Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

I cybercriminali stanno diventando sempre più sofisticati e in grado di aggirare con successo la protezione esistente. Qualsiasi settore di un'azienda può essere esposto a rischi, con conseguente alterazione dei processi aziendali critici, danneggiamento della produttività e aumento dei costi operativi.

Con Kaspersky EDR, l'azienda può:

- **MONITORARE** in modo efficiente le minacce, oltre il malware generico
- **RILEVARE** efficacemente le minacce grazie all'uso di tecnologie avanzate
- **AGGREGARE** a livello centrale dati non elaborati e verdetti
- **RISPONDERE** rapidamente agli attacchi
- **PREVENIRE** azioni dannose da parte delle minacce rilevate

... il tutto attraverso un'intuitiva interfaccia Web che semplifica l'indagine e la reazione.

Kaspersky EDR e aspetti principali del report Endpoint Security 2020 di IDC*

- **Una soluzione EPP poco efficace può ridurre drasticamente il valore di uno strumento EDR**

  Kaspersky offre difese potenti e complete degli endpoint (EPP+EDR) tramite un unico agente

- **Le modalità di utilizzo del personale e il risparmio di tempo diventano quindi le nuove metriche ROI per valutare gli strumenti EDR**

  Kaspersky applica elevati livelli di automazione a problemi complessi, senza impegnare il tempo prezioso dei vostri esperti di sicurezza

- **L'EDR deve sfruttare i dati che si trovano al di fuori degli endpoint**

  Kaspersky aumenta l'efficacia dell'EDR aggiungendo il rilevamento e la visibilità delle minacce avanzate basate sulla posta e sul Web attraverso un unico strumento

Prima migliorate le difese dell'endpoint

Per i cybercriminali l'obiettivo primario è costituito da endpoint aziendali, all'interno dei quali tutti i dati, utenti e sistemi confluiscono per portare avanti i diversi processi aziendali. Per proteggere gli endpoint aziendali e impedire che vengano utilizzati come punti di ingresso nell'infrastruttura, il team responsabile della sicurezza IT deve individuare dei modi per potenziare la sicurezza esistente. L'implementazione dell'intero ciclo di protezione degli endpoint (dal classico blocco automatico delle minacce a una risposta all'incidente rapida ed efficace) richiede tecnologie preventive supportate da funzionalità di difesa avanzate.

Kaspersky Endpoint Detection and Response (EDR) offre una potente protezione su tutti gli endpoint aziendali e strumenti di difesa avanzati, consentendo l'automazione delle attività di routine per rilevare gli attacchi ATP, assegnare loro la priorità, analizzarli e neutralizzarli.

Caratteristiche principali

- Kaspersky EDR migliora la nostra più collaudata e premiata piattaforma di protezione degli endpoint (EPP), il nostro fiore all'occhiello, **Kaspersky Endpoint Security for Business**, con potenti funzionalità EDR che rafforzano ulteriormente i livelli di sicurezza complessivi. Con un singolo agente avrete a disposizione strumenti automatici di protezione dalle minacce comuni e tecnologie avanzate contro gli attacchi più sofisticati, in modo che la gestione degli incidenti risulti più semplice e i requisiti di manutenzione siano ridotti al minimo. Gli endpoint non sono sottoposti a carichi di lavoro supplementari e non ci sono costi aggiuntivi, ma solo la consapevolezza che le vostre workstation e i vostri server sono completamente protetti dalle minacce più sofisticate e mirate.
- Kaspersky EDR riduce il tempo necessario per la raccolta delle prove iniziali, fornisce un'analisi telemetrica completa e ottimizza l'automazione dei processi EDR, riducendo i tempi complessivi di risposta agli incidenti senza la necessità di consumare ulteriori risorse di sicurezza IT.
- Kaspersky EDR può essere assorbito in **Kaspersky Anti Targeted Attack Platform**, che combina le funzionalità EDR e il rilevamento avanzato delle minacce a livello di rete. Gli specialisti della sicurezza IT possono ora disporre di tutti gli strumenti necessari per gestire un rilevamento multilivello sia sugli endpoint che nella rete, applicando tecnologie all'avanguardia, effettuando indagini efficaci e fornendo una risposta rapida e centralizzata, il tutto attraverso un'unica soluzione.

* IDC PERSPECTIVE, Endpoint Security 2020:
The Resurgence of EPP and the Manifest Destiny of EDR

Kaspersky EDR è ideale se la vostra organizzazione desidera:

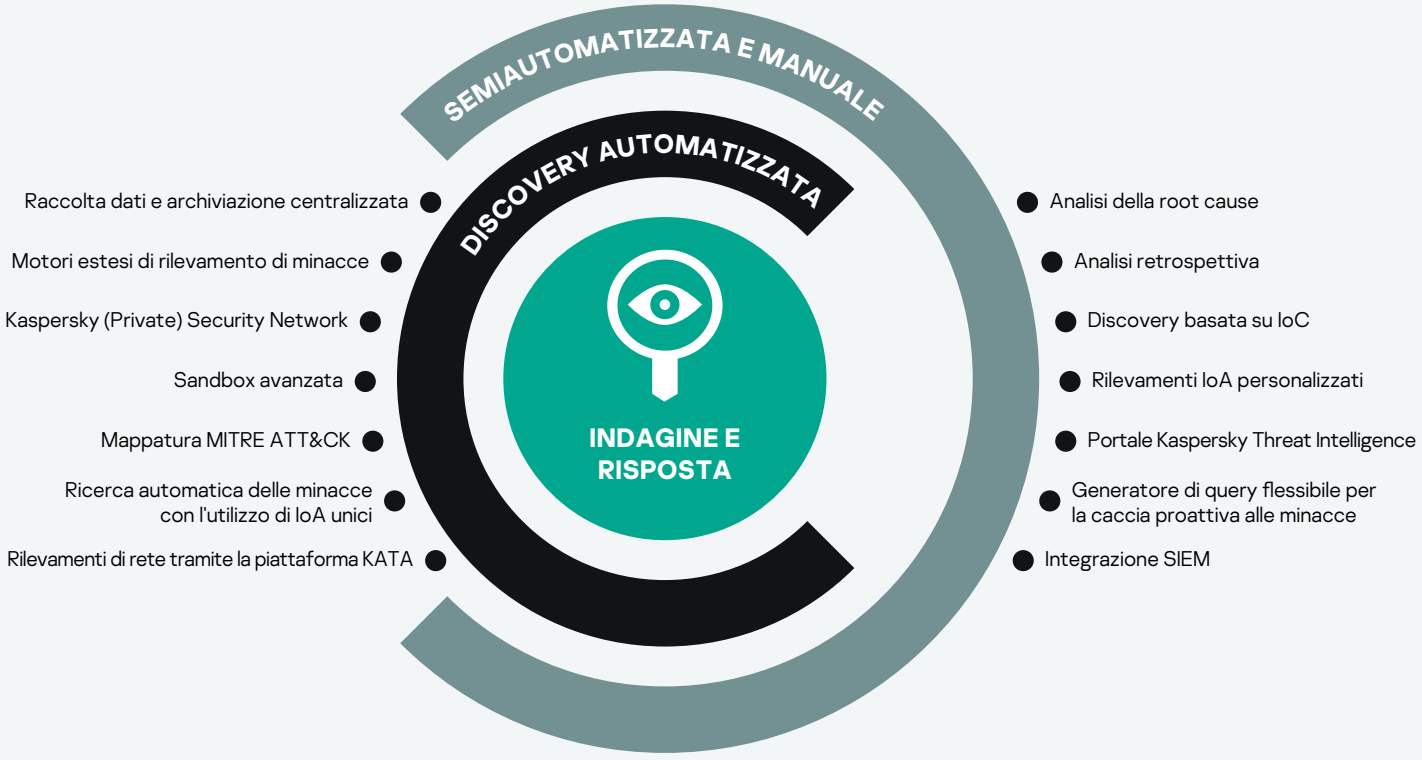
- Aggiornare la sicurezza con una soluzione aziendale di facile uso per la risposta agli incidenti
- Automatizzare l'identificazione delle minacce e le risposte, senza interruzioni dell'attività durante le indagini
- Migliorare la visibilità degli endpoint e il rilevamento delle minacce grazie a tecnologie avanzate
- Comprendere le tattiche, le tecniche e le procedure specifiche (TTP) utilizzate dagli autori delle minacce per raggiungere i loro obiettivi, consentendo un'allocazione più efficace delle difese e delle risorse di sicurezza
- Stabilire processi unificati ed efficaci per la ricerca di minacce, la gestione degli incidenti e i processi di risposta
- Aumentate l'efficienza del SOC interno, senza sprecare tempo ad analizzare i registri degli endpoint irrilevanti
- Favorire la conformità facendo rispettare i registri degli endpoint, le revisioni degli avvisi e la documentazione dei risultati delle indagini

Scoprire e contenere rapidamente le minacce più sofisticate

Kaspersky EDR fornisce una protezione degli endpoint di alto livello e aumenta l'efficienza del SOC, offrendo un rilevamento avanzato delle minacce e consentendo l'accesso ai dati retrospettivi, anche in situazioni in cui gli endpoint compromessi sono inaccessibili o quando i dati sono stati crittografati durante un attacco. Potenziamento delle capacità di indagine grazie ai nostri esclusivi indicatori di attacco (IoA), all'arricchimento MITRE ATT&CK e a un generatore di query flessibile, oltre all'accesso alla knowledge base di Threat Intelligence Portal. Tutto questo facilita il rilevamento efficace delle minacce e la risposta rapida agli incidenti, con una conseguente limitazione e prevenzione dei danni.

Casi d'uso:

- **Ricerca proattiva di prove di intrusione sull'intera rete**
- **Rilevamento rapido e correzione di un'intrusione, prima che l'aggressore possa causare danni e interruzioni di servizio**
- **Analisi rapida e gestione centralizzata degli incidenti, anche su migliaia di endpoint, senza ripercussioni sul business**
- **Validazione degli avvisi e dei potenziali incidenti rilevati da altre soluzioni di sicurezza**
- **Automatizzazione delle attività manuali, per ridurre al minimo le attività manuali, liberare risorse e ridurre la probabilità di un "sovraccarico di allarmi"**



Gartner Peer Insights Customer Choice per le soluzioni EDR 2020 nomina Kaspersky "Top Vendor"

Kaspersky è uno dei soli 6 fornitori al mondo ad aver ricevuto il riconoscimento Gartner Peer Insights Customer Choice per la soluzione Endpoint Detection and Response per il 2020, ottenendo la più alta valutazione rispetto a qualsiasi altro fornitore per il nostro servizio e supporto, il massimo riconoscimento dei clienti per Kaspersky EDR.

Esclusione di responsabilità Gartner

I premi Gartner Peer Insights Customer Choice vengono attribuiti sulla base di opinioni soggettive dei singoli utenti finali espresse in recensioni, valutazioni e dati applicati secondo una metodologia documentata; non rappresentano le opinioni di, né equivalgono all'approvazione di, Gartner o delle relative affiliate.

MITRE | ATT&CK®

Qualità di rilevamento confermata dalla valutazione MITRE ATT&CK

L'importanza dell'analisi delle TTP (tattiche, tecniche e procedure) durante l'indagine sull'incidente e il ruolo di MITER ATT&CK nel mercato della sicurezza odierno:

- Kaspersky EDR ha partecipato al MITRE Evaluation Round2 (APT29) e ha dato prova di un alto livello di prestazioni nel rilevamento delle principali tecniche ATT&CK dell'ambito Round2 applicate nelle fasi cruciali degli odierni attacchi mirati.
- Le rilevazioni di Kaspersky EDR si sono arricchite con i dati della knowledge base MITRE ATT&CK, per un'analisi approfondita dei TTP dell'avversario.

Per saperne di più, visitate il sito kaspersky.com/MITRE

I vantaggi di business di Kaspersky EDR in tutta l'impresa:

- Supporto per l'individuazione e la rimozione delle falle di sicurezza e riduzione del "dwell time"
- Automatizzazione delle attività manuali durante il rilevamento delle minacce e la risposta
- Riduzione dell'impegno del personale IT e addetto alla sicurezza, che può dedicarsi ad altre attività cruciali
- Semplificazione dei processi di analisi delle minacce e risposta agli incidenti
- Riduzione del tempo necessario a identificare e rispondere alle minacce
- Consente di ottenere la piena conformità

E se volete ancora di più... Kaspersky Managed Detection and Response

L'aggiunta a Kaspersky EDR di una difesa 24 ore su 24 completamente gestita e personalizzata equivale a far sì che le risorse di sicurezza IT possano essere conservate affidando a Kaspersky le attività di elaborazione relative agli incidenti o rivolgendosi a noi per richiedere il parere di esperti e l'esperienza unica di rilevamento delle minacce quando il team interno non dispone di specialisti della sicurezza sufficientemente qualificati per affrontare scenari specifici.

Per scoprire di più su Kaspersky EDR, visita il nostro sito Web.

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Novità sulle minacce informatiche: www.securelist.it
IT Security News: https://www.kaspersky.it/blog/category/business/
Sicurezza IT per piccole e medie imprese: www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security

www.kaspersky.it

Offriamo tecnologie di protezione comprovate. Siamo indipendenti. Siamo trasparenti. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia possa migliorare le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Soluzioni di Cybersecurity Kaspersky, per un futuro più sicuro.

Per saperne di più:
www.kaspersky.it/about/transparency

**Proven.
Transparent.
Independent.**