kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Endpoint Detection and Response Optimum

Cree una verdadera defensa en profundidad con una respuesta automática instantánea y un sencillo análisis de la causa raíz

El problema

El 91 % de todas las organizaciones se vio afectado por ciberataques en 2019, y **1 de cada 10** se enfrentó a un ataque dirigido[1].

Las amenazas complejas suponen una interrupción

Los días de malware simplista desaparecieron hace tiempo y las amenazas se han complicado mucho más, lo que ha producido más interrupciones y mayores pérdidas a las empresas, al tiempo que permanecen inadvertidas durante más tiempo

Le están atacando

Estas complejas amenazas se han vuelto mucho más baratas y frecuentes, de modo que las organizaciones que creían que estaban las tenían controladas ahora tienen que cubrirse la espalda.

La eficiencia es imprescindible

La falta de recursos que las organizaciones enfrentan ahora, incluidas dos de las más valiosas, el tiempo y el personal calificado, implica más leña para el fuego.

Cómo podemos ayudar

«Una solución EPP débil destruirá el valor de una herramienta EDR»[2]

«Las personas y el tiempo se convierten así en la nueva métrica de ROI para la herramienta EDR»[2]

Kaspersky Endpoint Detection and Response (EDR) Optimum le ayuda a estar seguro frente a amenazas complejas y avanzadas al proporcionar detección avanzada, investigación simplificada y respuesta automatizada.

Más allá de las capacidades esenciales

Proporciona una visibilidad profunda, herramientas de investigación sencillas y opciones de respuesta automatizadas para no solo detectar la amenaza, sino para revelar su alcance y orígenes completos y responder al instante, evitando las interrupciones del negocio.

Verdadera defensa en profundidad

Ofrece un kit de herramientas de detección y respuesta altamente automatizado y fácil de usar junto con las capacidades de protección de endpoints inigualables y la detección avanzada de Kaspersky Endpoint Security for Business, lo que constituye una única solución unificada.

La herramienta inteligente garantiza la eficiencia

Libera tiempo y optimiza los recursos de mano de obra y la sobrecarga de IT al proporcionar controles centralizados sencillos y un alto nivel de automatización. Un flujo de trabajo optimizado desde una única consola disponible tanto en las instalaciones como en la nube[3].

Ventajas clave

- Protéjase frente a amenazas avanzadas y complejas más frecuentes y disruptivas
- Ahorre tiempo y recursos con una herramienta sencilla y automatizada
- Vea el alcance completo de las amenazas complejas en toda la red
- Comprenda la causa raíz de la amenaza y cómo ocurrió realmente
- Evite daños adicionales con una respuesta automática rápida

Casos de uso cruciales de EDR

Responda a las preguntas importantes

- ¿Cuál es el contexto de la alerta?
- ¿Qué acciones se han realizado ya ante la alerta?
- ¿Sigue activa la amenaza detectada?
- ¿Se ha atacado a otros hosts?
- ¿Qué camino llevó el ataque?
- ¿Cuál es la verdadera causa raíz de la amenaza?

Conozca el alcance completo de la amenaza

Una vez que sepa que está en riesgo de una amenaza global, por ejemplo, la autoridad reguladora le pide que realice un análisis de un indicador específico de compromiso (IoC), puede:

- Importar IoC de fuentes de confianza y ejecutar análisis periódicos para detectar señales de un ataque
- Investigar detenidamente una alerta, generar IoC basándose en amenazas descubiertas y ejecutar análisis en toda la red para averiguar si otros hosts se han visto afectados

Responder al instante a las amenazas prolíficas

- Poner en cuarentena automáticamente los archivos asociados a amenazas complejas en todos los endpoints
- Aislar automáticamente los hosts infectados al encontrar un IoC asociado con una amenaza de propagación rápida
- Evitar que el archivo malicioso se ejecute y se propague por toda la red durante la investigación

[1] Informe de riesgos de IT globales de Kaspersky, Kaspersky, 2019

[2] IDC, seguridad de endpoints 2020: El resurgimiento del EPP y el destino manifiesto de la EDR, Doc # US45794219, 2020

[3] Existen algunas restricciones en cuanto a la gama de funciones y funcionalidades que se pueden gestionar a través de la consola en la nube. Para obtener la información completa, visite https://kas.pr/epp-management-options

Ahora puede:

Vea el alcance completo de la amenaza

Vea las alertas de seguridad en sus endpoints y analícelas más a fondo para comprender la amplitud y profundidad de la amenaza. Esto ayuda a garantizar que los incidentes se abordan por completo y que no queda ningún resto de la amenaza en el endpoint.

Simplifique su flujo de trabajo

El flujo de trabajo optimizado desde una única consola disponible tanto en las instalaciones como en la nube se combina con escenarios y controles EDR sencillos, como visualización detallada, exploración de IoC y opciones de respuesta que no requieren demasiada experiencia en ciberseguridad ni demasiado tiempo.

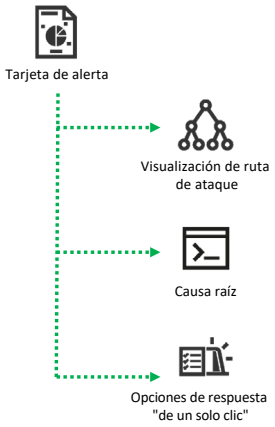
Dé un impulso a sus defensas

La adición de Kaspersky Sandbox crea una completa solución integrada de seguridad de endpoints que ofrece defensas sencillas a varios niveles, eficaces y altamente automatizadas contra amenazas genéricas, complejas y evasivas.

Analice datos de alerta enriquecidos

Kaspersky EDR Optimum enriquece los incidentes con la información necesaria y le ayuda a comprender las conexiones entre diferentes eventos mediante la visualización de rutas de propagación de ataques.

La visibilidad se proporciona en todos los hosts de la red mediante el análisis de indicadores de compromiso (IoC) importados o generados.



Responda automáticamente

Configure respuestas automatizadas para amenazas descubiertas en todos los endpoints basadas en exploraciones de IoC, o responda instantáneamente a incidentes tras el descubrimiento con opciones de un solo clic.

Las opciones de respuesta incluyen: aislar el host, poner en cuarentena el archivo, iniciar el análisis del host e impedir que se ejecute el archivo.

Otras opciones de EDR

Kaspersky Endpoint Detection and Response Optimum es una de las numerosas opciones de EDR que ofrecemos, cada una de ellas adaptada a las necesidades específicas de los clientes. Es posible que también desee considerar:

Kaspersky Endpoint Detection and Response

La solución de EDR, reconocida por el sector y el cliente, es perfecta para organizaciones de IT con equipos de seguridad de IT maduros, lo que ayuda a llegar al fondo de los ataques más sofisticados, avanzados y dirigidos. Ofrece detección de amenazas mejorada, investigación eficaz, detección proactiva de amenazas y respuesta centralizada a incidentes.
https://www.kaspersky.es/enterprise-security/endpoint-detection-response-edr

Kaspersky Managed Detection and Response

La detección, priorización, investigación y respuesta totalmente gestionadas y personalizadas, respaldadas por más de 20 años de investigación de amenazas constantemente destacadas, le permite obtener todas las ventajas principales de tener su propio centro de operaciones de seguridad sin tener que establecer uno.
https://www.kaspersky.es/enterprise-security/managed-detection-and-response

Para obtener más información sobre cómo Kaspersky Endpoint Detection and Response Optimum aborda las ciberamenazas al mismo tiempo que facilita el uso de su equipo de seguridad y sus recursos, visite
http://www.kaspersky.com/enterprise-security/edr-security-software-solution

Noticias sobre ciberamenazas: www.securelist.com
Noticias sobre seguridad de IT: business.kaspersky.com
Seguridad de IT para grandes empresas: kaspersky.es/enterprise-security
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.es

Seguridad probada, independiente y transparente. Nos comprometemos a construir un mundo más seguro en el que la tecnología nos mejore la vida. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Proven. Transparent. Independent.