Solución integral para
la detección y eliminación
de malware

# Kaspersky Scan Engine

kaspersky PREPARADOS PARA EL FUTURO

# Introducción

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

Kaspersky Scan Engine (KSEn) brinda una protección integral para portales y aplicaciones 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 encontrar 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 electrónico
- Puertas de enlace web y proxy
- Tiendas de aplicaciones y mercados

## Funcionalidad clave

### Dos modos principales

Servicio de tipo REST que recibe solicitudes HTTP de aplicaciones de cliente, analiza los objetos transferidos en estas solicitudes y devuelve respuestas HTTP con resultados de 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. Luego, se filtran las páginas web que contenga contenido malintencionado, de phishing o de adware.

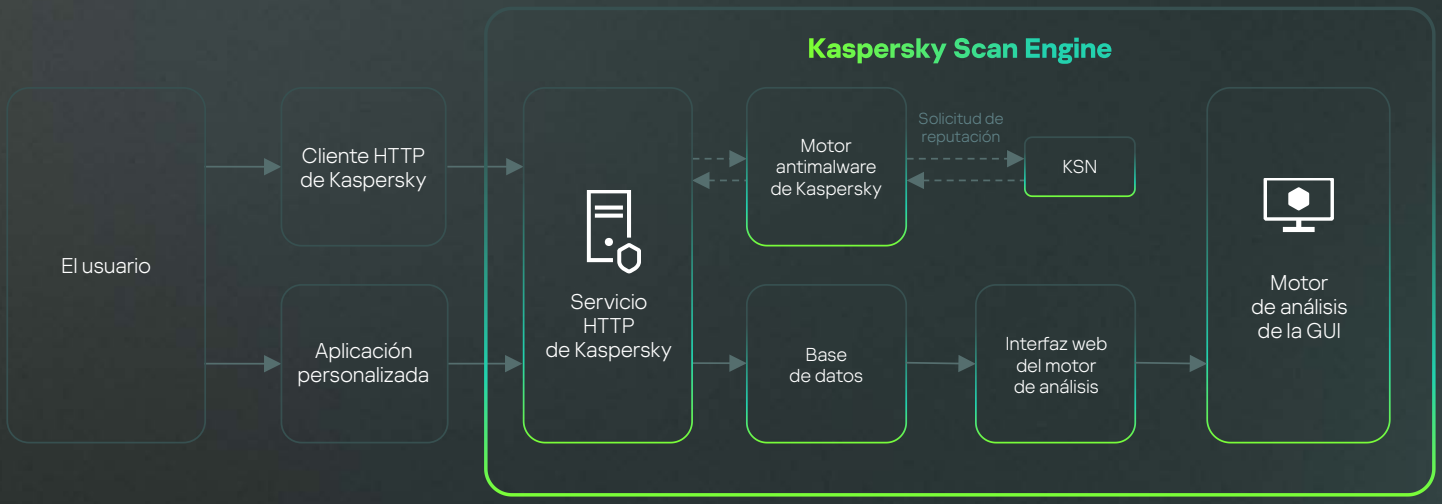
### KSEn para Linux

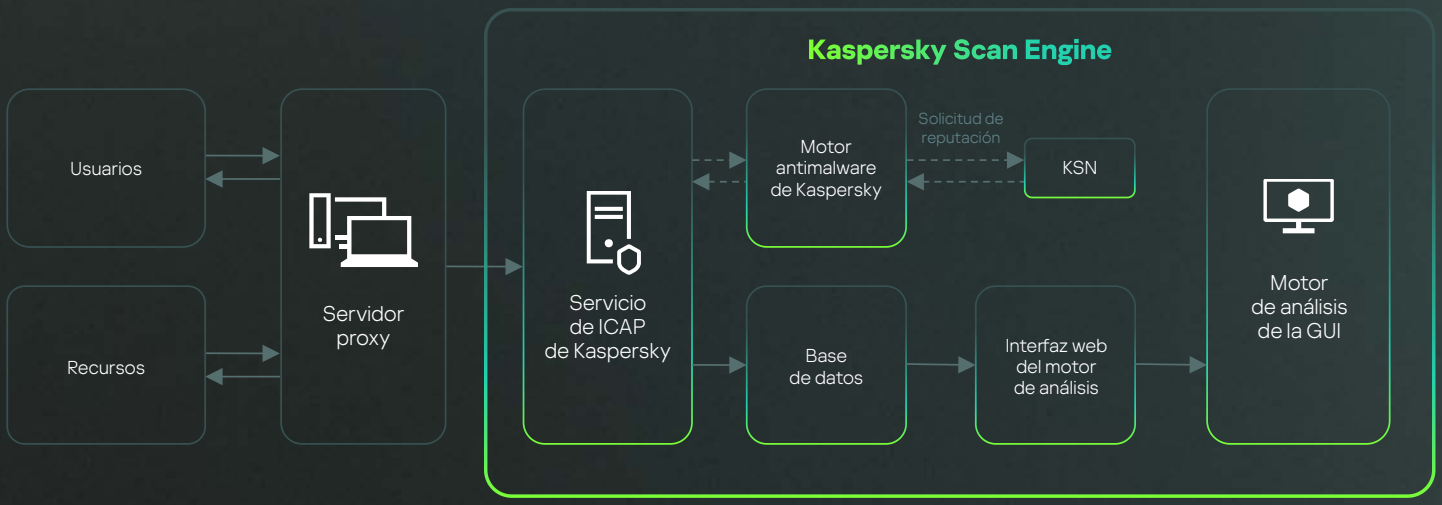
También está disponible como contenedor Docker para Linux (en modo ICAP y HTTP). Se puede implementar como contenedor individual para Docker Swarm, Kubernetes, AWS EKS y cualquier entorno en la nube similar.

### 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 del producto.

# Casos de uso




## Integración con cualquier solución de red

Gracias al código fuente abierto y a la API similar a REST con una gran cantidad de funciones, ahora usted puede integrar fácilmente 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 (AWS S3 bucket, 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 gestión de documentos, flujo de desarrollo de software y otros sistemas que requieren la comprobación de archivos en busca de malware.

# Funciones principales

## Antimalware galardonado

La premiada tecnología antimalware de Kaspersky proporciona los mejores índices de detección de malware de su clase y puede reaccionar instantáneamente a amenazas emergentes.

## de contenido

Filtra las URL maliciosas, de phishing y de adware.

## Detección

Detección de objetos multiempaquetados. Mayor número 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 infectados, archivos y objetos codificados. Cualquier amenaza detectada puede eliminarse por completo o, si es posible, solo puede eliminarse la carga maliciosa, dejando el resto del archivo a salvo.

## Actualizar

Motor antivirus actualizable: las tecnologías de detección y la lógica de procesamiento se pueden actualizar o modificar mediante actualizaciones regulares de la base de datos 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

El componente de reconocimiento de formato hace posible un nivel de filtrado adicional. Puede utilizar este componente para reconocer y omitir archivos de determinados formatos durante el proceso de análisis. Se admiten decenas de formatos, incluidos archivos ejecutables, de Office, multimedia y archivos.

## Compatibilidad con TLS

La comunicación a través del protocolo TLS es compatible cuando se ejecuta el modo de servicio parecido a 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 administrar a través 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 API Protección contra ataques de fuerza bruta de contraseñas en la interfaz de usuario web.

## Cambios en la arquitectura

El motor de análisis está dividido en 2 módulos que pueden ser publicados 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, Dell Isilon OneFS.

## Mejora operativa

Systemd es totalmente compatible para trabajar con los servicios (comenzar/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 por enviar.

# Premios

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

SE Labs INTELLIGENCE-LED TESTING BEST Small Business Endpoint WINNER 2021

AV comparatives Lowest False Positives 2022 BRONZE

AV comparatives Top Rated 2022

AV comparatives ATP 2022 BRONZE

AV comparatives Top Rated 2020

SE Labs AAA July 2022 Enterprise Advanced Security EDR Detection

SE Labs AAA Oct-Dec 2022 Enterprise Endpoint Security EPS Protection

AV comparatives Certified EPR 2022 Strategic Leader

AV-TEST av-test.org 2022 AWARD BEST USABILITY Kaspersky Endpoint Security

AV-TEST av-test.org 2021 AWARD BEST PROTECTION Kaspersky Endpoint Security

AV-TEST av-test.org 2021 AWARD BEST PERFORMANCE Kaspersky Endpoint Security

AV-TEST av-test.org 2022 AWARD BEST PERFORMANCE Kaspersky Endpoint Security

Más información

# Kaspersky Scan Engine

¡La versión de prueba gratuita de 30 días está disponible!
Haga clic en el siguiente enlace y solicite una prueba de KSEn.

Más información

www.kaspersky.es

© 2023 AO Kaspersky Lab.
Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture