DATASHEET

Bitdefender

GravityZone AI Visibility and Control

Reduzca continuamente la exposición ante las amenazas relacionadas con la IA. Disminuya el riesgo y la carga que conlleva la respuesta.

Los empleados ya utilizan herramientas de IA y la mayoría de las organizaciones no cuentan con una forma fiable de ver cuáles están en ejecución ni de clasificar y reducir la exposición al riesgo que supone cada una de ellas.

GravityZone AI Visibility and Control descubre la IA que se utiliza en los endpoints que usted administra, clasifica la exposición que conlleva cada herramienta y le ofrece las pruebas necesarias para decidir qué permitir, monitorizar o restringir.

Qué le ofrece AI Visibility and Control:

Asegure la adopción de la IA de su empresa para evitar filtraciones de datos

Un inventario centralizado descubre la IA que se utiliza en los endpoints que usted ya administra y le ayuda a identificar la shadow AI, para que sepa qué existe antes de decidir qué hacer al respecto.

Reducir los riesgos de IA que más importan

Los hallazgos se agrupan por categoría de riesgo y se clasifican por gravedad, cada uno vinculado a los usuarios y endpoints implicados, para que los equipos reducidos actúen en lo que realmente importa.

Gobernar la adopción de la IA sin añadir complejidad

Actúe basándose en esas pruebas aplicando el filtrado web, el control de aplicaciones y los controles de endurecimiento que ya tiene en su consola GravityZone, sin necesidad de ejecutar una herramienta independiente.

CÓMO FUNCIONA AI VISIBILITY AND CONTROL

1. Descubrir

Descubra la IA en uso gracias al agente de GravityZone que ya está en sus endpoints.

- ↳ LLM y chatbots
- ↳ Asistentes de IA
- ↳ Agentes de IA
- ↳ Servidores MCP
- ↳ Herramientas y capacidades
- ↳ Asistentes de programación
- ↳ Servicios SaaS con IA

2. Evaluar

Vea qué uso genera exposición real y qué merece su atención en primer lugar.

- ↳ Hallazgos clasificados por gravedad y prioridad
- ↳ Hallazgos vinculados a los usuarios y endpoints afectados
- ↳ Información sobre la última detección
- ↳ Pruebas seguras, sin recopilar contenido del prompt

3. Actuar

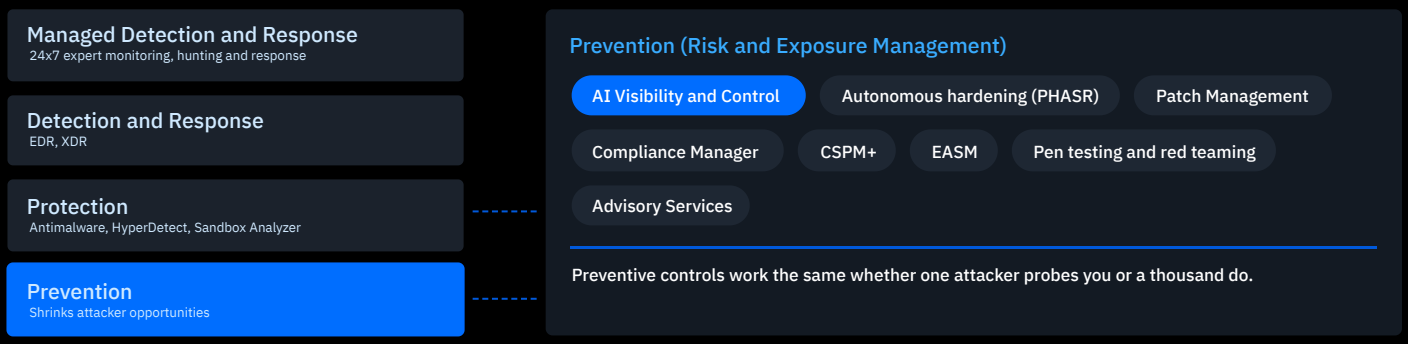
Actúe basándose en esas pruebas aplicando los controles que ya tiene en su consola GravityZone.

- ↳ Control de acceso web
- ↳ Control de aplicaciones
- ↳ Política de endurecimiento de endpoints
- ↳ Endurecimiento del agente basado en el comportamiento (con PHASR)

Un complemento para la plataforma GravityZone. El descubrimiento comienza utilizando los agentes ya implementados después de activar la licencia.

DATASHEET

Bitdefender



Cómo funciona AI Visibility and Control y qué lo hace diferente

↳ El descubrimiento se lleva a cabo desde el agente de GravityZone que ya está en sus endpoints y detecta herramientas de IA que no serían detectables a nivel de red, como los modelos locales.

↳ El producto ofrece una visibilidad amplia del uso de la IA: chatbots y LLM públicos, modelos locales, agentes, servidores MCP, asistentes de programación y servicios SaaS.

↳ Los hallazgos se agrupan por categoría de riesgo y muestran gravedad y prioridad, categoría de servicio, usuarios y endpoints afectados, origen y nivel de confianza, y fechas de primera y última detección.

↳ Las pruebas son seguras por diseño. Un hallazgo incluye lo necesario para respaldar una decisión sin recopilar contenido del prompt ni los datos que sus empleados introducen en las herramientas de IA.

↳ Cuando también se dispone de licencia de PHASR, el endurecimiento trata a un agente de IA como un actor autónomo. Un agente que necesita PowerShell puede conservar el acceso a él, mientras que el usuario humano en la misma máquina no, de modo que PHASR restringirá el acceso innecesario a PowerShell para la persona, pero no para los agentes de IA que se ejecutan en la máquina.

¿Por qué el descubrimiento comienza en el endpoint?

La mayoría del uso de la IA nunca cruza una puerta de enlace de red de forma reconocible. Los runtimes locales, los asistentes de programación del editor y los servidores MCP residen en el endpoint, donde GravityZone ya se ejecuta.

Asegure el uso de la IA sin bloquearla por defecto

Las restricciones generales detienen el trabajo útil y se sortean. Por el contrario, GravityZone restringe solo lo que genera riesgo real. Cuando se dispone de licencia de PHASR, el endurecimiento autónomo reduce el acceso arriesgado de cada usuario y de cada agente de IA a lo que realmente necesitan.

Adoptar la IA no tiene por qué significar perder visibilidad sobre ella.

Solicite una demostración de GravityZone AI Visibility and Control: Bitdefender.com/AIVC

Oficina central en Rumanía
Orhideea Towers
Calle Orhideelor 15A,
Distrito 6,
Bucarest 060071
T: +40 21 4412452

OFICINA CENTRAL EN ESTADOS UNIDOS
6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309 (Estados Unidos)
T: +1 954-776-6262