kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Lleve sus defensas de endpoint al siguiente nivel y encare las amenazas evasivas de frente, sin complicaciones.

Es momento de subir de nivel. Tiene todo preparado no solo para proteger su organización con las tecnologías anti-malware tradicionales, sino también para identificar, analizar y neutralizar de manera eficaz esas amenazas diseñadas para evadir la protección tradicional y quedar ocultas en lo profundo de los sistemas, listas para hacer daño.

Las herramientas legítimas del sistema se utilizan en aproximadamente el **30 % de los ataques exitosos** para iniciar scripts y programas, descargar elementos, analizar redes u obtener acceso remoto al host infectado.
Informe de analistas de respuesta ante incidentes, Kaspersky, 2020

Los desafíos:

Interrupción grave

El malware, el ransomware, el spyware financiero y otras amenazas se están haciendo cada vez más inteligentes en evadir la detección, y cada vez es más barato montar ataques. Así, el riesgo de un ataque grave es mayor que nunca, al igual que los niveles de daño e interrupción involucrados.

Infraestructuras complejas

En la actualidad, la gran mayoría de los gerentes de TI y profesionales de seguridad deben proteger una amplia gama de diferentes endpoints (computadoras portátiles, servidores, entornos virtuales y en la nube, y estaciones de trabajo remotas), al tiempo que deben lidiar con niveles de complejidad de TI apenas manejables

Cómo encontrar un equilibrio

La ciberseguridad, en su mayor parte, se trata de encontrar el equilibrio óptimo entre losrecursos disponibles y el nivel más alto de protección alcanzable de manera realista. Y el tiempo de su especialista de TI es uno de los recursos más escasos de todos.

La respuesta

Kaspersky Endpoint Detection and Response (EDR) Optimum ayuda a identificar, analizar y neutralizar las amenazas evasivas gracias a que facilita la detección avanzada, es fácil de usar, simplifica la investigación y automatiza la respuesta.

Incluso en los ataques exitosos, las pérdidas financieras fueron un **32 % menores** si se dio una respuesta rápida a las vulneraciones.
Informe de analistas de respuesta ante incidentes, Kaspersky, 2020

Armado y listo para todo

En función de los mecanismos de detección avanzados, que incluyen el aprendizaje automático y el análisis mejorado de comportamiento, Kaspersky EDR Optimum ofrece una visibilidad profunda de las amenazas, análisis y herramientas de investigación sencillas y respuesta automatizada. Podrá ver la amenaza, entenderla, revelar todo su alcance y responder instantáneamente, y así evitar la interrupción comercial.

Una sola consola

Kaspersky EDR Optimum aporta detección avanzada, capacidades de análisis y respuesta al ecosistema de seguridad de Kaspersky, y así mejora las defensas en todo el espectro de endpoints, que incluye computadoras portátiles, servidores, cargas de trabajo de nube y entornos virtuales. La implementación centralizada y la gestión unificada de Kaspersky EDR Optimum están disponibles desde la nube o en las instalaciones.

Simple y eficiente

Kaspersky EDR Optimum está creada para equipos de ciberseguridad pequeños con recursos limitados que buscan actualizar sus capacidades de respuesta ante incidentes. El desempeño se ve optimizado para una máxima eficiencia y mínima intervención humana. De esta manera, se aprovecha completamente el tiempo de los especialistas en seguridad al automatizar y centralizar toda la administración y los flujos de trabajo optimizados.

Ventajas clave

- Protéjase contra las amenazas evasivas más frecuentes y disruptivas
- Defienda cada endpoint: computadoras portátiles, servidores, cargas de trabajo de nube
- Vea el alcance completo de cualquier amenaza en toda la red
- Comprenda la causa raíz de la amenaza y cómo ocurrió realmente
- Evite daños adicionales con una respuesta automática rápida
- Ahorre tiempo y recursos con una herramienta simple y automatizada

Casos de uso de EDR cruciales

Detección avanzada

La detección avanzada es necesaria para descubrir amenazas evasivas:

- Prevención de exploits y detección de amenazas de comportamiento con tecnología de aprendizaje automático (ML)
- Heurística, registros inteligentes, tecnologías basadas en ML
- Simulador integrado para la detección previa a la ejecución de comportamiento malicioso
- Sandbox para un mejor análisis de comportamiento (disponible con Kaspersky Sandbox)
- Nuestros expertos y sistemas de IA recolectan y analizan datos de inteligencia de amenazas recogidos en todo el mundo.

Respuesta a preguntas vitales

Las amenazas evasivas suelen ocultarse a simple vista y deben investigarse para poder erradicarlas en su totalidad. EDR permite encontrar las respuestas a las siguientes preguntas:

- ¿Me están atacando ahora?
- ¿Este ataque lanzado contra toda la industria afectó mi infraestructura?
- ¿De dónde provino esta amenaza?
- ¿Qué llegó a hacer en mis hosts?
- ¿Existe alguna capa oculta de esta amenaza?
- ¿Se han visto afectados otros endpoints?

Responda rápidamente

Tan pronto como se descubran amenazas, responda con un solo clic o dé una respuesta automática:

- Impida que el archivo malicioso se ejecute y se propague por toda la red durante o después de la investigación
- Ponga en cuarentena automáticamente los archivos asociados a amenazas evasivas en todos los endpoints
- Aísle automáticamente los hosts infectados cuando se encuentra un indicador de compromiso (IoC) asociado con una amenaza de propagación rápida

Ahora puede hacer mucho más

Ahora puede comprender la totalidad del alcance de cualquier amenaza que lo ataque y cómo se desarrolla en sus endpoints, y así aprovechar la detección basada en aprendizaje automático y la visibilidad de las detecciones. Y puede estar seguro de que cada amenaza se haya atendido en su totalidad, que no haya nada hurgando dentro de su sistema, buscando hacer más daño.

Defienda las infraestructuras híbridas

Las infraestructuras suponen desafíos de seguridad únicos, así como también beneficios significativos. Ahora puede mejorar la protección de sus datos e infraestructura para servidores virtuales y físicos, implementaciones de VDI y cargas de trabajo de la nube pública con la funcionalidad esencial de EDR.

Evite la fatiga de alerta y aproveche al máximo sus recursos con gestión centralizada en todos sus cargas de trabajo y endpoints híbridos, y flujo de trabajo de EDR optimizado desde la nube o en las instalaciones.

Protección de endpoints en múltiples niveles

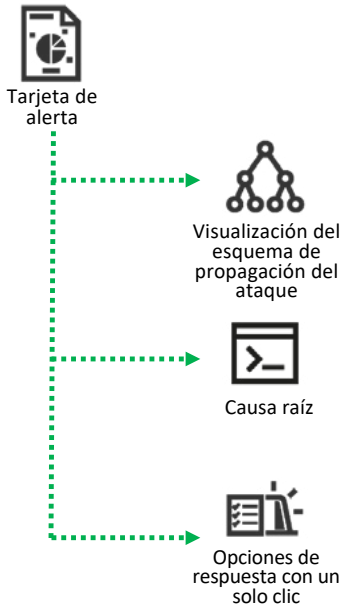
Las tecnologías de EDR no existen en un vacío: solo pueden funcionar de manera efectiva desde una base sólida de protección fuerte de endpoints. La protección de endpoints de múltiples niveles impide que se distraiga al encargarse de amenazas básicas e incidentes de los que ya se debería haber encargado el software anti-malware automatizado. Es por eso que Kaspersky EDR Optimum opera en conjunto con una de nuestras plataformas de protección de endpoints más probada y galardonada[1]: Kaspersky Endpoint Security for Business y Kaspersky Hybrid Cloud Security.

[1] https://www.kaspersky.co.uk/top3

Analice las amenazas

En una sola tarjeta de incidente, se recopilan datos enriquecidos sobre la detección y un esquema detallado de propagación del ataque para realizar un análisis rápido y tomar decisiones informadas para una respuesta 'en un solo clic' o automatizada.

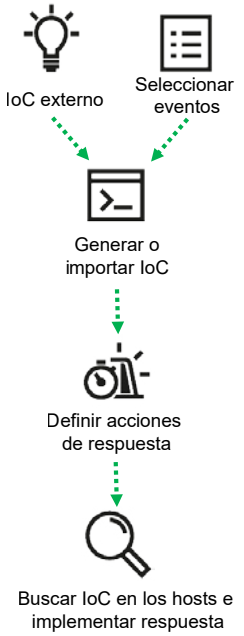
Los IoC pueden importarse de fuentes confiables o generarse en función de la investigación a fin de descubrir amenazas evasivas que acechan en los endpoints de toda su infraestructura.



Automatice su respuesta

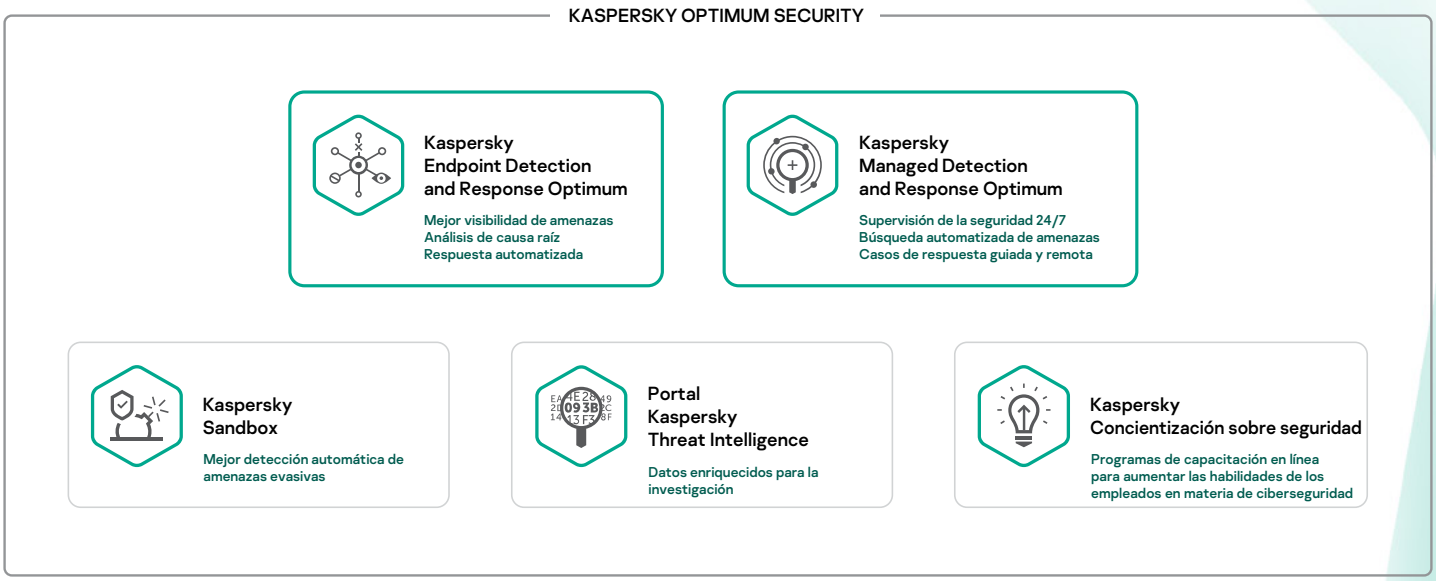
Responda instantáneamente a amenazas durante la investigación con opciones 'en un solo clic' disponibles en la tarjeta de incidente o configure respuestas automatizadas al momento de la detección en base al análisis de IoC. Las posibles acciones de respuesta son:

- Aislar host
- Poner archivo en cuarentena
- Prevenir la ejecución
- Iniciar un análisis de áreas críticas



Su plataforma Kaspersky Optimum Security

EDR es parte de un ecosistema que abarca múltiples tecnologías, herramientas y servicios: Kaspersky EDR Optimum es el componente clave de Kaspersky Optimum Security, una solución más amplia que refuerza varios aspectos de sus defensas contra amenazas evasivas, sin monopolizar sus recursos:



Un enfoque por etapas

Kaspersky Optimum Security se basa en Kaspersky Security Foundations. Cuando tenga todo preparado para hacerlo, puede elegir avanzar a su paso hacia Kaspersky Expert Security, la aplicación de poderosas herramientas que protegen contra las amenazas más avanzadas.

Kaspersky Security Foundations

Bloquee automáticamente la gran mayoría de las amenazas.

- Prevención automatizada multivectorial de los incidentes que provocan las amenazas básicas, que son la gran mayoría de los ciberataques
- La etapa inicial para organizaciones de cualquier tamaño y complejidad en el desarrollo de una estrategia de defensa integrada
- Protección fiable de los endpoints para quienes tienen equipos de TI pequeños y conocimientos de seguridad limitados

Kaspersky Optimum Security

Aumente sus defensas contra las amenazas evasivas. Ideal para empresas que:

- Tienen un pequeño equipo de seguridad de TI con conocimientos técnicos básicos de ciberseguridad.
- Tienen un entorno de TI que crece en tamaño y complejidad, lo que aumenta la superficie de ataque.
- No tienen suficientes recursos de ciberseguridad y necesitan una mayor protección.
- Tienen necesidad creciente de desarrollar una capacidad de respuesta ante incidentes.

Kaspersky Expert Security

Preparación para repeler ataques complejos y similares a APT. Para empresas que tienen:

- Entornos de TI complejos y distribuidos.
- Un equipo de seguridad de TI maduro, o un centro de operaciones de seguridad (SOC) establecido.
- Pocas ganas de someterse a riesgo, que impliquen costos mayores de los incidentes de seguridad y las filtraciones de datos.
- Necesidad de cumplir normativas

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://latam.kaspersky.com/enterprise-security/edr-security-software-solution.

Noticias sobre ciberamenazas: www.securelist.es
Noticias sobre seguridad de TI: business.kaspersky.com

latam.kaspersky.com