kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Funzionalità di rilevamento avanzate per proteggersi da minacce avanzate e sconosciute senza ricorrere a un esperto di sicurezza IT

I cyberattacchi avanzati di oggi sono in grado di paralizzare un'intera azienda, impattare pesantemente sul fatturato e distruggerne la reputazione. Il furto di risorse finanziarie e segreti commerciali, la perdita di fiducia dei clienti dovuta all'interruzione dei servizi e i numerosi altri effetti negativi delle minacce complesse influiscono pesantemente sulla stabilità e la prosperità di un'azienda. Da soli, i tradizionali strumenti progettati per proteggere il perimetro della rete (firewall, email/web gateway, server proxy), così come le workstation e i server (protezione antivirus e soluzioni di Endpoint Protection Platform con funzionalità di base), non bastano a prevenire cyberattacchi in continua evoluzione. Proprio per questo, le aziende più lungimiranti devono prendere seriamente in considerazione strumenti specializzati nel rilevamento, nell'analisi e nella risposta agli incidenti complessi.

La soluzione Kaspersky Sandbox è adatta a:

- Aziende senza un security team dedicato, in cui le funzioni di sicurezza IT sono affidate al dipartimento IT.
- Piccole aziende che non desiderano aumentare il numero delle risorse di sicurezza IT.
- Grandi organizzazioni con un'infrastruttura geograficamente distribuita e senza esperti di sicurezza IT on site.
- Aziende che desiderano assicurarsi che gli analisti di sicurezza IT a tempo pieno siano completamente concentrati sui task critici.

Kaspersky realizza da più di vent'anni strumenti di protezione per aziende di tutte le dimensioni, i settori e i livelli di maturità della sicurezza IT. Grazie a un impegno continuo di ricerca e sviluppo, oltre ai progressi compiuti nel threat hunting, nell'analisi e nella risposta alle minacce, Kaspersky è sempre in prima linea nella lotta al cybercrimine.

Il portafoglio di prodotti e servizi Kaspersky per contrastare le minacce complesse include:

- Kaspersky Anti Targeted Attack, una soluzione all'avanguardia per il rilevamento e l'analisi di minacce complesse e attacchi mirati a livello di rete
- Kaspersky Endpoint Detection and Response, una soluzione per rilevare, analizzare e rispondere alle minacce informatiche complesse dirette contro workstation e server
- Portale Kaspersky Threat Intelligence, per l'accesso a Cloud Sandbox, con report di analisi sulle minacce APT e altri servizi

Tuttavia, per utilizzare efficacemente questi servizi e soluzioni, le aziende devono disporre di un dipartimento di sicurezza IT completo, con livelli di esperienza e competenza appropriati. La carenza globale di esperti specializzati nella gestione delle minacce complesse, così come il costo di risorse specializzate, costituiscono spesso il principale ostacolo all'acquisto di soluzioni e servizi di questo tipo da parte delle aziende.

Basata su una tecnologia brevettata (brevetto n. US 10339301B2), la soluzione Kaspersky Sandbox aiuta le aziende a combattere le moderne minacce, sempre più complesse e numerose, capaci di eludere la protezione endpoint. Integrando le funzionalità di Kaspersky Endpoint Security for Business, Kaspersky Sandbox permette di incrementare notevolmente il livello di protezione di workstation e server contro malware sconosciuti, nuovi virus e ransomware, exploit zero-day e altre minacce, senza ricorrere a un analista di sicurezza informatica altamente specializzato.

Questo evita alle piccole aziende i costi di selezione e assunzione di personale altamente specializzato e aiuta le grandi aziende Enterprise con reti distribuite a ottimizzare i costi da sostenere per garantire una protezione efficace delle sedi remote, alleggerendo al tempo stesso il workload manuale degli analisti di sicurezza.

Opzioni di distribuzione e implementazione:
La soluzione Kaspersky Sandbox viene fornita come immagine ISO, con CentOS 7 e tutti i componenti necessari della soluzione già preconfigurati. Può essere implementata in un server fisico o in un server virtuale basato su VMware ESXi.

Integrazione:
- I sistemi SIEM possono ricevere informazioni sui rilevamenti effettuati da Kaspersky Sandbox. Tali informazioni vengono inviate tramite Kaspersky Security Center insieme agli altri eventi in generale.
- In Kaspersky Sandbox è implementata un'API per l'integrazione con altre soluzioni, che consente di inviare file a Kaspersky Sandbox per la scansione e di richiedere alla soluzione i dati relativi alla reputazione dei file.

Scalabilità
Con una configurazione base che supporta fino a 1.000 endpoint protetti, la soluzione è in grado di scalare facilmente garantendo protezione continua alle infrastrutture di grandi dimensioni.

Clustering
È possibile organizzare più server in cluster per aumentare i livelli di capacità e disponibilità.

Licenze
La soluzione Kaspersky Sandbox viene concessa in licenza come appliance software. Una singola licenza include il supporto per un massimo di 1.000 utenti di Kaspersky Endpoint Security for Business.

Come funziona

Kaspersky Sandbox sfrutta le best practice dei nostri esperti per contrastare le minacce complesse e gli attacchi di livello APT. Inoltre, questa soluzione è strettamente integrata con Kaspersky Endpoint Security for Business e viene gestita tramite Kaspersky Security Center, la nostra console di gestione unificata basata su policy.

L'agente di Kaspersky Endpoint Security for Business richiede informazioni su un oggetto sospetto alla cache operativa dei risultati condivisa, che si trova nel server Kaspersky Sandbox. Se l'oggetto è già stato analizzato, Kaspersky Endpoint Security for Business riceve il verdetto e applica una o più delle seguenti opzioni di remediation:

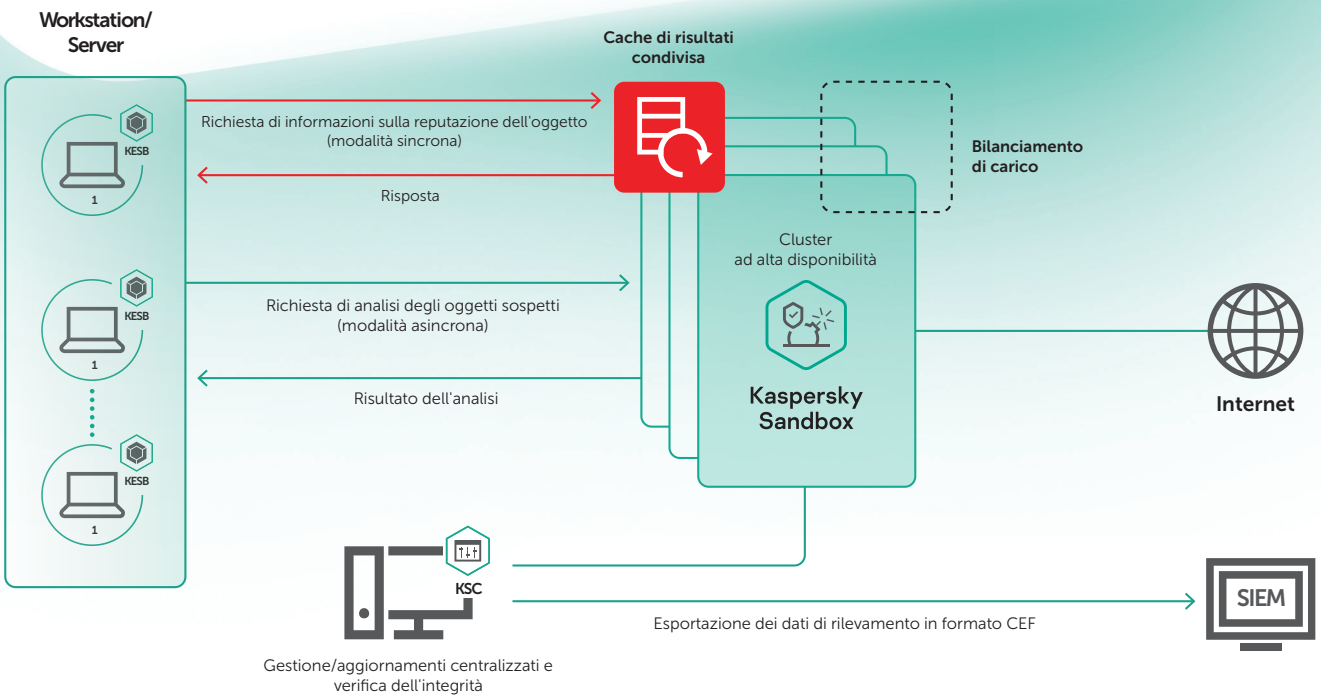
- Rimozione e quarantena
- Notifica all'utente
- Avvio di una scansione delle aree critiche
- Ricerca dell'oggetto rilevato anche negli altri sistemi della rete gestita

Se non è possibile ottenere dalla cache le informazioni relative alla reputazione di un oggetto, l'agente di Kaspersky Endpoint Security for Business invia il file sospetto alla sandbox e attende la risposta. La sandbox riceve una richiesta di analizzare l'oggetto ed esegue l'oggetto da testare in un ambiente isolato dall'infrastruttura reale.

La scansione dei file viene eseguita in macchine virtuali dotate di strumenti che emulano un tipico ambiente di lavoro (sistemi operativi/applicazioni installate). Per determinare le intenzioni malevole di un oggetto viene eseguita un'analisi comportamentale, vengono raccolti e analizzati gli artefatti e, se l'oggetto esegue azioni dannose, la sandbox lo identifica come malware. Durante l'analisi nella sandbox, all'oggetto viene assegnato un verdetto.

Terminato il processo di emulazione dell'oggetto, il verdetto ottenuto viene inviato in tempo reale alla cache operativa condivisa dei verdetti, permettendo agli altri host in cui è installata la soluzione Kaspersky Endpoint Security for Business di ottenere velocemente informazioni sulla reputazione dell'oggetto analizzato, senza doverlo analizzare nuovamente. Questo approccio garantisce l'elaborazione rapida degli oggetti sospetti, riduce il carico sui server Kaspersky Sandbox e migliora i livelli di velocità ed efficienza della risposta alle minacce.

Kaspersky Sandbox è un add-on essenziale a Kaspersky Endpoint Security for Business. Blocca automaticamente le minacce avanzate, sconosciute e complesse senza richiedere risorse aggiuntive e lascia agli analisti di sicurezza IT il tempo per concentrarsi su altri task.



Novità sulle minacce informatiche: www.securelist.it
IT Security News: business.kaspersky.com/it
Sicurezza IT per le PMI: kaspersky.com/business
Sicurezza IT per le azienda Enterprise: kaspersky.com/enterprise

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. Soluzioni di Cybersecurity, per un futuro più sicuro.

Per saperne di più: kaspersky.com/transparency

Proven.
Transparent.
Independent.