Kaspersky Next EDR Optimum

Lleve sus defensas de endpoint al siguiente nivel y enfrente a las amenazas evasivas

kaspersky

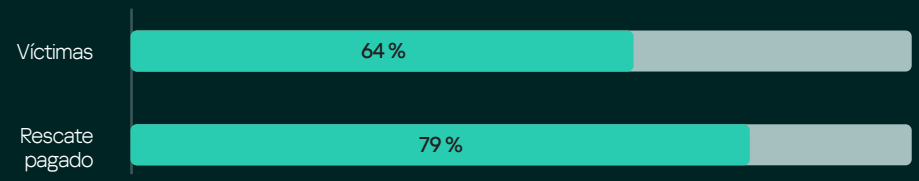
Kaspersky Next EDR Optimum

El 64 % de las organizaciones ya fueron víctimas de ataques de ransomware.

El 79 % de ellas pagaron el rescate a sus atacantes.

How business executives perceive ransomware threats, Kaspersky, mayo de 2022

Es momento de subir de nivel. Identifique, analice y neutralice las amenazas diseñadas para eludir las protecciones tradicionales.



Los desafíos:

Amenazas que evaden detecciones

El malware, ransomware, spyware y otras amenazas son cada vez más inteligentes a la hora de evitar la detección tradicional, ya que usan herramientas de sistemas legítimos y otras técnicas avanzadas en sus ataques.

Ransomware como servicio

Los hackers de hoy pueden adquirir herramientas listas para usar y atacar a cualquier objetivo: robar datos, hacerle daño a la infraestructura y exigir cantidades cada vez más imporantes de rescates.

Recursos limitados

Ahora las infraestructuras son más complejas y diversas, mientras que los recursos (tiempo, dinero y personal) son cada vez menos. Es la combinación perecta para desperdiciar los costosos programas informáticos.

"Apreciamos las soluciones integrales de Kaspersky, su confabilidad y su servicio y asistencia rápidos. Garantizan que nuestro entorno de TI esté disponible".

Marcelo Mendes CISO, NEO

leer caso práctico

Cómo podemos ayudar

Kaspersky Next es nuestra línea de productos estrella, diseñada para brindarle ayuda para que disfrute de una mejor seguridad, sin inconvenientes. No impora si busca funcionalidades de EDR esencial o está planifcando adoptar XDR en el futuro, la protección robusta, nativa de nube y adaptable de Kaspersky Next, con el respaldo de un historial de ciberseguridad sin igual, está a tan solo unos clics de distancia.

Kaspersky Next EDR Optimum le permite identifcar, analizar y neutralizar las amenazas evasivas gracias a que facilita las funcionalidades de detección avanzada fácil de usar, investigación simplifcada y respuesta automática.

Protección avanzada

Nuestros mecanismos de detección avanzada incluyen análisis del comporamiento y aprendizaje automático.

Todo se combina con herramientas simples de análisis visual y acciones de respuesta rápida para que pueda comprender en su totalidad la amenaza y su alcance, y detenerla antes de que se produzca cualquier daño.

Se reduce la supericie de ataque en el lado del endpoint y en la nube con funciones de descubrimiento y bloqueo de nube, y con la seguridad para MS Ofice 365.

Una solución

La seguridad de endpoints avanzada se integra a un producto EDR simple para una mayor protección de computadoras porátiles, estaciones de trabajo, servidores, cargas de trabajo en la nube y entornos viruales.

Solo se requiere una única consola para la implementación y la administración: en la nube o local.

Simple y efciente

Desarrollamos Kaspersky Next EDR Optimum pensando en pequeños equipos de ciberseguridad, como aquellos que buscan mejorar sus capacidades de respuesta ante incidentes y desarrollar habilidades, pero no cuentan con mucho tiempo.

Automatizamos y optimizamos la mayoría de las tareas para que solo inviera su tiempo en lo imporante. Además, brindamos la capacitación que usted y su equipo de TI necesitan para aprovechar al máximo sus nuevas capacidades de seguridad.

Ahora es posible:

- **Evitar ciberamenazas** con anticipación
- **Proteger sus sistemas** y datos de amenazas evasivas
- **Descubrir amenazas actuales** antes de que actúen
- **Reconocer amenazas evasivas** en todos los endpoints
- **Comprender la amenaza** y analizarla con rapidez
- **Evitar daños** con una respuesta automática rápida
- **Ahorrar tiempo y recursos** con una herramienta simple
- **Defender cada endpoint:** computadoras porátiles, servidores, cargas de trabajo de nube
- **Trabaje con una consola con Vista pro** o Vista de expero: ¡Usted elige!

Ahora tiene lo siguiente:

- **Seguridad de endpoints de última generación**
- **Funciones de detección avanzada** basada en el aprendizaje automático
- **Análisis de indicadores de compromiso** (IoC)
- **Herramientas de investigación** y análisis visuales
- Todos los datos necesarios en una **única tarjeta de alera**
- **Guía de respuestas** y automatización incorporadas
- **Consola única local o en la nube** y automatización
- Compatibilidad con todas las estaciones de trabajo, **servidores viruales y físicos, implementaciones VDI y cargas de trabajo en nubes públicas**
- **Personal de Seguridad informática** completamente capacitado

Reciba las respuestas a sus preguntas, cuando más impora

¿Me están atacando?

- **Aplique la detección avanzada** basada en el aprendizaje automático
- **Descargue y analice IoC** desde securelist.com u otras fuentes para encontrar amenazas avanzadas

¿Cómo sucedió?

- Analice la amenaza **en un árbol de procesamiento visual**
- Descubra sus acciones **en un gráfco con desgloses**
- **Comprenda la causa raíz** y descubra el punto de entrada a la infraestructura

¿Cómo puedo neutralizar la amenaza?

- **Emplee diversas opciones de respuesta:** aísle el host, impida la ejecución del archivo o elimine el archivo
- **Analice otros hosts** en busca de indicios de la amenaza analizada
- **Aplique respuestas automáticas** en hosts sobre el descubrimiento de amenazas (IoC)

¿Qué sucede con las demás amenazas?

- **La seguridad de endpoints avanzada** está preparada para detener la mayoría de las amenazas de inmediato
- **Reduzca su supericie de ataque de forma automática** y ajuste sus directivas
- **Controle las aplicaciones y los dispositivos** que sus usuarios pueden emplear

¿Cómo encuentro el tiempo para todo esto?

- **Automatice la administración de vulnerabilidades y parches**: la forma clave de proteger sus endpoints
- **Administre el cifrado nativo** de forma remota de todos los empleados para proteger los datos corporativos
- **Automatice las tareas de administración** de TI y de seguridad que insumen mucho tiempo

¿Cómo lo evito en el futuro?

- **Aplique la información que aprendió**: sepa qué direcciones IP y sitios web debe bloquear, qué directivas debe modifcar y a qué empleados debe capacitar
- **Redacte reglas para evitar** dichas amenazas en el futuro
- **Proteja su nube: descubra, restrinja y bloquee accesos** a recursos en la nube, servicios, mensajería instantánea no autorizados, entre otros
- **Obtenga visibilidad y control** sobre MS SharePoint Online, OneDrive y Teams

¿Cómo puedo mejorar?

- **Use nuestra guía de respuestas** en la tarjeta de alera
- **Acceda a Threat Intelligence Poral** y conozca las novedades de inteligencia de amenazas
- **Mejore su experiencia** analizando amenazas y respondiendo a ellas
- **Benefíciese de las capacitaciones** y cerifcaciones integradas, con tareas interactivas en un entorno simulado

Construya sus defensas
Impulse la seguridad con una investigación y respuesta esencial

Si necesita
- Capacidades mejoradas de visibilidad y respuesta
- Seguridad ampliada en la nube
- Controles de clase empresarial

[1] Indicador de compromiso

Kaspersky Next: Su seguridad a prueba del futuro

Kaspersky Next EDR Optimum forma pare de nuestra gama de productos de Kaspersky Next y ofrece controles y una sólida protección de endpoints, con la transparencia y la velocidad de EDR, y la visibilidad integral y el conjunto de potentes herramientas de XDR, en tres simple niveles de productos, según sus necesidades de ciberseguridad más apremiantes. A medida que sus necesidades crezcan, será fácil cambiar de uno a otro y actualizar con agilidad la función de seguridad.

Protecting your IT infrastructure everyday.

ventas@antivirus-mexico.com
55 6390 0121, 55 6385 1112
55 8100 4594
antivirus-mexico.com