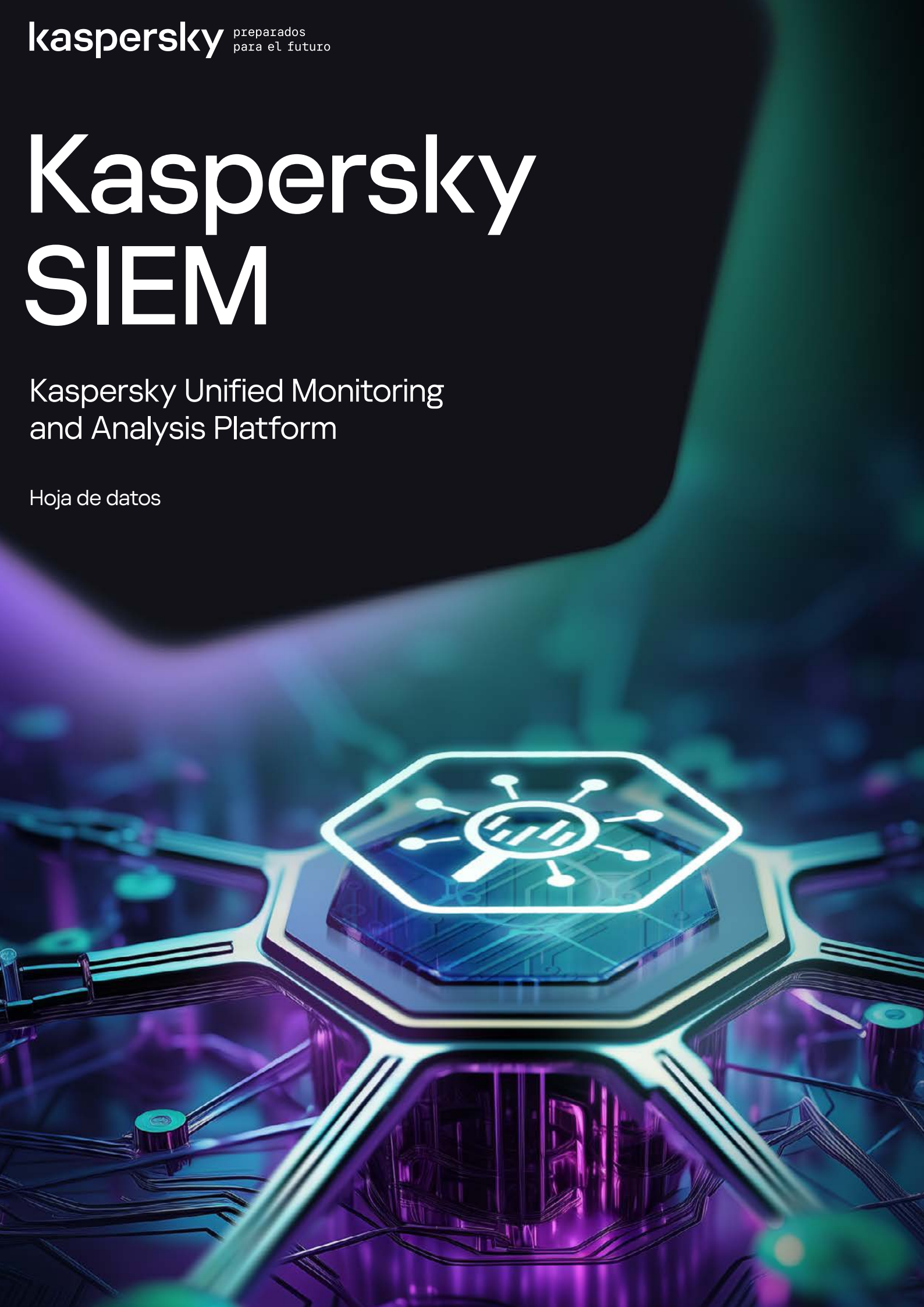
kaspersky preparados para el futuro

Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Hoja de datos



Acerca de Kaspersky SIEM y su arquitectura

Kaspersky Unified Monitoring and Analysis Platform es una solución SIEM integrada de última generación para la gestión de datos y eventos de seguridad. Se distingue en la recepción, el procesamiento y el almacenamiento de eventos de información sobre la seguridad, y en el análisis y la correlación de datos entrantes. La plataforma también cuenta con una función de búsqueda, genera alertas cuando se detectan amenazas potenciales y admite respuestas automatizadas a las alertas generadas y la búsqueda de amenazas.

La arquitectura modular de alto rendimiento permite procesar cientos de miles de eventos por segundo (EPS) en cada instancia y reduce el coste total de propiedad (TCO) mediante la optimización de los requisitos del sistema.

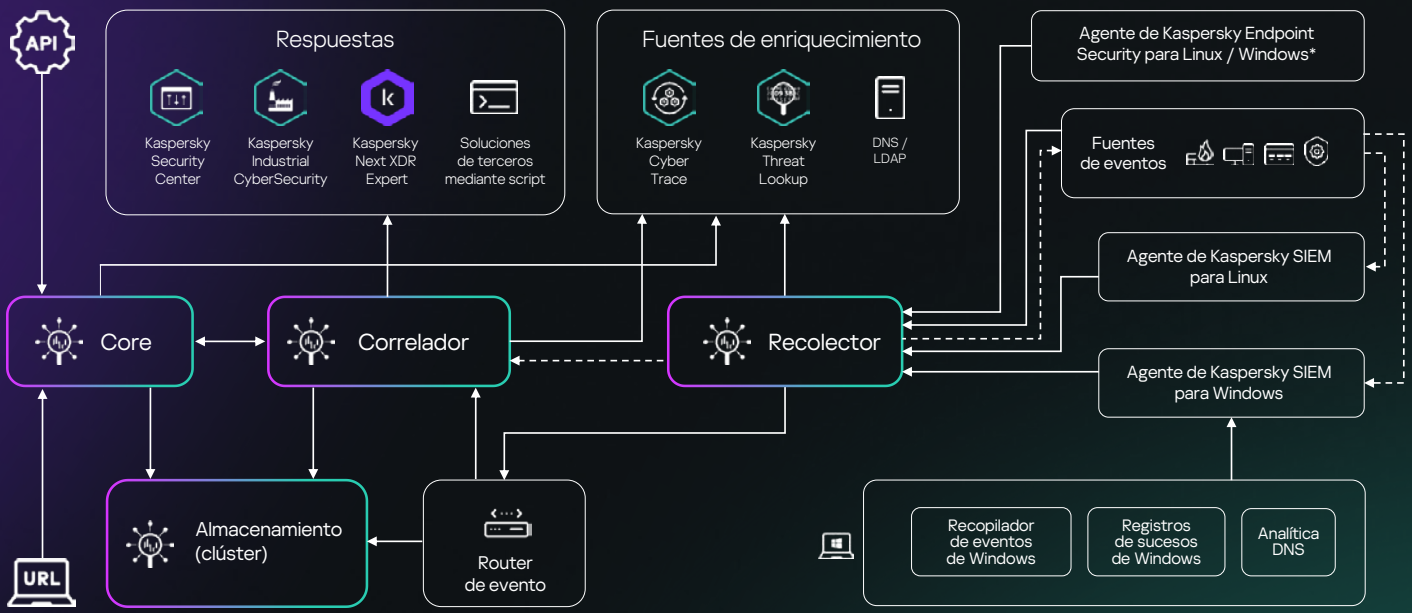
A través de la incorporación de productos de terceros y de Kaspersky en un sistema de seguridad de la información centralizado, Kaspersky SIEM es una parte fundamental de una estrategia de defensa integral capaz de proteger entornos corporativos e industriales y detectar ciberataques que comienzan en TI y pasan a los sistemas de TO.

Gracias a la arquitectura de microservicios de la solución, los administradores pueden crear y configurar los microservicios que necesitan para usar Kaspersky SIEM como un sistema de administración de registros o un sistema SIEM integral.

La solución recibe eventos de seguridad de varias fuentes, incluidos productos de Kaspersky, sistemas operativos, aplicaciones de terceros, herramientas de seguridad y diferentes bases de datos, y correlaciona los eventos y los enriquece con datos de fuentes de inteligencia sobre amenazas con el objetivo de identificar actividad sospechosa en las infraestructuras de la red corporativa y proporcionar notificaciones oportunas de los incidentes de seguridad.

Mediante la recopilación de registros de todos los controles de seguridad y la correlación de los datos en tiempo real, **Kaspersky SIEM agrega y proporciona toda la información necesaria para la investigación y la respuesta a incidentes.**

Además, Kaspersky SIEM facilita la detección de amenazas previamente desconocidas por parte de los buscadores de amenazas al permitirles analizar y correlacionar datos históricos, así como establecer referencias estadísticas para identificar anomalías.



¿Por qué escogernos?

Ahorra hasta un 50 % en los requisitos de instalación de instalación de virtualización o hardware y reduce el TCO con una solución en módulos de alto rendimiento que supera constantemente a los proveedores SIEM tradicionales en cuanto a la rentabilidad y que puede gestionar cientos de miles de EPS en cada instancia.

Mantén la flexibilidad con nuestras opciones de licencia. Realizamos un seguimiento del flujo promedio de EPS por día después de agregarlos y filtrarlos para limitar las saturaciones y no restringir el acceso a Kaspersky SIEM en caso de que se produzcan.

Aprovecha las ventajas de una amplia variedad de integraciones de terceros y de Kaspersky con opciones de respuesta integradas Otros proveedores no pueden igualar nuestro nivel de integración fluida con nuestros propios productos, lo que incluye una sola interfaz para la integración de Threat Intelligence, la capacidad de usar nuestros sensores de endpoint como agentes SIEM y mucho más.

Almacene datos localmente sin compromisos, de forma rentable y sin superar el presupuesto durante un período extendido con las opciones de almacenamiento en frío y calor usando ClickHouse y el Sistema de archivos distribuido de Hadoop (HDFS) o los discos locales, mientras puede realizar búsquedas rápidas en ambas áreas al mismo tiempo.

Mejora la relevancia de los datos, acelera la detección y la evaluación gracias al enriquecimiento con inteligencia sobre amenazas táctica, operativa y estratégica proporcionada a través de Kaspersky Threat Intelligence Portal por nuestro equipo líder mundial de investigadores y analistas.

Utilice la arquitectura de múltiples inquilinos incorporada con un MSSP y la solución para grandes empresas que ofrece compatibilidad con la arquitectura de múltiples inquilinos nativa donde una única instalación SIEM en la infraestructura principal de las organizaciones permite la creación de SIEM aislados para inquilinos que reciben y procesan sus propios eventos.

¿Por qué Kaspersky?

Kaspersky SIEM saca provecho de años de conocimientos acumulados y habilidades refinadas de los 5 Centros de Experiencia.

Más información

27

Desarrollamos herramientas y brindamos servicios desde hace **más de 27 años** para mantener su seguridad con nuestras tecnologías más probadas y más premiadas.

Más información

Somos una **empresa de ciberseguridad privada internacional** con miles de clientes y partners en todo el mundo y nos comprometemos a ser transparentes e independientes.

Más información

Kaspersky Unified Monitoring and Analysis Platform

Más información

www.kaspersky.es

© 2025 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture