kaspersky

Kaspersky
Managed Detection
and Response

Le ponemos fin a los incidentes antes de que lo hagan con tu negocio

Mejora la resiliencia de tu ciberseguridad con una protección administrada e ininterrumpida

Kaspersky Managed Detection and Response es un servicio liderado por expertos que ofrece supervisión, detección, investigación y respuesta rápida las 24 horas del día ante ciberataques sofisticados. De esta manera, aumentan los controles de seguridad existentes con detección liderada por personas e inteligencia global frente a amenazas. El servicio refuerza inmediatamente tu postura de seguridad de TI y TO, independientemente del tamaño o del sector de la organización.

Ventajas clave

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

Un SOC listo para usar de manera ininterrumpida con un equipo global de expertos, lo que elimina la necesidad de crear, dotar de personal y mantener tus operaciones de seguridad internas.

Una reducción en la carga de trabajo del equipo de seguridad interno, ya que nos delegas la supervisión, la evaluación y la investigación.

Seguridad basada en resultados que combina la experiencia humana, la inteligencia frente a amenazas y la IA para detener los incidentes antes de que puedan afectar a tu negocio.

El trabajo remoto, el rápido crecimiento del intercambio de información digital, la creciente disparidad de habilidades globales y la creciente cantidad de ciberamenazas capaces de eludir los controles automatizados tradicionales están ejerciendo una enorme presión sobre las organizaciones de todos los tamaños. En este entorno, es fundamental responder de forma rápida y eficaz a cada incidente.

Una descripción general de las ciberamenazas actuales[1]

1 Vectores iniciales de ataque

31 % de cuentas válidas

13 % relación de confianza

39 % de un exploit de una aplicación pública

2 Explora y completa tareas

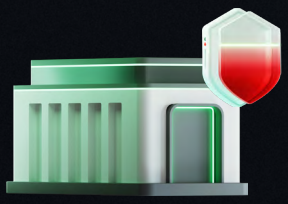
Los atacantes suelen utilizar herramientas legítimas (como Mimikatz, PsExec o SoftPerfect Network Scanner) en infraestructuras que carecen de controles adecuados en la configuración del sistema.

3 Impacto

42 % archivos cifrados

17 % filtración de datos

11 % en persistencia instalada para impactos en el futuro



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

Duración del ataque

Rápido	Media	Largo plazo
45 %	20 %	35 %
Hasta 1 día	13 días	253 días

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

GTO Grandeza de México

Daniel Huerta Santos
Gerente de Ciberseguridad, Gobierno del estado de Guanajuato

Más información

1 Informe Kaspersky MDR e Incident Response

Lo que ofrece Kaspersky MDR

Protección continua contra amenazas avanzadas desde el primer día

Kaspersky MDR se activa en cuestión de minutos sin necesidad de infraestructura adicional, utilizando nuestros analistas del SOC e inteligencia frente a 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 principales y una corrección completa y rápida. De este modo, se garantiza una protección contra amenazas conocidas y de día cero desde el primer día.

Operaciones de seguridad lideradas por expertos y mejoradas con inteligencia

Con Kaspersky MDR, tus operaciones de seguridad son administradas por expertos globales con una amplia experiencia en la primera línea y certificaciones líderes del sector. Su trabajo se intensifica con la Inteligencia frente a amenazas líder en el mercado y los mecanismos de IA integrados en el servicio, lo que ayuda a enriquecer cada alerta, acelerar la detección y reducir el Tiempo medio de respuesta (MTTR).

Eficiencia operativa y previsibilidad de costes

- Kaspersky MDR elimina la complejidad y el coste que supone crear un SOC interno desde cero, ya que es un proceso que puede agotar tu presupuesto y retrasar mejoras significativas en materia de seguridad durante meses o incluso años.
- Si ya tienes tu propio SOC, el servicio se encarga de la supervisión ininterrumpida, la evaluación de alertas y la clasificación de incidentes, lo que libera a tus analistas para que puedan concentrarse en tareas estratégicas de mayor valor.

Casos de uso

- Protección preconfigurada e ininterrumpida para las organizaciones que no tienen operaciones de seguridad
- Administración compartida de las operaciones de seguridad para reforzar los equipos internos de ciberseguridad
- Protección avanzada para la infraestructura de TO
- Protección continua específica para los sistemas integrados

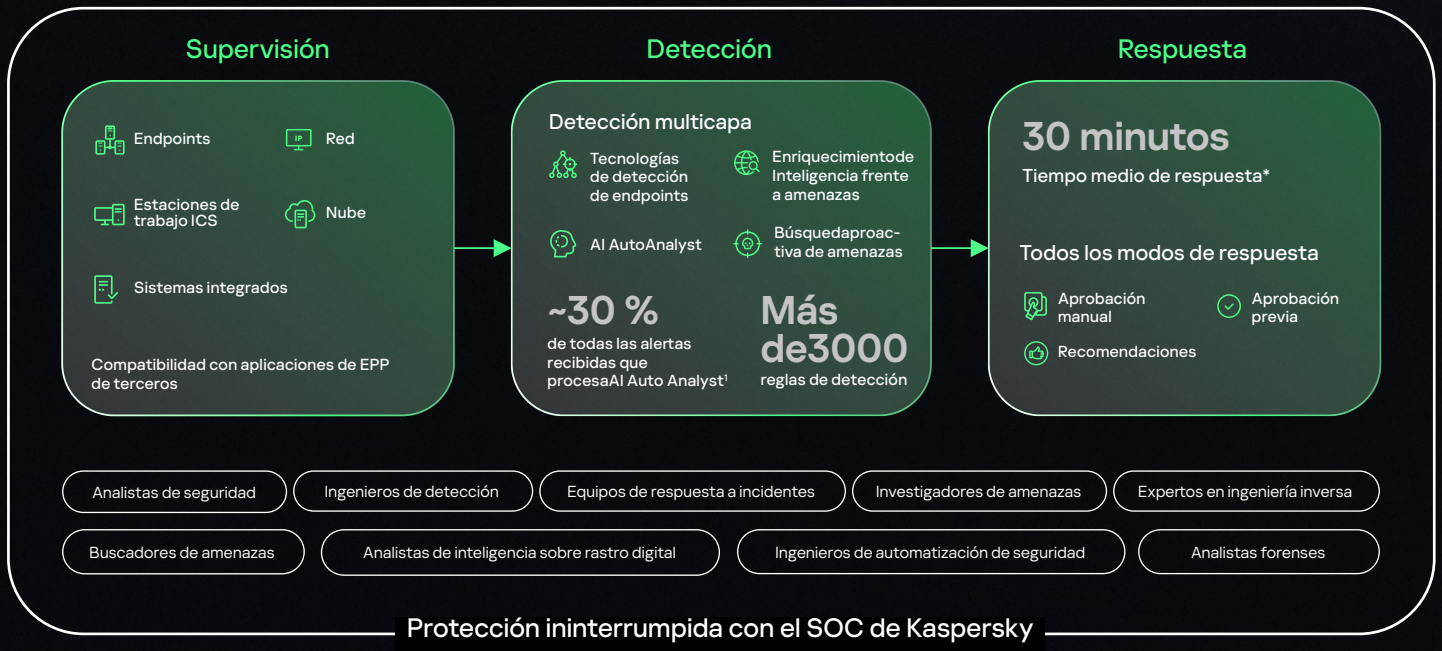
30 minutos
ese es nuestro MTTR promedio[2]

30 %
de todas las alertas recibidas que procesa AI Auto Analyst[1]

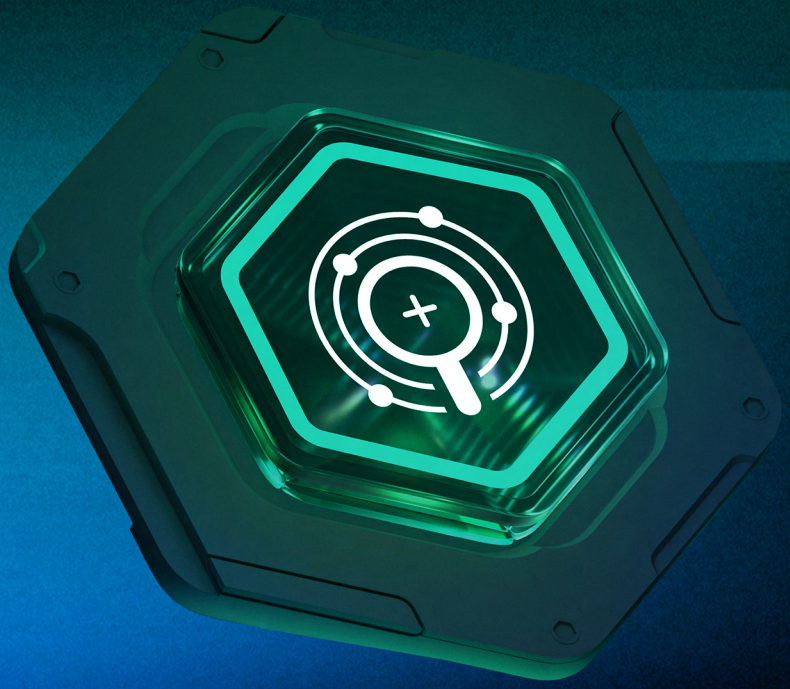
Hasta 15 minutos
es lo que demora en activarse Kaspersky MDR

Hasta 2 años
es el tiempo que lleva crear operaciones internas de seguridad desde cero

70 %
de los equipos de seguridad tienen dificultades para seguir el ritmo de la cantidad de alertas generadas por sus herramientas de seguridad[3]



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

Programa una demostración

www.kaspersky.com

#kaspersky
#bringonthefuture