kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Funciones de detección avanzadas para proteger contra amenazas desconocidas y evasivas, sin necesidad de contratar profesionales de seguridad de IT

Los ciberataques avanzados de hoy en día tienen la capacidad de paralizar empresas y causar estragos financieros y de reputación. El robo de activos financieros y secretos comerciales, la pérdida de confianza de los clientes debido a la interrupción de los servicios y otros de los numerosos efectos negativos de las amenazas complejas suponen un grave impacto en la estabilidad y prosperidad de las empresas. Para evitar los ciberataques en rápida evolución, las herramientas tradicionales diseñadas para proteger el perímetro de la red (firewalls, pasarelas de correo electrónico/web, servidores proxy), así como las estaciones de trabajo y los servidores (protección antivirus y soluciones de tipo plataforma de protección de endpoints con funcionalidad básica), no son suficientes por sí solas. Por este motivo, las empresas con visión de futuro deben plantearse seriamente la adopción de herramientas especializadas para detectar, investigar y responder frente a incidentes complejos.

La solución Kaspersky Sandbox es adecuada para las siguientes entidades:

- Empresas que no cuentan con un equipo de seguridad exclusivo, en las que la función de seguridad de IT se asigna al departamento de IT.
- Pequeñas empresas que no desean incurrir en recursos de seguridad de IT adicionales.
- Grandes organizaciones con una infraestructura distribuida geográficamente y sin especialistas en seguridad de IT in situ.
- Empresas que necesitan garantizar que sus analistas de seguridad de IT están totalmente centrados en tareas críticas.

Desde hace más de veinte años, Kaspersky crea herramientas de protección para empresas de todos los tamaños, sectores y niveles de madurez en seguridad de IT. Gracias a la investigación y el desarrollo continuos y a los avances que hemos realizado en la búsqueda, la investigación y la respuesta frente a las amenazas, Kaspersky permanece a la vanguardia de la lucha contra el cibercrimen.

El portfolio de productos y servicios de Kaspersky para contrarrestar las amenazas complejas incluye lo siguiente:

- Kaspersky Anti Targeted Attack, una solución de vanguardia para la detección e investigación de amenazas complejas y ataques dirigidos en el ámbito de la red.
- Kaspersky Endpoint Detection and Response, una solución para detectar, investigar y responder a ciberamenazas complejas dirigidas a estaciones de trabajo y servidores
- Kaspersky Threat Intelligence Portal, que proporciona acceso al sandbox basado en la nube con informes de análisis sobre amenazas de APT y otros servicios

Sin embargo, para sacar partido de forma eficaz a estas soluciones y servicios, las empresas deben contar con un departamento de seguridad de IT integral con la experiencia y los conocimientos adecuados. La escasez mundial de especialistas formados para hacer frente a amenazas complejas, así como el coste que supone contratarlos, suelen ser los factores principales que frenan a las empresas a la hora de adquirir estos tipos de soluciones y servicios.

Kaspersky Sandbox, basado en tecnología patentada (patente núm. US 10339301B2), ayuda a las empresas a combatir el creciente número y complejidad de las amenazas modernas que pueden burlar la protección de endpoints existente. Como complemento de la funcionalidad de Kaspersky Endpoint Security for Business, Kaspersky Sandbox permite a las organizaciones aumentar de forma significativa el nivel de protección de sus estaciones de trabajo y servidores frente a malware previamente desconocido, nuevos virus y ransomware, exploits de día cero y otros, sin necesidad de contar con analistas de seguridad de la información altamente especializados.

De este modo, las pequeñas empresas se ahorran el gasto de tener que buscar y contratar a estos profesionales tan cotizados. También ayuda a las grandes empresas con redes distribuidas a optimizar los costes para una protección eficaz de sus oficinas remotas, a la vez que aligera la carga de trabajo manual de sus analistas de seguridad.

Opciones de entrega e implementación:
Kaspersky Sandbox se proporciona como imagen ISO, con CentOS 7 preconfigurado y todos los componentes de la solución necesarios. Se puede implementar en un servidor físico o en servidores virtuales basados en VMware ESXi.

Integración:
- Los sistemas SIEM pueden recibir información sobre las detecciones realizadas por Kaspersky Sandbox. Esta información se envía a través de Kaspersky Security Center en el flujo general de eventos.
- Se ha implementado una API en Kaspersky Sandbox para su integración con otras soluciones, lo que permite enviar archivos a Kaspersky Sandbox para su análisis y solicitar la reputación de los archivos.

Escalabilidad
La configuración básica permite proteger hasta 1000 endpoints pero la solución se amplía fácilmente y proporciona protección continua para grandes infraestructuras

Agrupación en clústeres
Se pueden agrupar varios servidores para lograr más capacidad y una alta disponibilidad.

Licencias
Kaspersky Sandbox tiene licencia de dispositivo de software. Una licencia admite hasta 1000 usuarios de Kaspersky Endpoint Security for Business.

Funcionamiento

Kaspersky Sandbox aprovecha nuestras prácticas recomendadas de expertos para combatir amenazas complejas y ataques de nivel de APT, y está estrechamente integrado con Kaspersky Endpoint Security for Business. Se gestiona desde Kaspersky Security Center, nuestra consola de gestión unificada basada en políticas.

El agente de Kaspersky Endpoint Security for Business solicita datos sobre un objeto sospechoso de la caché compartida de veredictos operativa, ubicada en el servidor de Kaspersky Sandbox. Si el objeto ya se ha analizado, Kaspersky Endpoint Security for Business recibe el veredicto y aplica una o más opciones de corrección:

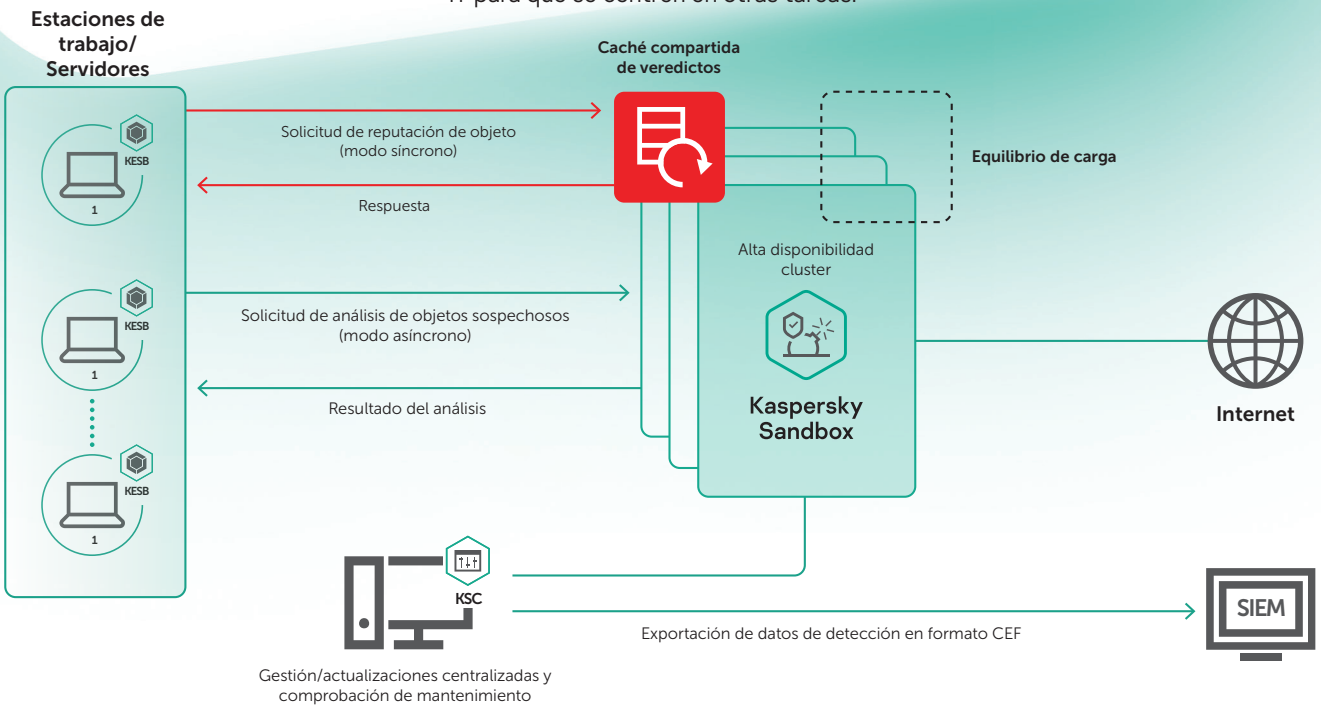
- Retirar y poner en cuarentena
- Notificarlo al usuario
- Iniciar un análisis de áreas críticas
- Buscar el objeto detectado en otros equipos de la red gestionada.

Si no puede obtenerse de la caché el veredicto de la reputación de un objeto, el agente de Kaspersky Endpoint Security for Business envía el archivo sospechoso al sandbox y espera una respuesta. El sandbox recibe una solicitud para analizar el objeto, momento en el que el objeto de prueba se ejecuta en un entorno aislado de la infraestructura real.

El análisis de archivos se realiza en máquinas virtuales equipadas con herramientas que emulan un entorno de trabajo típico (sistemas operativos/aplicaciones instaladas). Para detectar la intención maliciosa de un objeto, se realiza un análisis del comportamiento, se recopilan y analizan los artefactos y, si el objeto realiza acciones maliciosas, el sandbox lo reconoce como malware. Durante el análisis de sandbox, se asigna un veredicto al objeto.

Una vez finalizado el proceso de emulación de objetos, el veredicto resultante se envía en tiempo real a la caché compartida de veredictos operativa, lo que permite que otros hosts con Kaspersky Endpoint Security for Business instalado obtengan rápidamente datos sobre la reputación del objeto analizado sin tener que volver a analizar el mismo archivo. Este método garantiza un procesamiento rápido de objetos sospechosos, reduce la carga de los servidores de Kaspersky Sandbox y mejora la velocidad y la eficacia de la respuesta a las amenazas.

Kaspersky Sandbox es un complemento indispensable de Kaspersky Endpoint Security for Business. Bloquea automáticamente amenazas avanzadas, desconocidas y complejas sin necesidad de recursos adicionales y libera a los analistas de seguridad de IT para que se centren en otras tareas.



Noticias de ciberamenazas: www.viruslist.es
Noticias de seguridad de IT: business.kaspersky.com
Seguridad de IT para pymes: https://www.kaspersky.es/small-to-medium-business-security
Seguridad de IT para grandes empresas: kaspersky.es/enterprise-security

www.kaspersky.es

Seguridad probada, independiente y transparente. Nos comprometemos a construir un mundo más seguro en el que la tecnología nos mejore la vida. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Más información en kaspersky.es/transparency

Proven. Transparent. Independent.