Kaspersky Endpoint Detection and Response

kaspersky BRING ON THE FUTURE

Los cibercriminales son cada vez más sofisticados y capaces de eludir con éxito la protección existente. Cada área de su negocio puede estar expuesta a riesgos, interrumpiendo los procesos críticos para el negocio, dañando la productividad y aumentando los costos operativos.

Gracias a Kaspersky EDR, su organización podrá hacer lo siguiente:

- **MONITOREAR** eficientemente las amenazas, más allá del malware
- **DETECTAR** amenazas de manera eficaz usando tecnologías avanzadas
- **AGREGAR** centralmente datos sin procesar y veredictos
- **RESPONDER** rápidamente a los ataques
- **EVITAR** acciones maliciosas mediante la detección de amenazas

...todo esto a través de una interfaz web intuitiva que facilita la investigación y la reacción.

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

- **Una solución de EPP débil dañará el valor de una herramienta de EDR**

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

- **Así, las personas y el tiempo se convierten en la nueva métrica del retorno de la inversión para las herramientas de 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 de los endpoints**

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

Primero fortalezca las defensas de sus endpoints

Para los cibercriminales, los endpoints corporativos, donde los datos, los usuarios y los sistemas corporativos funcionan en conjunto para generar e implementar procesos empresariales, son particularmente vulnerables. Para proteger sus endpoints corporativos y evitar que se utilicen como puntos de entrada a su infraestructura, sus equipos de seguridad de TI deben probar formas de fortalecer la seguridad existente. La implementación de un ciclo de protección de endpoints completo, desde el bloqueo automático de amenazas comunes hasta la ejecución de respuestas ágiles y adecuadas ante incidentes complejos, requiere tecnologías de prevención que se complementan con funciones de defensa avanzadas.

Kaspersky Endpoint Detection and Response (EDR) ofrece una seguridad poderosa con visibilidad integral en todos los endpoints de la red corporativa juntos, con defensas superiores, lo que permite la automatización de tareas rutinarias para descubrir, priorizar, investigar y neutralizar amenazas complejas y ataques de tipo APT.

Puntos importantes

- Kaspersky EDR mejora nuestra plataforma de protección de endpoints (EPP) insignia más probada y premiada, **Kaspersky Endpoint Security for Business**, con potentes capacidades de EDR, lo que refuerza aún más sus niveles generales de seguridad. Un solo agente que ofrece protección automática contra amenazas comunes y defensa avanzada contra ataques complejos simplifica el manejo de incidentes y reduce los costos de mantenimiento. Sin carga adicional en endpoints ni costos imprevistos: solo saber que sus estaciones de trabajo y servidores están completamente protegidas contra las amenazas y los ataques selectivos más sofisticados.
- Kaspersky EDR reduce el tiempo necesario para la recopilación inicial de pruebas, proporciona un análisis de telemetría completo y maximiza la automatización de los procesos de EDR, reduciendo los tiempos de respuesta a incidentes generales sin la necesidad de atraer recursos de seguridad de TI adicionales.
- Kaspersky EDR puede ser parte de **Kaspersky Anti Targeted Attack Platform**, combinando las capacidades de EDR y el descubrimiento avanzado de amenazas a nivel de red. Los especialistas de seguridad de TI cuentan con todas las herramientas necesarias para manejar la detección de amenazas multidimensional en un nivel superior, tanto en los endpoints como en la red, de modo que aplican tecnologías de vanguardia, realizan investigaciones eficaces y proporcionan una respuesta rápida y centralizada, todo en una única solución.

*PERSPECTIVA DE IDC, Endpoint Security 2020: El resurgimiento de EPP y el Destino Manifiesto de la EDR

Kaspersky EDR es ideal si su organización desea:

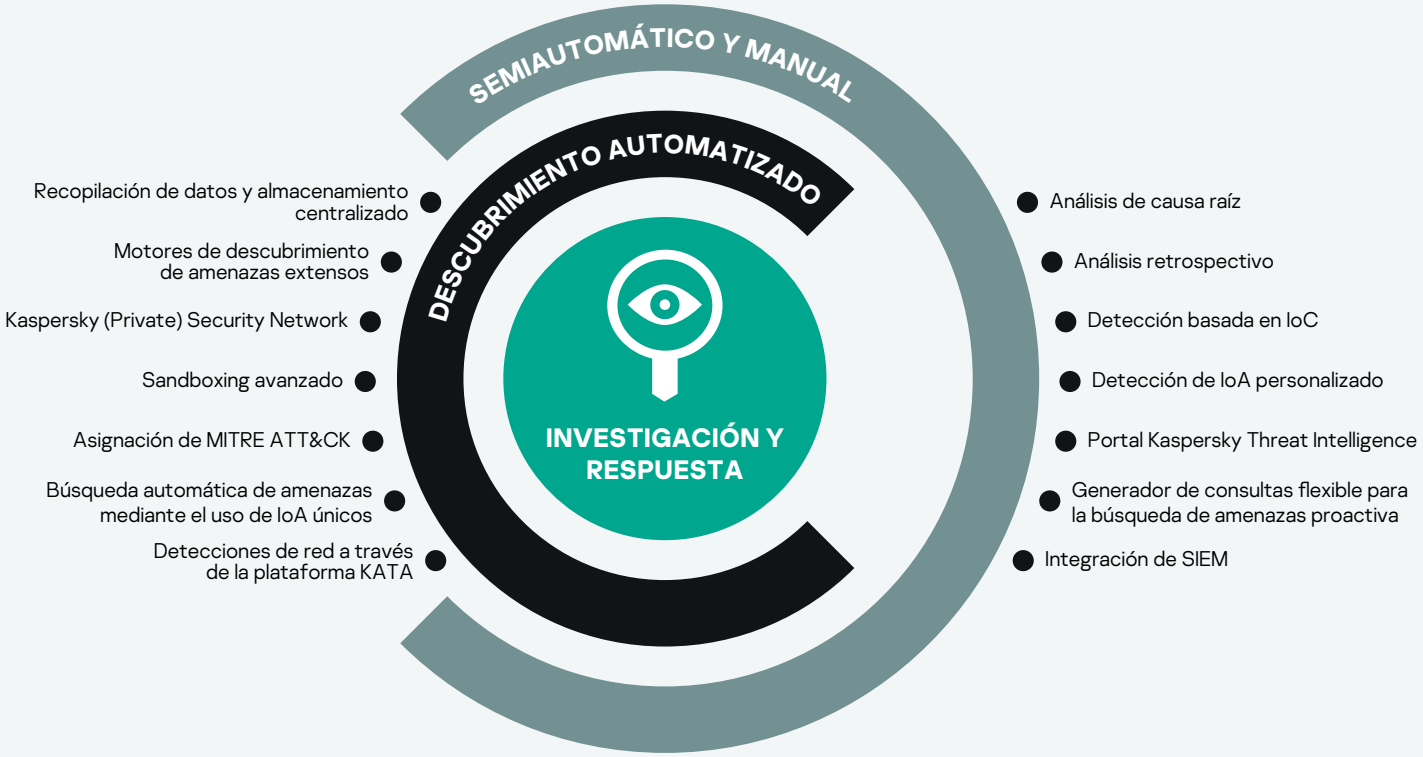
- Actualizar su seguridad con una solución empresarial fácil de usar para la respuesta a incidentes
- Automatizar la identificación y respuesta a amenazas, sin interrumpir el negocio durante las investigaciones
- Mejorar la visibilidad de su endpoint y la detección de amenazas a través de tecnologías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

Casos prácticos:

- **Búsqueda proactiva de evidencia de intrusión en toda su red**
- **Detección y corrección rápidas de una intrusión antes de que el intruso pueda causar daños e interrupciones importantes**
- **Investigación rápida y gestión centralizada de incidentes en miles de endpoints con un flujo de trabajo fluido**
- **Validación de alertas e incidentes potenciales detectados por otras soluciones de seguridad**
- **Automatización de operaciones de rutina, a fin de ayudar a minimizar las tareas manuales, liberar recursos y reducir la probabilidad de tener una "sobrecarga de alertas"**



La elección de los clientes de Gartner Peer Insights para soluciones EDR 2020 nombra a Kaspersky como proveedor principal

Kaspersky es uno de los 6 proveedores en todo el mundo en recibir el reconocimiento Gartner Peer Insights Customer's Choice por la solución Endpoint Detection and Response en 2020, con la calificación más alta de cualquier proveedor por nuestro servicio y soporte: el mejor cumplido del cliente para Kaspersky EDR.

Exención de responsabilidad de Gartner

Gartner Peer Insights Customers' Choice refleja las opiniones de usuarios finales vertidas en reseñas, calificaciones y datos, recopilados usando una metodología documentada, y que de ninguna forma representan la opinión, ni constituyen 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 tácticas, técnicas y procedimientos (TTP) en la investigación de incidentes complejos y el papel de MITRE ATT&CK en el mercado de seguridad actual:

- Kaspersky EDR ha participado en la Ronda de evaluación MITRE 2 (APT29) y ha demostrado un alto nivel de rendimiento en la detección de técnicas clave de ATT&CK del alcance de la ronda 2 aplicadas en etapas cruciales de los ataques dirigidos de hoy
- Las detecciones de Kaspersky EDR están enriquecidas con datos de la base de conocimientos de MITRE ATT&CK, para un análisis profundo de los TTP de su adversario

Obtenga más información en kaspersky.com/MITRE

Ventajas comerciales de Kaspersky EDR para toda la empresa:

- Ayuda a eliminar brechas de seguridad y a reducir el "tiempo de permanencia" de los ataques
- Permite automatizar tareas manuales durante la detección de amenazas y su respuesta ante estas
- Permite liberar al personal de TI y seguridad de TI para que se dediquen a otras tareas importantes
- Permite simplificar el análisis de amenazas y la respuesta a incidentes
- Permite reducir el tiempo necesario para identificar las amenazas y responder a ellas
- Ayuda a permitir el cumplimiento total

Y si desea aún más... Kaspersky Managed Detection and Response

Agregar defensas las 24 horas del día totalmente administradas y adaptadas individualmente a Kaspersky EDR significa que sus recursos de seguridad de TI se pueden conservar descargando las tareas de procesamiento relacionadas con incidentes a Kaspersky, o contactándonos para obtener opiniones de expertos y experiencia única en la búsqueda de amenazas cuando su equipo interno carece de especialistas en seguridad suficientemente calificados para cumplir con escenarios específicos.

Para obtener más información sobre Kaspersky EDR, visite:

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

Noticias de amenazas cibernéticas: securelist.com
Noticias sobre seguridad de TI: business.kaspersky.com
Seguridad de TI para pymes: kaspersky.com/business
Seguridad de TI para grandes empresas: latam.kaspersky.com/enterprise

latam.kaspersky.com

Hemos sido probados. Somos independientes. Somos transparentes. Estamos comprometidos con la construcción de un mundo más seguro, en el que la tecnología permita mejorar nuestras vidas. Por esta razón lo protegemos, de modo que todos disfruten las infinitas oportunidades que aporta, sin importar su ubicación. Contrate ciberseguridad para disfrutar un futuro más seguro.

Obtenga más información en latam.kaspersky.com/transparency

Proven. Transparent. Independent.