



Lista de características

Kaspersky Managed Detection and Response

Contenido

Descripción general de Kaspersky MDR	3
¿Cómo funciona Kaspersky MDR?	4
Características de Kaspersky MDR	5
Productos de Kaspersky compatibles	7
Lo que distingue a Kaspersky MDR	8



Descripción general de Kaspersky MDR



Kaspersky Managed Detection and Response

Kaspersky Managed Detection and Response (MDR) brinda detección, priorización, investigación y respuestas continuas. Proporciona todos los principales beneficios de un centro de operaciones de seguridad (SOC) sin tener que crear uno realmente.

El objetivo principal del servicio de MDR es detectar amenazas en cada etapa de un ciberataque, tanto antes del riesgo real como después de que los actores maliciosos hayan penetrado en la infraestructura corporativa. Esto se logra mediante el uso de sistemas de seguridad preventivos y la búsqueda de amenazas, ambos componentes integrales de Kaspersky MDR.

Cuando se combina con Kaspersky Incident Response, cubre todo el ciclo de gestión de incidentes, desde la detección de amenazas hasta la corrección luego del ataque.

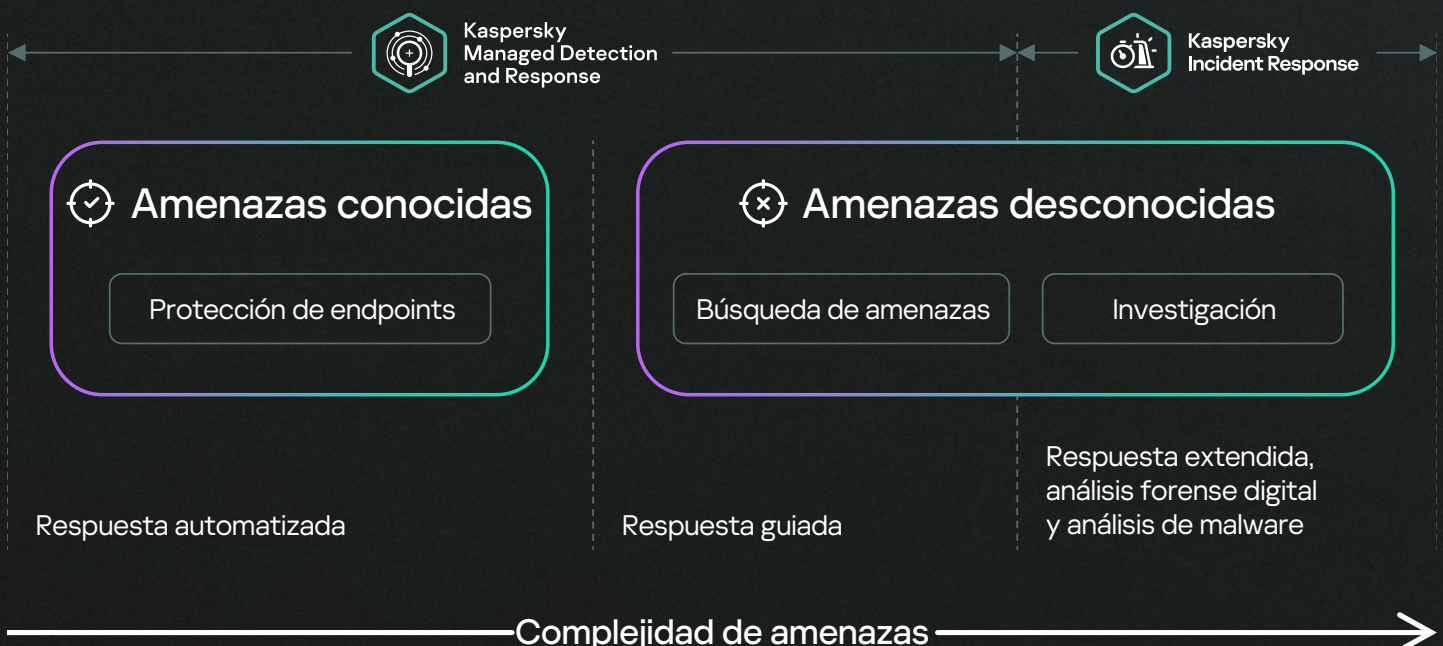


Kaspersky Incident Response

Kaspersky Incident Response obtiene un panorama detallado del incidente. El servicio cubre el ciclo completo de investigación de incidentes y respuestas, desde la acción inicial ante las amenazas y la recopilación de pruebas hasta la identificación de rastros adicionales de piratería informática y la preparación de un plan de mitigación de ataques.

La **sinergia entre** Kaspersky MDR y Kaspersky Incident Response es perfecta y fácil de usar. Cuenta con el respaldo de un equipo de expertos que supervisa su infraestructura de TI en todo momento, de modo que estén listos para responder de forma inmediata a ciberataques de cualquier complejidad.

La sinergia entre los servicios



Los principales componentes de Kaspersky MDR



SOC de Kaspersky

El equipo de expertos globales que proporciona el servicio hace casi una década.



Consola de MDR

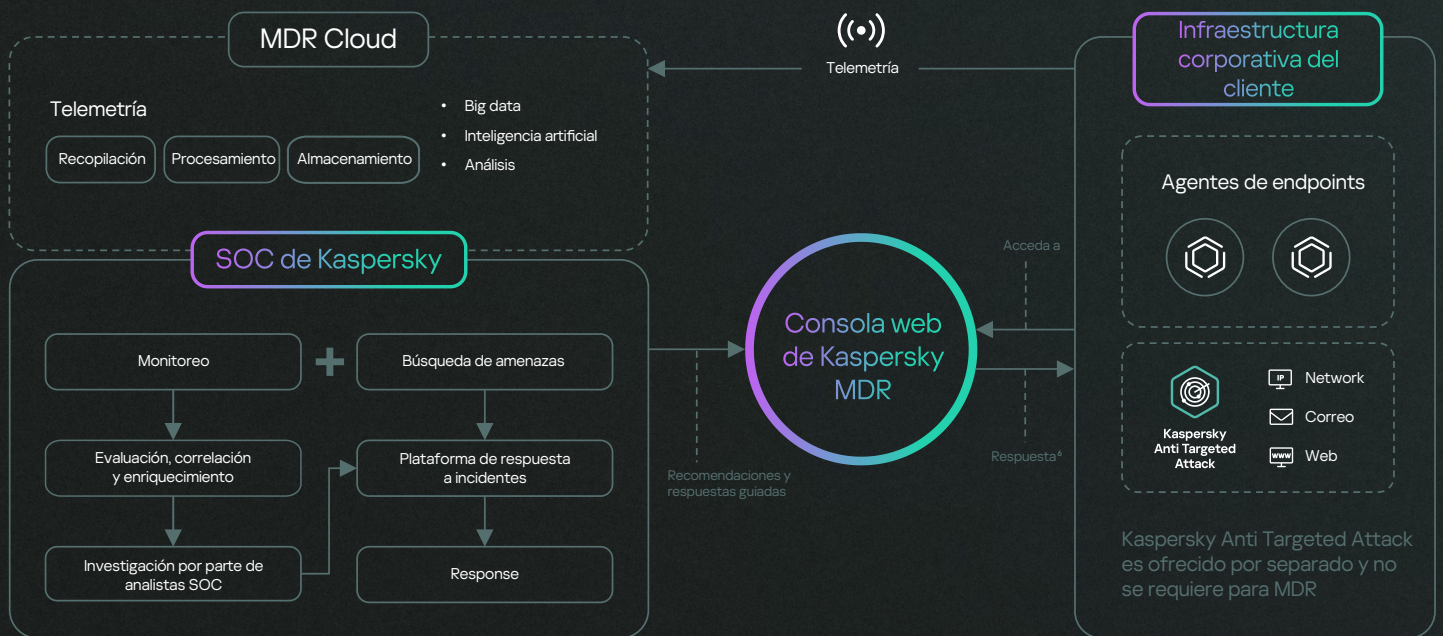
Proporciona una interfaz para gestionar y mantener el sistema de protección de la red del cliente administrado por Kaspersky MDR.



Protección de endpoints

Una aplicación de Kaspersky que protege los endpoints y los datos almacenados en ellos contra el malware y otras amenazas.

Arquitectura de Kaspersky MDR



¿Cómo funciona?

1

El sistema de **Kaspersky Endpoint Security for Business (KESB)** instalado en los establecimientos del cliente obtiene y reenvía datos de telemetría al SOC de Kaspersky.

2

La **telemetría** se analiza con herramientas de aprendizaje automático, con la participación directa de los expertos del SOC de Kaspersky.

3

El **equipo del SOC de Kaspersky** investiga alertas e informa al cliente sobre toda actividad maliciosa, además de ofrecer recomendaciones y respuesta guiada paso a paso.

¹ La respuesta automatizada se inicia cuando el cliente la aprueba en la consola de Kaspersky MDR (si el cliente no lo hace, la consola de MDR pedirá la autorización antes de implementar la respuesta automatizada).

Características de Kaspersky MDR

Protección completa:

Característica

Descripción



Supervisión de seguridad ininterrumpida

Kaspersky MDR brinda una supervisión constante de su entorno de TI, lo que garantiza que cualquier actividad sospechosa se identifique y se aborde de inmediato, independientemente del momento en que se produzca.



Cacería de amenazas

El servicio utiliza análisis avanzados, aprendizaje automático e inteligencia sobre amenazas de Kaspersky para buscar, de forma proactiva, indicios de riesgos en la infraestructura. Los analistas de Kaspersky MDR realizan actividades de búsqueda de amenazas en su entorno para identificar las amenazas ocultas que las herramientas automáticas podrían no detectar.



Casos de respuesta guiada y remota

Una vez que se confirma una amenaza, Kaspersky MDR brinda procedimientos de respuesta guiados. También puede realizar acciones de respuesta remota para mitigar la amenaza.

Si necesita acciones de respuesta más detalladas, puede solicitar Kaspersky Incident Response junto con un análisis forense digital y un análisis de malware (compra por separado).



Acceso directo a los equipos de expertos de Kaspersky

Los clientes de MDR pueden consultar a los analistas del SOC de Kaspersky para recibir ayuda experta durante un incidente. Solo tiene que enviar una solicitud en la pestaña de comunicación del incidente. Nuestros analistas brindan información adicional, orientación y apoyo para garantizar una respuesta eficaz frente a las amenazas complejas.

Si se compra la suscripción a Kaspersky Incident Response, también se incluye el acceso directo al Equipo Global de Respuesta a Emergencias para llevar a cabo investigaciones y acciones detalladas ante incidentes.



Envío de incidentes

Si sospecha que su entorno está en riesgo, puede informar sobre incidentes de forma manual en la consola de Kaspersky MDR. Esto resulta especialmente útil cuando un cliente observa una actividad inusual que podría no activar las alertas automáticas o cuando el conocimiento interno sugiere algo que está mal y que la supervisión externa podría no detectar.



Compatibilidad con aplicaciones EPP de terceros

Esta configuración permite instalar aplicaciones EPP de terceros y desplegar la solución Kaspersky Managed Detection and Response en la infraestructura de la organización.

Visibilidad y conocimiento mejorados

Característica

Descripción



Paneles fáciles de usar de MDR

Los paneles brindan información sobre incidentes en curso, así como de los activos, las respuestas y las herramientas adecuadas para trabajar con ellos, lo que ofrece una visión de la situación en tiempo real.



Visibilidad de activos

Esta función proporciona visibilidad de todos los activos de la red para garantizar que todos los endpoints estén controlados y protegidos.



Comprobación de estado de MDR

La función de Comprobación de estado de MDR le permite comprobar qué activos están protegidos por Kaspersky MDR actualmente y cuáles no han enviado telemetría durante un cierto período de tiempo.



Administrar la solución a través de la API de REST

Para recuperar datos de Kaspersky MDR, lo que permite la integración con otros sistemas o aplicaciones personalizadas para el posterior análisis o la elaboración de informes. La API de REST funciona a través de HTTP y consiste en un conjunto de métodos de solicitud o respuesta. Le permite administrar Kaspersky MDR a través de la solución de un tercero, no solo a través de la consola de MDR.



Métodos de notificación del usuario en la consola de MDR

Los usuarios con un estado activo pueden recibir notificaciones de Kaspersky Managed Detection and Response por correo electrónico o Telegram sobre incidentes registrados y sus actualizaciones.

Ubicación de los analistas del SOC de Kaspersky:

- ① Rusia
- ② Medio Oriente
- ③ Europa
- ④ Latinoamérica



Protegemos más de 220.000 empresas en aproximadamente 200 países y territorios

Productos compatibles de Kaspersky

Escenario para la activación de Kaspersky MDR

Productos Kaspersky

Lo que brinda

Clientes de endpoints de Kaspersky, nuevos o ya existentes.

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security para Mac
- Kaspersky Endpoint Security for Linux

Protección y detección a escala completa de los endpoints del cliente.

Clientes existentes o nuevos con infraestructuras virtuales

- Kaspersky Security for Virtualization Light Agent para Windows
- Kaspersky Security for Virtualization Light Agent para Linux

Supervisión y protección a escala completa de máquinas virtuales.

Clientes existentes o nuevos que usan Kaspersky Anti Targeted Attack

- Kaspersky Anti Targeted Attack
- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security para Mac
- Kaspersky Endpoint Security for Linux

Kaspersky MDR recibe incidentes críticos que no pueden ser entregados por Kaspersky Endpoint Security, como detecciones de IPS/IDS/Sandbox.

Kaspersky MDR permite que los usuarios de KATA aborden detecciones de APT avanzadas desde KATA.

Cliente nuevo con productos de endpoints de terceros

- Kaspersky Endpoint Security for Windows en la configuración del Agente de EDR

Supervisión y detección de incidentes sin protección antivirus completa.

La combinación de productos puede variar según el escenario.

Kaspersky Endpoint Security for Windows en la configuración del Agente de EDR

Kaspersky Endpoint Security for Windows ahora puede instalarse junto con aplicaciones EPP de terceros en el modo del Agente de EDR, lo que significa que Kaspersky MDR ahora puede integrarse en la infraestructura del cliente incluso si no tiene KESB. En este caso, KES funciona como agente de supervisión y no proporciona capacidades de protección de endpoints.

Lo que hace que Kaspersky MDR se destaque



Desarrollado por un líder en ciberseguridad

Kaspersky es la empresa de seguridad de TI independiente más grande del mundo. Nuestra presencia global y nuestro enfoque en el liderazgo de la tecnología y la inteligencia de amenazas respaldan nuestros productos y soluciones, que protegen más de 220.000 empresas en aproximadamente 200 países y territorios.

Durante los últimos 10 años, los productos de Kaspersky participaron en 927 pruebas y evaluaciones independientes y recibieron 680 primeros puestos.

[Más información](#)



Presencia global y cobertura en todas las industrias

Kaspersky MDR funciona de forma ininterrumpida en todo el mundo y ayuda a las organizaciones de todos los tamaños e industrias con diferentes niveles de madurez de seguridad de TI.

Nuestros clientes están felices de compartir sus historias de éxito con Kaspersky MDR.

[Más información](#)



Compatibilidad con EPP de terceros

Kaspersky Endpoint Security for Windows puede instalarse junto con aplicaciones EPP de terceros en el modo de Agente de EDR.

[Más información](#)



Inteligencia de amenazas única

Kaspersky MDR se basa en varios petabytes de datos de amenazas recopilados continuamente en todo el mundo y en más de dos décadas de análisis de expertos. Las fuentes de inteligencia de Kaspersky no se limitan a las OSINT (inteligencias de fuentes abiertas), sino que también incluyen tecnologías patentadas que recopilan inteligencia sobre amenazas que están activas actualmente en entornos reales.



Expertos reconocidos

El SOC de Kaspersky es un equipo de expertos que detectan e investigan incidentes de seguridad complejos para organizaciones de todas las industrias y diferentes regiones hace casi 10 años. El equipo cuenta con numerosos certificados y acreditaciones.



Transparencia e información práctica

La solución no solo emite alertas, también brinda recomendaciones e información práctica sobre cómo responder ante las amenazas detectadas y mitigarlas.

Todos los años, publicamos nuestros análisis de MDR, que incluyen las principales tendencias y el panorama de amenazas actual que podrían enfrentar nuestros clientes.

[Más información](#)



Amplia compatibilidad con sistemas operativos

Es compatible con todos los sistemas operativos populares, como Windows, Linux y Mac.



Windows



Linux



MacOS





Kaspersky Managed Detection and Response

Más
información

latam.kaspersky.com

© 2024 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas son
propiedad de sus respectivos propietarios.

#kaspersky
#bringonthefuture