kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Implementazione di difese informatiche solide ed efficaci, grazie alla tempestiva risposta automatica agli incidenti e all'analisi semplificata delle root cause

Il problema

Nel corso del 2019 ha subito almeno un cyberattacco il 91% delle aziende: inoltre, **1 impresa su 10** ha dovuto fronteggiare un attacco di natura mirata[1].

Le minacce complesse causano vere e proprie devastazioni

L'epoca del malware generico è ormai finita da tempo. Le minacce sono divenute molto più complesse: provocano seri danni e ingenti perdite alle aziende sottoposte ad attacco; sfuggono inoltre più a lungo al rilevamento

Siete sotto attacco

Le minacce complesse sono oggi molto più frequenti e presentano costi inferiori rispetto al recente passato: pertanto, le aziende che ritenevano di essere sufficientemente protette devono ora coprirsi bene le spalle.

L'efficienza è un fattore indispensabile

La penuria di risorse adeguate sta attualmente affliggendo molte imprese: mancano soprattutto tempo e personale qualificato.

In che modo Kaspersky può aiutare

Kaspersky Endpoint Detection and Response (EDR) Optimum consente di proteggersi efficacemente dalle minacce complesse e avanzate, grazie a sofisticate funzionalità di rilevamento, attività di investigation semplificate e innovative procedure di risposta automatizzata agli attacchi.

"Una soluzione EPP particolarmente debole è destinata a distruggere l'effettivo valore di uno strumento EDR"[2]

"Tempo e persone divengono così i nuovi parametri in termini di ROI per quanto riguarda lo strumento EDR"[2]

Ben oltre le funzionalità essenziali

Fornisce una visibilità dettagliata delle minacce agli endpoint, strumenti di investigation di facile uso e numerose opzioni di risposta automatizzata. Oltre a rilevare le minacce, la soluzione individua l'entità e la provenienza delle stesse, fornendo una risposta istantanea e assicurando la business continuity.

Una solida difesa informatica

Offre un toolkit altamente automatizzato, facile da usare, per le attività di rilevamento e risposta alle minacce: unitamente alle ineguagliabili funzionalità di protezione endpoint e rilevamento avanzato di Kaspersky Endpoint Security for Business costituisce una singola soluzione unificata.

Uno strumento intelligente, in grado di garantire piena efficienza

Consente di liberare tempo prezioso, ottimizza l'impiego del personale ed evita sovraccarichi del sistema IT fornendo semplici controlli centralizzati e un elevato livello di automazione. Assicura inoltre un flusso di lavoro semplificato tramite un'unica console, disponibile sia on-premise che nel cloud[3].

Vantaggi chiave

- Efficace protezione dalle minacce avanzate e complesse più frequenti e distruttive
- Significativi risparmi in termini di tempo e risorse, grazie all'impiego di uno strumento semplice e automatizzato
- Perfetta visibilità delle minacce complesse presenti sull'intera rete aziendale
- Possibilità di comprendere immediatamente la root cause della minaccia e il modo in cui quest'ultima si è verificata
- Una rapida risposta automatizzata consente di evitare ulteriori danni

Fondamentali use case della soluzione

Risposta a quesiti di particolare importanza

- In quale contesto si è sviluppata l'emergenza?
- Quali azioni si sono intraprese al momento dell'allerta?
- La minaccia rilevata è ancora attiva?
- Sono sotto attacco altri host?
- Quale percorso ha preso l'attacco?
- Qual è l'effettiva root cause della minaccia?

Individuazione della reale entità della minaccia

Una volta che si è scoperto di essere sottoposti a una minaccia globale, ad esempio nel momento in cui l'autorità di regolamentazione chiede di eseguire una scansione in base a uno specifico indicatore di compromissione (IoC), è possibile:

- Importare gli IoC da fonti attendibili ed effettuare scansioni periodiche alla ricerca dei segnali dell'attacco in corso
- Analizzare accuratamente l'allerta segnalata, generare gli IoC in base alle minacce rilevate ed eseguire le necessarie scansioni sull'intera rete, per determinare l'eventuale coinvolgimento di ulteriori host

Risposta istantanea alle minacce che si propagano rapidamente

- Messa in quarantena automatica dei file associati a minacce complesse su tutti gli endpoint
- Isolamento automatico degli host infetti; ricerca di un IoC associato a una minaccia che si diffonde con rapidità
- Vengono impedite l'esecuzione e la propagazione di file dannosi su tutta la rete durante l'analisi condotta dall'azienda

[1] Rapporto Kaspersky sui rischi globali IT, Kaspersky, 2019

[2] IDC, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR, Doc # US45794219, 2020

[3] Esistono alcune limitazioni riguardo alle funzionalità che si possono gestire attraverso la console cloud. Per ulteriori informazioni visitare https://kas.pr/epp-management-options

EDR

Visualizzare l'effettiva entità della minaccia

Visualizzazione degli avvisi di sicurezza sugli endpoint aziendali e conduzione di ulteriori analisi per comprendere la reale portata della minaccia. Ciò consente un'accurata gestione degli incidenti e garantisce l'assenza di elementi residui della minaccia a livello di endpoint.

Semplificare il flusso di lavoro

Perfetta combinazione di scenari e controlli EDR con un flusso di lavoro semplificato grazie a un'unica console, disponibile sia on-premise che nel cloud: le funzionalità comprendono la visualizzazione drill-down, la scansione degli IoC e opzioni di risposta che non richiedono avanzate competenze in materia di Cybersecurity, né un eccessivo impiego di tempo.

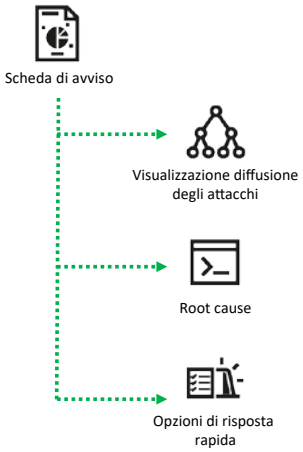
Migliorare sensibilmente le difese informatiche

L'ulteriore aggiunta di Kaspersky Sandbox genera una soluzione completa ed efficace di endpoint security integrata, in grado di offrire difese multilivello altamente automatizzate, facili da usare, nei confronti delle cyberminacce "commodity", complesse ed elusive.

Analizzare in modo dettagliato i dati relativi all'allerta in corso

Kaspersky EDR Optimum fornisce informazioni approfondite sugli incidenti informatici e consente di comprendere i legami esistenti tra eventi di vario genere grazie alla visualizzazione del percorso di diffusione dell'attacco.

Si ottiene una perfetta visibilità su tutti gli host della rete, mediante la scansione relativa agli Indicatori di Compromissione (IoC) importati o appositamente generati.



Rispondere alle minacce in modo automatico

Si possono impostare risposte automatizzate in relazione alle minacce individuate su tutti gli endpoint grazie alle scansioni IoC; tramite semplici opzioni "single-click" è inoltre possibile fornire una risposta istantanea agli incidenti nel momento stesso in cui si scopre la minaccia.

Le opzioni di risposta comprendono: isolamento dell'host, messa in quarantena del file, avvio della scansione sull'host e blocco dell'esecuzione dei file.

Adesso è possibile: Ulteriori opzioni EDR

Kaspersky Endpoint Detection and Response Optimum è una delle numerose opzioni EDR da noi offerte: ognuna di esse è personalizzabile in base alle specifiche esigenze del cliente. Ulteriori soluzioni di sicurezza disponibili:

Kaspersky Endpoint Detection and Response

Efficace soluzione EDR perfetta per le aziende IT con team di sicurezza in possesso di avanzate competenze in materia di Cybersecurity. Consente di neutralizzare anche gli attacchi di natura avanzata e mirata più sofisticati. Assicura la massima efficacia nel rilevamento delle minacce e nel processo di incident investigation; offre un threat hunting proattivo e attività di incident response centralizzate.
https://www.kaspersky.it/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

Garantisce 24 ore su 24 attività di rilevamento, assegnazione delle priorità, investigation e response completamente gestite e personalizzabili, supportate da oltre 20 anni di esperienza e ricerche in materia di Cybersecurity. Questa soluzione consente di ottenere tutti i principali vantaggi derivanti dal disporre di un proprio centro operativo per la sicurezza IT, senza di fatto doverne creare alcuno.
https://www.kaspersky.com/enterprise-security/managed-detection-and-response

Per saperne di più sul modo in cui Kaspersky Endpoint Detection and Response Optimum neutralizza le cyberminacce senza alcun impatto sulla business continuity e sulle attività del security team aziendale, visitare
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Distributore per l'Italia
Avangate Security Srl
Via F. Sforza, 40 - 20122 Milano
T. +39 059 8341380
Web: www.avangate.it

Novità sulle minacce informatiche: www.securelist.it
IT Security News:business.kaspersky.com
Sicurezza IT per grandi aziende:
www.kaspersky.it/enterprise-security
Portale Threat Intelligence opentip.kaspersky.com

www.kaspersky.it

Offriamo tecnologie di protezione comprovate. Siamo indipendenti. Siamo trasparenti. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia migliori le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Bring on cybersecurity for a safer tomorrow.

Proven. Transparent. Independent.