

Kaspersky Anti Targeted Attack Platform

I cybercriminali odierni sono specializzati nella progettazione di metodi unici e innovativi di penetrazione e compromissione dei sistemi. Man mano che le minacce si evolvono e diventano sempre più sofisticate e devastanti, il rilevamento rapido e la rapidità e l'appropriatezza della risposta hanno assunto un'importanza fondamentale.

È fondamentale che le imprese ripensino in continuazione le loro difese di sicurezza IT,

per essere sempre un passo avanti rispetto alle crescenti cyberminacce e per limitare le eventuali perdite finanziarie.

Cybersecurity senza eguali in una soluzione centralizzata

Oggi i criminali informatici professionisti favoriscono un approccio multivettoriale. Kaspersky Anti Targeted Attack Platform combina il rilevamento avanzato delle minacce a livello di rete e le funzionalità EDR, offrendo al contempo agli specialisti della sicurezza IT tutti gli strumenti necessari per gestire un rilevamento delle minacce multidimensionale di qualità superiore, applicare tecnologie all'avanguardia, svolgere indagini efficaci, dare la caccia alle minacce in modo proattivo e fornire una risposta rapida e centralizzata, il tutto attraverso un'unica soluzione.

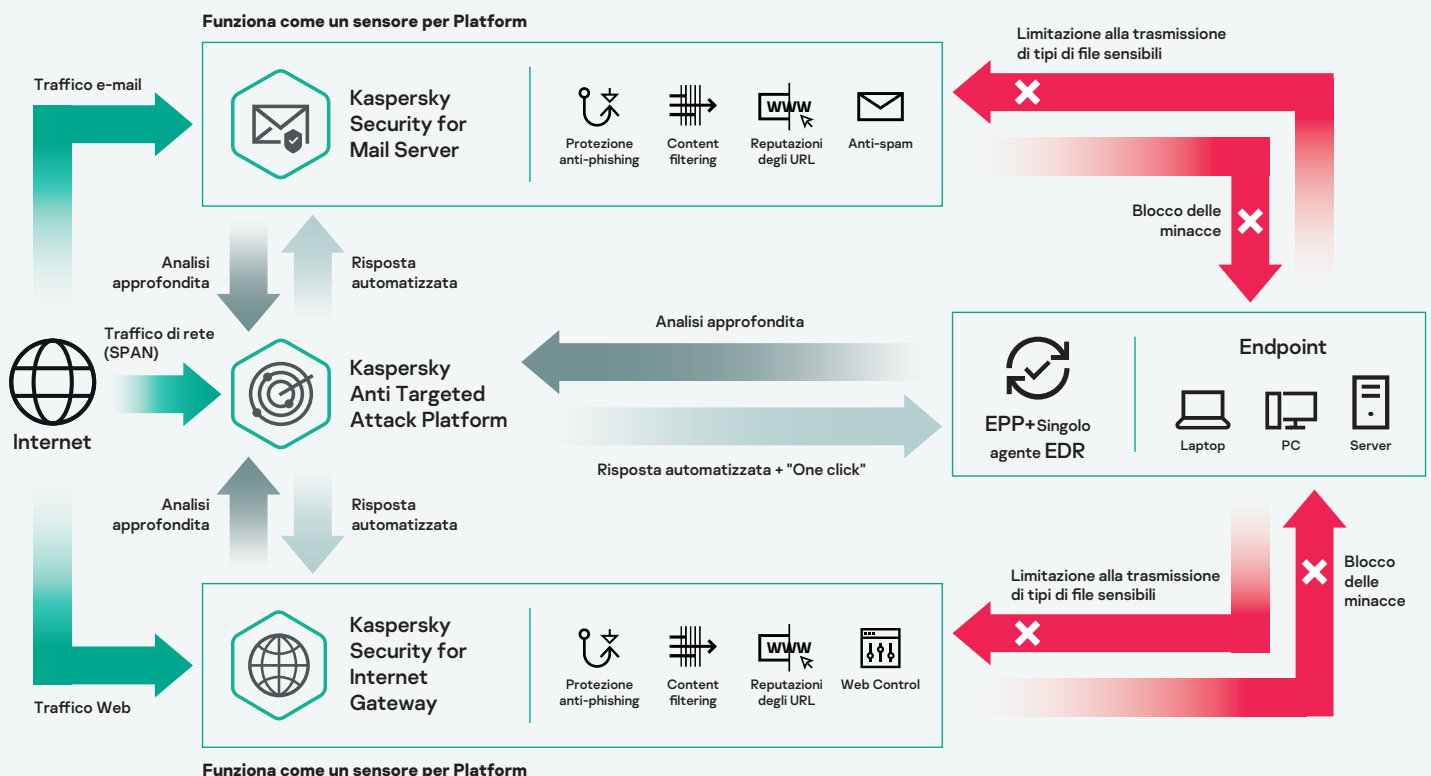
Gli attacchi più sofisticati monitorati e sotto controllo

Kaspersky Anti Targeted Attack Platform:

- **RIDUZIONE** del tempo necessario a identificare e rispondere alle minacce
- **SEMPLIFICAZIONE** dei processi di analisi delle minacce e risposta agli incidenti
- **CONTRIBUISCE** a eliminare le falle di sicurezza e a ridurre il "dwell time"
- **AUTOMATIZZAZIONE** delle attività manuali; durante il rilevamento delle minacce e la risposta
- **RIDUZIONE** del carico di lavoro del personale IT e responsabile della sicurezza, che può dedicarsi ad altre attività
- **SUPPORTO** la conformità totale alle normative

La piattaforma funge da soluzione Extended Detection and Response per fornire una protezione APT all-in-one basata sulla nostra Threat Intelligence e mappata sul framework MITRE ATT&CK. Tutti i potenziali punti di accesso delle minacce, rete, Web, posta, PC, laptop, server e macchine virtuali sono sotto il vostro controllo.

Kaspersky Anti Targeted Attack Platform è pienamente integrato con Kaspersky Endpoint Security for Business e condivide un singolo agente con Kaspersky EDR. Esso si integra sia con Kaspersky Security for Mail Server che con Kaspersky Security for Internet Gateway, che fungono da sensori per Platform, fornendo una risposta automatizzata alle minacce più complesse della posta elettronica e provenienti da Internet.



Una soluzione di sicurezza affidabile che fornisce completa privacy

Tutte le analisi degli oggetti avvengono in loco, senza flusso di dati in uscita. Kaspersky Private Security Network fornisce aggiornamenti della reputazione in entrata in tempo reale, pur preservando il completo isolamento dei dati aziendali.

Una piattaforma unificata per accelerare l'innovazione della trasformazione digitale tramite:

- **Continuità aziendale integrale.** Integriamo la sicurezza e la conformità nei nuovi processi fin dall'inizio
- **Visibilità completa** sull'infrastruttura IT aziendale
- **Massima flessibilità** tramite implementazione in ambienti fisici e virtuali, ovunque siano necessari visibilità e controllo
- **Automazione delle attività di scoperta e risposta**, ottimizzando il rapporto costo-efficacia della sicurezza, della risposta agli incidenti e dei team SOC
- **Integrazione stretta e diretta** con prodotti per la sicurezza esistenti, migliorando i livelli di sicurezza complessiva e proteggendo gli investimenti effettuati sulle tecnologie di sicurezza già implementate

Funzionalità principali:



Architettura multilivello a sensori: visibilità ad ampio raggio ottenuta attraverso una combinazione di sensori di rete, Web ed email e agenti endpoint.



Motori estesi di rilevamento di minacce: interazione con i dati dei sensori di rete (analisi del traffico di rete) e con gli agenti degli endpoint (funzionalità EDR) per fornire verdetti in tempi rapidi e meno falsi positivi.



Sandbox avanzata: fornisce un ambiente sicuro per l'analisi approfondita dell'attività delle minacce, supportando la randomizzazione dei componenti del sistema operativo, l'accelerazione del tempo nelle macchine virtuali, le tecniche anti-evasione, la simulazione dell'attività degli utenti e la mappatura dei risultati sulla base delle conoscenze MITRE ATT&CK, tutti fattori che contribuiscono a un rilevamento altamente efficiente basato sul comportamento.



Analisi retrospettiva: anche in situazioni in cui gli endpoint compromessi sono inaccessibili o quando i dati sono stati crittografati, mediante la raccolta automatica dei dati, degli oggetti e dei verdetti e l'archiviazione centralizzata.



Due modalità di interazione della Threat Intelligence: confronto automatizzato con i dati sulla reputazione globale di Kaspersky Security Network e la ricerca manuale delle minacce e le indagini attraverso Kaspersky Threat Intelligence Portal.



Caccia automatica alle minacce in tempo reale: gli eventi sono correlati a un insieme unico di indicatori di attacco (IoA) generati dai rilevatori di minacce Kaspersky e mappati sulla matrice MITRE ATT&CK, fornendo chiare descrizioni degli eventi, esempi e raccomandazioni di risposta.



Rilevamento proattivo delle minacce con il nostro potente generatore di query potente e flessibile: gli analisti possono costruire query complesse per cercare un comportamento atipico, attività sospette e minacce specifiche all'infrastruttura.

In breve

Protezione dei dati affidabile, sicurezza dell'infrastruttura IT, stabilità dei processi aziendali e compliance sono i prerequisiti per uno sviluppo sostenibile delle aziende moderne.

Kaspersky Anti Targeted Attack Platform consente di creare difese efficaci per proteggere le infrastrutture dalle minacce APT e dagli attacchi mirati, assicurando al contempo una compliance normativa senza impiego di risorse aggiuntive. Gli incidenti complessi vengono identificati, analizzati e risolti con la massima tempestività, senza bisogno di interventi manuali da parte dei team di sicurezza IT e SOC che possono così aumentare la loro efficienza, grazie a una soluzione centralizzata in grado di ottimizzare l'automazione e la qualità dei risultati.

Comprovata come la soluzione più efficace del settore



SE Labs ha testato Kaspersky Anti Targeted Attack Platform rispetto a una serie di attacchi hacker e ci ha assegnato una valutazione di tripla A.



Nel test di "ICSA Labs: Advanced Threat Defense (Q3 2019)", Kaspersky Anti Targeted Attack Platform ha fornito percentuali di rilevamento del 100%, con zero falsi positivi.



THE RADICATI GROUP, INC.

A TECHNOLOGY MARKET RESEARCH FIRM

Radicati Group inserisce Kaspersky Lab tra i "Top Player" nel suo report **Advanced Persistent Threat (APT) Protection – Market Quadrant 2020**.



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

Una delle sole 6 aziende al mondo a essere riconosciuta come Gartner Peer Insights Customer Choice per le soluzioni EDR 2020, il massimo riconoscimento dei clienti per la nostra soluzione Extended EDR, Kaspersky Anti Targeted Attack Platform basata su 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'elemento centrale di Kaspersky Anti Targeted Attack Platform, Kaspersky EDR, ha partecipato al secondo turno di valutazione MITRE (APT29), dando prova di alti livelli di performance nel rilevamento delle principali tecniche ATT&CK applicate nelle fasi cruciali degli attacchi mirati.

Maggiori informazioni sono disponibili all'indirizzo kaspersky.com/MITRE

Per saperne di più su Kaspersky Anti Targeted Attack Platform, visitate il sito:

kaspersky.com/enterprise-security/anti-targeted-attack-platform

Novità sulle minacce informatiche: www.securelist.it
IT Security News: [https://www.kaspersky.it/blog/category/business/Sicurezza IT per piccole e medie imprese](https://www.kaspersky.it/blog/category/business/Sicurezza%20IT%20per%20piccole%20e%20medie%20imprese):
www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security

www.kaspersky.it

© 2020 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.



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.**