



Kaspersky Next
EDR Optimum

Unpacking Kaspersky Next EDR Optimum



¿Qué es Kaspersky Next EDR Optimum?

Kaspersky Next EDR Optimum proporciona una sólida protección de endpoints, controles mejorados, capacitaciones, administración de parches y más, todo mejorado con la funcionalidad esencial de EDR.

La visibilidad, investigación y respuesta a las amenazas son sencillas, rápidas y guiadas, para ayudar a los equipos de TI y de seguridad informática a desviar los ataques rápidamente y con recursos mínimos.



¿Por qué Kaspersky Next EDR Optimum, y por qué ahora?

La evolución del panorama de las amenazas hace que la EDR sea un requisito, no una opción.

Durante muchos años, las pequeñas y medianas empresas (pymes) y organizaciones de nivel inferior lograron depender de las EPP para defenderse de una amplia gama de amenazas básicas. Pero los atacantes de hoy en día ponen sus energías en organizaciones de todos los tamaños, industrias y niveles de preparación, y están montando ataques más peligrosos.

Esta evolución del entorno de amenazas significa que, con el tiempo, las amenazas cada vez más sofisticadas y que antes solo afectaban a las organizaciones de mayor tamaño ahora están apuntando a pymes y empresas más pequeñas, que no poseen los recursos internos necesarios para enfrentarlas de manera efectiva.

En particular, la llegada de las amenazas evasivas (que utilizan herramientas legítimas para los ataques, incluyen escenarios listos para eludir EPP, son económicas y están disponibles en la red oscura) han aumentado de manera significativa los riesgos de ciberseguridad para las organizaciones que utilizan soluciones de EPP tradicionales.

Si solo acostumbras a necesitar EPP, mejorar tus defensas con la detección y respuesta de endpoints (EDR) puede parecer un gran paso adelante en cuanto a las herramientas y habilidades necesarias. Pero, por suerte, no tiene por qué serlo.

Agregar las capacidades apropiadas de EDR al EPP moderno puede proporcionar una defensa altamente eficaz contra amenazas más avanzadas y evasivas

Tu empresa sufre un ciberataque, ¿cómo reaccionarás?

Es tu primer día en un puesto nuevo de seguridad informática. Apenas comienzas a trabajar, todo indica que la empresa está bajo ataque.

¿Qué harías? ¿Cómo reaccionarías?

Más información

<https://www.kaspersky.com/response-game/es-la/>

Actualizar a EDR no tiene por qué ser un reto

Muchas organizaciones tienen tiempo y recursos limitados (o un departamento de seguridad de IT pequeño y no tienen planes de ampliarlo), pero deben comprender lo que sucede en su infraestructura y ser capaces de responder a amenazas evasivas antes de que se produzca el daño.

Agregar las capacidades apropiadas de EDR al EPP moderno puede proporcionar una defensa altamente eficaz contra amenazas más avanzadas y evasivas. Por lo tanto, si eres nuevo en EDR, debes buscar una solución que permita respuestas automatizadas y/o rápidas y precisas con un solo clic, como la cuarentena de archivos, el aislamiento del host, la detención de un proceso, la eliminación de un objeto, etc.

A medida que adquieras más destreza —o si ya cuentas con especialistas en seguridad informática y/o EDR—, tu solución también debe proporcionar la información, los conocimientos y las herramientas necesarias para una investigación eficaz, como el análisis de la causa raíz, la creación de indicadores de compromiso (IoC) personalizados, la importación de IoC y su búsqueda en todos los endpoints.

Entre los resultados que puedes esperar de la EDR se incluyen los siguientes:

- Protección robusta contra las amenazas evasivas más frecuentes y que más interrupciones generan.
- Ahorro de tiempo y recursos con una herramienta sencilla y automatizada.
- Evaluar el alcance de un ataque mediante la búsqueda de IoC en todos los endpoints.
- Comprensión de la causa raíz de cada amenaza y cómo ocurrió realmente.
- Elusión de daños adicionales con una respuesta automática rápida.

Por lo tanto, si tu EPP no logra detener el número cada vez mayor de amenazas nuevas, desconocidas y evasivas; tienes una visibilidad limitada sobre lo que ocurre en los endpoints, o bien te preocupan las multas potenciales o la amenaza a la reputación de tu empresa, en caso de que ocurra un incidente de seguridad grave, una solución de EDR moderna como Kaspersky Next EDR Optimum es la forma ideal de comenzar tu camino de EDR.

Cómo puede ayudar Kaspersky Next EDR Optimum



Qué hace

Proporciona una protección sólida de endpoints, controles superiores, formación, administración de parches y más

La funcionalidad esencial de EDR incluye una clara visibilidad de las amenazas, una investigación sencilla y una respuesta guiada y directa, para desviar rápidamente los ataques con un mínimo de recursos



Funcionamiento

Mejora la visibilidad y la visualización de las amenazas

Simplifica el análisis de la causa raíz

Ofrece una respuesta rápida y automatizada

Consola en la nube o en las instalaciones



Valor empresarial

Protege tu empresa de peligrosas amenazas evasivas y mejora tu estrategia de ciberseguridad con una única solución

Permite que los equipos de TI o seguridad de TI trabajen con mayor eficacia y sin tener que hacer malabares con diversas herramientas y consolas

Automatiza una amplia gama de procesos para evitar la dependencia de los procesos de corrección tradicionales que podrían provocar tiempos de inactividad

Facilita la supervisión, detección e investigación de amenazas, así como la respuesta y prevención de ataques



¿A quién va dirigido?

Empresas con un equipo interno de seguridad informática (o solo de 1 a 3 especialistas en seguridad) que necesitan una visibilidad detallada de los endpoints y una respuesta automatizada para reducir las tareas de manipulación manual

¿Qué obtienes?



Protección de endpoints

antivirus para archivos, la Web y correos, protección de red, prevención de exploits, corrección, detección de comportamiento, HIPS, AMSI, anticifrado, prevención de ataques de BadUSB



Gestión de la seguridad

Firewall, controles web, de dispositivos y de aplicaciones, control adaptativo de anomalías, control de integridad de archivos, inspección de registros, control de integridad del sistema



Protección y gestión de dispositivos móviles

Protección, controles y administración, iOS MDM



Escenarios de TI

Evaluación de vulnerabilidades, administración de parches, eliminación de datos, inventario de software/hardware, instalación de sistemas operativos y aplicaciones de terceros, conexión remota



Cifrado

Cifrado y administración del cifrado



Protección en la nube

Descubrimiento y bloqueo de la nube, detección de datos, seguridad para MS O365



Educativo

Formación en ciberseguridad para administradores de TI



Capacidades de EDR

Análisis de causas raíz, análisis de IoC, respuesta automatizada y con un solo clic, guía de respuestas

Kaspersky Next EDR Optimum ayuda a las organizaciones a aumentar su seguridad al ritmo de sus entornos informáticos

¿Qué sucede si ya estás usando seguridad de Kaspersky?

A medida que las empresas se desarrollan y sus requisitos informáticos aumentan en complejidad, sus necesidades de seguridad crecen y se diversifican. Kaspersky Next EDR Optimum ayuda a las organizaciones a aumentar su madurez de seguridad en sintonía con sus entornos de TI al empezar a desarrollar procesos y experiencia en respuesta ante incidentes, así como a contrarrestar las amenazas avanzadas que tienen una superficie de ataque ampliada. Esto permite detectar, analizar y abordar los ataques de forma rápida y automática, reduciendo significativamente su impacto.

Tu solución de Kaspersky



Kaspersky
Endpoint Security
Cloud
Pro



Kaspersky
Endpoint Security
for Business
Advanced



Kaspersky
Total Security
for Business



Kaspersky
Endpoint Detection
and Response
Optimum

Migración recomendada



Kaspersky Next
EDR Optimum



Kaspersky Next
EDR Optimum



Kaspersky Next
EDR Optimum

Capacidades adicionales que obtendrás

- Monitor de integridad de archivos
- Inspección de registros
- Supervisión de la integridad del sistema
- Inventario de software/hardware
- Instalación de aplicaciones de terceros
- Instalación del sistema operativo en las instalaciones
- Posibilidad de utilizar la consola de empresa en las instalaciones o en la nube (vista de experto)
- Opción de consola sencilla en la nube
- Funciones esenciales de EDR, incluido el análisis de la causa raíz, la exploración de IoC y la respuesta automatizada
- Formación en ciberseguridad para administradores de TI
- Detección y bloqueo de servicios en la nube
- Data Discovery
- Seguridad de MS Office 365
- Opción de consola sencilla en la nube
- Formación en ciberseguridad para administradores de TI
- Detección y bloqueo de servicios en la nube
- Data Discovery
- Seguridad de MS Office 365

Más información sobre [Kaspersky Next EDR Optimum](#)



Kaspersky Next
EDR Optimum



Kaspersky Next
EDR Foundations

Más información



Kaspersky Next
XDR Expert

Más información

Noticias sobre amenazas online: securelist.lat
Noticias sobre seguridad de IT: business.kaspersky.com
Seguridad de TI para PYMES: kaspersky.com/business
Seguridad de TI para grandes empresas: kaspersky.com/enterprise

kaspersky.es

© 2024 AO Kaspersky Lab.
Las marcas comerciales y marcas de servicios registradas pertenecen a sus respectivos propietarios.

Obtén más información acerca de Kaspersky Next en:
<https://go.kaspersky.com/next>

Elige el nivel que más te convenga respondiendo a una breve encuesta en nuestra herramienta interactiva:
https://go.kaspersky.com/Kaspersky_Next_Tool

