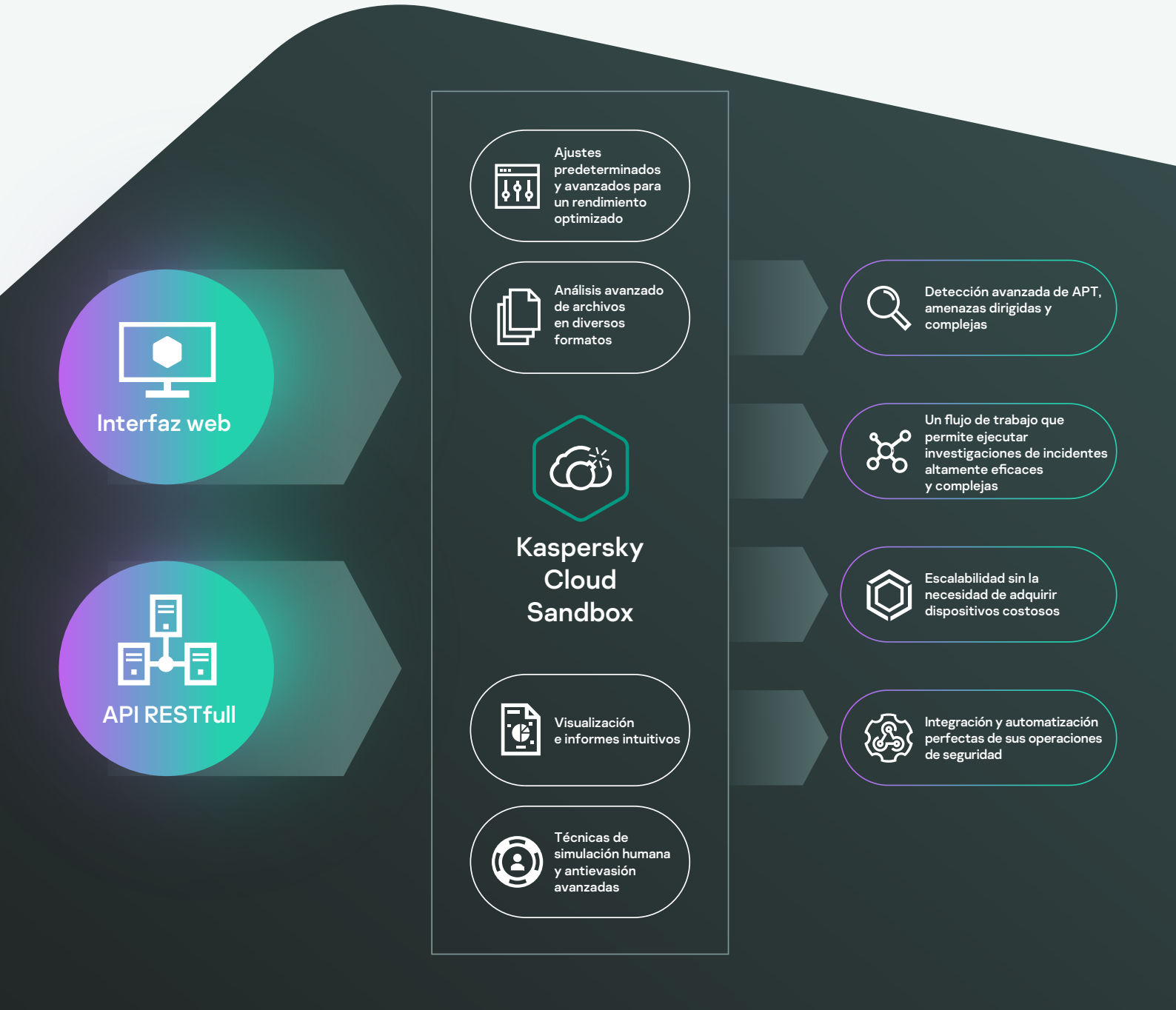
Kaspersky Cloud Sandbox

kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Cloud Sandbox

Es imposible evitar los ataques dirigidos actuales solo con herramientas antivirus tradicionales. Los motores antivirus son capaces de detener solo amenazas conocidas y sus variaciones, mientras que los sofisticados actores de las amenazas usan todos los medios a su disposición para evadir la detección automática. Las pérdidas derivadas de incidentes de seguridad de la información siguen creciendo de forma exponencial, lo que evidencia la importancia cada vez mayor de las capacidades de detección inmediata de amenazas para garantizar una respuesta rápida y contrarrestar las amenazas antes de que se produzca un daño significativo.

Tomar una decisión inteligente basada en el comportamiento de un archivo al tiempo que se analiza la memoria del proceso, la actividad de la red, etc., es la estrategia óptima para entender las sofisticadas amenazas dirigidas y personalizadas recientes. Aunque los datos estadísticos pueden carecer de información sobre malware modificado recientemente, las tecnologías sandbox son herramientas poderosas que permiten la investigación de los orígenes de las muestras de archivos, los IOC de recopilación basados en análisis de comportamiento y la detección de objetos maliciosos no identificados con anterioridad.



Generación de informes exhaustivos

- DLL cargados y ejecutados
- Conexiones externas con nombres de dominio y direcciones IP
- Archivos creados, modificados y eliminados
- Inteligencia detallada frente a amenazas con contexto práctico para cada indicador de compromiso (IOC) descubierto
- Volcados de memoria de procesos y volcados de tráfico de red (PCAP)
- Solicitudes y respuestas HTTP y DNS
- Extensiones mutuas creadas (mutexes)
- API RESTful
- Claves del registro creadas y modificadas
- Procesos creados por el archivo ejecutado
- Capturas de pantalla
- **y mucho más**

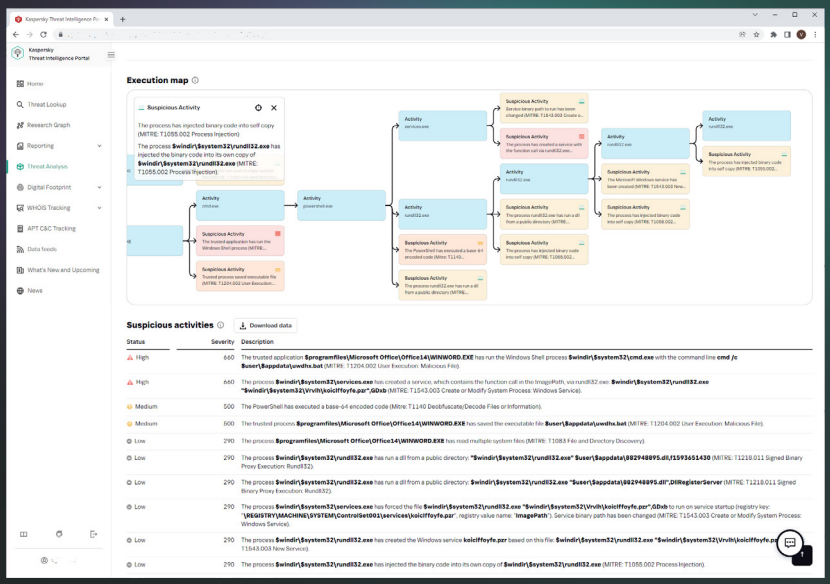
Detección y mitigación proactiva de amenazas

El malware utiliza una variedad de métodos para ocultar su ejecución y pasar desapercibido. Si el sistema no cumple con los parámetros requeridos, lo más probable es que el programa malicioso se autodestruya sin dejar rastro. Para que se ejecute el código malicioso, el entorno de sandbox debe ser capaz de imitar con precisión el comportamiento normal del usuario final.

Kaspersky Cloud Sandbox ofrece un enfoque híbrido que combina la inteligencia frente a amenazas proveniente de petabytes de datos estadísticos (gracias a Kaspersky Security Network y otros sistemas patentados), el análisis de comportamiento y una sólida antievasión con tecnologías de simulación del comportamiento humano, tales como auto clicker, desplazamiento de documentos y procesos ficticios.

Este producto se ha desarrollado en nuestro laboratorio interno de sandbox y ha evolucionado durante más de una década. La tecnología posee todo el conocimiento sobre el comportamiento de malware durante más de 20 años de investigación de amenazas continua. Esto nos permite detectar más de 360 000 nuevos objetos maliciosos cada día para proporcionar al cliente soluciones de seguridad líderes en el sector.

Como parte de nuestro portal de inteligencia frente a amenazas, Cloud Sandbox es el componente esencial en su flujo de trabajo de inteligencia frente a ellas. Threat Lookup recupera la inteligencia detallada de amenazas más reciente relacionada con direcciones URL, dominios, direcciones IP, hashes de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS/DNS, etc., mientras que Cloud Sandbox vincula ese conocimiento con los IOC generados por la muestra analizada.



Ahora, puede llevar a cabo investigaciones de incidentes complejas y eficaces, por lo que obtendrá una comprensión inmediata de la naturaleza de la amenaza y hará deducciones lógicas mientras realiza un análisis en profundidad con el fin de revelar los indicadores de amenazas interrelacionados.

La inspección puede consumir muchos recursos, especialmente cuando se trata de ataques de múltiples etapas. Kaspersky Cloud Research Sandbox potencia sus actividades forenses y de respuesta ante incidentes, proporcionando una escalabilidad para el procesamiento de archivos automático sin tener que adquirir dispositivos costosos ni preocuparse por los recursos del sistema.

www.kaspersky.es