Kaspersky Endpoint Detection and Response Optimum

Rafforzate le difese degli endpoint e affrontate le minacce elusive in tutta semplicità.

kaspersky 25 years

Kaspersky Endpoint Detection and Response Optimum

È ora di passare a un livello più avanzato. Sarete pronti non solo a proteggere la vostra azienda con le tecnologie anti-malware essenziali, ma anche a identificare, analizzare e neutralizzare in modo efficace le minacce deliberatamente progettate per eludere le tradizionali misure di protezione, che si nascondono in profondità nei vostri sistemi, pronte a sferrare nuovi e pericolosi attacchi.

Le sfide

Minacce che eludono il rilevamento

Malware, ransomware, spyware e altre minacce elusive stanno diventando sempre più abili nell'eludere i meccanismi di rilevamento tradizionali, utilizzando strumenti di sistema legittimi e altre tecniche di attacco avanzate.

Il 64% delle aziende è già stato vittima di attacchi ransomware. Di questo 64%, il 79% ha pagato il riscatto agli autori degli attacchi.

Kaspersky, maggio 2022

Ransomware-as-a-service

Gli hacker possono acquistare a costo minimo strumenti predefiniti per attaccare chiunque: rubando i dati, danneggiando l'infrastruttura e richiedendo somme sempre più ingenti di riscatto.

Risorse limitate

Le infrastrutture stanno diventando sempre più complesse e diffuse mentre le risorse (tempo, denaro e capacità di attenzione) stanno diminuendo. Non c'è spazio per lo shelfware.

"Di Kaspersky apprezziamo le soluzioni complete, l'affidabilità, il servizio e l'assistenza tempestivi. Tutto questo garantisce la disponibilità del nostro ambiente IT."

Marcelo Mendes, CISO, NEO
leggete il case study

In che modo Kaspersky può essere d'aiuto

Con avanzate funzionalità di detection facili da usare e processi semplici e automatizzati di detection e response, Kaspersky Endpoint Detection and Response (EDR) Optimum aiuta a identificare, analizzare e neutralizzare anche le minacce più sfuggenti.

Protezione avanzata

I nostri meccanismi di rilevamento avanzato includono tecnologie quali machine learning, analisi del comportamento e sandbox cloud.

Semplici strumenti di analisi visiva consentono di comprendere appieno la minaccia e il relativo ambito e le azioni di risposta rapide bloccano l'attacco prima che possa fare danni.

Un'unica soluzione

La sicurezza degli endpoint di ultima generazione è unita a una tecnologia EDR di facile utilizzo per la protezione ottimizzata di laptop, workstation, server, carichi di lavoro cloud e ambienti virtuali.

Tutti questi strumenti di gestione e distribuzione si trovano in un'unica posizione, tramite una singola console cloud o on-premises.

Semplicità ed efficienza

EDR Optimum è stato creato pensando ai team di cybersicurezza più piccoli, per chi sta cercando di eseguire l'upgrade delle capacità di risposta agli incidenti e di sviluppare competenze, senza tuttavia avere molto tempo a disposizione.

La maggior parte delle attività viene automatizzata e ottimizzata, lasciandovi più tempo da dedicare a ciò che conta davvero.

Vantaggi chiave

- **Prevenite diversi tipi** di minacce
- **Proteggete i vostri sistemi e i dati** dalle minacce elusive
- **Bloccate le minacce attive**prima che possano danneggiarvi
- **Riconoscete le minacce elusive** negli endpoint
- **Riconoscete la minaccia** e analizzatela rapidamente
- **Prevenite i danni** con una rapida risposta automatica
- **Risparmiate tempo e risorse** con un unico strumento semplificato
- **Difendete ogni singolo endpoint:** laptop, server, carichi di lavoro cloud

Funzionalità principali

- Sicurezza degli endpoint di ultima generazione **innata**
- **Rilevamento avanzato** basato su machine learning
- **Scansione IoC** (Indicator of Compromise, indicatori di compromissione)
- **Strumenti** di analisi e indagine di tipo visivo
- Tutti i dati necessari in **un'unica scheda di avviso**
- **Automazione e guida** integrata per la risposta
- **Un'unica console cloud e on-premises** e automazione
- Supporta **workstation, server fisici e virtuali, distribuzioni VDI e carichi di lavoro in cloud pubblici**

Casi di utilizzo chiave

Siamo sotto attacco?

- **Rilevamento avanzato**: basato su tecnologie di machine learning, inclusa la sandbox cloud, è in grado di rilevare automaticamente le minacce.
- **Scaricate ed esaminate gli IoC** da securelist.com o altre fonti per rilevare le minacce avanzate.

È possibile neutralizzale?

- **Utilizzate più opzioni di risposta**: isolate gli host, impedite l'esecuzione dei file o rimuoveteli.
- **Esaminate altri host** per rilevare indicatori della minaccia analizzata.
- **Applicate una risposta automatica** negli host quando rilevate una minaccia (IoC).

Come si accede ai corsi di formazione?

- **Consultate la guida alla risposta** nella scheda di avviso.
- **Accedete alThreat Intelligence Portal** e alle più recenti tecnologie di threat intelligence.
- **Sviluppate le vostre competenze** quando analizzate e rispondete alle minacce.

Com'è successo?

- Analizzate la minaccia in una **struttura dei processi visiva.**
- Tenete traccia delle relative azioni in un **grafico approfondito.**
- **Individuate la causa principale e il punto di ingresso** nell'infrastruttura.

Come si può impedire che accada di nuovo?

- **Utilizzate le informazioni acquisite:** ormai sapete quali sono gli IP e i siti Web da bloccare, i criteri da modificare e i dipendenti da formare.
- **Create regole per prevenire** tali minacce in futuro, ad esempio prevenendo l'esecuzione dei file.

E per tutte le minacce comuni?

- **La sicurezza degli endpoint di ultima generazione** mira a bloccare sul nascere la maggior parte delle minacce.
- **Potenziate l'applicazione delle patch** con Vulnerability e Patch Management.
- **Automatizzate la riduzione della superficie di attacco** e la regolazione dei criteri con i controlli endpoint.

Come funziona

Per una rapida dimostrazione, consultate questo video.

Da dove venite?

Disponete di un prodotto anti-malware, ma non è sufficiente?

Potenziate la vostra protezione degli endpoint

Sia che stiate utilizzando Kaspersky o una protezione degli endpoint di terze parti, questo è il momento giusto per pensare all'implementazione dell'EDR.

Non si tratta solo di migliorare le capacità di rilevamento e prevenzione, ma anche di essere preparati ad affrontare le minacce elusive, identificandole, analizzandole e neutralizzandole.

Scoprite di più su come proteggervi dalle minacce elusive con la **Guida per l'acquirente alla sicurezza di livello Optimum**.

Usate già Kaspersky?

Ottimizzate la sicurezza

Miglioriamo costantemente i nostri prodotti. Per utilizzarli al meglio effettuate un upgrade oppure passate al cloud e dimenticate completamente le fastidiose attività di routine.

Nella versione più recente di Kaspersky EDR Optimum:

- Risposta guidata nella scheda di avviso.
- Controllo degli oggetti critici di sistema prima di applicare la risposta.
- Reputazione dei file basata sulla threat intelligence nella scheda di avviso.
- Analisi della struttura dei processi con livello di approfondimento illimitato.

Scoprite di più sulle nuove funzionalità **qui**.

Non sei ancora cliente Kaspersky?

Ottimizzate la sicurezza

Migliaia di aziende di tutto il mondo utilizzano Kaspersky EDR Optimum perché offre:

- Potenti funzionalità EPP ed EDR di base in un unico prodotto
- Funzionalità EDR semplici da usare, progettate per i team di cybersicurezza più piccoli
- Una soluzione flessibile e leggera con distribuzione cloud e on-premises

Date un'occhiata a **Kaspersky Optimum Security**, una soluzione combinata contro le minacce elusive, basata sulla tecnologia EDR e MDR.

Avanzate con un approccio graduale

Gli strumenti utilizzati dovrebbero essere perfetti per le esigenze aziendali e di cybersicurezza, nonché per il team e le risorse. Per questo abbiamo semplificato la scelta del livello di cybersicurezza, principale argomento del momento, con tre opzioni differenti in base al profilo della vostra organizzazione.

Kaspersky Security Foundations

Blocco automatico della stragrande maggioranza delle minacce.

- Prevenzione automatica multi-vettore degli incidenti causati da minacce comuni, che costituiscono la stragrande maggioranza degli attacchi informatici.
- La base di partenza, per aziende di qualsiasi dimensione e complessità, per costruire una strategia integrata di difesa.
- Protezione degli endpoint affidabile per aziende con piccoli team IT e una competenza in crescita nel campo della cybersicurezza.

» Per saperne di più

Kaspersky Optimum Security

Costruite strategie di difesa contro le minacce elusive, se avete:

- Un piccolo team di sicurezza IT con una conoscenza di base in materia di cybersicurezza.
- Un ambiente IT con dimensioni e complessità in aumento, quindi con un incremento della superficie di attacco.
- Una carenza di risorse dedicate alla cybersicurezza, pur necessitando di una protezione potenziata.
- Una crescente necessità di sviluppare una capacità di risposta agli incidenti.

» Per saperne di più

Kaspersky Expert Security

Reazione immediata ad attacchi complessi e APT per le organizzazioni:

- Con ambienti IT complessi e distribuiti.
- Con un team di sicurezza IT maturo o un Security Operations Center (SOC) consolidato.
- Con una bassa propensione al rischio a causa dei costi più elevati derivanti dalla gestione di incidenti di sicurezza e violazioni dei dati.
- Operanti in un campo in cui la conformità alle normative è prioritaria.

» 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

Se volete andare oltre

Date un'occhiata a **Kaspersky EDR Expert**, un potente strumento EDR per fornire ai vostri esperti capacità di threat hunting approfondite, personalizzazione di vasta portata e meccanismi di rilevamento superiori.

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**

Novità sulle cyberminacce: securelist.com
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