Solución integral
para la detección
y eliminación de malware

Kaspersky Scan Engine

kaspersky BRING ON THE FUTURE

Introducción

Kaspersky Scan Engine (KSEn) proporciona la mejor solución de detección de amenazas, que además se puede integrar en casi cualquier aplicación.

Kaspersky Scan Engine (KSEn) brinda una protección integral para aplicaciones y portales web, servidores proxy, sistemas de almacenamiento en red y puertas de enlace de correo.

Se puede administrar e implementar fácilmente a través de ICAP y HTTP, como un servicio independiente, agrupación en clúster o contenedor Docker. KSEn utiliza los últimos métodos de detección para detectar y eliminar malware, como troyanos, amenazas de phishing, gusanos, rootkits, spyware y adware.

Escenarios de integración

- Portales web y servidores en la nube
- Servidores de archivos
- Almacenamiento conectado a la red
- Servidores de correo
- Puertas de enlace web y proxy
- Tiendas de aplicaciones y mercados

Funciones clave

Dos modos principales

Servicio tipo REST que recibe solicitudes HTTP desde las aplicaciones cliente, analiza objetos que se pasan en estas solicitudes y devuelve respuestas HTTP con los resultados del análisis.

Servicio ICAP que analiza el tráfico HTTP que pasa por un servidor proxy, NAS, firewall de aplicaciones web, NGFW o cualquier otra solución que se comunique a través del protocolo ICAP. Este modelo de integración también permite analizar las URL que solicitan los usuarios para filtrar las páginas web de contenido malicioso, de phishing o de adware.

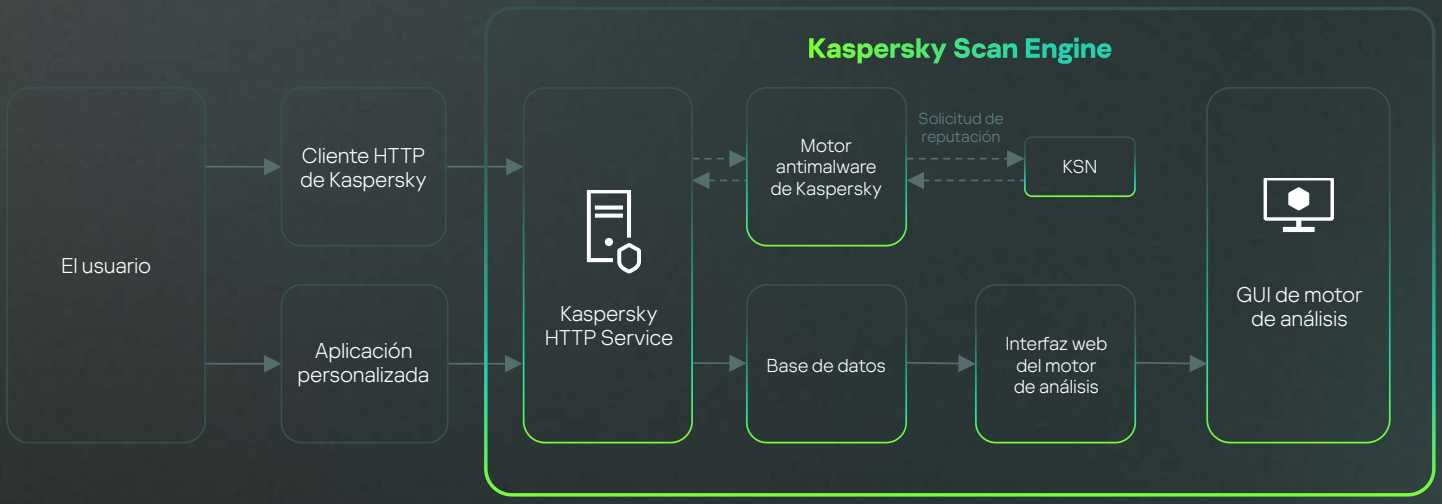
KSEn para Linux

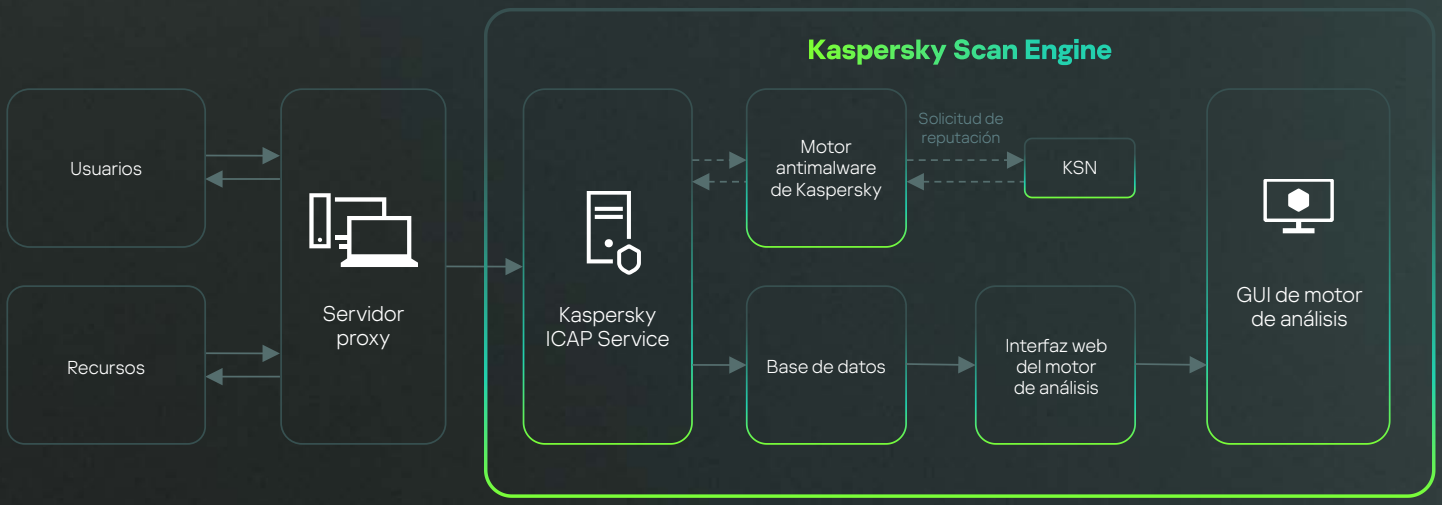
También está disponible como contenedor Docker para Linux (en modo ICAP y HTTP). Se puede implementar como contenedor individual para Docker Swarm, Kubernetes, AWS EKS y cualquier entorno de nube similar.

GUI

Kaspersky Scan Engine incluye una interfaz gráfica de usuario basada en Internet que permite configurar con facilidad el comportamiento del producto, revisar sus eventos de servicio y analizar los resultados.

Casos prácticos





Integración con cualquier solución de red

Gracias al código fuente abierto y a la API tipo REST con una gran cantidad de funciones, ahora es fácil integrar Kaspersky Scan Engine con la mayoría de las soluciones en su red.

Protección de portales web frente a la carga de malware.

Protección del almacenamiento en la nube pública (bucket de AWS S3, etc.) y privada (Nextcloud, ownCloud, más próximamente) frente a la carga de contenido malicioso.

Protección de las tiendas de aplicaciones y los mercados de software frente a la carga de aplicaciones maliciosas.

Análisis de almacenamiento de archivos Windows/Linux en busca de malware.

Complemento antimalware para puertas de enlace web/de correo de terceros. La lista de integraciones completas está disponible con solicitud previa y se actualiza constantemente.

Módulo antimalware para sistemas corporativos de administración de documentos, flujo de desarrollo de software y otros sistemas que requieren la comprobación de archivos en busca de malware.

Funciones principales

Protección antimalware galardonada

La tecnología antimalware galardonada de Kaspersky proporciona las mejores tasas de detección de malware y puede reaccionar a amenazas emergentes de forma inmediata.

Filtrado

Filtra las URL de actividad maliciosa, de phishing y de adware.

Detección

Detección de objetos multiempaquetados. Mayor cantidad de formatos de empaquetado y archivo compatibles.

Conectores de plataforma

Múltiples plataformas de terceros compatibles, de forma nativa o a través de conectores, como Amazon S3, Nextcloud, ownCloud, Kubernetes, etc.

Desinfección de archivos

Desinfección de archivos y documentos infectados, y objetos codificados. Cualquier amenaza detectada puede eliminarse por completo o, si es posible, solo puede eliminarse la carga maliciosa y dejar el resto del archivo a salvo.

Actualización

Motor antivirus actualizable: las tecnologías de detección y la lógica de procesamiento pueden actualizarse o modificarse a través de actualizaciones periódicas de la base de datos de antivirus.

Funciones avanzadas

Analizador heurístico avanzado y tecnologías de detección basadas en el aprendizaje automático.

Big data

Con tecnología de Big Data: Kaspersky Security Network proporciona información sobre la reputación de archivos y recursos web para garantizar una detección más rápida y precisa.

Escalabilidad

Kaspersky Scan Engine ofrece un rendimiento de primera categoría y se escala muy fácilmente.

Identificador de formatos

Es posible tener una capa de filtro adicional debido al componente Identificador de formatos. Puede utilizar este componente para reconocer y omitir archivos de determinados formatos durante el proceso de análisis. Es compatible con decenas de formatos, incluidos los archivos ejecutables, archivos de Office, archivos multimedia y archivos en general.

Compatibilidad con TLS

La comunicación a través del protocolo TLS es compatible cuando se ejecuta en modo de servicio tipo REST.

Modo de clúster

Kaspersky Scan Engine se puede ejecutar en modo de clúster: se pueden implementar varias instancias de Kaspersky Scan Engine en la misma red y administrarlas por medio de la interfaz de usuario web.

Nuevas funciones de Kaspersky Scan Engine 2.1

Desde junio de 2022

Seguridad y cumplimiento

Modo multiusuario y control de acceso basado en funciones. Auditoría de operaciones. Soporte de autenticación de clientes HTTP a través de tokens de API. Protección contra el forzamiento brusco de contraseñas en la interfaz de usuario web.

Cambios en la arquitectura

El motor de análisis está dividido en 2 módulos que se pueden lanzar por separado: (1) motor AV (KAV SDK) y (2) funcionalidad principal del producto (el motor de análisis como una envoltura en KAV SDK).

Mejora de la documentación

Manuales para la integración con SIEM (MicroFocus ArcSight, Splunk). Manuales para la integración con Oracle Solaris VScan, F5 Application Security Manager, GoAnywhere MFT y Dell Isilon OneFS.

Mejora operativa

Systemd es totalmente compatible para trabajar con los servicios (iniciar/detener/estado/reiniciar).

Mejora del modo de clúster

Los nodos inactivos se eliminan automáticamente del clúster y admiten clústeres heterogéneos (HTTP e ICAP).

Cambios en syslog

Múltiples destinos.
Filtro de eventos a enviar.

Premios

Premios recientes a productos de Kaspersky otorgados por laboratorios de pruebas independientes.

Leer más

Kaspersky Scan Engine

30 días de prueba gratuita

Haga clic en el siguiente vínculo y solicite una prueba de KSEn.

Leer más

latam.kaspersky.com

#kaspersky
#bringonthefuture