Kaspersky Next
EDR Optimum

Revelando 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 de las amenazas, su investigación y respuesta son simples, rápidas y guiadas para ayudar a los equipos de seguridad TI a desviar los ataques rápidamente y con recursos mínimos.

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

El entorno de amenazas en evolución hace que EDR no sea una opción, sino un requisito.

Durante muchos años, las pequeñas y medianas empresas (pymes) y organizaciones de nivel inferior podían depender de las plataformas de protección de endpoints (EPP) para defenderse de una amplia gama de amenazas básicas, producidas en masa y con un bajo nivel de esfuerzo. Pero los atacantes de hoy en día ponen sus energías en organizaciones de todos los tamaños, industrias y niveles de preparación, y llevan a cabo 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.

Las amenazas evasivas, que emplean herramientas legítimas para ataques y están diseñadas para evadir las soluciones EPP tradicionales, se han vuelto más comunes y accesibles económicamente a través de la red oscura. Esto ha incrementado significativamente los riesgos de ciberseguridad para las organizaciones que dependen de soluciones EPP convencionales.

Si se acostumbró a necesitar solo una EPP, aumentar sus defensas con detección y respuesta en endpoints (EDR) puede parecer un cambio significativo en términos de las herramientas y capacidades necesarias. Por suerte, esto no tiene que ser así.

Agregar las funciones apropiadas de EDR a EPP modernas puede proporcionar una defensa altamente eficaz contra amenazas evasivas más avanzadas

Su empresa está bajo ataque, ¿cómo reaccionaría?

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

¿Qué haría? ¿Cómo reaccionaría?

Más información en www.kaspersky.com/response-game

Adoptar EDR no tiene que ser un desafío

Muchas organizaciones tienen tiempo y recursos limitados (o un departamento de seguridad de TI pequeño sin planes de ampliarse), pero deben comprender lo que sucede en la infraestructura y ser capaces de responder a las amenazas evasivas antes de que se produzca el daño.

Agregar las funciones apropiadas de EDR a EPP modernas puede proporcionar una defensa altamente eficaz contra amenazas evasivas más avanzadas. Si aún no adoptó EDR, debería buscar una solución que ofrezca respuestas automatizadas o rápidas, de un solo clic y precisas, por ejemplo, para la cuarentena de archivos, el aislamiento de hosts, la interrupción de procesos, la eliminación de un objeto, etc.

A medida que aprende a usarla mejor (o si ya cuenta con EDR o especialistas de seguridad en TI), la solución debería ofrecer información, conocimientos y herramientas necesarias para la investigación efectiva, como análisis de causas raíz, creación de indicadores de compromiso (IoC) personalizados, importación de IoC y análisis de estos en todos los endpoints.

De esta manera, los resultados que puede esperar de EDR incluyen los siguientes:

- Protección robusta contra amenazas evasivas más frecuentes y disruptivas.
- Ahorro de tiempo y recursos con una herramienta simple y automatizada.
- Evaluación del alcance de un ataque mediante el análisis de todos los endpoints en busca de IoC.
- Comprensión de la causa raíz de cada amenaza y cómo ocurrió realmente.
- Rápida respuesta automatizada para evitar más daños.

Por lo tanto, si su EPP no puede detener el creciente número de amenazas nuevas, desconocidas y evasivas, si tiene una visibilidad limitada sobre lo que ocurre en los endpoints, o si le preocupa las multas potenciales y la pérdida de reputación de su empresa en caso de un incidente de seguridad grave, una solución de EDR moderna como Kaspersky Next EDR Optimum le ofrece una opción ideal para dar sus primeros pasos o avanzar en el camino del EDR.

¿Cómo puede ayudar Kaspersky Next EDR?

Lo que hace

Ofrece una protección avanzada de endpoints, controles superiores, capacitaciones, administración de parches y más

La funcionalidad de EDR esencial incluye una visibilidad clara de las amenazas, investigación simple y respuesta guiada y sin complicaciones, para desviar ataques de manera rápida y con recursos mínimos

Funcionamiento

Mejora la visibilidad y la visualización de las amenazas

Simplifica el análisis de la causa raíz

Ofrece una respuesta rápida y automatizada

Consola local o en la nube

Valor comercial

Protege a su empresa de amenazas evasivas peligrosas y mejora su posición de ciberseguridad con una solución única

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

Automatiza una amplia gama de procesos para evitar la dependencia en procesos de corrección tradicionales que pueden resultar en tiempos de inactividad

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

¿Para 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 obtiene?

Protección de endpoints

Antivirus web, de archivos y de correo, protección de red, detección de comportamiento, corrección, prevención de exploits, HIPS, AMSI, protección contra cifradores, prevención de ataques BadUSB

Gestión de la seguridad

Controles web, de aplicaciones, de dispositivos y de firewall, control de anomalías adaptable, monitor de integridad de archivos, inspección de registros, monitor de integridad del sistema

Protección y administración de dispositivos móviles

Protección, controles y administración, MDM (administración de dispositivos móviles) iOS

Escenarios 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 de nube

Cloud Discovery y Cloud Blocking, Data Discovery, seguridad para MS O365

Educación

Capacitación en ciberseguridad para administradores de TI

Capacidades de EDR

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

Kaspersky Next EDR Optimum ayuda a las organizaciones a desarrollar su seguridad junto con sus entornos de TI

¿Qué sucede si ya estoy usando Kaspersky?

A medida que las empresas se desarrollan y sus requisitos de TI aumentan en nivel de complejidad, las necesidades de seguridad también crecen y se diversifican. Kaspersky Next EDR Optimum ayuda a las organizaciones a aumentar su seguridad en sintonía con sus entornos de TI al empezar a desarrollar procesos y experiencia en respuesta ante incidentes, y contrarrestar las amenazas avanzadas que tienen una superficie de ataque ampliada. Esto permite que los ataques se detecten, analicen y enfrenten de manera rápida y automática, lo que reduce su impacto de forma significativa.

Su solución Kaspersky	Migración recomendada	Capacidades adicionales que obtendrá
Kaspersky Endpoint Security Cloud Pro	**Kaspersky Next EDR Optimum**	• Monitor de la integridad de los archivos • Inspección de registros • Monitor de integridad del sistema • Inventario de software/hardware • Instalación de aplicaciones de terceros • Instalación local de sistemas operativos • Capacidad de usar la consola empresarial de forma local o en la nube (vista de Experto)
Kaspersky Endpoint Security for Business Advanced **Kaspersky Total Security for Business**	**Kaspersky Next EDR Optimum**	• Opción de consola en la nube simple de usar • Funcionalidad de EDR esencial, incluidos análisis de causas raíz, análisis de IoC y respuesta automatizada • Capacitación en ciberseguridad para administradores de TI • Detección y bloqueo de servicios en la nube • Data Discovery • Seguridad de MS Office 365
Kaspersky Endpoint Detection and Response Optimum	**Kaspersky Next EDR Optimum**	• Opción de consola en la nube simple de usar • Capacitación en ciberseguridad para administradores de TI • Detección y bloqueo de servicios en la nube • Data Discovery • Seguridad de MS Office 365

Más información acerca de Kaspersky Next EDR Optimum

Kaspersky Next EDR Optimum

Kaspersky Next EDR Foundations — Más información

Kaspersky Next XDR Expert — Más información

Noticias sobre ciberamenazas: securelist.lat
Noticias sobre seguridad TI: business.kaspersky.com
Seguridad TI para pymes: kaspersky.com/business
Seguridad TI para grandes empresas: kaspersky.com/enterprise

latam.kaspersky.com

Obtenga más información acerca de Kaspersky Next en: https://go.kaspersky.com/next

Realice una encuesta breve con nuestra herramienta interactiva para elegir el nivel que más se adapte a sus necesidades: https://go.kaspersky.com/Kaspersky_Next_Tool