DATASHEET

Bitdefender

GravityZone AI Visibility and Control

Risiken durch KI-Nutzung sichtbar machen. Kontrolle gewinnen. Sicherheitsteams entlasten.

KI-Nutzung ist bei vielen Mitarbeitenden längst Standard. Doch den meisten Unternehmen fehlt der Überblick, welche Tools im Einsatz sind, welche Risiken damit verbunden sind und wo sie zuerst handeln sollten.

GravityZone AI Visibility and Control erkennt KI-Nutzung auf den von Ihnen verwalteten Endpoints, bewertet die damit verbundenen Risiken und liefert die Grundlage, um gezielt zu entscheiden, was erlaubt, überwacht oder eingeschränkt werden soll.

Ihre Vorteile mit AI Visibility and Control:

KI-Nutzung sicher machen und Datenschutzverletzungen vorbeugen

Ein zentrales Inventar zeigt, welche KI-Tools auf den bereits verwalteten Endpoints genutzt werden. So decken Sie Schatten-KI auf und wissen, was in Ihrer Umgebung vorhanden ist, bevor Sie über die nächsten Schritte entscheiden.

Die wichtigsten KI-Risiken zuerst angehen

Ergebnisse werden nach Risikokategorie gruppiert und nach Schweregrad priorisiert. Dabei werden die jeweils betroffenen Benutzer und Endpunkte klar zugeordnet, sodass auch kleine Teams gezielt auf die wichtigsten Risiken reagieren können.

KI-Einsatz steuern, ohne zusätzliche Komplexität

Nutzen Sie die Internetfilter-, Anwendungssteuerungs- und Härtungsfunktionen, die bereits in Ihrer GravityZone-Konsole verfügbar sind. Ein separates Tool ist nicht erforderlich.

SO FUNKTIONIERT AI VISIBILITY AND CONTROL

1. Erkennen

Erkennen Sie KI-Nutzung über den GravityZone-Agenten, der bereits auf Ihren Endpoints installiert ist.

- ↳ LLMs und Chatbots
- ↳ KI-Assistenten
- ↳ KI-Agenten
- ↳ MCP-Server
- ↳ Tools und Skills
- ↳ Coding-Assistenten
- ↳ KI-gestützte SaaS-Dienste

2. Bewerten

Sehen Sie, welche KI-Nutzung echte Risiken schafft und wo zuerst Handlungsbedarf besteht.

- ↳ Nach Schweregrad und Priorität bewertete Feststellungen
- ↳ Zuordnung zu betroffenen Benutzern und Endpoints
- ↳ Informationen zum letzten Auftreten
- ↳ Sichere Nachweise ohne Prompt-Inhalte

3. Handeln

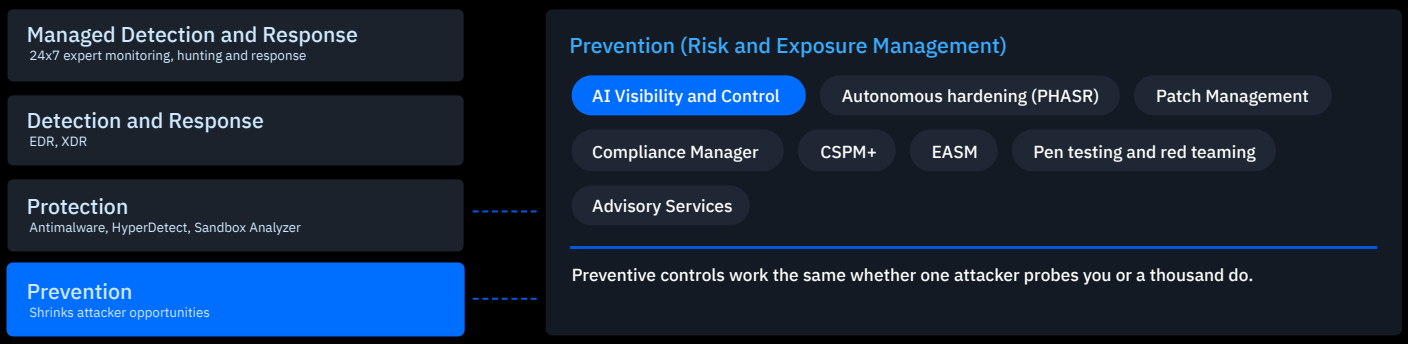
Setzen Sie Maßnahmen direkt über die Steuerungsfunktionen um, die bereits in Ihrer GravityZone-Konsole vorhanden sind.

- ↳ Internetzugangssteuerung
- ↳ Anwendungssteuerung
- ↳ Richtlinien zur Endpoint-Härtung
- ↳ Verhaltensbasierte Härtung (mit PHASR)

Ein Add-on für die GravityZone-Plattform. Nach der Aktivierung der Lizenz startet die Erkennung über die bereits installierten Agenten.

DATASHEET

Bitdefender



So schafft AI Visibility and Control Transparenz und Kontrolle

↳ Die Erkennung erfolgt über den GravityZone-Agenten, der bereits auf Ihren Endpoints installiert ist. So werden auch KI-Tools sichtbar, die auf Netzwerkebene nicht erkennbar wären, so etwa lokale Modelle.

↳ Die Lösung bietet umfassende Transparenz über KI-Nutzung: Chatbots und öffentliche LLMs, lokale Modelle, Agenten, MCP-Server, Coding-Assistenten und SaaS-Dienste.

↳ Ergebnisse werden nach Risikokategorie gruppiert und enthalten Schweregrad und Priorität, Servicekategorie, betroffene Benutzer und Endpoints, Quelle und Konfidenz sowie Datum des ersten und letzten Auftretens.

↳ Nachweise sind von Grund auf sicher konzipiert. Jedes Ergebnis liefert genug Kontext für eine fundierte Entscheidung, ohne Prompt-Inhalte oder Daten zu erfassen, die Ihre Mitarbeitenden in KI-Tools eingeben.

↳ Wenn PHASR ebenfalls lizenziert ist, behandelt die Härtung KI-Agenten als eigenständige Akteure. Ein Agent, der PowerShell benötigt, kann weiter darauf zugreifen, während der Benutzer auf demselben Gerät keinen Zugriff erhält. So schränkt PHASR unnötigen PowerShell-Zugriff für den Benutzer ein, nicht jedoch für KI-Agenten, die auf demselben Gerät ausgeführt werden.

Warum die Erkennung am Endpoint beginnt

Ein Großteil der KI-Nutzung ist auf Netzwerk-Gateways nicht eindeutig erkennbar. Lokale Laufzeitumgebungen, Coding-Assistenten in Editoren und MCP-Server befinden sich direkt auf dem Endpoint, auf dem GravityZone bereits ausgeführt wird.

KI-Nutzung absichern, ohne sie pauschal zu blockieren

Pauschale Einschränkungen behindern produktive Arbeit und werden oft umgangen. GravityZone schränkt nur das ein, was tatsächlich Risiko schafft. Ist PHASR lizenziert, reduziert autonome Härtung riskante Zugriffe für jeden Benutzer und jeden KI-Agenten auf das, was tatsächlich benötigt wird.

Wer KI einführt, muss nicht den Überblick verlieren.

Jetzt Demo zu GravityZone AI Visibility and Control anfordern: Bitdefender.com/AIVC

Als führender Anbieter von Cybersicherheitslösungen bietet Bitdefender Lösungen zur Prävention, Erkennung und Bereinigung von Bedrohungen. Millionen von Verbrauchern, Unternehmen und staatlichen Organisationen vertrauen auf das Expertenwissen von Bitdefender, wenn es um die Bekämpfung von Cybergefahren, den Schutz von Daten, digitale Identitäten und Privatsphäre und den Aufbau von Cyberresilienz geht. Bitdefenders umfangreiche Investitionen in Forschung und Entwicklung zahlen sich aus: So entdecken die Bitdefender Labs Hunderte neue Bedrohungen pro Minute und prüfen mehrere Milliarden Bedrohungsabfragen pro Tag. Bitdefender wurde 2001 gegründet, betreut Kunden in über 170 Ländern und ist weltweit mit Niederlassungen vertreten. Weitere Informationen finden Sie unter https://www.bitdefender.de.

Weitere Informationen erhalten Sie unter https://www.bitdefender.com/de-de/.

Hauptsitz Rumänien
Orhideea Towers
15A Orhideelor Road
6th District
Bukarest, 060071
T: +40 21 4412452

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