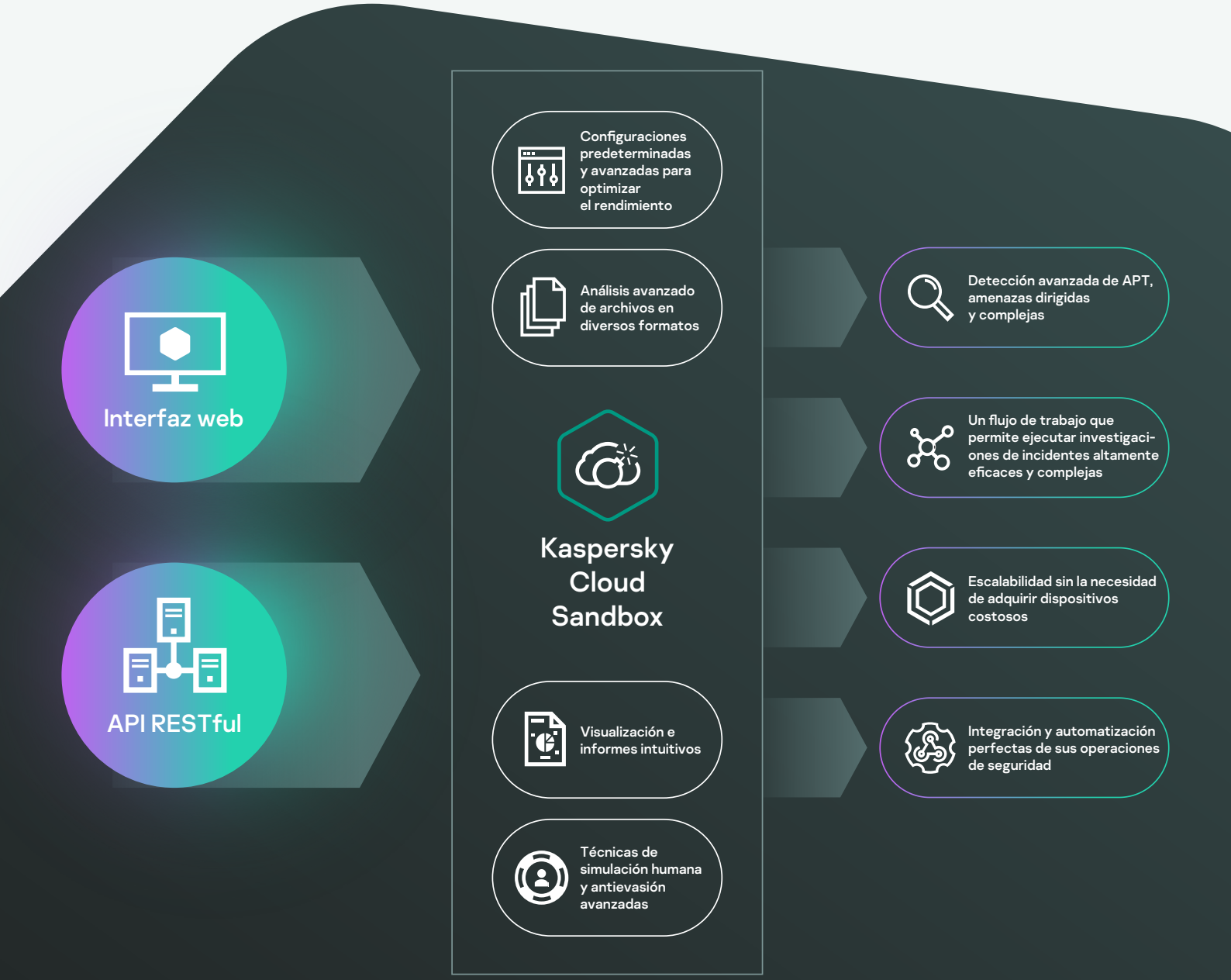
Kaspersky Cloud Sandbox

kaspersky BRING ON THE FUTURE

Kaspersky Cloud Sandbox

Es imposible evitar los ataques dirigidos de la actualidad 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 creciente 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, a la vez 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 integrales

- 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**

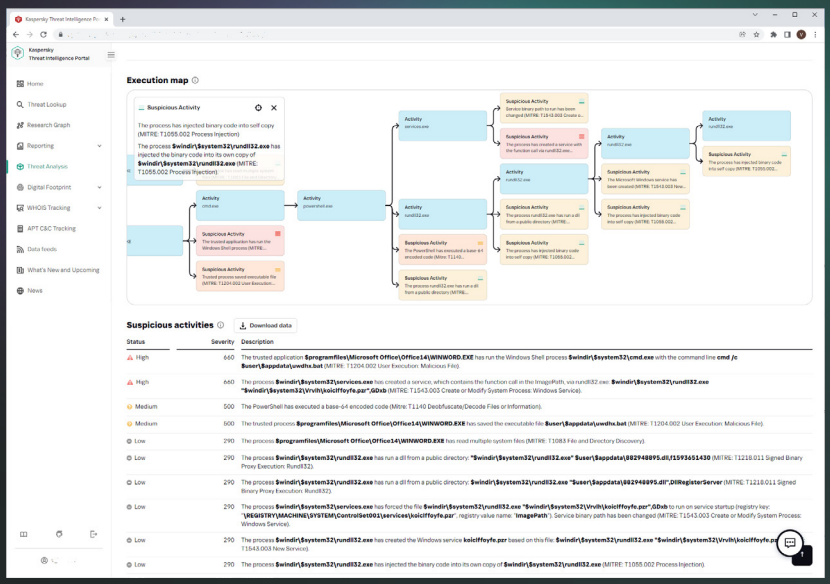
Detección y mitigación proactiva de amenazas

El malware utiliza una variedad de métodos para ocultar su ejecución a fin de que no lo detecten. Si el sistema no cumple con los parámetros requeridos, el programa malicioso se autodestruirá con toda seguridad, sin dejar rastros. 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 desarrolló en nuestro laboratorio interno de sandbox y evolucionó durante más de una década. La tecnología posee todo el conocimiento sobre el comportamiento de malware que adquirimos durante más de 20 años de investigación de amenazas continua. Esto nos permite detectar más de 360 000 nuevos objetos maliciosos cada día para proporcionarle al cliente soluciones de seguridad líderes en el rubro.

Como parte de nuestro Portal de inteligencia de amenazas, Cloud Sandbox es un componente importante en su flujo de trabajo de inteligencia de amenazas. Threat Lookup recupera la última inteligencia detallada de amenazas 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, con 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 de los recursos del sistema.

latam.kaspersky.com