kaspersky BRING ON THE FUTURE

Kaspersky Optimum Security

Ottenete il miglior livello di cybersecurity grazie alla managed protection e alla endpoint detection and response sugli endpoint cloud-enabled

La sfida

Dovete riuscire a difendere efficacemente la vostra azienda dalle minacce nuove, sconosciute ed elusive, senza perdere tempo e senza sottrarlo alle limitate risorse a vostra disposizione.

Il 30% degli attacchi andati a segno ha coinvolto strumenti di sistema legittimi[1]

Gli attacchi avanzati sono in aumento

Le minacce elusive di oggi, progettate per bypassare efficacemente le tradizionali difese degli endpoint, comportano un rischio senza precedenti per le aziende, poiché gli attacchi sono sempre più difficili da individuare, analizzare e gestire. 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
- ingenti danni alla reputazione e perdita di clienti
- multe e perdita di profitti.

La protezione degli endpoint va rafforzata

Gli attacchi elusivi di ultima generazione sono diventati sempre più efficienti, poiché i cybercriminali sfruttano legittimi tool di sistema, metodi e tecnologie pronti all'uso, che permettono loro di accedere e permanere all'interno della vostra infrastruttura, attuando azioni dannose in modo rapido e silente.

A complicare ulteriormente la situazione ci sono la dissoluzione del perimetro aziendale e lo smart working diffuso, che mettono ancora più a rischio gli endpoint, tradizionalmente punti d'accesso privilegiati all'infrastruttura aziendale.

Le risorse sono già sfruttate al massimo

Per garantire il vantaggio in più che oggigiorno l'endpoint security richiede, è necessario sviluppare adeguate capacità di incident response all'interno della vostra azienda.

Ma i costi associati a un progetto simile possono facilmente sfuggire di mano:

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

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.

Il 45% degli attacchi è stato individuato a causa di file sospetti o attività sospette sugli endpoint[1]

Protezione avanzata dalle minacce

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.

Soluzione chiavi in mano, rapida e scalabile

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

Kaspersky Optimum Security fornisce una advanced detection e response rapida, tramite cloud. I vostri cybersecurity engineer potranno affrontare anche le minacce prima considerate imbattibili con la massima rapidità e precisione.

Un investimento Optimum

Non ci sarà bisogno di assumere personale e formare lo staff esistente, né di impazzire per far funzionare un complicato deployment: Kaspersky Optimum Security semplifica e aiuta ad automatizzare i processi cruciali di incident response, adattandosi ai vostri requisiti specifici.

Risponde alle vostre necessità con opzioni on-premise e in cloud, e con un set di tool di sicurezza pronto all'uso, che vi aiuterà a ridurre la complessità del vostro sistema IT e ad aumentare la produttività dei vostri utenti, con costi di implementazione trasparenti.

Vantaggi chiave

- Siate sempre un passo avanti e 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 incident response, sfruttando gli strumenti EDR (Endpoint Detection and Response) semplicissimi da usare
- Riducete il rischio di infezione mediante corsi di formazione per i vostri dipendenti che aumentino la loro security awareness
- Risparmiate preziose risorse sfruttando l'automazione e le funzionalità gestite
- Risparmiate tempo e fatica con una soluzione che offre numerose funzionalità gestite attraverso un'unica console, su cloud oppure on-premise

Funzionalità principali

Kaspersky Optimum Security offre una vasta gamma di funzionalità essenziali per la protezione dalle minacce elusive. Il suo core sono la detection, l'analisi e la renspose.

Il 55% degli attacchi ha impiegato settimane o più per essere individuato[1]

Advanced detection

- Algoritmi di analisi del comportamento basati sull'apprendimento automatico rilevano comportamenti sospetti in modo rapido e preciso
- Il threat hunting automatizzato, basato su Indicatori d'Attacco proprietari, rileva minacce complesse nascoste, con l'aiuto degli esperti Kaspersky
- Adaptive Anomaly Control gestisce automaticamente la configurazione degli strumenti per ridurre la superficie d'attacco in base ai profili degli utenti

Indagini semplificate

- 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, tutte le detection ottenute tramite gli Indicatori di Attacco vengono esaminate da Kaspersky con assoluta priorità per potervi fornire consigli personalizzati

Risposta 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

Come metterlo in pratica

Kaspersky Optimum Security include una serie di tool e funzioni fondamentali, che lavorano insieme efficacemente per prevenire, rilevare e rispondere ai threat durante le varie fasi di un attacco:

Penetrazione

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

Installazione

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

Rooting

Viene impiegata una serie di strumenti (inclusi quelli legittimi e nativi del sistema) per ottenere persistenza e iniziare i movimenti laterali, se necessario

Security Awareness dei dipendenti

Riduzione della superficie di attacco

Prevenzione automatizzata delle minacce

Meccanismi di rilevamento avanzati, inclusi analisi del comportamento basata su ML e sandbox

Threat hunting automatizzato con IoA[2]

Root cause analisie scansione IoC[3]

Scenari di risposta guidata e remota

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

Ulteriore protezione

Potete potenziare ulteriormente le vostre difese con una serie di strumenti mirati ai vari aspetti della vostra sicurezza: detection, investigation e awareness.

Le e-mail dannose costituivano il 31% dei cyber attacchi andati a segno, quindi molti di essi avrebbero potuto essere evitati dai dipendenti stessi[1]

Un ulteriore livello di detection

Individuate i threat nuovi e sconosciuti ancor più rapidamente ed efficacemente con **Kaspersky Sandbox**: uno strumento che analizza automaticamente le minacce in un ambiente isolato, sfruttando algoritmi di detection e tecniche anti-evasione brevettate. Le risposte preimpostate vengono applicate automaticamente ai threat rilevati, aumentando significativamente le vostre abilità di detection, e senza necessità di alcuna gestione oltre al deployment iniziale.

Un vantaggio aggiunto per le indagini

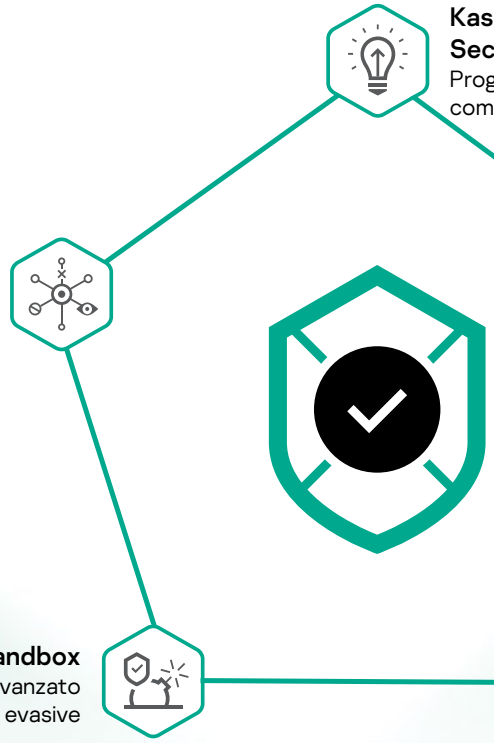
Aiutate i vostri specialisti della cybersecurity ad analizzare e capire le minacce ancor più profondamente e rapidamente con le più recenti informazioni su file, hash, IP e URL associati ai threat. Ottenete una maggiore consapevolezza senza costi aggiuntivi, grazie al semplicissimo **Portale Kaspersky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

Le persone sono la chiave della vostra sicurezza

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.

Come funziona

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 in-house le vostre abilità di detection and response. Kaspersky Optimum Security riunisce diversi prodotti in un'unica soluzione:



Kaspersky Security Awareness
Programmi di formazione online per aumentare le competenze di cybersecurity dei dipendenti

Kaspersky Endpoint Detection and Response Optimum
Visibilità avanzata delle minacce
Analisi delle cause principali
Risposta automatizzata

Kaspersky Managed Detection and Response Optimum
Monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7
Ricerca automatica delle minacce
Scenari di risposta guidata e remota

Kaspersky Sandbox
Rilevamento automatico avanzato delle minacce evasive

Kaspersky Threat Intelligence Portal
Integrazione dei dati per l'indagine

In funzione

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.

Il 56% dei partecipanti afferma che la propria azienda è a rischio, a causa di una carenza di addetti alla cybersecurity[2]

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 in cloud
- Una soluzione con vari livelli di protezione, che si occupa sia di exploit comuni che di threat elusivi, oltre a gestire il potenziale errore umano

Facilità di gestione

- La console di gestione in cloud permette un controllo rapido ed efficiente da qualsiasi postazione nel mondo
- Le opzioni on-premise e cloud-based garantiscono la stessa esperienza di gestione
- Il deployment è rapido 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, senza bisogno di un lungo processo di familiarizzazione o formazione

Risparmiare tempo e risorse

- La managed protection aiuta le aziende che non dispongono di uno staff di sicurezza IT o di esperienza in materia a beneficiare della detection and response senza grandi investimenti
- I processi fondamentali di cybersecurity vengono automatizzati, rendendo la risposta agli incidenti più veloce, più precisa e più efficiente
- Una migliore security awareness dei dipendenti fa sì che meno minacce riusciranno a penetrare le vostre difese, generando meno incidenti da gestire!

L'approccio step-by-step di Kaspersky

Insieme possiamo costruire le vostre difese, partendo dall'affidabile protezione offerta da Kaspersky Security Foundations e salendo gradualmente fino alle capacità di incident response di Kaspersky Optimum Security, per raggiungere il top 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

Blocca automaticamente la stragrande maggioranza dei threat

- Prevenzione automatica multi-vettore degli incidenti causati da exploit comuni, che costituiscono la stragrande maggioranza dei cyber attacchi.
- 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 cybersecurity

Kaspersky Optimum Security

Costruisce difese contro minacce elusive per chi:

- Dispone di un piccolo team di sicurezza IT con una conoscenza di base in materia di cybersecurity
- Dispone di un ambiente IT con dimensioni e complessità crescenti, quindi con un incremento della superficie d'attacco
- Soffre di una carenza di risorse di cybersecurity, pur necessitando di una protezione potenziata
- Lo sviluppo di abilità di incident response diventa sempre più importante

Kaspersky Expert Security

Necessità di reazione immediata ad attacchi complessi e APT dove:

- Gli ambienti IT sono complessi e distribuiti
- Il team di sicurezza IT è maturo oppure è presente un Security Operations Center (SOC)
- C'è una bassa propensione al rischio a causa degli alti costi degli incidenti di sicurezza e delle violazioni dei dati
- La compliance alle normative è un problema

Per scoprire di più su come Kaspersky Optimum Security gestisce le cyberminacce risparmiando tempo e fatica al vostro team di sicurezza e alle vostre risorse, vi preghiamo di visitare: http://go.kaspersky.com/optimum.

1 Kaspersky Incident Response Analyst Report 2019, Kaspersky, 2020
2 (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Aggiornamenti sulle minacce informatiche: www.securelist.it
News sulla sicurezza IT: www.kaspersky.it/blog/category/business/

www.kaspersky.it

2021 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.