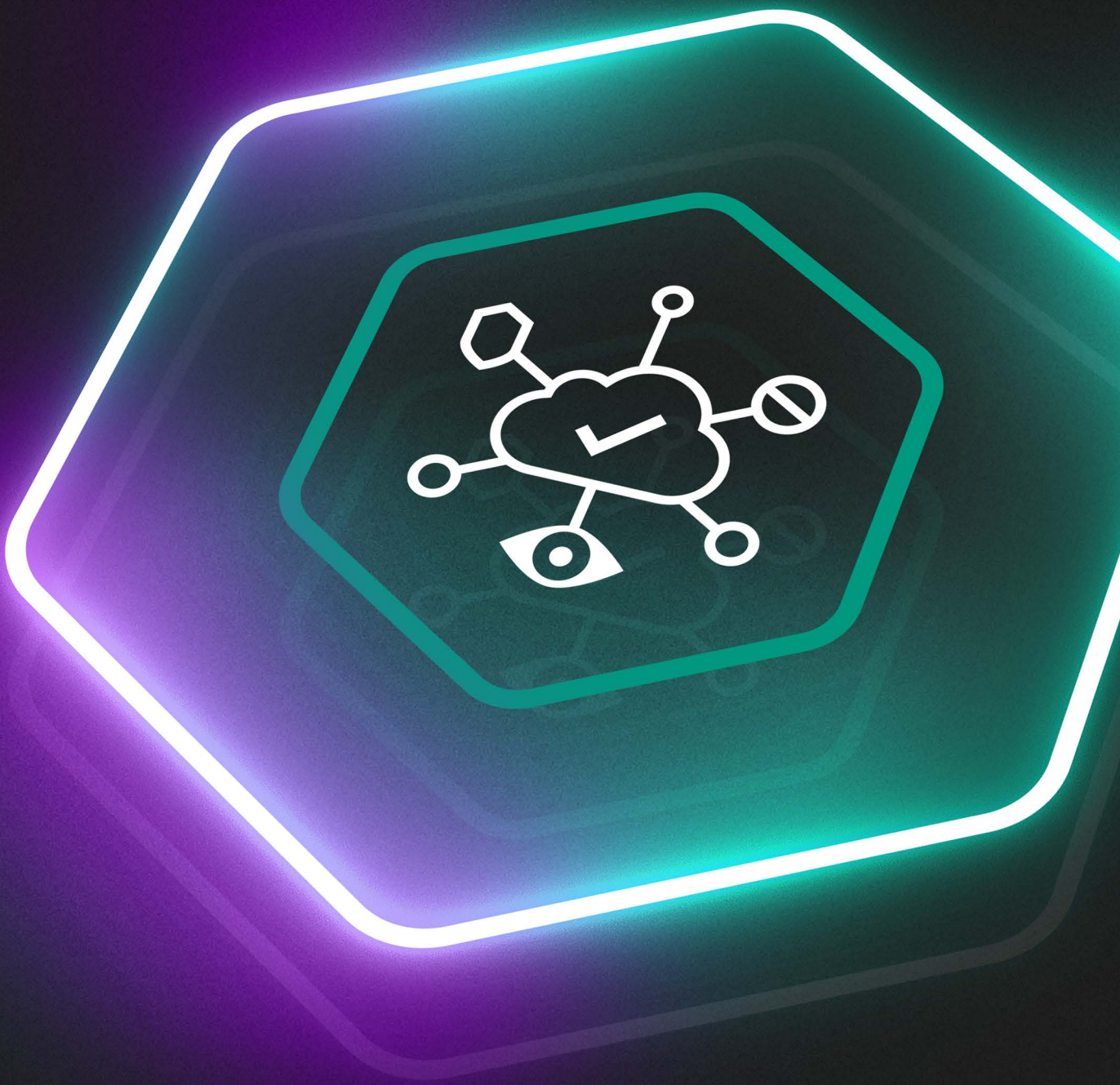

Kaspersky Endpoint Detection and Response

Expert

kaspersky BRING ON THE FUTURE

Una sola consola

Kaspersky EDR Expert es una solución única que se puede administrar tanto desde una plataforma de administración central basada en la nube como desde una consola fuera de línea en entornos herméticos.

Kaspersky Endpoint Detection and Response Expert

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.

Primero fortalezca las defensas de sus endpoints

Los endpoints corporativos es donde los datos, usuarios y sistemas corporativos funcionan en conjunto para generar e implementar procesos empresariales. Estos endpoints siguen siendo el objetivo principal de los ciberdelincuentes.

Kaspersky Endpoint Detection and Response (EDR) Expert ofrece visibilidad integral de todos los endpoints en su red corporativa y proporciona defensas de nivel superior. De esta manera, se facilita la automatización de tareas EDR rutinarias para detectar, priorizar, investigar y neutralizar amenazas complejas y ataques de tipo APT.

Desafíos actuales

Los equipos de seguridad de TI carecen de la visibilidad y la transparencia que necesitan para supervisar los endpoints de manera efectiva. La detección de un incidente puede demorar más de lo esperado, como semanas o incluso meses, solo porque puede resultar difícil identificar y comprender con exactitud lo que sucedió, cómo sucedió y cómo solucionarlo.

Ineficiencia. Obligar a los analistas a trabajar en múltiples consolas descentralizadas ralentiza todo el proceso y, al mismo tiempo, genera oportunidades para el error humano. Y lo mismo ocurre con obligar a los profesionales de la seguridad de TI a gestionar manualmente los procesos de detección de rutina.

Falta de inteligencia pertinente. La incapacidad de poner en funcionamiento la inteligencia de amenazas y la falta de una visión clara de las tácticas, técnicas y procedimientos del adversario pueden obstaculizar tanto la priorización de alertas como la investigación y respuesta adicionales.

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

1 Controlar y supervisar eficazmente todos sus endpoints

Al poder ver todos los aspectos del panorama completo: dónde se originó la amenaza, cómo se propagó, a qué hosts afectó y qué se puede y se debe hacer exactamente para evitar las consecuencias.

2 Agilizar el trabajo de su equipo de TI

La contención rápida y precisa de amenazas y la resolución de incidentes en infraestructuras distribuidas se realiza mediante acciones centralizadas y automatizadas para facilitar el trabajo del equipo de seguridad de TI. Ya no necesita recursos adicionales. Olvide los tiempos de inactividad y la pérdida de productividad.

3 Buscar y mitigar las amenazas de forma correcta y rápida

Los datos sin procesar y los veredictos se agregan de forma centralizada, y las capacidades de investigación se potencian a través de nuestros exclusivos indicadores de ataque (IoA), a través del enriquecimiento de MITRE ATT&CK y un generador de consultas flexible, y a través del acceso a nuestra base de conocimiento del portal Threat Intelligence Portal. Todo esto facilita de forma significativa la caza eficaz de amenazas y la respuesta rápida a los incidentes, para limitar los daños y prevenirlos.

Desafíos actuales

Déficit de respuestas e investigación. El solo hecho de comprender que algo está sucediendo en la infraestructura y que la solución de seguridad de la información detectó una amenaza potencial no garantiza que las acciones posteriores sean efectivas. Es importante poder responder a la amenaza de manera efectiva en tiempo real y poder investigar el incidente a fondo para evitar que se repita.

Desperdicio de recursos costosos. Los analistas no pueden concentrarse por completo en las amenazas complejas si se ven obligados a perder el tiempo lidiando con alertas triviales que deberían haberse gestionado automáticamente con una solución eficaz de protección de endpoints. Además de ser un desperdicio de recursos, esto puede provocar el agotamiento de los analistas y que se pasen por alto alertas importantes en medio de todo el "ruido".

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

4 Responder con mayor rapidez y eficacia

La investigación guiada y una respuesta más rápida y precisa son cruciales para hacer frente a los ataques complejos y de tipo APT. Kaspersky EDR Expert proporciona un flujo de trabajo fluido con administración centralizada de incidentes e investigación guiada en todos los endpoints de la red corporativa.

5 Obtener el máximo valor de su solución y de sus expertos

No tiene sentido contratar a analistas costosos para trabajar con su solución EDR si su EPP los hace lidiar con alertas que no requieren sus habilidades. Nuestras soluciones EDR se basan en nuestra solución EPP más probada y premiada, que gestiona automáticamente la gran mayoría de las alertas y libera a los analistas para que se concentren en lo que realmente requiere su atención y experiencia. Nuestros productos EPP y EDR funcionan juntos como una solución única a través del mismo agente de endpoint.

Kaspersky EDR Expert es ideal si su organización desea lo siguiente:

- 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.
- Entender las tácticas, técnicas y procedimientos (TTP) específicos usados por los atacantes para lograr sus objetivos, lo que permite defensas más potentes y la asignación efectiva de recursos de seguridad.
- Mejorar la visibilidad de endpoints y la detección de amenazas con tecnologías avanzadas.
- Establecer procesos unificados y eficaces de búsqueda de amenazas, administración de incidentes y respuestas.
- Aumentar la eficiencia de su SOC interno para que no pierda el tiempo analizando registros y alertas de endpoints irrelevantes.
- Ayudar al cumplimiento con la aplicación de registros de endpoints, revisiones de alertas y la documentación de los resultados de la investigación.

Kaspersky EDR Expert le da el poder para hacer lo siguiente:

- **Detectar amenazas utilizando los mejores y más avanzados métodos. La elaboración de perfiles de la actividad del actor potencial de amenazas es una forma eficaz de detectar actividad maliciosa dentro de una infraestructura.**

Kaspersky EDR Expert permite cargar Indicadores de compromiso **(IoC)** centralizados desde fuentes de datos de amenazas y admite análisis de IoC programados automáticamente, lo que agiliza el trabajo de los analistas.

Con nuestro motor de Indicadores de ataque **(IoA)**, Kaspersky EDR Expert puede identificar acciones sospechosas utilizando el conjunto único de IoA generado por los buscadores de amenazas de Kaspersky, proporcionando capacidades de búsqueda de amenazas automatizadas en tiempo real.

Para brindarle una imagen más precisa de lo que está sucediendo, se puede enviar un archivo o proceso a **Sandbox** para un análisis de comportamiento, ya sea de forma manual o automática.

Las detecciones de IoA y Sandbox se asignan a **MITRE ATT&CK** para el análisis posterior de las tácticas, técnicas y los procedimientos del adversario. Los eventos individuales en el árbol del incidente se enriquecen con el contexto de la base de conocimientos de MITRE, incluyendo la identificación de las tácticas definidas por MITRE utilizadas y la visualización del evento en el gráfico de incidentes.

Recomendaciones para contrarrestar las amenazas

El análisis automático de todos los eventos de endpoints, correlacionados con los datos de inteligencia adquiridos, brinda descripciones claras de eventos, ejemplos y recomendaciones para contrarrestar las amenazas.

- Investigar las causas del incidente y evitar que se repita. Kaspersky EDR Expert proporciona protección de endpoints de alto nivel y aumenta la eficiencia de su SOC, brindando 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 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.
- Elegir una opción conveniente de almacenamiento de telemetría para análisis forense. Una base de datos centralizada almacena la telemetría del endpoint durante 30 días de forma predeterminada, así como objetos y veredictos sin límite de tiempo, lo que significa que el análisis forense se puede realizar sin depender de la disponibilidad del endpoint. Si llega a necesitar más tiempo de retención de telemetría, se puede aumentar a 60 o 90 días. En instalaciones locales, usted puede determinar el período de almacenamiento de datos, dependiendo de la capacidad y las características de su hardware.
- Responder de la manera que más le convenga. Sus expertos en seguridad de TI están equipados con herramientas que permiten una respuesta de "un solo clic" a través de la consola de administración central, lo que reduce la cantidad de tareas manuales y acorta los tiempos de respuesta de horas a minutos.
- Trabajar sin problemas y de manera eficiente. Las herramientas de visualización del árbol de actividades de endpoints y del árbol de eventos desplegable permiten a sus investigadores basarse fácilmente en elementos de datos interesantes durante la evaluación de la ruta de amenazas o profundizar para obtener más información. Vincular eventos y consolidar alertas ayuda a revelar el efecto total de un ataque.

Funcionamiento

Premios y reconocimientos de la industria

Los productos de Kaspersky son evaluados regularmente por empresas de investigación globales, y nuestra capacidad para ayudar a nuestros clientes a protegerse contra ciberataques es ampliamente reconocida y probada. Somos el proveedor de ciberseguridad más probado y más premiado.

Kaspersky Endpoint Detection and Response obtiene la máxima calificación en la prueba de SE Labs

Kaspersky EDR consiguió el máximo premio AAA en la prueba Enterprise Advanced Security de SE Labs (antes conocida como Breach Response Test). La solución se destacó por su capacidad para detectar ataques complejos dirigidos, seguir el comportamiento malicioso desde el principio hasta el final de un ataque y no generar resultados falsos positivos. Durante la evaluación, el producto se expuso a las herramientas, técnicas y procedimientos utilizados por los grupos de amenazas avanzadas.

IDC MarketScape nombró a Kaspersky como uno de los principales actores en la seguridad moderna de endpoints para empresas y pymes

Para ayudar a las organizaciones a evaluar las mejores plataformas de protección de endpoints y las soluciones de detección y respuesta de endpoints para sus necesidades, el IDC MarketScape revisó los datos presentados por los proveedores de MES entre abril y septiembre de 2021, para posicionar las capacidades de las empresas.

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 participó en la Ronda de evaluación MITRE 2 (APT29) y demostró 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.

latam.kaspersky.com

Para obtener más información sobre cómo Kaspersky EDR Expert puede fortalecer a su equipo de seguridad de TI, comuníquese con nosotros.