

GravityZone AI Visibility and Control

Diminuisce continuamente l'esposizione alle minacce legate all'IA. Riduci il peso e i rischi legati alla risposta.

I dipendenti già impiegano strumenti IA, ma la maggior parte delle aziende non ha un modo affidabile per capire quali siano in uso, né per classificarli e ridurre il rischio che ognuno di essi comporta.

GravityZone AI Visibility and Control individua le IA in uso sugli endpoint che gestisci, classifica il livello di rischio associato ad ogni strumento e ti dà le informazioni necessarie per decidere cosa consentire, monitorare o limitare.

Ecco cosa ti offre AI Visibility and Control:

Rendi sicura l'adozione dell'IA in azienda per prevenire violazioni di dati

Un inventario centralizzato individua le soluzioni IA in uso sugli endpoint che già gestisci, aiutandoti a scoprire la shadow IA, così sai cosa c'è prima di decidere come gestirlo.

Riduci i rischi legati all'IA che contano di più

I risultati sono raggruppati per categoria di rischio e classificati per gravità, oltre che correlati agli utenti e agli endpoint coinvolti, così anche dei team ridotti possono concentrarsi su ciò che conta davvero.

Gestisci l'adozione dell'IA senza aumentare la complessità

Intervieni sulla base di queste prove usando i controlli di filtraggio web, di controllo delle applicazioni e di rafforzamento della sicurezza già presenti nella tua console GravityZone, senza ricorrere a strumenti separati.

COME FUNZIONA AI VISIBILITY AND CONTROL

1. Individuazione

Scopri l'IA in uso, attraverso l'agente GravityZone già presente sui tuoi endpoint.

- ↳ LLM e chatbot
- ↳ Assistenti IA
- ↳ Agenti IA
- ↳ Server MCP
- ↳ Strumenti e abilità
- ↳ Assistenti di codifica
- ↳ Servizi SaaS basati sull'IA

2. Valutazione

Scopri quale uso porta a un'esposizione reale e a cosa dovresti prestare attenzione per primo.

- ↳ Risultati classificati per gravità e priorità
- ↳ Risultati correlati agli utenti e agli endpoint interessati
- ↳ Informazioni sull'ultima rilevazione
- ↳ Prove sicure, nessun contenuto di prompt

3. Intervento

Intervieni sulla base di queste prove usando controlli già presenti nella tua console GravityZone.

- ↳ Controllo dell'accesso al web
- ↳ Controllo delle applicazioni
- ↳ Policy di rafforzamento degli endpoint
- ↳ Rafforzamento degli agenti comportamentali (con PHASR)

Un'estensione della piattaforma GravityZone. La fase di individuazione inizia usando gli agenti già installati, dopo l'attivazione della licenza.

Managed Detection and Response
24x7 expert monitoring, hunting and response**Detection and Response**
EDR, XDR**Protection**
Antimalware, HyperDetect, Sandbox Analyzer**Prevention**
Shrinks attacker opportunities**Prevention (Risk and Exposure Management)****AI Visibility and Control**

Autonomous hardening (PHASR)

Patch Management

Compliance Manager

CSPM+

EASM

Pen testing and red teaming

Advisory Services

Preventive controls work the same whether one attacker probes you or a thousand do.

Come funziona AI Visibility and Control e in cosa si distingue

- La scoperta avviene tramite l'agente GravityZone già presente sui tuoi endpoint, individuando strumenti IA che non sarebbero rilevabili a livello di rete, come ad esempio dei modelli locali.
- Il prodotto offre un'ampia visibilità sull'utilizzo dell'IA: chatbot e LLM pubblici, modelli locali, agenti, server MCP, assistenti di codifica e servizi SaaS.
- I risultati sono raggruppati per categoria di rischio e riportano il livello di gravità e priorità, la categoria di servizio, gli utenti e gli endpoint interessati, la fonte e il grado di affidabilità, nonché la data di prima e ultima rilevazione.
- Le prove sono intrinsecamente sicure. I risultati sono sufficientemente attendibili da giustificare una decisione, senza dover raccogliere i contenuti dei prompt o i dati che il tuo personale inserisce negli strumenti di IA.
- Dove è presente anche una licenza per PHASR, il rafforzamento considera un agente IA come un attore a sé stante. Un agente che ha bisogno di PowerShell può continuare a usarlo, mentre l'utente umano sulla stessa macchina non ne ha bisogno: quindi PHASR limiterà l'accesso non necessario a PowerShell per l'utente umano, ma non per gli agenti IA in esecuzione sulla macchina.

Perché la scoperta inizia dall'endpoint

La maggior parte dell'utilizzo dell'IA non supera mai un gateway di rete in una forma riconoscibile. I runtime locali, gli assistenti di codifica degli editor e i server MCP risiedono sugli endpoint, dove GravityZone è già in esecuzione.

Utilizzo sicuro dell'IA senza blocchi predefiniti

Le restrizioni generiche ostacolano il lavoro utile e vengono aggirate. GravityZone limita solo ciò che comporta un rischio reale. Dove è presente una licenza per PHASR, il rafforzamento autonomo limita gli accessi a rischio per ogni utente e agente IA a ciò di cui hanno legittimamente bisogno.



Adottare l'IA non significa per forza perderla di vista.

Richiedi una demo di GravityZone AI Visibility and Control:
Bitdefender.com/AIVC

Bitdefender è un leader nella cybersecurity che offre soluzioni di prevenzione, rilevamento e risposta alle minacce in tutto il mondo. Proteggendo milioni di utenti, aziende ed enti governativi, Bitdefender è uno degli esperti di riferimento del settore per eliminare le minacce, proteggere la privacy, l'identità digitale e i dati, e consentire la resilienza informatica. Grazie ai suoi investimenti in ricerca e sviluppo, Bitdefender Labs scopre centinaia di nuove minacce ogni minuto e convalida circa miliardi di query sulle minacce ogni giorno. Fondata nel 2001, Bitdefender ha clienti in oltre 170 paesi con uffici in tutto il mondo. Per maggiori informazioni, visitare <https://www.bitdefender.com/it-it/>.

Per maggiori informazioni, visitare <https://www.bitdefender.com/it-it/>.

Tutti i diritti riservati. © 2026 Bitdefender.

Tutti i marchi, i nomi commerciali e i prodotti a cui si fa riferimento nel presente documento appartengono ai rispettivi proprietari.

Sede in Romania
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452

Sede in Italia
6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309
T: +1 954-776-6262