

Kaspersky Anti Targeted Attack Platform

Los cibercriminales de hoy en día se especializan en el diseño de métodos únicos e innovadores de penetración y riesgo de sistemas. A medida que las amenazas continúan evolucionando y se vuelven más sofisticadas y devastadoras, la detección rápida y la respuesta más rápida y adecuada se han convertido en esenciales.

Es vital que las empresas sigan reconsiderando sus defensas de seguridad de TI

para estar un paso por delante de las crecientes tasas de ciberamenazas y limitar las pérdidas financieras incurridas.

Kaspersky Anti Targeted Attack Platform:

- **REDUCCIÓN** del tiempo necesario para identificar y responder a las amenazas
- **SIMPLIFICACIÓN** del análisis de amenazas y la respuesta ante incidentes
- **ELIMINACIÓN** de brechas de seguridad y reducción del "tiempo de espera" durante los ataques
- **AUTOMATIZACIÓN** de las tareas manuales durante la detección y la respuesta ante amenazas
- **LIBERACIÓN** del personal de IT y de seguridad para otras tareas prioritarias
- **FACILITA** el pleno cumplimiento de los requisitos normativos

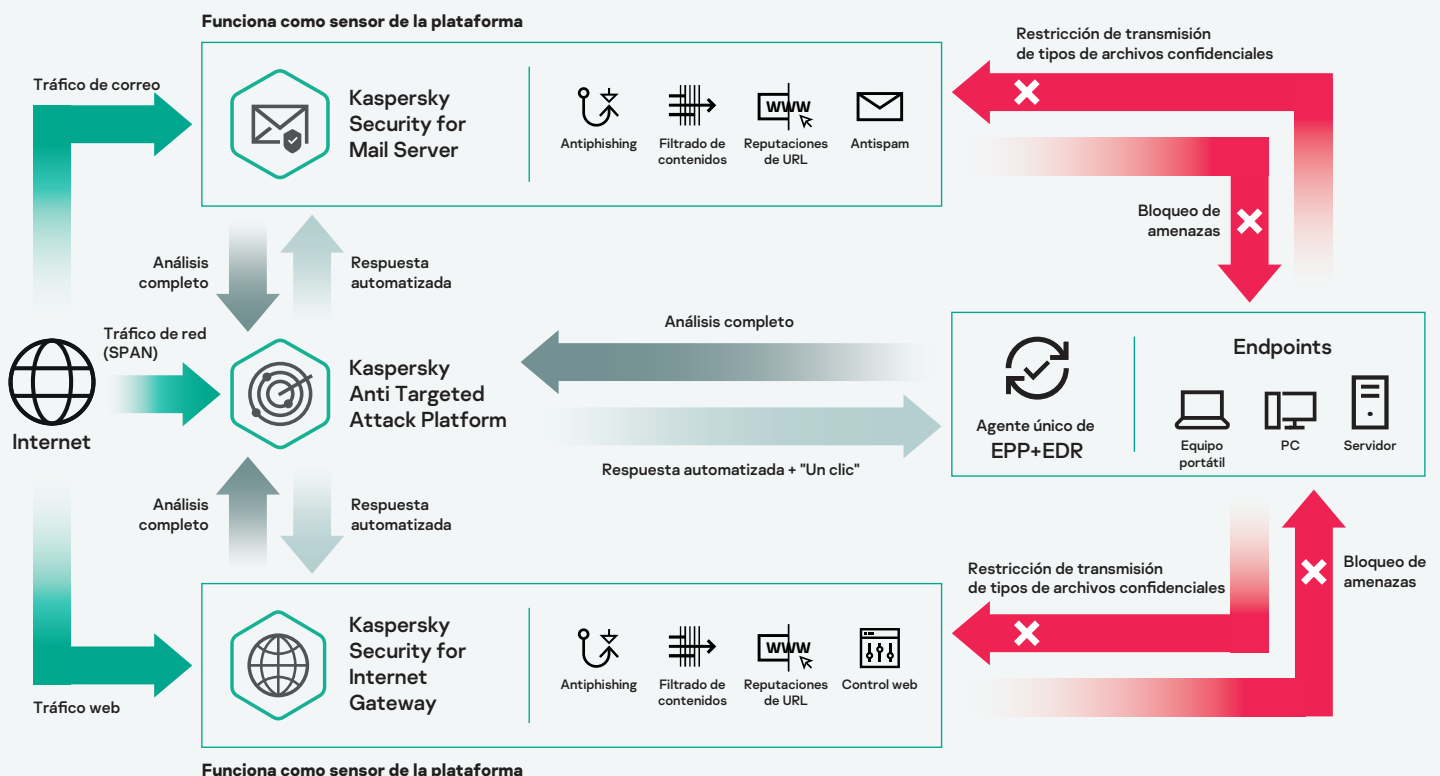
Ciberseguridad inigualable en una solución unificada

Los cibercriminales profesionales en estos días están a favor de un enfoque multivectorial. Kaspersky Anti Targeted Attack Platform combina el descubrimiento de amenazas avanzadas a nivel de red y las capacidades de EDR, al tiempo que ofrece a los especialistas en seguridad de TI todas las herramientas que necesitan para manejar el descubrimiento de amenazas multidimensionales superior, aplicar tecnologías de vanguardia, realizar investigaciones efectivas, buscar amenazas de manera proactiva y entregar una respuesta rápida y centralizada, todo ello a través de una única solución.

Los ataques más sofisticados bajo su enfoque y control

La plataforma actúa como una solución extendida de detección y respuesta que ofrece protección APT integral impulsada por nuestra inteligencia de amenazas y asignada al marco MITRE ATT&CK. Todos los puntos de entrada de amenazas potenciales (red, web, correo, PC, portátiles, servidores y máquinas virtuales) están bajo su control.

Kaspersky Anti Targeted Attack Platform está completamente integrado con **Kaspersky Endpoint Security for Business**, compartiendo un solo agente con Kaspersky EDR. También se integra con **Kaspersky Security for Mail Server** y **Kaspersky Security for Internet Gateway**, que sirven como sensores para la Plataforma, proporcionando una respuesta automatizada a amenazas de correo electrónico y web más complejas.



Una solución de seguridad fiable que ofrece total privacidad

Todos los análisis de objetos se realizan en los sistemas in situ, sin flujos de datos de salida, y Kaspersky Private Security Network ofrece actualizaciones sobre reputación de entrada en tiempo real, a la vez que garantiza el aislamiento total de los datos corporativos.

Una solución unificada para acelerar la innovación en la transformación digital mediante:

- **Continuidad empresarial integral.** Incorporamos seguridad y cumplimiento en los nuevos procesos desde el principio
- **Visibilidad completa** de su infraestructura de TI corporativa
- **Máxima flexibilidad,** que permite la implementación en entornos físicos y virtuales, donde la visibilidad y el control son necesarios.
- **Automatización de las tareas de descubrimiento de amenazas y la respuesta ante ellas,** lo que permite optimizar la rentabilidad de sus equipos de seguridad, la respuesta a incidentes y la eficacia del Centro de operaciones de seguridad (SOC)
- **Integración directa y sencilla** con los productos de seguridad existentes, para mejorar los niveles globales de seguridad y proteger las inversiones anteriores en este ámbito

Características principales:



Arquitectura de sensor de múltiples capas: visibilidad completa lograda a través de una combinación de sensores de red, web y correo electrónico, y agentes de endpoint.



Extensos motores de detección de amenazas: trabajan con datos de sensores de red (análisis de tráfico de red) y agentes de endpoint (capacidades EDR) para obtener veredictos rápidos y menos falsos positivos.



Sandbox avanzado: proporciona un entorno seguro para el análisis profundo de la actividad de las amenazas, que admite la aleatorización de los componentes del sistema operativo, la aceleración del tiempo en las máquinas virtuales, las técnicas antievasión, la simulación de la actividad del usuario y la asignación de resultados a la base de conocimientos de MITRE ATT&CK, todo lo cual contribuye a una detección altamente eficiente basada en el comportamiento.



Análisis retrospectivo: incluso en situaciones en las que los endpoints comprometidos son inaccesibles o cuando los datos se han cifrado, a través de datos automatizados, recopilación de veredictos y objetos y almacenamiento centralizado.



Dos modos de interacción de Threat Intelligence: comparación automatizada con datos de reputación global de Kaspersky Security Network y consultas manuales de búsqueda e investigación de amenazas a través del Portal de Kaspersky Threat Intelligence.



Búsqueda automática de amenazas en tiempo real: los eventos se correlacionan con un conjunto único de Indicadores de ataque (IoA) generados por los cazadores de amenazas de Kaspersky y asignados a la matriz MITRE ATT&CK, lo que proporciona descripciones claras de eventos, ejemplos y recomendaciones de respuesta.



Búsqueda proactiva de amenazas con nuestro potente generador de consultas flexible: los analistas pueden crear consultas complejas para buscar comportamientos atípicos y actividades sospechosas, y amenazas específicas para su infraestructura.

En resumen

La protección de datos fiable, la seguridad de la infraestructura de IT, la estabilidad de los procesos empresariales y el cumplimiento son requisitos previos para el desarrollo corporativo sostenible en la actualidad.

Kaspersky Anti Targeted Attack Platform le ayuda como organización con una seguridad de IT madura a crear defensas fiables que protejan su infraestructura corporativa de amenazas de tipo APT y ataques dirigidos, y a cumplir las iniciativas de conformidad normativa, sin requerir recursos de seguridad de IT adicionales. Los incidentes complejos se identifican, se investigan y se responde a ellos rápidamente, lo que aumenta la eficacia del equipo de seguridad de IT o de SOC al liberarlo de las tareas manuales, gracias a una solución unificada que maximiza el uso de la automatización y la calidad del resultado.

La solución más efectiva del sector constatada con cifras



SE Labs probó Kaspersky Anti Targeted Attack Platform contra una variedad de ataques de piratería y **nos otorgó una calificación triple A.**



En la prueba independiente "ICSA Labs: Advanced Threat Defense (Q3 2019)", Kaspersky Anti Targeted Attack Platform **logró tasas de detección del 100 %, sin falsos positivos.**



THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

The Radicati Group reconoce a Kaspersky como **principal proveedor en su Cuadrante del mercado de protección contra APT (amenazas persistentes avanzadas) de 2020.**



Gartner Peer Insights Customers' Choice nombra a Kaspersky como el principal proveedor de soluciones EDR del año 2020

Como uno de los únicos 6 proveedores en todo el mundo en ser reconocido como la Gartner Peer Insights Customer Choice para las soluciones EDR en 2020, la mejor clasificación del cliente para nuestra solución EDR extendida, Kaspersky Anti Targeted Attack Platform con Kaspersky EDR en su núcleo.

Exención de responsabilidad de Gartner

Gartner Peer Insights Customers Choice representa las opiniones subjetivas de revisiones, valoraciones y datos de usuarios finales individuales aplicados respecto a una metodología documentada, y de ninguna forma representan la opinión ni el aval de Gartner o de sus filiales.

MITRE | ATT&CK®

Calidad de detección confirmada por la evaluación de MITRE ATT&CK

El elemento central de Kaspersky Anti Targeted Attack Platform, Kaspersky EDR, participó en la Ronda de evaluación MITRE 2 (APT29), demostrando altos niveles de rendimiento en la detección de técnicas clave de ATT&CK aplicadas en etapas cruciales de los ataques dirigidos actuales.

Más información en kaspersky.com/MITRE

Para obtener más información sobre Kaspersky Anti Targeted Attack Platform, visite:

kaspersky.es/enterprise-security/anti-targeted-attack-platform

Noticias de ciberamenazas: www.securelist.es
Noticias sobre seguridad de IT: business.kaspersky.es
Seguridad de IT para pymes: kaspersky.es/business
Seguridad de IT para grandes empresas: kaspersky.es/enterprise

www.kaspersky.es

2020 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.



Seguridad probada. Somos una compañía independiente. Somos transparentes. Nos comprometemos a construir un mundo más seguro en el que la tecnología mejore nuestras vidas. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Más información en kaspersky.es/transparency



**Proven.
Transparent.
Independent.**