

Fortalezca su postura de seguridad con Managed Detection and Response



Detecte e investigue amenazas avanzadas y responda a estas en todo el entorno de TI

Dell Managed Detection and Response

Combinación de la experiencia en seguridad de Dell Technologies y un profundo conocimiento de los entornos de TI con la plataforma selecta de análisis de seguridad XDR líder en la industria de su elección.

¿Cuán segura es su empresa?

A los equipos de TI les resulta difícil mantenerse a la par del creciente volumen de amenazas de seguridad en constante evolución. En 2022, hubo 5500 millones de ataques de malware en todo el mundo, 100 millones más que en 2021.¹

La protección completa de su organización requiere una detección rápida y una respuesta eficaz a las nuevas amenazas en todo el entorno. Esto resulta difícil debido a productos y herramientas puntuales que fragmentan la visibilidad, los desafíos para encontrar y retener profesionales de seguridad calificados y los equipos de TI que ya están completamente ocupados con las demandas críticas y las operaciones diarias.

Detección y respuesta administradas ante amenazas

Dell Managed Detection and Response es un servicio 24x7 integral completamente administrado que monitorea, detecta e investiga amenazas y responde a estas en todo el entorno de TI, lo que ayuda a las organizaciones con 50 o más terminales a mejorar de manera rápida y considerable su postura de seguridad, así como a reducir la carga para el equipo de TI.

El servicio aprovecha dos funcionalidades clave:

- La experiencia de analistas de seguridad de Dell Technologies adquirida durante años de experiencia ayudando a organizaciones de todo el mundo a proteger mejor sus empresas.
- Plataformas de análisis de seguridad de detección y respuesta extendidas (XDR) líderes en la industria que incorporan análisis habilitados por IA de telemetría y eventos de múltiples vectores de ataque.

Beneficios clave:

- Detección y respuesta unificadas en todo el ecosistema
- La base de datos de amenazas actualizada continuamente mantiene la protección al día
- Posibilidad de detección incluso de las tácticas de los actores de amenazas más sigilosos
- Vista completa de la actividad integral de los atacantes
- Un equipo de profesionales de seguridad de Dell Technologies cuya experiencia incluye seguridad, infraestructura avanzada, nube y más
- Ayuda de expertos en la implementación del SaaS XDR nativo de la nube
- Inicio rápido de respuesta ante incidentes cibernéticos cuando ocurre una infracción
- Alineación continua con [el nivel más alto de cumplimiento de normas de seguridad para los proveedores de servicio](#)

Solución de servicio completo

Los analistas de seguridad de Dell Technologies ayudan con la configuración inicial, el monitoreo, la detección, la corrección y la respuesta, todo por un precio predecible. Trabajan en estrecha colaboración con su equipo de TI para comprender el entorno, asesorar sobre las mejoras en la postura de seguridad y ayudar a implementar el agente de software XDR en los terminales.

Las alertas se monitorean y revisan 24x7. Si una alerta amerita investigación, los analistas determinan y ejecutan la respuesta adecuada. Si una amenaza es maliciosa o requiere su acción, se le informará y, si es necesario, se le proporcionarán instrucciones paso a paso.

En caso de que se produzca un incidente de seguridad, Dell Technologies lo ayuda a iniciar el proceso para volver a poner en marcha su empresa.

Elija su plataforma XDR

Sus necesidades y preferencias de seguridad y tecnología son únicas. Le damos la flexibilidad de elegir entre tres opciones líderes en la industria: Secureworks® Taegis™ XDR, CrowdStrike Falcon® XDR o Microsoft Defender XDR para que pueda obtener una plataforma XDR que se adapte a sus necesidades.²

Características clave

Soporte de confianza

- Colaboración estrecha con usted para comprender su entorno, resolver investigaciones y asesorarle sobre mejoras en la postura de seguridad.
- Monitoreo 24x7 con la plataforma XDR seleccionada de su elección que incorpora análisis habilitados por IA de telemetría y eventos de múltiples vectores de ataque.
- Consejo de expertos para la implementación y configuración de la plataforma XDR.

Configuración de seguridad y respuesta ante amenazas

- Al utilizar las capacidades de XDR, el equipo de SOC de Dell puede automatizar la corrección o colaborar con usted para abordar las amenazas detectadas durante el monitoreo.
- Entrega de instrucciones detalladas y fáciles de entender para contener la amenaza incluso en situaciones complejas.
- Se incluyen hasta 40 horas de configuración de seguridad relacionada con el servicio por trimestre.

Detección e investigación 24x7

- Procesos y alertas adaptados al entorno de seguridad de su organización y automatizados para operaciones diarias eficientes.
- Búsqueda proactiva de amenazas específica para el entorno de cada cliente a fin de detectar nuevas amenazas o variaciones de amenazas conocidas que evaden los sistemas de seguridad.
- El resumen diario de alertas menos críticas permite que el equipo de SOC de Dell centre su atención en las alertas críticas.
- Informes trimestrales sobre investigaciones, análisis de tendencias de alertas y orientación sobre la postura de seguridad.

Inicio de respuesta ante incidentes cibernéticos

- 40 horas anuales de asistencia remota de respuesta ante incidentes permiten que las actividades de investigación comiencen rápidamente.
- Orientación de nuestros expertos en seguridad certificados que han ayudado a organizaciones de todos los tamaños a recuperarse de eventos de seguridad graves.

Comience a proteger su entorno hoy con Dell

Dado que el costo total promedio de una infracción de ransomware alcanza los US\$5,13 millones, un 13 % más que en 2022, ahora es el momento de obtener más información sobre si el servicio Dell Managed Detection and Response es adecuado para usted.³

Comuníquese hoy mismo con el representante de ventas.

1. Statista, [Annual number of malware attacks worldwide from 2015 to 2022](#)

2. Se requiere un mínimo de 500 terminales para usar Microsoft Defender XDR

3. IBM, [Cost of a Data Breach Report 2023](#)