DATASHEET

Bitdefender

GravityZone AI Visibility and Control

Réduisez en continu l'exposition aux menaces IA et la charge de réponse

Les employés utilisent déjà des outils d'IA, mais la plupart des organisations ne disposent d'aucun moyen fiable de savoir de quels outils il s'agit. Elles ne peuvent pas non plus classer et réduire les risques associés à chacun d'eux.

GravityZone AI Visibility and Control identifie les outils d'IA utilisés sur les endpoints que vous gérez, évalue les risques associés et vous fournit les informations nécessaires pour décider lesquels autoriser, surveiller ou restreindre.

Avec GravityZone AI Visibility and Control, vous pouvez :

Sécuriser l'adoption de l'IA pour prévenir les fuites de données

Un inventaire centralisé répertorie les outils utilisés sur les endpoints que vous gérez déjà, pour vous aider notamment à repérer ceux qui relèvent de l'IA fantôme. Ainsi, vous pouvez décider en toute connaissance de cause de ce qu'il faut en faire.

Réduire les principaux risques liés à l'IA

Regroupés par catégorie de risque, les résultats sont classés en fonction de leur niveau de gravité et des utilisateurs et endpoints concernés, pour que les équipes aux moyens limités traitent d'abord les risques les plus importants.

Gérer l'adoption de l'IA sans compliquer vos opérations

Vous pouvez tirer parti des informations fournies en vous appuyant sur le filtrage Web, le contrôle des applications et les dispositifs de durcissement déjà disponibles dans votre console GravityZone, sans faire appel à un outil distinct.

LE FONCTIONNEMENT DE GRAVITYZONE AI VISIBILITY AND CONTROL

1. Découvrir

Découvrez les outils d'IA utilisés, grâce à l'agent GravityZone déjà installé sur vos endpoints

- ↳ LLM et chatbots
- ↳ Assistants IA
- ↳ Agents AI
- ↳ Serveurs MCP
- ↳ Outils et skills
- ↳ Assistants de codage
- ↳ Services SaaS reposant sur l'IA

2. Évaluer

Faites le point sur le risque réel d'exposition et sur ce que vous devez traiter en premier.

- ↳ Résultats classés par niveau de gravité et de priorité
- ↳ Résultats liés aux utilisateurs et endpoints concernés
- ↳ Informations sur les dernières utilisations
- ↳ Preuves fiables, pas de contenu issu des prompts

3. Agir

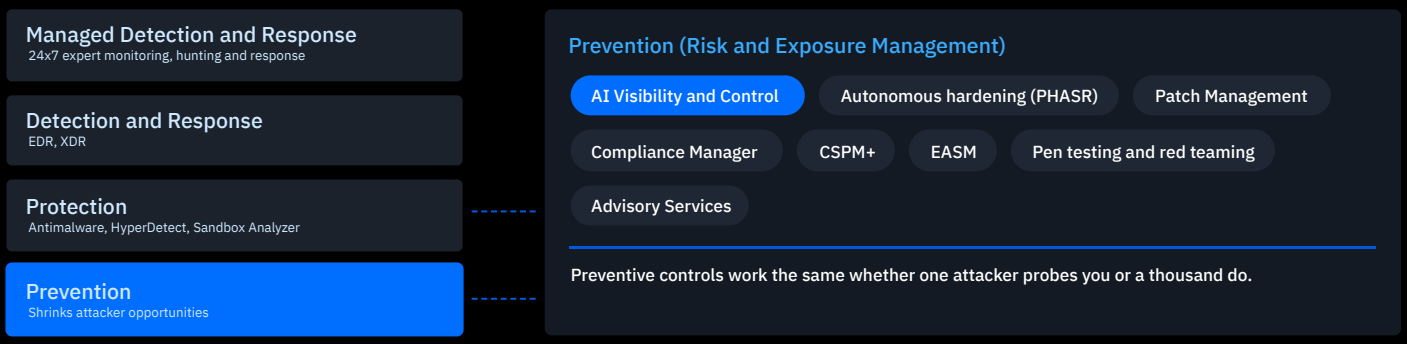
Tirez parti des informations fournies en vous appuyant sur les dispositifs déjà disponibles dans votre console GravityZone.

- ↳ Contrôle de l'accès au Web
- ↳ Contrôle des applications
- ↳ Politique de durcissement des endpoints
- ↳ Durcissement des agents en fonction du comportement (avec PHASR)

Module complémentaire à ajouter à la plateforme GravityZone. Après l'activation de la licence, la découverte commence à l'aide des agents déjà déployés.

DATASHEET

Bitdefender



Son fonctionnement et ce qui le distingue

↳ La découverte s'effectue via l'agent GravityZone déjà présent sur vos endpoints, permettant d'identifier des outils d'IA qui ne seraient pas détectables au niveau du réseau, tels que les modèles exécutés localement.

↳ Le produit offre une excellente visibilité sur l'utilisation de l'IA dans son ensemble : chatbots et LLM publics, modèles locaux, agents, serveurs MCP, assistants de codage et services SaaS.

↳ Les résultats sont regroupés par catégorie de risque et indiquent le niveau de sévérité et de priorité, la catégorie de service, les utilisateurs et endpoints affectés, la source et le niveau de confiance, ainsi que les dates de première et de dernière détection.

↳ Les renseignements sont sûrs par nature. Chaque résultat donne suffisamment d'informations pour éclairer votre décision, sans s'appuyer sur le contenu des prompts ou sur les données saisies par vos collaborateurs dans les outils d'IA.

↳ Lorsqu'une licence PHASR est également active, le durcissement considère l'agent d'IA comme un acteur à part entière. Si un agent a besoin de PowerShell, il peut conserver cet accès tandis que PHASR le restreint pour l'utilisateur sur la même machine lorsqu'il n'est pas nécessaire.

Pourquoi la découverte commence-t-elle sur les endpoints ?

La plupart des usages de l'IA ne dépassent jamais la passerelle réseau sous une forme reconnaissable. Les environnements d'exécutions locaux, les assistants de codage des éditeurs et les serveurs MCP se trouvent sur l'endpoint, qui est déjà couvert par GravityZone.

Sécurisez l'utilisation de l'IA sans la bloquer par défaut

Les restrictions généralisées entravent le travail et finissent par être contournées. GravityZone cible uniquement les risques réels. Avec PHASR, le durcissement autonome limite les accès à risque de chaque utilisateur et agent d'IA à ce dont ils ont réellement besoin.

Il est possible d'adopter l'IA sans en perdre le contrôle.

Demandez une démonstration de GravityZone AI Visibility and Control : bitdefender.com/AIVC

Leader mondial de la cybersécurité, Bitdefender fournit des solutions de pointe en matière de prévention, de détection et de réponse aux menaces. Protégeant des millions d'environnements de particuliers, d'entreprises et de gouvernements, Bitdefender est l'un des experts les plus fiables de l'industrie pour l'élimination des menaces, la protection de la vie privée, de l'identité numérique et des données, et la cyber-résilience. Grâce à des investissements importants dans la recherche et le développement, les Bitdefender Labs découvrent des nouvelles menaces chaque minute et répondent des milliards de requêtes de menaces par jour. Fondée en 2001, Bitdefender a des clients dans plus de 170 pays et possède des bureaux dans le monde entier. Pour plus d'informations, rendez-vous à l'adresse suivante : https://www.bitdefender.com/fr-fr/

Pour plus d'informations, rendez-vous sur : https://www.bitdefender.com/fr-fr/.

Siège en Roumanie
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T : +40 21 4412452

Siège aux États-Unis
6301 NW 5th Way,
#4300,
Fort Lauderdale
FL, 33309
Tél. : +1 954-776-6262