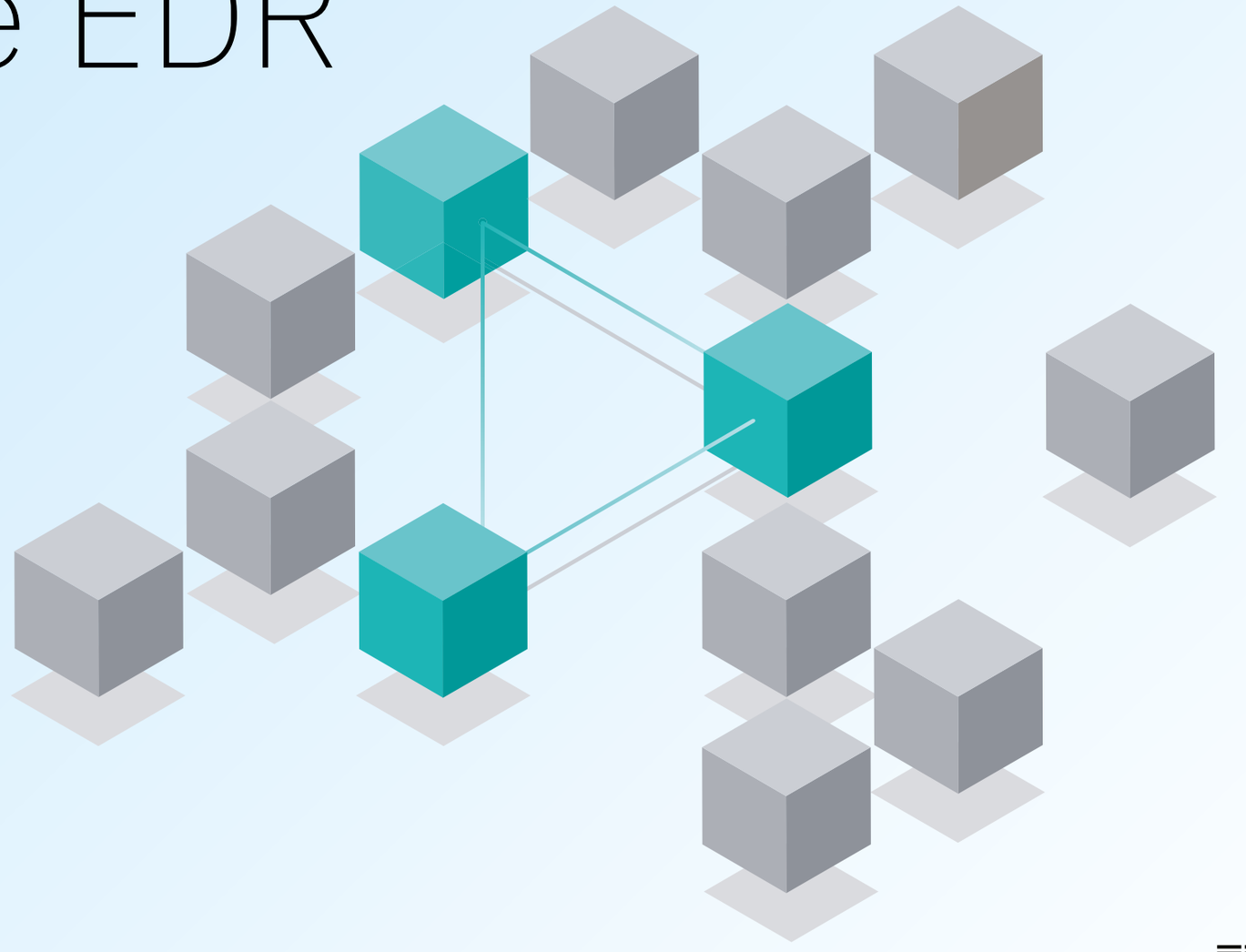
Manual del comprador de EDR

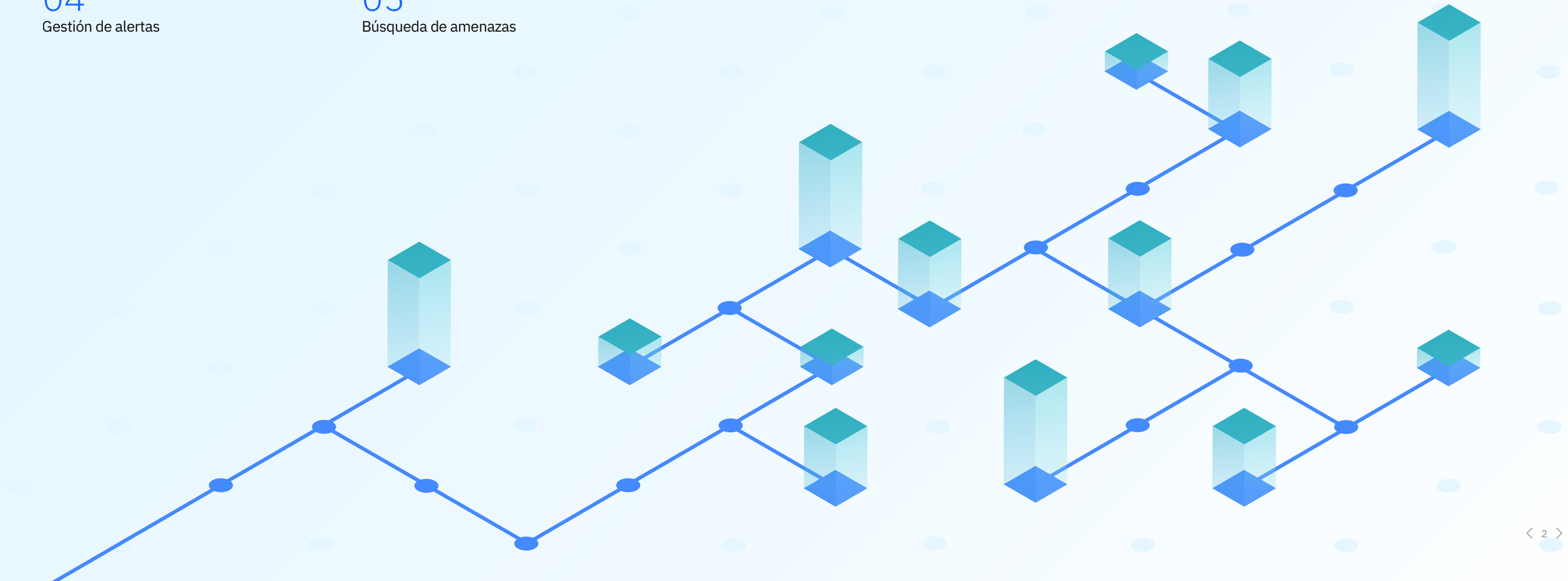
Cómo elegir la mejor solución de detección y respuesta de puntos de conexión para su empresa



REAQTA
an IBM Company

IBM

Contenido



01
Introducción

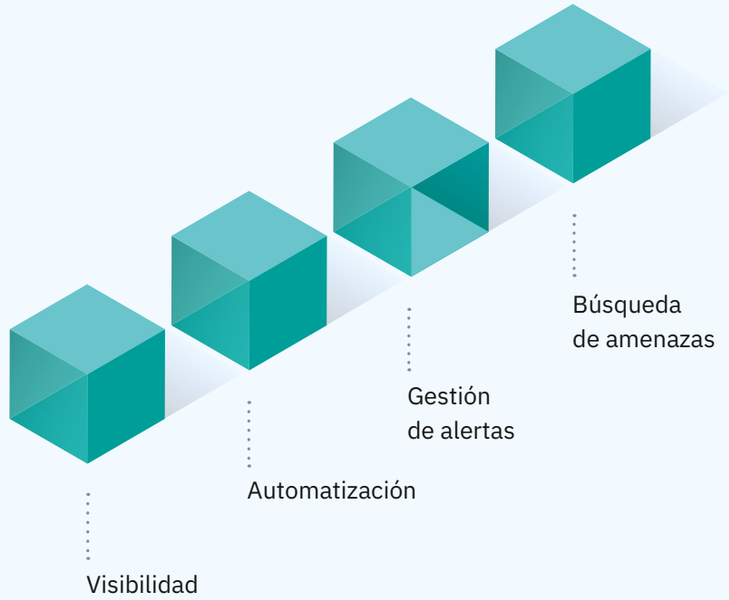
¿Qué es una solución de EDR y por qué la necesito?
En los últimos años, hemos sido testigos de una mayor proliferación e interconectividad de puntos de conexión y datos, además del auge de actividades maliciosas de agentes de amenaza. Estos factores han puesto en peligro la continuidad de organizaciones grandes y pequeñas. Cada vez más empresas son el blanco de ataques de ciberdelincuentes y estados nación.

Los métodos de protección tradicionales son eficaces con amenazas conocidas, pero vulnerables a técnicas de ataque sofisticadas y desconocidas, y no ofrecen visibilidad de los activos, que es uno de los principales impedimentos para proteger estos sistemas. Las habilidades de protección de punto de conexión especializadas suelen estar disponibles únicamente para las organizaciones más grandes o las que disponen de fondos suficientes. Además, como muchos ataques van a velocidad de máquina con diferentes piezas móviles, hemos llegado a una situación en la que a los equipos humanos que trabajan con soluciones de protección de puntos de conexión tradicionales les resulta imposible estar a la altura.

Una solución de detección y respuesta de puntos de conexión (EDR) bloquea y aísla el malware de forma proactiva y automática, mientras ofrece a los equipos de seguridad las herramientas adecuadas para hacer frente a estos retos. Una solución de EDR moderna puede garantizar la continuidad de la empresa al mitigar con eficacia las amenazas automatizadas y avanzadas que crecen a un ritmo acelerado, como los ataques de ransomware o sin archivos, sin aumentar las cargas de trabajo de los analistas y sin la ayuda de especialistas en seguridad altamente cualificados.

¿Le hace frente a algunos de estos retos?
- Soluciones insuficientes
- Poca visibilidad
- Falta de personal cualificado
- Exceso de alertas
- Amenazas latentes

Una solución de EDR moderna y eficaz comprende cuatro elementos fundamentales que analizaremos en los siguientes capítulos:



02

Visibilidad total del estado de su punto de conexión

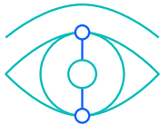
Uno de los principales obstáculos a la hora de proteger los puntos de conexión es la falta de visibilidad. Por eso, una solución de EDR moderna debe ofrecer visibilidad total y exhaustiva de las aplicaciones y los procesos en ejecución.

Cuando aparece una amenaza, se deben crear automáticamente alertas en tiempo real de su comportamiento mediante un seguimiento gráfico durante el desarrollo del ataque, lo que incluye correlación de MITRE ATT&CK para que los analistas tengan visibilidad total e información sobre lo que sucede.

Casi todas las soluciones de software de seguridad de punto de conexión funcionan con el sistema operativo, lo que crea un límite para el agente del punto de conexión. Esto restringe la capacidad y la visibilidad del agente al tiempo que consume más recursos informáticos. Tener un agente invisible que funciona al nivel del hipervisor no solo minimiza el uso de recursos, sino que también ofrece una visibilidad excepcional para controlar los comportamientos de los procesos sin que los atacantes puedan detectarlo.

En qué fijarse:

- Visibilidad total del punto de conexión
- Alertas en tiempo real
- Seguimiento
- Agente sin problemas
- Flujo de trabajo unificado



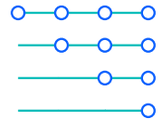
Preguntas para tener en cuenta:

→ ¿Ofrece su solución visibilidad total y exhaustiva de las aplicaciones y los procesos en ejecución?

→ Durante un ataque, ¿su solución le ofrece información relevante y en tiempo real para comprender mejor la amenaza?

→ Además de detectar una infracción y de avisarle, ¿su MSSP le ofrece respuesta y remediación integrales?

03
Automatización y facilidad de uso



Como se prevé que las amenazas y las superficies de ataque aumenten en 2022 y en años venideros, a muchas organizaciones les resulta difícil ir un paso por delante de los ciberdelincuentes. Una solución de EDR moderna debería disminuir la carga de trabajo creciente mediante la automatización inteligente y, además, debería ser fácil de usar para poder prescindir de especialistas en seguridad altamente cualificados.

Para sacar el máximo partido de una solución de EDR rápidamente, los compradores deben automatizar y simplificar. Con la automatización basada en IA, la mayor parte del trabajo queda en manos de los algoritmos al minimizar la interacción humana. Gracias a estos algoritmos de IA, usar el software es cada vez más fácil, y los equipos pueden ponerse manos a la obra rápidamente sin habilitaciones interminables.

Durante un ataque, los tiempos de respuesta son fundamentales: la investigación debe durar menos de un minuto para eliminar amenazas avanzadas antes de que perjudiquen su infraestructura.

Los compradores deben buscar una solución de EDR que pueda ejecutarse de forma autónoma y ofrecer funciones de detección y respuesta automatizadas. De esta forma, los analistas tendrán un panorama claro y en tiempo real de la evolución del ataque y podrán ofrecer remediación guiada para volver a la normalidad lo antes posible.

En qué fijarse:
- Detección autónoma
- Remediación guiada
- Análisis de agentes
- Tiempos de respuesta cortos
- Facilidad de uso

Preguntas para tener en cuenta:

→ ¿Se necesitan habilidades avanzadas para operar la solución de EDR?

→ Para reducir las cargas de trabajo de los analistas, ¿la solución de EDR funciona de forma autónoma?

→ En cuanto a los tiempos de respuesta, ¿las amenazas se analizan en el cloud o en el agente?

→ Si las amenazas se analizan en el cloud, ¿qué sucede si no hay conexión a internet?

04 Gestión de alertas

El diferenciador clave de una solución de EDR frente a los antivirus tradicionales es que un antivirus se basa en firmas disponibles para la detección y debe conocer la amenaza para bloquearla. En cambio, un EDR sigue un enfoque conductual para identificar malware y otras posibles amenazas por la forma en que se comportan en el punto de conexión. Además, a diferencia de un antivirus, los sistemas de EDR son ligeros por naturaleza y no necesitan actualizaciones frecuentes.

Por tanto, la IA que se usa en una solución de EDR moderna debe ser capaz de detectar amenazas rápidamente, con gran precisión y alta fidelidad para limitar al máximo el volumen de alertas y la carga de trabajo de los analistas. Los compradores deben informarse sobre las técnicas de aprendizaje automático y de IA utilizadas. En comparación con los motores de IA que se basan en modelos preentrenados y análisis para detectar amenazas, una solución de EDR que usa un modelo de aprendizaje inicial para identificar el comportamiento habitual de cada punto de conexión ofrece mayor precisión en las detecciones y alertas cuando hay situaciones anómalas.

Para reducir el tiempo de respuesta y disminuir el exceso de alertas para los analistas, una solución de EDR moderna debe contar con un sistema de gestión de alertas eficaz y basado en IA que pueda aprender de los analistas y aplicar sus decisiones de forma autónoma a la hora de manejar alertas en el día a día. Implementar un sistema de gestión de alertas basado en IA totalmente automatizado es fundamental para contrarrestar el exceso de alertas, reducir la pérdida de empleados y recuperar el control.

En qué fijarse:
- Alertas de alta fidelidad
- Aplicación de modelos de IA
- Prevención de exceso de alertas
- Gestión de alertas automatizada

Preguntas para tener en cuenta:

→ ¿Su solución le permite gestionar y cerrar alertas de forma automática?

→ ¿Los analistas ganan tiempo con su solución?

→ ¿Qué hace su solución para reducir los falsos positivos?

→ Si un empleado se marcha de la empresa, ¿cómo se retienen sus conocimientos de la infraestructura?

05
Búsqueda de amenazas

La búsqueda de amenazas es una parte esencial de una solución de EDR moderna y es necesaria para mantener un entorno seguro y sin peligros, ya que puede determinar con rapidez si hay nuevas amenazas en el entorno e identificar puntos vulnerables. La minería de datos le permite buscar y eliminar amenazas latentes que, de otro modo, podrían pasar inadvertidas y permanecer en un entorno durante meses, o incluso años, a la espera de que el atacante las use.

Por naturaleza, las amenazas en memoria y sin archivos son difíciles de localizar, y es aún más difícil seguirlas cuando los atacantes usan variaciones mientras se mueven dentro de una infraestructura grande. Una solución de EDR moderna debe automatizar las tareas de búsqueda y usar minería de datos. De esta forma, los equipos de seguridad pueden buscar de forma automática amenazas que compartan similitudes de comportamiento y funciones con otros incidentes, y ofrecer resultados en cuestión de segundos.

La flexibilidad en la búsqueda de amenazas es muy importante. Los compradores deben centrarse en una solución de EDR que ofrezca una gran biblioteca de cuadernos de estrategias de detección predefinidos que puedan implementarse al instante, así como de cuadernos de estrategias personalizados que puedan crearse con facilidad y sin conocimientos de scripts en situaciones específicas según las necesidades de seguridad de la organización.

La búsqueda de amenazas suele compararse con buscar una aguja en un pajar. Las búsquedas de un EDR deben ofrecer resultados exhaustivos y granulares en tiempo real. Para lograrlo, deben ser capaces de acceder a parámetros de búsqueda específicos y combinarlos de forma inclusiva o exclusiva. Para ayudar aún más a los analistas y ahorrarles tiempo, los resultados deben mostrarse en una interfaz gráfica de usuario sencilla que permita buscar de forma intuitiva cualquier evento, desde cualquier punto de conexión y en cualquier momento.

En qué fijarse:
- Búsqueda de amenazas latentes
- Búsqueda automatizada
- Creación de cuadernos de estrategias personalizados
- Que no se necesiten scripts
- Minería de datos
- Funcionalidades en tiempo real
- Información gráfica

Preguntas para tener en cuenta:

→ ¿Los usuarios pueden crear cuadernos de estrategias y estrategias de detección a medida?

→ ¿Puede automatizar los escenarios de búsqueda de amenazas?

→ ¿Ofrece información gráfica de una búsqueda de amenazas para acelerar el proceso de clasificación?

→ ¿Se necesitan conocimientos de scripts para crear cuaderno de estrategias?

Próximos pasos

Infórmese sobre IBM Security ReaQta y solicite una demostración.

IBM España, S.A.
Santa Hortensia, 26-28
28002 Madrid