Kaspersky Endpoint Detection and Response

Las empresas están mejorando su estrategia de seguridad para responder a las amenazas avanzadas y a los ciberataques modernos. Para los cibercriminales, los endpoints siguen siendo el principal objetivo, pero las amenazas actuales eluden las medidas de seguridad de endpoints tradicionales, interrumpen procesos fundamentales para la empresa que perjudican la productividad y aumentan los costes operativos.

Los retrasos cuestan dinero

Iniciar la recuperación una semana después de la detección de un incidente cuesta a las empresas un 200 % más que la respuesta inmediata.
Encuesta sobre riesgos de IT empresariales de Kaspersky Lab

Kaspersky EDR es ideal para organizaciones que deseen:

- Automatizar la identificación y respuesta ante amenazas sin interrumpir sus actividades
- Mejorar la visibilidad de endpoints y la detección de amenazas a través de tecnologías avanzadas, como aprendizaje automático (ML), sandbox, análisis de indicadores de compromiso (IOC) e inteligencia de amenazas
- Mejorar la seguridad con una solución empresarial fácil de usar para la respuesta ante incidentes
- Establecer procesos de búsqueda de amenazas, gestión de incidentes y respuesta unificados y eficaces

Mejora del cumplimiento:

La inteligencia de amenazas en tiempo real se comparte localmente a través de Kaspersky Private Security Network.

- Sin dependencia de la nube y flujo de datos de salida a través de la integración con KPSN.
- Todos los datos forenses se almacenan de manera centralizada en Kaspersky EDR en el entorno propio de la empresa.

Búsqueda activa de amenazas:

Si añaden Kaspersky Managed Protection, un servicio de búsqueda de amenazas que funciona las 24 horas del día, a una implementación de Kaspersky EDR, las empresas obtienen acceso a la investigación sobre amenazas globales. Además, los investigadores de amenazas de Kaspersky Lab pueden:

- Revisar los datos recopilados en el entorno de la empresa
- Notificar rápidamente al equipo de seguridad de la empresa si se detecta actividad maliciosa
- Proporcionar asesoramiento sobre cómo responder al problema y corregirlo

Información destacada

Respuesta adaptable ante amenazas

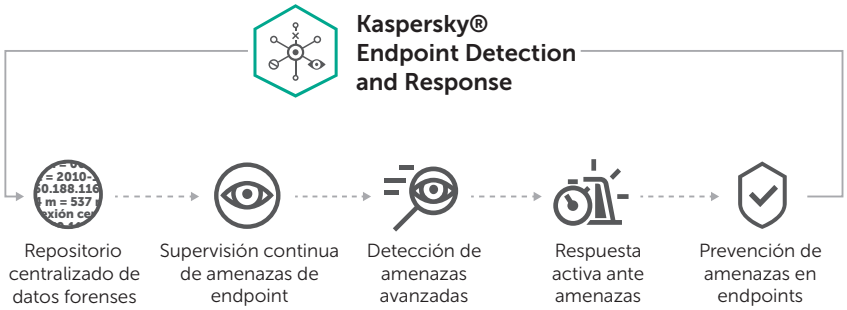
Kaspersky EDR incluye una amplia gama de respuestas automatizadas que ayudan a las empresas a evitar el uso de procesos de corrección tradicionales (como el borrado de datos o la repetición de la generación de imágenes) que pueden tener como resultado un costoso tiempo de inactividad y la pérdida de productividad.

Búsqueda proactiva de amenazas

Con la búsqueda rápida, que utiliza una base de datos centralizada, además de la búsqueda de indicadores de compromiso (IOC), Kaspersky EDR puede cambiar radicalmente el flujo de trabajo de seguridad. En lugar de tener que esperar a recibir alertas, su equipo de seguridad puede buscar amenazas de manera activa mediante al análisis proactivo de los endpoints para detectar anomalías y brechas de seguridad.

Interfaz web intuitiva

La interfaz de Kaspersky EDR, fácil de usar y basada en navegador, proporciona al personal de seguridad visibilidad y control unificados de: detección, investigación, prevención, alertas e informes. Como se puede supervisar y controlar una amplia gama de funciones a través de una única interfaz, su equipo de seguridad puede realizar las tareas de seguridad de manera más eficaz y eficiente, sin tener que alternar entre herramientas distintas y varias consolas.



Descubrimiento y contención rápido de amenazas avanzadas

Kaspersky Endpoint Detection and Response (Kaspersky EDR) ayuda a las empresas a detectar, investigar y responder con las siguientes ventajas:

- Mejora de la visibilidad de los endpoints
- Automatización de tareas de respuesta manual
- Potenciamiento de las capacidades de investigación

Además, es compatible con las soluciones de seguridad de endpoints tradicionales.

Kaspersky EDR ayuda a los equipos de seguridad, a realizar el control selectivo de un endpoint con la precisión de un especialista en ciberrespuesta. Con Kaspersky EDR, su organización puede:

- SUPERVISAR amenazas de manera eficiente, más allá del malware
- DETECTAR amenazas de manera eficaz con tecnologías avanzadas
- UNIFICAR los datos forenses de manera centralizada
- RESPONDER rápidamente 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.

Casos de uso:

- Búsqueda proactiva de pruebas de intrusiones, incluidos indicadores de compromiso (IOC), en toda la red en tiempo real
- Rápida detección y corrección de una intrusión antes de que el intruso pueda causar daños e interrupciones importantes
- Integración con productos SIEM para correlacionar las alertas y la actividad en el endpoint
- Validación de alertas y posibles incidentes detectados por otras soluciones de seguridad
- Rápida investigación y gestión centralizada de incidentes en miles de endpoints con un flujo de trabajo perfecto
- Automatización de operaciones rutinarias para minimizar las tareas manuales, liberar recursos y reducir la probabilidad de "sobrecarga de alertas"

Seguridad de endpoints avanzada

Kaspersky Lab demuestra nuestro continuo liderazgo en protección de endpoints con la combinación en una sola solución de cinco elementos fundamentales:

- Un potente motor antimalware de próxima generación con aprendizaje automático
- Detección y respuesta en endpoints (Kaspersky EDR)
- Un servicio de búsqueda de amenazas que funciona las 24 horas: Kaspersky Managed Protection
- Acceso a inteligencia de amenazas en tiempo real a través de Kaspersky Security Network
- Controles avanzados de endpoint (dispositivo/web/aplicación, cifrado y más)

Ampliación de la seguridad de endpoints tradicional

Como Kaspersky EDR es compatible con una amplia gama de productos de seguridad tradicionales de varios proveedores, también puede funcionar en paralelo a la seguridad de endpoints de una empresa y añadir:

- Funcionalidad de próxima generación para la detección y prevención avanzadas
- Procesos centralizados de investigación y respuesta

Además, la empresa no tendrá que sustituir su solución de seguridad actual.

Análisis de objetos en un entorno virtual aislado

Kaspersky EDR incluye un sandbox avanzado local que extrae automáticamente cualquier archivo en cualquier endpoint para realizar un análisis en profundidad. Proporciona a la empresa un Virus Lab interno sin tener que enviar datos fuera de la red.

Detección avanzada con aprendizaje mecánico

El motor de aprendizaje mecánico de Kaspersky EDR (Analizador de ataques dirigidos o TAA) crea una referencia del comportamiento de los endpoints.
Eso permite generar un registro histórico que se puede utilizar para descubrir cómo se ha producido una brecha. Además, al correlacionar los datos forenses, la inteligencia de amenazas y los veredictos del motor de seguridad, contribuye a detectar anomalías.

Beneficios comerciales en toda la empresa:

Reducción de costes

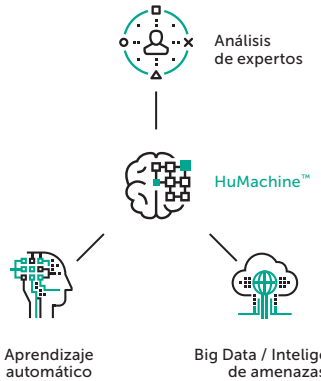
- Automatización de tareas manuales durante la detección y la respuesta ante amenazas
- Aceleración de la contención de amenazas para ahorrar dinero y recursos
- Liberación del personal de IT y de seguridad para otras tareas
- Reducción al mínimo de las interrupciones de la actividad durante las investigaciones

Aceleración del retorno de la inversión

- Flujo de trabajo eficiente
- Reducción del tiempo necesario para identificar y responder a las amenazas
- Mejora del cumplimiento (por ejemplo, PCI DSS) mediante la aplicación de registros de endpoint, revisión de alertas y documentación de los resultados de la investigación

Mitigación de los riesgos de ataque

- Eliminación de brechas de seguridad y reducción del "tiempo de espera" durante los ataques
- Simplificación del análisis de amenaza y la respuesta ante incidentes
- Ampliación de la seguridad existente con validación de amenazas



Kaspersky Lab Iberia
Ciberseguridad de empresa: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.lat/**
Noticias de seguridad de IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.es

© 2018 Kaspersky Lab Iberia, España. Todos los derechos reservados. Las marcas registradas y logos son propiedad de sus respectivos dueños.