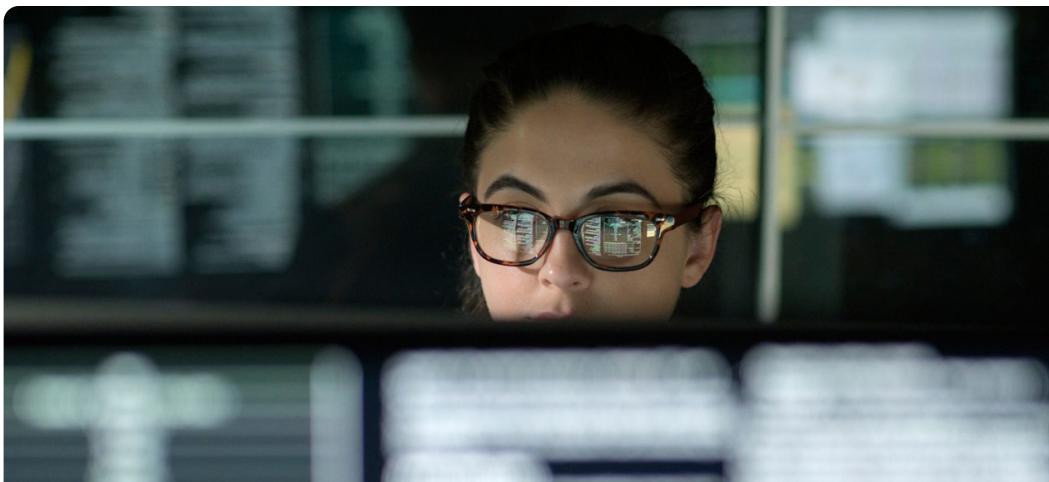


# Prevención y respuesta ante amenazas avanzadas en todo el entorno informático



## Managed Detection and Response Pro

### Combinamos la gestión de vulnerabilidades con la detección y respuesta gestionadas en una sola solución para ayudarle a proteger el entorno de TI

En 2022, el coste medio de una vulneración de datos fue de 4,35 millones de dólares.<sup>1</sup> De hecho, en 2021 se publicaron casi 22 000 vulnerabilidades nuevas, un número que no hace más que crecer.<sup>2</sup> Las organizaciones deben encontrar una forma de proteger su entorno ante la creciente cantidad de amenazas a la seguridad y las implicaciones asociadas a las vulneraciones.

A fin de proteger el entorno de TI, es preciso abordar las vulnerabilidades, investigando las amenazas y respondiendo de forma eficaz. Las organizaciones también se enfrentan al desafío de encontrar y retener profesionales de seguridad cualificados, y las organizaciones de TI se ven abrumadas por las exigencias críticas de las operaciones empresariales diarias.

Por eso hemos diseñado Managed Detection and Response Pro. MDR Pro es una solución totalmente gestionada que ofrece funciones de identificación y priorización de vulnerabilidades, así como detección y respuesta ante amenazas ininterrumpida. Nuestros expertos colaboran con su equipo de seguridad interno para proteger su entorno de TI, mejorar incesantemente el estado de seguridad y ayudarle a estar preparado de forma continua.

### Identifique vulneraciones y establezca prioridades en toda la superficie de ataque

Los expertos de Dell utilizan tecnología líder para analizar su entorno de TI periódicamente, lo que le proporciona una vista completa de las vulnerabilidades en los puntos finales, la infraestructura de red y los recursos de cloud. Nuestros expertos aplican prestaciones de aprendizaje automático para detectar vulnerabilidades de las que se esté abusando activamente en todo tipo de entornos, ya que es más probable que sean objeto de ataque a corto plazo. De este modo, puede priorizar la aplicación de parches en las vulnerabilidades con más riesgo y los recursos esenciales.

Identifique vulneraciones y establezca prioridades para prestarles atención inmediata

### Principales beneficios:

- Mantiene las defensas actualizadas gracias a funciones periódicas de análisis y gestión de las vulneraciones.
- Ofrece una imagen completa de las vulneraciones en los puntos finales, la infraestructura de red y la cloud.
- Prioriza las vulnerabilidades críticas para solucionarlas antes de que puedan aprovecharse de ellas.
- Unifica la detección y respuesta en todo el ecosistema.
- Detecta nuevos tipos de ataque mediante una base de datos sobre las amenazas que se actualiza incesantemente.
- Correlaciona los eventos y efectúa un seguimiento de toda la actividad del atacante.
- Aprovecha los conocimientos expertos del equipo de seguridad de Dell.

## Detecte a los atacantes y responda antes de que causen daños

Managed Detection and Response es un servicio completamente gestionado, integral e ininterrumpido que supervisa, detecta e investiga amenazas en todo el entorno de TI y responde ante estas. Las organizaciones con 50 puntos finales o más pueden mejorar significativamente el estado de seguridad, así como reducir la carga del equipo de TI.

El servicio utiliza dos capacidades clave:

- Los conocimientos de los analistas de seguridad de Dell Technologies, adquiridos a lo largo de años de experiencia ayudando a las organizaciones de todo el mundo a proteger mejor sus empresas.
- El software de análisis de seguridad avanzado XDR, creado con base en más de 20 años de trabajo en operaciones de seguridad, investigación e inteligencia para la detección de amenazas obtenida de casos reales y experiencia en la detección y respuesta ante amenazas avanzadas.

### Funciones principales

#### Investigación y detección de amenazas

- Dell colabora con usted para conocer su entorno y ayudarle a implementar el agente de software en los puntos finales correspondientes sin cargos adicionales.
- Se aprovechan los datos sobre atacantes obtenidos al participar en más de 1400 respuestas a incidentes el pasado año.
- Se proporcionan instrucciones paso a paso para contener la amenaza incluso en situaciones complejas.
- Cada trimestre incluye hasta 40 horas de orientación para la corrección remota.
- Las 40 horas anuales de asistencia para la respuesta remota ante incidentes permiten que las labores de investigación comiencen rápidamente.

#### Identificación de vulnerabilidades y establecimiento de prioridades

- Se realizan análisis mensuales en busca de vulneraciones, con análisis adicionales según acuerden el equipo de Dell y el cliente.
- Se crea un inventario de recursos que se coteja con las bases de datos de vulneraciones conocidas, a fin de detectar puntos débiles y las actualizaciones necesarias.
- Se colabora con el cliente en lo referente a la priorización de las vulneraciones de mayor riesgo para gestionar la aplicación de parches y orientarle al respecto.
- Se llevan a cabo análisis con una plataforma avanzada basada en aprendizaje automático
- Se efectúan revisiones trimestrales para informar al cliente sobre las tendencias de las vulneraciones en su entorno y en el sector.

## Proteja su entorno con Dell hoy mismo

A medida que la frecuencia y el coste de las vulneraciones siguen en aumento, Managed Protection and Response Pro le ayudará a proteger su entorno de TI, así como sus recursos más importantes de los atacantes malintencionados, al tiempo que mejora el estado de seguridad de su organización.

Póngase en contacto con su representante de ventas hoy mismo.

<sup>1</sup> IBM. (2022). "Cost of a Data Breach Report 2022". Última consulta el 20 de septiembre de 2022. URL: <https://www.ibm.com/downloads/cas/3R8N1DZJ>.

<sup>2</sup> Tenable (2021). "Tenable's 2021 Threat Landscape Retrospective". Última consulta en agosto de 2022. URL: <https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective>.

Copyright © 2023 Dell Inc. o sus filiales. Todos los derechos reservados. Dell Technologies, Dell, EMC, Dell EMC y otras marcas comerciales son marcas comerciales de Dell Inc. o sus filiales. Otras marcas comerciales pueden pertenecer a sus respectivos propietarios. La disponibilidad y los términos de servicio varían según la región y el producto. March 2023-LC | Managed Detection and Response Pro