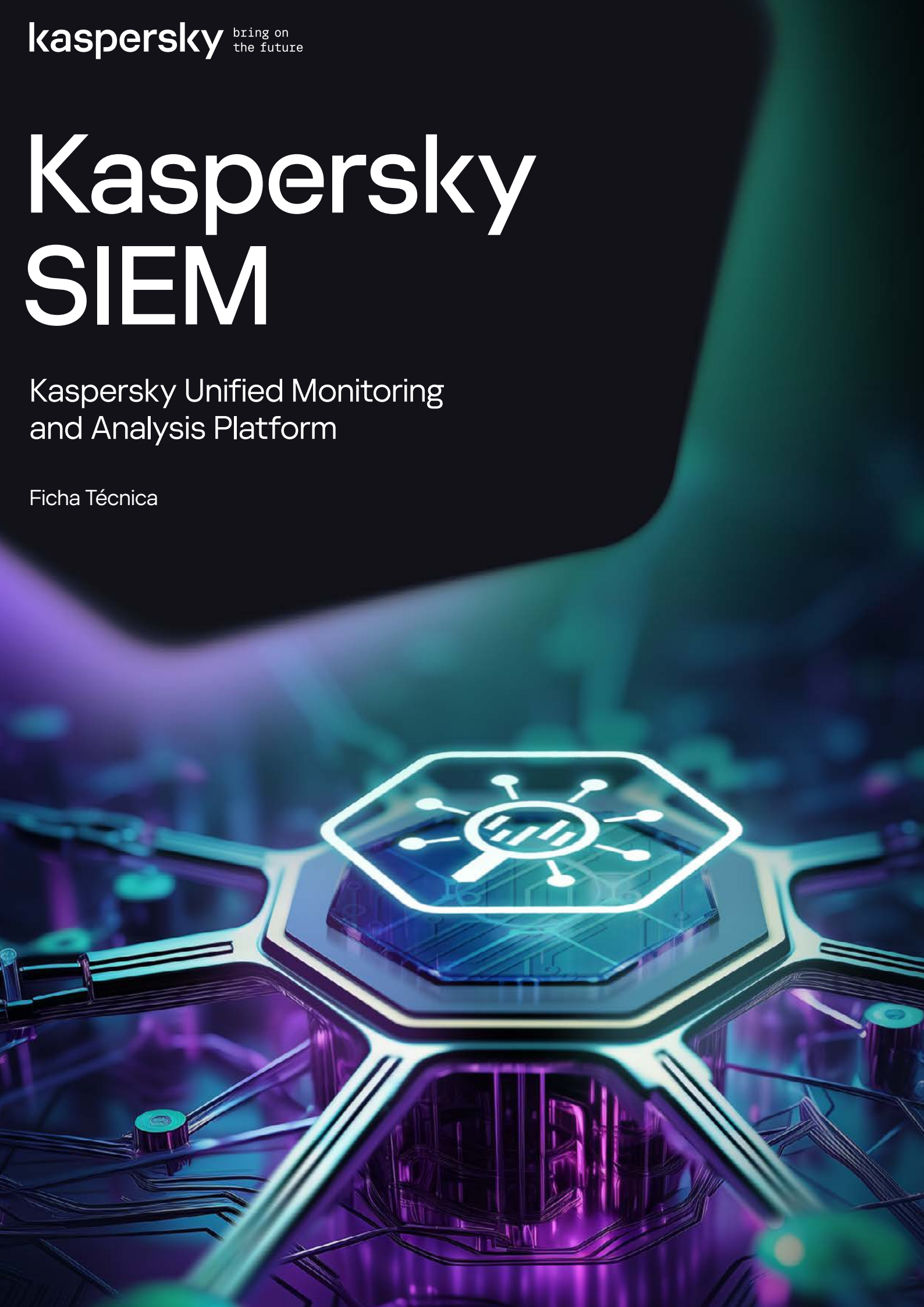
kaspersky bring on the future

Kaspersky SIEM

Kaspersky Unified Monitoring and Analysis Platform

Ficha Técnica



Acerca de Kaspersky SIEM y su arquitectura

Kaspersky United Monitoring and Analysis Platform es una solución SIEM 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, en el análisis y la correlación de datos entrantes. La plataforma también ofrece una función de búsqueda, genera alertas ante amenazas potenciales y admite respuestas automatizadas tanto para las alertas como para 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 costo total de propiedad (TCO) mediante la optimización de los requisitos del sistema.

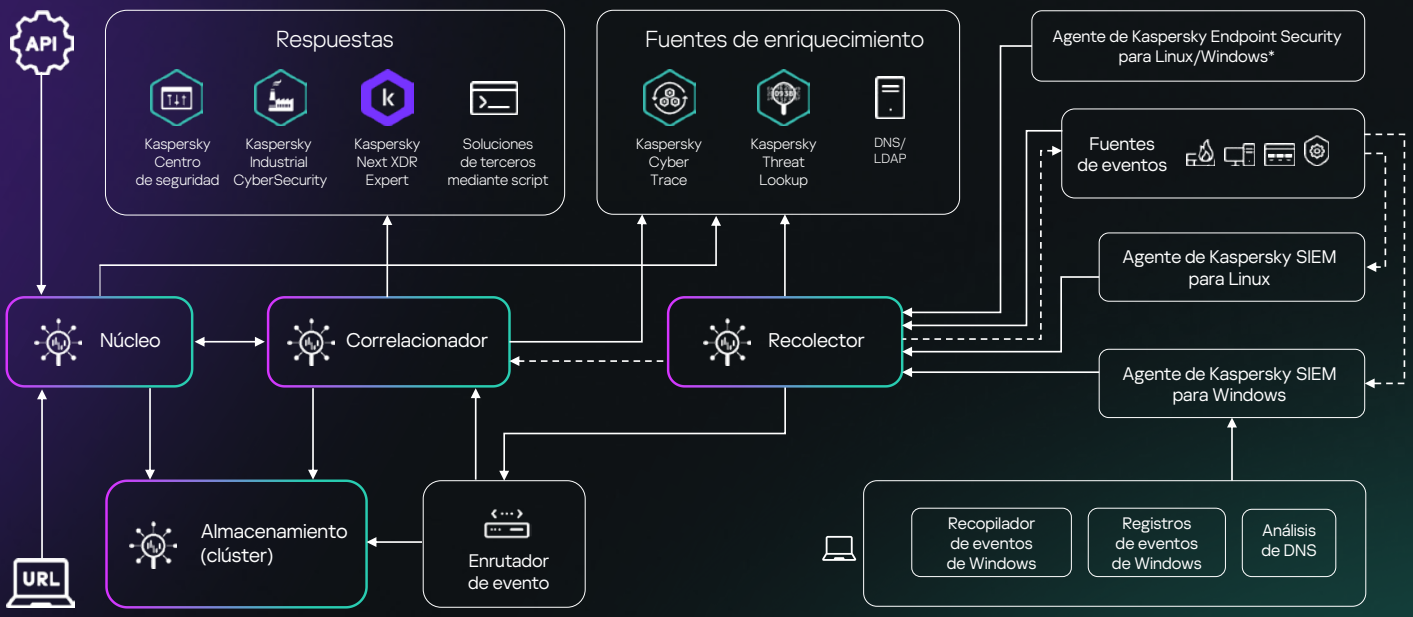
Mediante la integración de productos de terceros y de Kaspersky en un sistema centralizado de seguridad de la información, Kaspersky SIEM se posiciona como un componente esencial en una estrategia de defensa integral. Es capaz de proteger entornos corporativos e industriales, detectando ciberataques que se originan en sistemas IT y se propagan a sistemas OT.

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 recopila eventos de seguridad de diversas fuentes, incluidos productos de Kaspersky, sistemas operativos, aplicaciones de terceros, herramientas de seguridad y bases de datos. Estos eventos se correlacionan y se enriquecen con datos provenientes de fuentes de inteligencia sobre amenazas, con el objetivo de identificar actividades sospechosas en las infraestructuras de la red corporativa y proporcionar notificaciones oportunas sobre incidentes de seguridad.

Al agregar registros de todos los controles de seguridad y correlacionar los datos en tiempo real, **Kaspersky SIEM proporciona la información necesaria para investigar y responder incidentes.**

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



¿Por qué elegirnos?

Ahorre hasta 50 % en requisitos de instalación de virtualización o hardware y reduzca el TCO con una solución modular 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.

Manténgase flexible 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.

Benefíciese de la amplia variedad de integraciones de Kaspersky y de terceros, 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.

Mejore la relevancia de los datos y acelere la detección y evaluación mediante el enriquecimiento con inteligencia sobre amenazas en los niveles táctico, operativo y estratégico, proporcionada por nuestro equipo global de investigadores y analistas a través de Kaspersky Threat Intelligence Portal.

Aproveche la arquitectura de múltiples inquilinos integrada en un MSSP y la solución para grandes empresas, que permite una compatibilidad nativa con esta arquitectura. Una única instalación de SIEM en la infraestructura principal de la organización puede crear instancias de SIEM aisladas para cada inquilino, donde estos 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.

Conozca más

27

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

Conozca más

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

Conozca más

Kaspersky Unified Monitoring and Analysis Platform

Conozca más

latam.kaspersky.com

#kaspersky
#bringonthefuture