



Búsqueda, detección y
respuesta continuas de
amenazas dirigidas a su empresa

Kaspersky Managed Detection and Response

kaspersky bring on
the future

Desafíos a los que se enfrentan las empresas

55 %

de las empresas informa que sus dispositivos se infectaron con software malicioso*

20 %

de las empresas se enfrenta a APT**

18 %

de los encuestados informa que la causa de los incidentes de su empresa fue la falta de personal de ciberseguridad calificado***

2500 millones de USD

Pérdidas extremas debido a un ciberataque exitoso****

Mejora la solidez de tu ciberseguridad con la protección administrada continua

El trabajo remoto, el rápido desarrollo de métodos de intercambio de información, la creciente disparidad de habilidades globales y la creciente cantidad de ciberataques capaces de eludir los controles automatizados tradicionales de prevención y detección están ejerciendo una enorme presión sobre organizaciones de todos los tamaños. Es fundamental que puedan responder con rapidez y eficacia.

Kaspersky Managed Detection and Response (MDR) es un servicio que ofrece protección administrada continua frente a ciberamenazas y ataques sofisticados que las medidas de seguridad automatizadas tradicionales pasan por alto.

La solución aumenta el nivel de seguridad de TI para organizaciones pequeñas y medianas que carecen de experiencia en ciberseguridad al proporcionarles un servicio integral de despliegue rápido. Para los equipos con vasta experiencia en ciberseguridad avanzada, ofrece mayor flexibilidad, ya que les permite delegar las tareas de detección y clasificación de incidentes a los expertos de Kaspersky, o recibir una opinión profesional adicional sobre los incidentes que ellos mismos detectaron.

Kaspersky MDR fortalece y mejora la resistencia de las organizaciones frente a las ciberamenazas, optimiza los recursos existentes, ayuda a utilizar de forma eficiente los recursos existentes y optimiza las futuras inversiones en seguridad de TI.

Características principales



Supervisión y detección de amenazas continuas



Descripción general de todos los recursos protegidos con su estado actual



Respuesta guiada automatizada



Acceso directo a los analistas de SOC de Kaspersky



API REST para la integración con IRP/SOAR



Web Console con paneles e informes



Almacenamiento de telemetría sin procesar durante 3 meses



Envío de incidentes personalizados



Almacenamiento del historial de incidentes de seguridad durante 1 año

* IT Security Economics, 2022

** Kaspersky MDR Analyst Report, 2023

*** Kaspersky Human Factor 360 Report, 2023

**** Global financial stability report. The Last Mile: Financial Vulnerabilities and Risks, 2024

Fuentes de telemetría y alertas para Kaspersky MDR



Kaspersky Endpoint Security for Windows



Kaspersky Endpoint Security for macOS



Kaspersky Endpoint Security for Linux



Kaspersky Virtualization Light Agent



Kaspersky Anti-Targeted Attack

Funcionamiento

1

Los analistas del SOC de Kaspersky investigan alertas de seguridad y analizan de forma proactiva eventos de telemetría que reciben de los productos de Kaspersky instalados en la red del cliente. Esta telemetría se correlaciona con la información sobre ciberamenazas de Kaspersky, que se basa en más de 25 años de experiencia investigando algunos de los ciberataques y las campañas dirigidas más célebres del mundo, a fin de identificar tácticas, técnicas y procedimientos conocidos, nuevos y emergentes utilizados por los atacantes. Los IoA únicos facilitan la detección de amenazas sin software maliciosos ocultas que imitan actividades legítimas.

2

Como parte del evento que gestiona los procesos en Kaspersky MDR, los mecanismos de inteligencia artificial (IA) ayudan a reducir la cantidad de falsos positivos y agiliza la investigación de incidentes por parte del equipo del SOC.

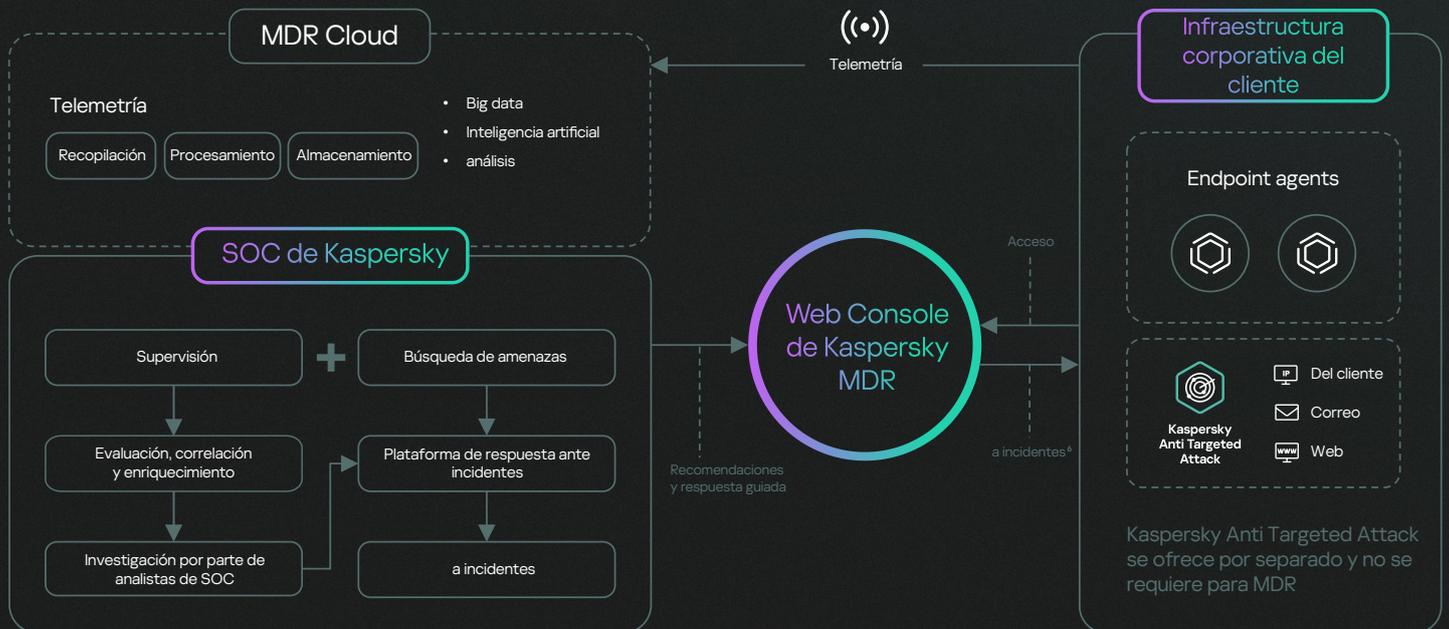
3

Cuando se detecta una amenaza potencial, Kaspersky MDR la clasifica por nivel de gravedad y notifica al cliente por correo electrónico o Telegram. Siempre que es posible, el análisis de causas raíz ayuda a identificar la fuente del ataque y comparte recomendaciones para contener las amenazas detectadas, responder a ellas y mitigarlas.

4

Los clientes pueden optar por delegar de forma parcial o completa las capacidades de respuesta* al equipo del SOC de Kaspersky. Las preguntas relacionadas con el incidente se pueden discutir en un chat en la Web Console de Kaspersky MDR.

Arquitectura de Kaspersky MDR



Kaspersky MDR es compatible con soluciones antivirus de terceros. La respuesta automatizada se inicia cuando el cliente la aprueba en el portal de Kaspersky MDR (si el cliente no lo hace, el portal de MDR pedirá la autorización antes de implementar la respuesta automatizada).

* Si se requiere un análisis más detallado y tienes una suscripción activa a Kaspersky Incident Response, el incidente puede enviarse al GERT de Kaspersky para su investigación.

Propuestas de valor



La tranquilidad que obtienes gracias a la protección continua frente a las amenazas sofisticadas más complejas



Todos los principales beneficios de tener tu propio SOC sin tener que pasar por la molestia y los gastos de crear uno



Menores costes de seguridad; no necesitas contratar ni capacitar a varios profesionales de seguridad de TI costosos para cubrir todas las bases



Permite que tus recursos de seguridad de TI internos se vuelvan a enfocar en la gestión de otros problemas críticos para la empresa

Reconocimiento global y trayectoria inigualable

Kaspersky participa en una amplia variedad de pruebas independientes y trabaja de cerca con empresas de analistas globales líderes. Kaspersky cuenta con **reconocimiento global** como líder de ciberseguridad, y Kaspersky MDR, como todos nuestros productos, ha recibido numerosos premios. Las características de detección y respuesta de Kaspersky MDR se complementan con la experiencia reconocida globalmente de uno de los equipos de detección de amenazas más exitoso y experimentado del sector, el equipo altamente calificado y experimentado del SOC de Kaspersky.





Kaspersky Managed Detection and Response

Más
información

www.kaspersky.es

© 2024 AO Kaspersky Lab.
Las marcas registradas y logos son propiedad de sus
respectivos dueños.

#kaspersky
#bringonthefuture