete il livello più adatto a voi:

Kaspersky Security Foundations

Blocco automatico della stragrande maggioranza delle minacce.

» Per saperne di più

Kaspersky Optimum Security

Potenziate le misure di difesa contro le minacce elusive.

» Per saperne di più

Kaspersky Expert Security

Reazione immediata ad attacchi complessi e APT.

» Per saperne di più

Chi siamo

Siamo un'azienda di cybersicurezza globale privata con centinaia di migliaia di clienti e partner in tutto il mondo, che opera nell'ottica della trasparenza e dell'indipendenza. Da 25 anni creiamo strumenti e forniamo servizi per tenervi al sicuro con le nostre **tecnologie più testate e premiate**.

IDC

IDC MarketScape Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment

Attore principale

AV-Test

Advanced Endpoint Protection: Ransomware Protection Test

Protezione al 100%

Radicati Group

Advanced Persistent Threat (APT) Market Quadrant

Top Player

Date un'occhiata più da vicino

Per maggiori informazioni sul modo in cui Kaspersky EDR Optimum affronta le minacce informatiche riducendo al minimo l'impegno del team di sicurezza e delle risorse aziendali, consultate la pagina **https://www.kaspersky.it/enterprise-security/edr-security-software-solution**

[1] Endpoint Detection and Response
[2] Managed Detection and Response

Novità sulle cyberminacce: securelist.it
Novità sulla sicurezza IT:
www.kaspersky.it/blog/category/business
Sicurezza IT per PMI:
www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per l'azienda:
www.kaspersky.it/enterprise-security

kaspersky.it