Kaspersky Endpoint Detection and Response

kaspersky PREPARADOS PARA EL FUTURO

Los cibercriminales utilizan cada vez técnicas más sofisticadas y capaces de burlar la seguridad existente. Cada área de su empresa puede estar expuesta a riesgos, a sufrir una interrupción de los procesos críticos para el negocio, sufrir daños en la productividad y aumentar los costes operativos.

Con Kaspersky EDR, su organización puede:

- **SUPERVISAR** las amenazas de manera eficiente, más allá del malware
- **DETECTAR** las amenazas de manera eficaz con tecnologías avanzadas
- **AGREGAR** de forma centralizada los datos sin procesar y los veredictos
- **RESPONDER** con rapidez a los ataques
- **EVITAR** acciones maliciosas por parte de las amenazas detectadas

... todo ello a través de una potente interfaz web que facilita la investigación y la reacción.

Kaspersky EDR y conclusiones clave del informe Endpoint Security 2020 de IDC*

Una solución EPP débil destruirá el valor de una herramienta EDR

Kaspersky ofrece potentes defensas completas para endpoints (EPP + EDR) a través de un solo agente

Las personas y el tiempo se convierten así en la nueva métrica de retorno sobre la inversión para la herramienta EDR

Kaspersky aplica altos niveles de automatización a problemas complejos, liberando el valioso tiempo de sus expertos en seguridad

EDR debe aprovechar los datos que están fuera del endpoint

Kaspersky aumenta la eficacia de EDR añadiendo visibilidad y detección de amenazas avanzadas basadas en correo electrónico y en la web a través de una sola herramienta

En primer lugar, mejore las defensas de los endpoints

Para los cibercriminales, el principal objetivo siguen siendo los endpoints empresariales, en los que los datos, los usuarios y los sistemas corporativos se unen para generar e implementar procesos empresariales. Para proteger sus endpoints empresariales y evitar que se utilicen como puntos de entrada a su infraestructura, los equipos de seguridad de IT deben enfocarse en fortalecer las defensas existentes. La implementación de un ciclo de protección de endpoints completo, desde el bloqueo automático de amenazas comunes hasta la ejecución de respuestas rápidas y adecuadas ante incidentes complejos, requiere tecnologías de prevención que se complementen con funciones de defensa avanzadas.

Kaspersky Endpoint Detection and Response (EDR) ofrece una potente seguridad con visibilidad completa de todos los endpoints en la red corporativa junto con defensas de nivel superior, lo que facilita la automatización de tareas rutinarias para detectar, priorizar, investigar y neutralizar amenazas complejas y ataques de tipo APT.

Aspectos destacados

Kaspersky EDR aprovecha nuestra plataforma de protección de endpoint (EPP) estrella, más probada y más galardonada, **Kaspersky Endpoint Security for Business**, con potentes capacidades EDR, para fortalecer todavía más los niveles de seguridad generales. Contar con un solo agente para la protección automática contra amenazas comunes y la defensa avanzada contra ataques complejos simplifica la gestión de incidentes y reduce los requisitos de mantenimiento. Sin carga adicional en los endpoints ni costes imprevistos: solo saber que sus estaciones de trabajo y servidores están totalmente protegidos contra las amenazas y los ataques dirigidos más avanzados.

- Kaspersky EDR reduce el tiempo necesario para la recopilación inicial de pruebas, ofrece análisis de telemetría completo y maximiza la automatización de los procesos EDR, reduciendo así los tiempos de respuesta ante los incidentes sin necesidad de utilizar recursos de seguridad de IT adicionales.
- Kaspersky EDR se puede integrar en **Kaspersky Anti Targeted Attack Platform**, combinando las capacidades de EDR y el descubrimiento avanzado de amenazas a nivel de red. Los especialistas en seguridad de IT cuentan con todas las herramientas necesarias para manejar una detección de amenazas multidimensional superior tanto en los endpoints como en la red, con la aplicación de tecnologías de vanguardia, la realización de investigaciones eficaces y una respuesta rápida y centralizada, todo en una única solución.

**PERSPECTIVA DE IDC, Endpoint Security 2020: el resurgir de EPP y el Manifest Destiny de EDR

Kaspersky EDR es ideal si su organización desea:

- Mejorar su seguridad con una solución empresarial fácil de usar para la respuesta a incidentes
- Automatizar la identificación y respuesta a amenazas, sin interrumpir el negocio durante las investigaciones
- Mejorar la visibilidad de su endpoint y la detección de amenazas a través de tecnologías avanzadas
- Entender las tácticas, técnicas y procedimientos (TTP) específicos empleados por los actores de amenazas para lograr sus objetivos, lo que permite defensas más efectivas y una asignación más eficiente de los recursos de seguridad
- Establecer procesos de búsqueda de amenazas, gestión de incidentes y respuesta unificados y eficaces
- Aumentar la eficiencia de su centro de operaciones de seguridad interno: no pierda su tiempo analizando registros de endpoints irrelevantes
- Ayudar al cumplimiento mediante la aplicación de registros de endpoints, revisiones de alertas y la documentación de los resultados de la investigación

Descubrir y contener rápidamente las amenazas más sofisticadas

Kaspersky EDR proporciona protección de endpoints de alto nivel y aumenta la eficiencia del centro de operaciones de seguridad, proporcionando detección avanzada de amenazas y acceso a datos retrospectivos, incluso en situaciones en las que los endpoints comprometidos son inaccesibles o cuando los datos se han cifrado durante un ataque. Capacidades de investigación mejoradas a través de nuestros indicadores de ataque únicos (IoA), enriquecimiento de MITRE ATT & CK y un generador de consultas flexible, además de acceso a nuestra base de conocimientos del portal de inteligencia de amenazas; todo esto facilita la búsqueda de amenazas efectiva y la respuesta rápida a incidentes, lo que lleva a la limitación y prevención de daño.

Casos de uso:

- **Búsqueda proactiva de evidencias de intrusión en toda su red**
- **Rápida detección y corrección de una intrusión antes de que el intruso pueda causar daños e interrupciones importantes**
- **Rápida investigación y gestión centralizada de incidentes en miles de endpoints con un flujo de trabajo perfecto**
- **Validación de alertas y posibles incidentes detectados por otras soluciones de seguridad**
- **Automatización de operaciones rutinarias para minimizar las tareas manuales, liberar recursos y reducir la probabilidad de "sobrecarga de alertas"**

Gartner peerinsights customers' choice 2020™

Gartner Peer Insights Customers' Choice nombra a Kaspersky como el principal proveedor de soluciones EDR del año 2020

Kaspersky es uno de los tan solo 6 proveedores en todo el mundo que han recibido el reconocimiento de Gartner Peer Insights Customers' Choice por la solución Endpoint Detection and Response en 2020, con la clasificación más alta de todos los proveedores por nuestro servicio y asistencia, la mayor felicitación por parte de los clientes para Kaspersky EDR.

Exención de responsabilidad de Gartner

Gartner Peer Insights Customers Choice representa las opiniones subjetivas de revisiones, valoraciones y datos de usuarios finales individuales aplicados respecto a una metodología documentada, y de ninguna forma representan la opinión ni el aval de Gartner o de sus filiales.

MITRE | ATT&CK®

Calidad de detección confirmada por la evaluación de MITRE ATT&CK

Reconocimiento de la importancia del análisis de TTP (tácticas, técnicas y procedimientos) en la investigación de incidentes complejos y el papel de MITRE ATT&CK en el mercado de la seguridad actual:

- Kaspersky EDR ha participado en la segunda ronda de la evaluación MITRE (APT29) y ha demostrado un alto nivel de rendimiento en la detección de las técnicas ATT&CK dentro del alcance de esta segunda ronda aplicadas en etapas cruciales de los ataques dirigidos actuales
- Las detecciones de Kaspersky EDR están enriquecidas con datos de la base de conocimientos de MITRE ATT&CK para lograr un análisis más profundo de las tácticas, técnicas y procedimientos de los adversarios

Más información en kaspersky.com/MITRE

Beneficios comerciales de Kaspersky EDR para toda la empresa:

- Eliminación de brechas de seguridad y reducción del "tiempo de espera" durante los ataques
- Automatización de tareas manuales durante la detección y la respuesta ante amenazas
- Liberación del personal de IT y de seguridad para otras tareas prioritarias
- Simplificación del análisis de amenaza y la respuesta ante incidentes
- Reducción del tiempo necesario para identificar y responder a las amenazas
- Garantía de logro del cumplimiento total

Y si quiere todavía más... Kaspersky Managed Detection and Response

Agregar defensas totalmente administradas y adaptadas individualmente a Kaspersky EDR las 24 horas del día significa que sus recursos de seguridad de TI podrán delegar las tareas de procesamiento relacionadas con los incidentes a Kaspersky, o consultar con nuestro equipo para obtener opiniones de expertos y aprovechar nuestra experiencia única en la búsqueda de amenazas cuando su equipo local carezca de especialistas en seguridad suficientemente cualificados para dar respuesta a escenarios específicos.

Para obtener más información sobre Kaspersky EDR, visite:

kaspersky.com/enterprise-security/endpoint-detection-response-edr

Noticias de ciberamenazas: www.securelist.es
Noticias sobre seguridad de IT: business.kaspersky.es
Seguridad de IT para pymes: kaspersky.es/business
Seguridad de IT para grandes empresas: kaspersky.es/enterprise

www.kaspersky.es

2020 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.

Seguridad probada. Somos una compañía independiente. Somos transparentes. Nos comprometemos a construir un mundo más seguro en el que la tecnología mejore nuestras vidas. 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.

Más información en kaspersky.es/transparency

Proven. Transparent. Independent.