

## EDR

### Detección y respuesta en endpoints

Identifica las amenazas nuevas, desconocidas y evasivas que eluden la protección de los endpoints, y automatiza las tareas de seguridad de rutina

## MDR

### Detección y respuesta gestionadas

Ofrece una protección administrada continua, incluso contra las amenazas sin malware más complejas e innovadoras

## XDR

### Detección y respuesta gestionadas

Detecta de forma proactiva amenazas complejas en varios niveles de la infraestructura y responde y contrarresta automáticamente estas amenazas

## Funcionamiento

- Permite la detección avanzada y la búsqueda de amenazas que evaden los mecanismos de prevención
- Mejora la visibilidad y la visualización de las amenazas
- Simplifica el análisis de la causa raíz
- Ofrece una respuesta centralizada y automatizada

- Recopila la telemetría de los productos de seguridad, analiza de forma proactiva los metadatos de la actividad del sistema en busca de cualquier indicio de un ataque activo o inminente, y brinda una respuesta administrada o guiada

- Integra varias herramientas y aplicaciones de seguridad
- Supervisa los datos de los endpoints, las redes, las nubes, los servidores web, los servidores de correo, etc. para detectar y eliminar amenazas complejas
- Simplifica la administración de la seguridad de la información, al automatizar la interacción entre productos

## ¿A quién va dirigido?

- Empresas con un equipo interno de seguridad de la información que necesitan una visibilidad detallada de los endpoints y una respuesta centralizada para reducir las tareas de manipulación manual

- Empresas que buscan ampliar la capacidad interna de seguridad de la información, al librarse de tareas clave de detección y respuesta
- Organizaciones que podrían no tener el presupuesto o el personal especializado disponible para crear su propio SOC interno

Organizaciones experimentadas en materia de seguridad que desean una plataforma única que ofrezca lo siguiente:

- Una imagen coherente de lo que ocurre en toda la infraestructura
- Búsqueda de amenazas e inteligencia de amenazas integradas
- Priorización de incidentes superior y menos alertas de falsos positivos

## Valor empresarial

- Le proporciona al personal de seguridad la visibilidad y el control unificados necesarios para buscar activamente amenazas en lugar de esperar alertas
- Maximiza las capacidades de los equipos de seguridad de la información existentes, al automatizar una serie de procesos de análisis, investigación y respuesta
- Impulsa la rentabilidad, al permitir que los equipos de seguridad de TI trabajen con mayor eficacia y sin tener que hacer malabares con diversas herramientas y consolas

- Resuelve la crisis de talento en ciberseguridad, lo que garantiza una protección instantánea contra amenazas complejas
- Permite externalizar procesos de administración de incidentes para poder orientar mejor los recursos internos, que son limitados y costosos, a los resultados decisivos que se obtienen
- Reduce los costos de seguridad generales sin la necesidad de implementar soluciones de seguridad complejas ni de emplear una amplia gama de especialistas en seguridad internos

- Proporciona una protección integral contra el panorama cambiante de amenazas
- El enfoque del ecosistema maximiza la eficiencia de las herramientas de ciberseguridad utilizadas, ahorra recursos y reduce los riesgos
- Simplifica el trabajo de los especialistas en seguridad de TI y les proporciona el contexto adicional necesario para investigar los ataques multivectoriales
- Minimiza el tiempo medio de detección (MTTD) y tiempo medio de respuesta (MTTR), fundamentales para combatir las amenazas complejas y los ataques dirigidos
- Permite una respuesta centralizada y automatizada en la pila completa de tecnología de seguridad

Si tu organización tiene experiencia en materia de seguridad y desea beneficiarse de las capacidades de la solución XDR, echa un vistazo a



Kaspersky  
Expert  
Security

Más información [↗](#)