kaspersky BRING ON THE FUTURE

Kaspersky Sandbox

Capacidades de detección avanzadas que le protegerán contra amenazas desconocidas y evasivas – sin tener que contratar profesionales de seguridad en TI

Los ciberataques avanzados actuales tienen el poder de paralizar a las empresas y causarles desastres financieros y en su reputación. El robo de activos financieros y secretos comerciales, la pérdida de confianza del cliente debido a la caída de los servicios y muchos otros efectos negativos de las amenazas complejas causan un grave impacto en la estabilidad y prosperidad de la empresa. Para evitar los ciberataques que evolucionan rápidamente, las herramientas tradicionales diseñadas para proteger el perímetro de la red (por ejemplo, firewalls, puertas de enlace de correo electrónico/web, servidores proxy), así como las estaciones de trabajo y los servidores (por ejemplo, protecciones antivirus y soluciones de tipo plataformas para la protección de endpoints con funciones básicas), son insuficientes por sí mismos. Por esta razón las empresas con una visión orientada hacia el futuro deben considerar seriamente el uso de herramientas especializadas para detectar, analizar y responder a incidentes complejos.

La solución de Kaspersky Sandbox es adecuada para:

- Empresas que no cuentan con un equipo de seguridad dedicado, donde las tareas de seguridad en TI se asignan al departamento de TI.
- Empresas pequeñas que no desean invertir en recursos para la seguridad de TI adicionales.
- Empresas grandes con una infraestructura distribuida geográficamente y que no cuentan con especialistas en la seguridad de TI localmente.
- Empresas que necesitan asegurarse de que sus analistas en seguridad de TI de tiempo completo estén totalmente enfocados en tareas críticas.

Durante más de veinte años, Kaspersky ha creado herramientas de protección para las empresas de cualquier tamaño, área y nivel de madurez en la seguridad de TI. Debido a nuestra continua investigación y desarrollo, y a los avances que hemos hecho en la búsqueda, investigación y respuesta contra amenazas, Kaspersky sigue a la vanguardia en la lucha contra los delitos cibernéticos.

La cartera de productos y servicios de Kaspersky para contrarrestar amenazas complejas incluye:

- Kaspersky Anti Targeted Attack, una solución de vanguardia para detectar e investigar amenazas complejas y ataques dirigidos al nivel de la red.
- Kaspersky Endpoint Detection and Response, una solución para detectar, investigar y responder ante ciberamenazas complejas dirigidas a estaciones de trabajo y servidores
- Kaspersky Threat Intelligence Portal, una solución que proporciona acceso a Cloud Sandbox, con informes analíticos sobre amenazas persistentes avanzadas (APT) y otros servicios.
-

Sin embargo, para utilizar de manera efectiva estas soluciones y servicios, las empresas necesitan contar con un departamento de seguridad en TI completamente desarrollado, con la experiencia y los conocimientos adecuados. La escasez mundial de especialistas capacitados para enfrentar amenazas complejas, y el costo de contratarlos, a menudo es el factor principal que impide que las empresas adquieran este tipode soluciones y servicios.

Basado en tecnología patentada (con la patente núm. US 10339301B2) Kaspersky Sandbox ayuda a las empresas a luchar contra la creciente cantidad y complejidad de las amenazas modernas que pueden eludir la protección de los endpoints. Al complementar la funcionalidad de Kaspersky Endpoint Security for Business, Kaspersky Sandbox permite que las empresas aumenten significativamente el nivel de protección de sus estaciones de trabajo y servidores contra malware anteriormente desconocido, nuevos virus, ransomware, vulnerabilidades de día cero y más, sin que sea necesario contratar analistas para la seguridad de la información altamente especializados.

Esto ahorra a las pequeñas empresas el costo de buscar y contratar a estos profesionales altamente valorados. También ayuda a las grandes empresas que cuentan con redes distribuidas a optimizar costos para lograr una protección efectiva de sus oficinas remotas, a la vez que alivia la carga de trabajo manual para sus analistas de seguridad.

Opciones de entrega e implementación:
Kaspersky Sandbox se proporciona como una imagen ISO, con CentOS 7 preconfigurado y todos los componentes de solución necesarios. Puede implementarse 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 del Kaspersky Security Center en el flujo de eventos generales.
- En Kaspersky Sandbox se implementa una API para la integración con otras soluciones, lo cual permite enviar archivos a Kaspersky Sandbox para su escaneo y solicitar su reputación.

Escalabilidad
Con la configuración básica que admite protección para hasta 1,000 endpoints, la solución puede escalarse fácilmente, lo cual proporciona protección continua para grandes infraestructuras

Uso de clústeres
Pueden agruparse varios servidores para obtener más capacidad y alta disponibilidad.

Licencias
Kaspersky Sandbox cuenta con licencia como dispositivo de software. Una sola licencia incluye soporte hasta para 1,000 usuarios de Kaspersky Endpoint Security for Business.

Cómo funciona

Kaspersky Sandbox aprovecha las mejores prácticas recomendadas de los expertos para combatir amenazas complejas y ataques al nivel de las APT, y se integra estrechamente con Kaspersky Endpoint Security for Business. Se administra desde el Kaspersky Security Center, nuestra consola de administración unificada basada en políticas.

El agente de Kaspersky Endpoint Security for Business solicita datos sobre un objeto sospechoso a la memoria caché operativa compartida para veredictos, la cual se encuentra en el servidor de Kaspersky Sandbox. Si el objeto ya fue escaneado antes, Kaspersky Endpoint Security for Business recibe el veredicto y aplica una o más opciones de corrección:

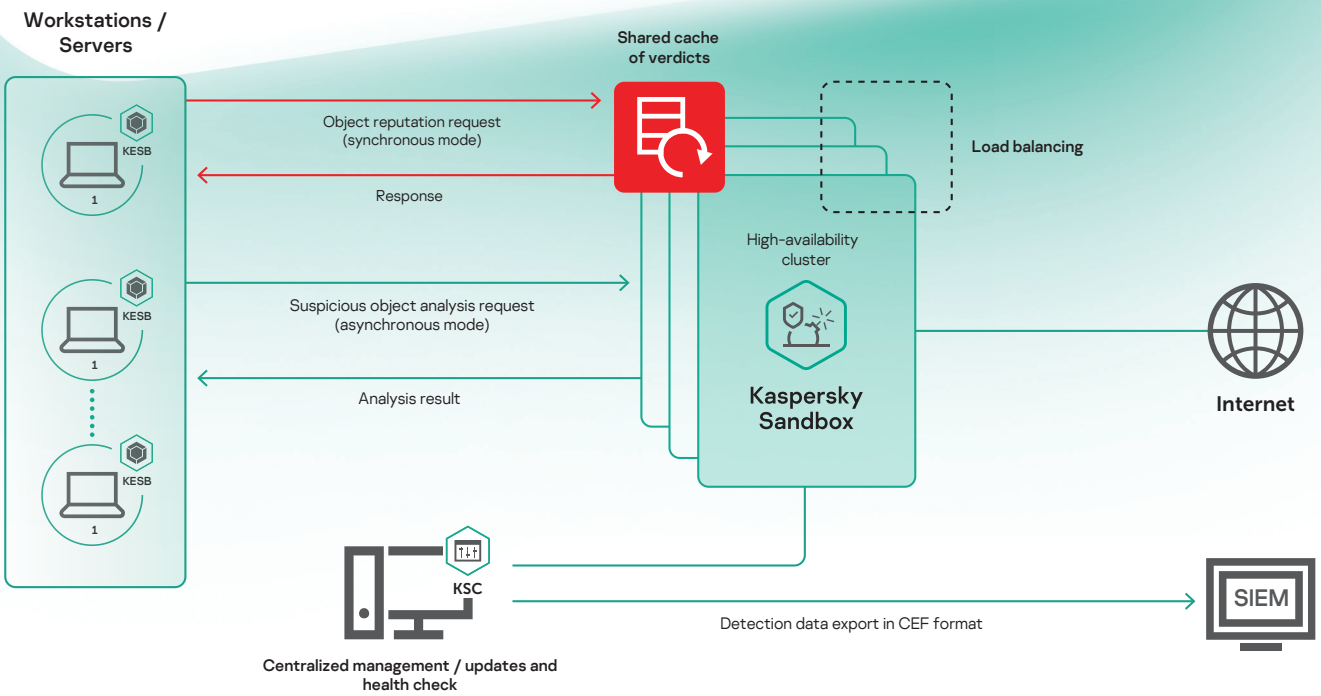
- Lo elimina y lo pone en cuarentena
- Notifica al usuario
- Inicia un análisis de áreas críticas
- Busca el objeto detectado en otras máquinas que se encuentren dentro de la red administrada.

Si el veredicto sobre la reputación de un objeto no puede obtenerse de la memoria caché, el agente de Kaspersky Endpoint Security for Business envía el archivo sospechoso a Sandbox y espera una respuesta. Sandbox recibe una solicitud para escanear el objeto, momento en el cual el objeto que está a prueba se ejecuta en un entorno aislado de la infraestructura real.

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

Una vez que se completa el proceso de simulación de objetos, el veredicto resultante se envía en tiempo real a la memoria caché operativa compartida para veredictos, lo cual permite que otros hosts que tengan Kaspersky Endpoint Security for Business instalado obtengan información rápidamente sobre la reputación del objeto escaneado sin tener que analizar el mismo archivo nuevamente. Este enfoque garantiza el procesamiento rápido de los objetos sospechosos, reduce la carga en los servidores de Kaspersky Sandbox y mejora la velocidad y la eficiencia de la respuesta a las amenazas.

Kaspersky Sandbox es una adición esencial a Kaspersky Endpoint Security for Business. Bloquea automáticamente amenazas avanzadas, desconocidas y complejas sin la necesidad de contar con recursos adicionales, y libera a los analistas en seguridad de TI para que se concentren en otras tareas.



Noticias sobre las amenazas cibernéticas: www.securelist.com
Noticias sobre la seguridad de TI: business.kaspersky.com
Seguridad de TI para PYMES: kaspersky.com/business
Seguridad de TI para empresas: kaspersky.com/enterprise

latam.kaspersky.com

Tenemos experiencia. Somos independientes. Somos transparentes. Estamos comprometidos en desarrollar un mundo más seguro, donde la tecnología mejore nuestras vidas. Es por eso que lo protegemos, para que todos en cualquier parte tengan las innumerables oportunidades que ofrece. Acceda a la ciberseguridad

Proven. Transparent. Independent.