DATASHEET

Bitdefender

GravityZone AI Visibility and Control

Reduceți constant expunerea la amenințările asociate utilizării AI.
Reduceți riscurile și efortul necesar pentru răspuns.

Angajații folosesc deja instrumente AI, iar majoritatea organizațiilor nu dispun de o modalitate fiabilă de a vedea ce instrumente sunt utilizate și de a clasifica și reduce expunerea la riscurile asociate fiecăruia.

GravityZone AI Visibility and Control identifică instrumentele AI utilizate pe endpointurile pe care le administrați, clasifică gradul de expunere la riscuri asociat fiecăruia și vă oferă informațiile necesare pentru a decide ce să permiteți, să monitorizați sau să restricționați.

Ce vă oferă AI Visibility and Control:

Adoptați în siguranță soluții AI în compania dumneavoastră pentru a preveni brețele de securitate a datelor

Un inventar centralizat identifică instrumentele AI utilizate pe endpointurile pe care le administrați deja și vă ajută să descoperiți utilizarea neautorizată a instrumentelor AI (shadow AI), astfel încât să știți ce este prezent înainte de a decide ce măsuri luați.

Reduceți cele mai importante riscuri asociate AI

Rezultatele sunt grupate pe categorii de risc și clasificate în funcție de severitate, fiecare fiind asociat utilizatorilor și endpointurilor vizate, astfel încât echipele compacte să se concentreze pe ceea ce contează.

Gestionați adoptarea soluțiilor AI fără complexitate suplimentară

Acționați pe baza acestor informații folosind funcționalitățile de filtrare web, control al aplicațiilor și consolidare a securității disponibile deja în consola GravityZone, fără a fi necesar un instrument separat.

CUM FUNCȚIONEAZĂ AI VISIBILITY AND CONTROL

1. Descoperiți

Identificați instrumentele AI utilizate prin intermediul agentului GravityZone instalat deja pe endpointurile dumneavoastră.

- ↳ LLM-uri și chatboturi
- ↳ Asistenți AI
- ↳ Agenți AI
- ↳ Servere MCP
- ↳ Instrumente și skill-uri
- ↳ Asistenți de programare
- ↳ Servicii SaaS bazate pe AI

2. Evaluați

Vedeți ce tipuri de utilizare generează o expunere reală și ce necesită atenție cu prioritate.

- ↳ Rezultate clasificate în funcție de severitate și prioritate
- ↳ Rezultate asociate utilizatorilor și endpointurilor afectate
- ↳ Informații privind ultima detectare
- ↳ Dovezi sigure, fără conținutul prompturilor

3. Acționați

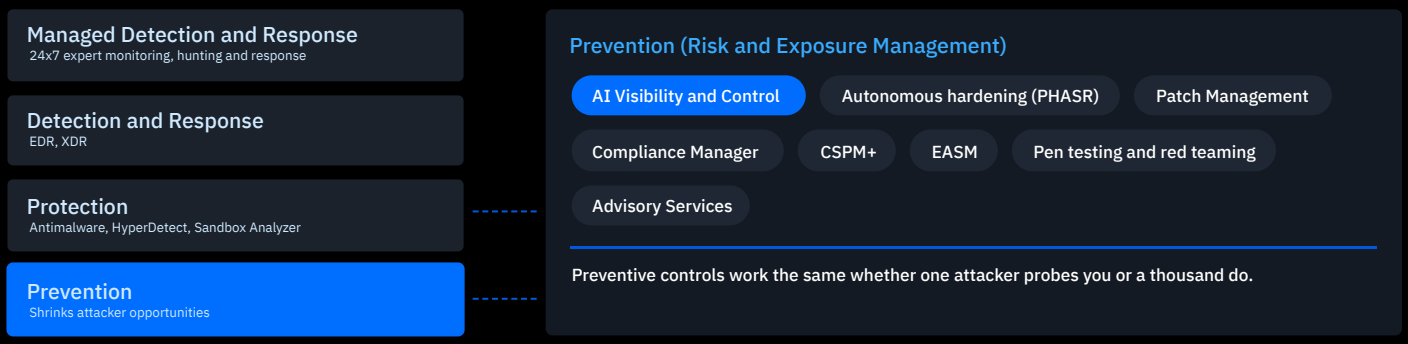
Acționați pe baza acestor informații folosind controalele disponibile deja în consola GravityZone.

- ↳ Controlul accesului web
- ↳ Controlul aplicațiilor
- ↳ Politică de consolidare a securității endpointurilor
- ↳ Consolidarea securității agenților pe baza comportamentului(cu PHASR)

Un add-on pentru platforma GravityZone. După activarea licenței, descoperirea începe prin intermediul agenților deja implementați.

DATASHEET

Bitdefender



Cum funcționează AI Visibility and Control și prin ce se remarcă

↳ Descoperirea are loc prin intermediul agentului GravityZone instalat deja pe endpointuri, ceea ce permite identificarea instrumentelor AI care nu ar putea fi detectate la nivelul rețelei, precum modelele locale.

↳ Produsul oferă vizibilitate extinsă asupra utilizării AI: chatboturi și LLM-uri publice, modele locale, agenți, servere MCP, asistenți de programare și servicii SaaS.

↳ Rezultatele sunt grupate pe categorii de risc și includ severitatea și prioritatea, categoria serviciului, utilizatorii și endpointurile afectate, sursa și nivelul de încredere, precum și datele primei și ultimei detectări.

↳ Dovezile sunt sigure prin design. Fiecare rezultat oferă suficiente informații pentru luarea unei decizii, fără a colecta conținutul prompturilor sau datele introduse de utilizatori în instrumentele AI.

↳ În cazul în care există și o licență PHASR, procesul de consolidare a securității tratează un agent AI ca pe o entitate distinctă. Un agent care are nevoie de PowerShell își poate păstra accesul la acesta, chiar dacă utilizatorul de pe aceeași mașină nu are nevoie de un astfel de acces; prin urmare, PHASR va restricționa accesul inutil al utilizatorului la PowerShell, dar nu și accesul agenților AI care rulează pe acel dispozitiv.

De ce descoperirea începe la nivelul endpointului

Majoritatea activităților care implică AI nu traversează niciodată un gateway de rețea într-o formă recognoscibilă. Mediile locale de execuție, asistenții de programare integrați în editoare și serverele MCP se află pe endpoint, unde GravityZone rulează deja.

Protejați utilizarea AI fără a o bloca în mod implicit

Restricțiile generale blochează activitățile utile și ajung să fie ocolite. GravityZone restricționează doar ceea ce generează riscuri reale. În cazul în care există o licență PHASR, procesul autonom de consolidare a securității limitează accesul riscant al fiecărui utilizator și agent AI la ceea ce îi este necesar în mod legitim.

Puteți adopta soluții AI fără a pierde vizibilitatea asupra utilizării lor.

Solicitați o demonstrație pentru GravityZone AI Visibility and Control: Bitdefender.com/AIVC

Bitdefender este un lider recunoscut în domeniul securității IT, care oferă soluții de prevenție, detecție și răspuns la incidente de securitate cibernetică. Milioane de sisteme folosite de oameni, companii și instituții guvernamentale sunt protejate de soluțiile companiei, ceea ce face Bitdefender unul dintre cei mai de încredere experți în combaterea amenințărilor informatice, în protejarea confidențialității, a identității digitale și datelor și în consolidarea rezilienței la atacuri. Ca urmare a investițiilor susținute în cercetare și dezvoltare, laboratoarele Bitdefender descoperă sute de noi amenințări informatice în fiecare minut și validează zilnic miliarde de interogări privind amenințările. Fondată în 2001, compania Bitdefender are clienți în peste 170 de țări și birouri pe toate continentele. Pentru mai multe informații, accesați https://www.bitdefender.ro.

Sediul din România
Orhideea Towers
Șoseaua Orhideelor,
nr. 15A,
sector 6,
București 060071
T: +40 21 4412452

Sediul din SUA
6301 NW 5th Way,
#4300,
Fort Lauderdale,
FL, 33309
T: +1 954-776-6262

Pentru mai multe informații, accesați https://www.bitdefender.ro.