kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Detection and Response Optimum

Proteja a sus clientes de amenazas evasivas, a la vez que reduce la carga en sus recursos

El reto

El 91 % de todas las organizaciones se vio afectada por ciberataques durante el 2019, de las cuales **1 de cada 10** experimentó un ataque dirigido[1].

Las amenazas son más perjudiciales

Los días del malware simplista ya quedaron atrás y las amenazas se han vuelto mucho más complejas. Incluso una sola amenaza que atraviese las defensas de su cliente podría generar pérdidas significativas para su negocio.

Los clientes cuentan con usted

Los clientes tienen altas expectativas de los SLA y la seguridad que usted proporciona; por tanto, no puede permitirse la integración de herramientas complicadas y desconectadas, ni tampoco perder tiempo o arriesgarse a crear brechas en la protección.

Es difícil mantenerse a la altura de la demanda

Mientras más clientes tenga, mayor será la presión para los ingenieros, quienes ya están bastante presionados por analizar eventos de varios clientes y responder ante ellos.

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]

Actualice la seguridad de sus clientes

Brinde a sus clientes confianza en la seguridad de su empresa con una protección mejorada contra ransomware evasivos, ataques a la cadena de suministro y vulneraciones de datos.

Verdadera defensa integral

Habilitado con aprendizaje automático, Kaspersky Endpoint Detection and Response Optimum incluye una protección de endpoints inigualable que se combina con una visibilidad más profunda, un análisis de la causa raíz y la respuesta automatizada de EDR, todo desde la nube[3].

Automatización y simplificación

La automatización de las operaciones le permite analizar las amenazas y responder ante ellas con mayor rapidez, mientras que la simplificación en los controles y el flujo de trabajo ayudan a optimizar el trabajo de sus ingenieros y a cubrir más terreno en menos tiempo.

El valor de EDR

Obtenga respuestas a preguntas importantes

- ¿Cuál es el contexto de la alerta?
- ¿Cuál es el contexto de la alerta?
- ¿Sigue activa la amenaza detectada?
- ¿Qué camino llevó el ataque?
- ¿Se ha atacado a otros hosts?
- ¿Cuál es la verdadera causa raíz de la amenaza?
- ¿Puedo evitar que ocurran amenazas como esta en el futuro?

Vea 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

Responda al instante

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

Ventajas clave

- Proteja a sus clientes contra amenazas básicas y evasivas altamente disruptivas
- Comprenda la causa origen de la amenaza y cómo ocurrió realmente
- Evite daños adicionales con una respuesta automática rápida
- Ahorre tiempo y recursos con una herramienta sencilla
- Llegue a los clientes de todas las industrias con tecnologías altamente comercializables
- Admite una administración centralizada multiusuario
- Suscripción mensual disponible con un modelo de pago por uso

[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 administrar a través de la consola en la nube. Para obtener la información completa, visite kas.pr/epp-management-options

Ahora es posible:

Permanezca en control

Combine la velocidad y precisión de la automatización con la experiencia humana en una nube única o en una consola local. Los niveles superiores de protección, prevención y control, junto con capacidades básicas de EDR, crean un potente conjunto de herramientas que no requieren altos niveles de experiencia ni mucho tiempo para ejecutarse.

Vea el alcance completo de la amenaza

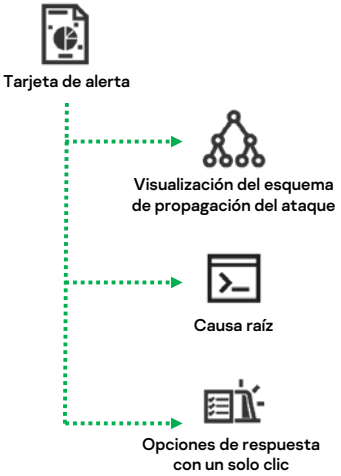
Consulte el contexto y los detalles de las alertas de seguridad sobre los endpoints para comprender la amenaza en su totalidad, asegurándose de que los incidentes se aborden completamente y que no queden restos de la amenaza en los hosts.

Tareas de IT optimizadas

Manténgase al día con los parches de aplicación y sistema operativo, implemente software y SO de terceros con solo unos clics y automatice tareas rutinarias para varios hosts.

Identifique la causa raíz

Analice la amenaza detectada en una sola tarjeta de alerta, la cual contiene toda la información necesaria para la investigación, al igual que la correlación y visualización de eventos, como inyecciones de procesos, caídas de archivos, conexiones y cambios en el registro.



Responda automáticamente

Encuentre amenazas similares en toda la red y automatice la respuesta según IoC importados o generados. Alternativamente, responda de inmediato a los incidentes apenas se descubran con opciones de "un solo clic".

Casos de uso

Estos son algunos ejemplos de cómo se puede utilizar Kaspersky Endpoint Detection and Response Optimum para detectar, investigar y responder ante diversas amenazas.

Sin archivos

Problema: Se detectó actividad maliciosa en la memoria de un proceso legítimo.

Solución: Según los datos de la tarjeta de incidente generada automáticamente, el funcionario de seguridad de TI observa el proceso original que inyectó código malicioso en un proceso legítimo y bloquea instantáneamente el archivo para que no implemente este código. Para resolver aún más el incidente, el funcionario encuentra todos los hosts infectados del mismo modo mediante un escaneo de IoC y bloquea todo el vector de infección.

Componente persistente

Problema: Se detectó un archivo malicioso con extensión común que EPP puso en cuarentena. Sin embargo, ¿cuál fue el alcance real del incidente?

Solución: El empleado ya registró toda la actividad del host correspondiente, la cual está disponible en la tarjeta de alerta. Ahora puede realizar un análisis de la causa raíz y averiguar qué herramientas legítimas del sistema (como PowerShell) se utilizaron en el ataque, las cuales persisten mediante el cambio de ejecución automática o el almacenamiento de una carga codificada en el registro. Se analizan todos los hosts del sistema para este IoC, se encontraron otras infecciones y se aplicó una respuesta automatizada.

Ransomware

Problema: Un empleado recibe un correo electrónico de phishing con una dirección URL para un archivo .hta, el cual inicia un script de PowerShell que descarga ransomware y un componente desconocido.

Solución: Se detecta el ransomware y se corrige automáticamente mediante una protección de endpoints, mientras que la funcionalidad de EDR ayuda a determinar el origen y otros elementos del ataque (por ejemplo, cambios en el registro, conexiones al servidor de C&C, etc.). El host se aísla rápidamente en el transcurso de la investigación y se configura un análisis de IoC y una respuesta automática para evitar ataques similares en el futuro.

Kaspersky Managed Detection and Response

La detección, priorización, investigación y respuesta totalmente administradas 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.com/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 **https://www.kaspersky.com/enterprise-security/edr-security-software-solution**

Noticias de amenazas cibernéticas: 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
Asociación con MSP: www.kaspersky.com/msp
msp@kaspersky.com

latam.kaspersky.com

Hemos pasado pruebas. Somos independientes. Somos transparentes. 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. Incorpore ciberseguridad para disfrutar un futuro más seguro.

Proven.
Transparent.
Independent.