DATASHEET

Bitdefender

GravityZone AI Visibility and Control

Continuously reduce AI threat exposure. **Cut response burden and risk.**

Employees are already using AI tools, and most organizations have no reliable way to see which ones are running and to rank and reduce the risk exposure each one carries.

GravityZone AI Visibility and Control discovers the AI in use across the endpoints you manage, ranks the exposure each tool carries, and gives you the evidence to decide what to allow, monitor or restrict.

What AI Visibility and Control gives you:

Secure your business' AI adoption to prevent data breaches

A centralized inventory discovers the AI in use across the endpoints you already manage, helping you uncover shadow AI, so you know what is present before deciding what to do about it.

Reduce the AI risks that matter most

Findings are grouped by risk category and ranked by severity, each tied to the users and endpoints involved, so lean teams act on what matters.

Govern AI adoption without adding complexity

Act on that evidence using the web filtering, application control and hardening controls already in your GravityZone console, with no separate tool to run.

HOW AI VISIBILITY AND CONTROL WORKS

1. Discover

Discover the AI in use, from the GravityZone agent already on your endpoints.

- ↳ LLMs and chatbots
- ↳ AI assistants
- ↳ AI agents
- ↳ MCP servers
- ↳ Tools and skills
- ↳ Coding assistants
- ↳ AI enabled SaaS services

2. Assess

See which usage creates real exposure, and what deserves attention first.

- ↳ Findings ranked by severity and priority
- ↳ Findings tied to affected users and endpoints
- ↳ Last seen information
- ↳ Safe evidence, no prompt content

3. Act

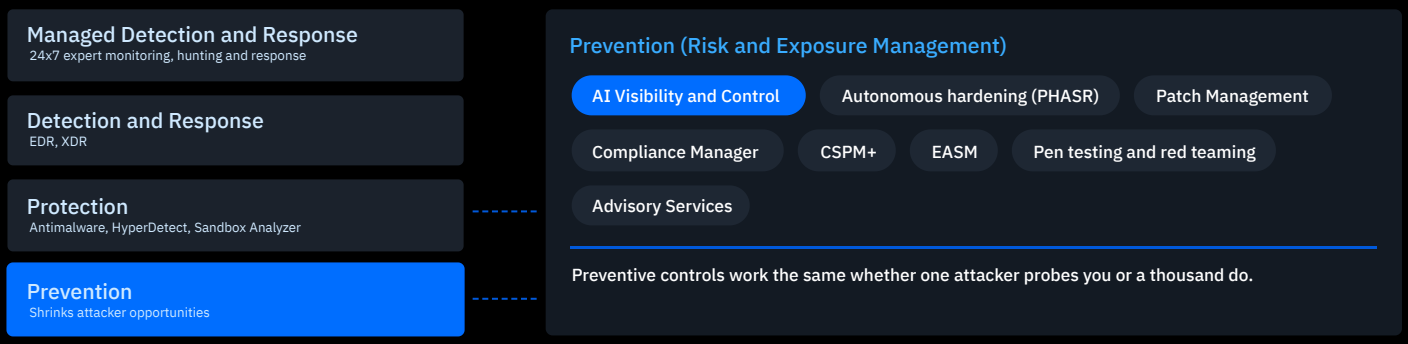
Act on that evidence using controls already in your GravityZone console.

- ↳ Web access control
- ↳ Application control
- ↳ Endpoint hardening policy
- ↳ Behavioral agent hardening (with PHASR)

An add-on to the GravityZone platform. Discovery starts using the agents already deployed after the license is activated.

DATASHEET

Bitdefender



How AI Visibility and Control works and how it stands out

↳ Discovery runs from the GravityZone agent already on your endpoints, uncovering AI tools that would not be detectable at the network level such as local models.

↳ The product delivers broad visibility into AI usage: Chatbots and public LLMs, local models, agents, MCP servers, coding assistants and SaaS services.

↳ Findings are grouped by risk category and carry severity and priority, service category, affected users and endpoints, source and confidence, and first and last seen dates.

↳ Evidence is safe by design. A finding carries enough to support a decision, without collecting prompt content or the data your people put into AI tools.

↳ Where PHASR is also licensed, hardening treats an AI agent as an actor in its own right. An agent that needs PowerShell can keep it while the human on the same machine does not, so PHASR will restrict unnecessary access to PowerShell for the human but not for AI agents running on the machine.

Why discovery starts on the endpoint

Most AI usage never crosses a network gateway in a recognizable form. Local runtimes, editor coding assistants, MCP servers live on the endpoint, where GravityZone already runs.

Secure AI usage without blocking by default

Blanket restrictions stop useful work and get routed around. GravityZone restricts only what creates real risk. Where PHASR is licensed, autonomous hardening narrows the risky access for each user and each AI agent to what they legitimately need.

Adopting AI does not have to mean losing sight of it.

Request a demo of GravityZone AI Visibility and Control.

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

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