

kaspersky



Kaspersky
Managed Detection
and Response

Frenamos los
incidentes antes
de que frenen su
negocio



Kaspersky Managed Detection and Response es un servicio prestado por expertos que proporciona monitoreo continuo, detección, investigación forense y respuesta ante incidentes sofisticados. El servicio complementa los controles de seguridad existentes con detección liderada por humanos e inteligencia de amenazas de alcance global. El servicio fortalece de inmediato la postura de seguridad de TI y TO, sin importar el tamaño de la empresa o el sector al que pertenezca.

Ventajas clave



Protección avanzada y continua de toda la superficie de ataque (los endpoints, la red, la nube y mucho más) desde el primer día.



Un SOC listo para usar, disponible 24/7, con un equipo global de expertos: elimina la necesidad de crear, dotar de personal y mantener sus propias operaciones de seguridad internas.



Una menor carga de trabajo para su equipo de seguridad interno, ya que nos delega el monitoreo, el triaje y la investigación.



Seguridad basada en resultados que combina la experiencia humana, la inteligencia sobre amenazas y la IA para poner freno a los incidentes antes de que puedan afectar a su negocio.

Fortalezca la resiliencia operativa de su infraestructura con un servicio de seguridad administrada que opera en régimen 24/7.

El trabajo remoto, el crecimiento acelerado del intercambio de información digital, la ampliación de la brecha mundial de competencias y el aumento de ciberamenazas capaces de eludir los controles automatizados tradicionales ejercen presión constante sobre organizaciones de cualquier tamaño. En estas condiciones, es fundamental responder de forma rápida y eficaz a cada incidente.

Panorama de las ciberamenazas actuales¹

1 Vectores de ataque inicial



31 %
de cuentas
válidas



13 %
relaciones
de confianza



39 %
exploits para
aplicaciones
públicas

2 Muévase y complete tareas

Los atacantes suelen utilizar herramientas legítimas (como Mimikatz, PsExec, SoftPerfect Network Scanner) en infraestructuras que carecen de controles adecuados de configuración del sistema.

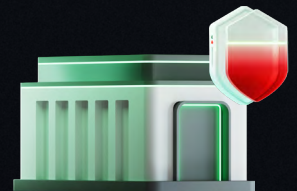


3 Impacto

42 %
archivos
cifrados

17 %
filtración
de datos

11 %
persistencia instalada
para ataques futuros



Las pruebas demuestran que los atacantes suelen volver después de perpetrar un ataque.



Duración del ataque

Rápido **45 %**
hasta 1 día

Promedio **20 %**
13 días

Duradero **35 %**
253 días

Kaspersky MDR detectó y neutralizó un ataque de día cero que, de lo contrario, podría haber causado graves trastornos en nuestras operaciones.



Daniel Huerta Santos

Gerente de Ciberseguridad, Gobierno del estado de Guanajuato

[Leer más](#)

Lo que brinda Kaspersky MDR

Protección continua contra amenazas avanzadas, desde el primer día

Kaspersky MDR se activa en cuestión de minutos sin necesidad de infraestructura adicional, gracias a la labor de nuestros analistas de SOC y la inteligencia sobre amenazas, amenazas para ofrecer una detección multicapa en varios dominios. Basándose en miles de millones de señales de telemetría, permite la búsqueda proactiva de amenazas, la investigación de las causas raíz y una corrección completa y rápida. De este modo, se garantiza una protección contra amenazas conocidas y de día cero desde el primer día.

Casos de uso



Protección llave en mano 24/7 para organizaciones que no tienen departamento de SecOps



Administración conjunta de SecOps para reforzar los equipos internos de ciberseguridad



Protección avanzada para infraestructura OT



Protección continua específica para los sistemas integrados

Operaciones de seguridad lideradas por expertos y mejoradas con inteligencia

Con Kaspersky MDR, sus operaciones de seguridad son administradas por expertos de prestigio global, con una amplia experiencia de primera línea y certificaciones líderes del sector. Su trabajo se potencia con Threat Intelligence y mecanismos de IA líderes en el mercado integrados en el servicio, lo que ayuda a dar más información sobre cada alerta, acelerar la detección y reducir el tiempo medio de respuesta (MTTR).

30 minutos

nuestro MTTR promedio ²

30 %

de todas las alertas recibidas que procesa AI Auto Analyst ¹

Eficiencia operativa y costos predecibles

- Kaspersky MDR elimina la complejidad y el costo que supone crear un SOC interno desde cero, ya que es un proceso que puede agotar su presupuesto y retrasar mejoras significativas en materia de seguridad durante meses o incluso años.
- Si ya cuenta con un SOC propio, el servicio asume la carga del monitoreo 24/7, el triaje de alertas y la clasificación de incidentes, lo que libera a sus analistas para que se concentren en labores estratégicas de mayor valor.

Hasta 15 minutos

es lo que demora en activarse Kaspersky MDR

Hasta 2 años

es el tiempo que lleva crear operaciones internas de seguridad desde cero

70 %

de los equipos de seguridad tienen dificultades para procesar todas las alertas generadas por sus herramientas de seguridad



² Según nuestros informes anuales de los analistas de MDR

³ A portrait of the modern information security professional, 2024



Kaspersky Managed Detection and Response

Programe una
demostración

latam.kaspersky.com

© 2026 AO Kaspersky Lab.
Las marcas comerciales registradas y las marcas de
servicio pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture