

Sécurité de l'IA

Sécurisez les interactions IA entre utilisateurs, applications et agents.



AVANTAGES CLÉS

-  **Découvrez et classez toute l'activité liée à l'IA**
Découvrez chaque application et agent IA au sein de votre organisation.
-  **Appliquez des contrôles en ligne**
Appliquez des politiques en temps réel au niveau des prompts, sorties, API et actions des agents.
-  **Protégez les applications IA et les agents au moment de l'exécution**
Bloquez les attaques spécifiques à l'IA et appliquez des politiques basées sur les intentions et comportement.

Défi

L'IA transforme le fonctionnement des entreprises, mais elle introduit des risques que les outils de sécurité traditionnels ne peuvent pas traiter. L'utilisation des IA non managées, la fuite de données sensibles via des prompts, la manipulation de modèles et les agents autonomes créent des angles morts qui exposent les organisations et les rendent non conformes.

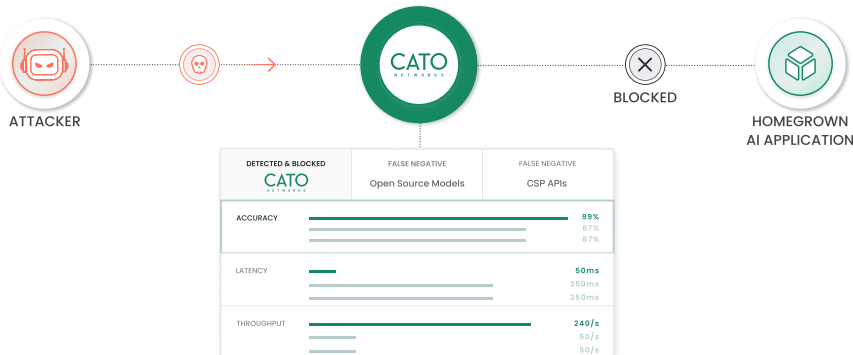
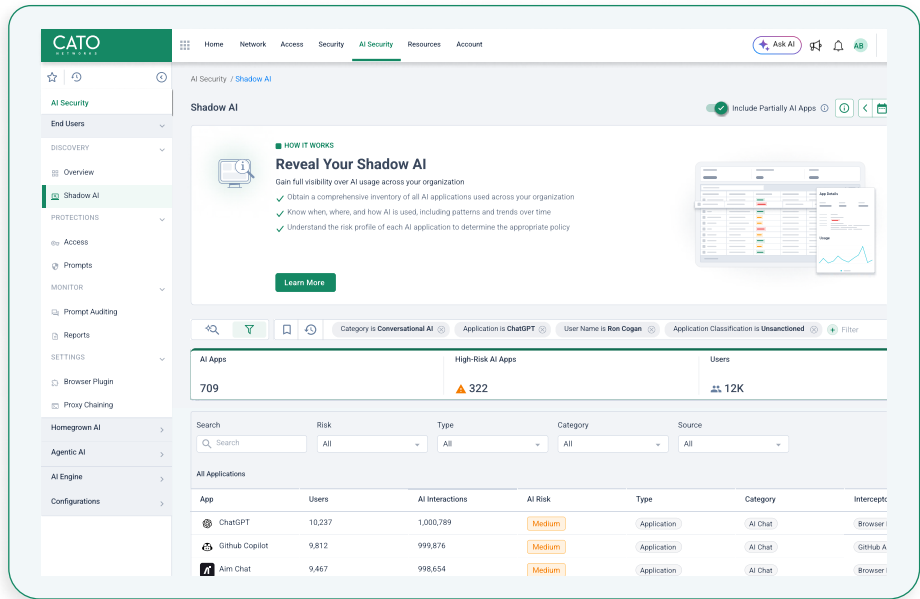
Solution

Cato IA Security sécurise et gouverne chaque interaction avec l'IA, de l'utilisation d'IA tierce aux applications d'IA développées en interne, en passant par les agents autonomes. Une plateforme avec l'ensemble des capacités de sécurité via l'IA, couvrant la découverte, la gouvernance, la protection des données et la défense en temps réel pour chaque interaction avec l'IA.

Sécurisez l'IA que vous utilisez, développez et exécutez

Découvrez et gouvernez l'utilisation de l'IA

Identifiez toutes les applications d'IA utilisées dans votre organisation. Obtenez une visibilité complète sur le Shadow AI, appliquez des politiques d'accès et de prompt, et protégez les données sensibles partagées avec les services d'IA grâce à des contrôles intégrés.

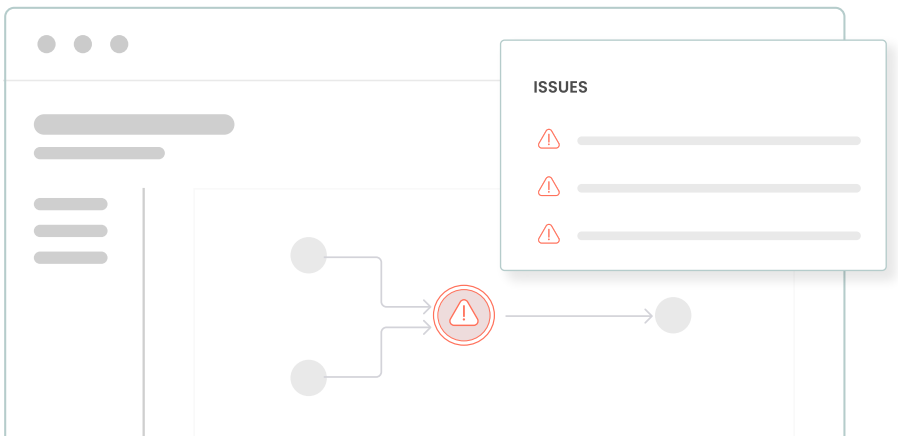


Protégez les applications d'IA développées en interne

Détectez et bloquez l'injection de prompts, l'exfiltration de données et les payloads malveillants avec des garde-fous en temps réel. Déployez via AI Gateway, proxy, API ou Outpost on-prem pour protéger toute application IA dans n'importe quel environnement.

Protégez les agents IA que vous créez et exécutez

Obtenez une visibilité sur les agents IA opérant dans votre environnement, y compris les serveurs MCP et les workflows des agents. Surveillez les interactions entre agents, modèles et outils pour maintenir une supervision à mesure que votre empreinte IA agentique se développe.



Principaux cas d'usage



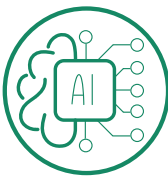
Découverte du Shadow AI

Identifiez toutes les applications et modèles d'IA en cours d'utilisation, autorisés ou non, avec classification des risques.



Protection des données liées à l'IA

Appliquez des politiques aux prompts pour empêcher les modèles d'IA d'atteindre les données sensibles, les informations personnelles et les secrets de l'entreprise.



Sécurité de l'IA agentique

Identifiez et contrôlez les agents IA, les serveurs MCP et les workflows autonomes à travers toute l'entreprise.



Sécurité d'exécution des applications IA

Garde-fous d'exécution pour les applications IA développées en interne contre les injections de prompt et les attaques de modèle.

Reconnaissance
de l'industrie



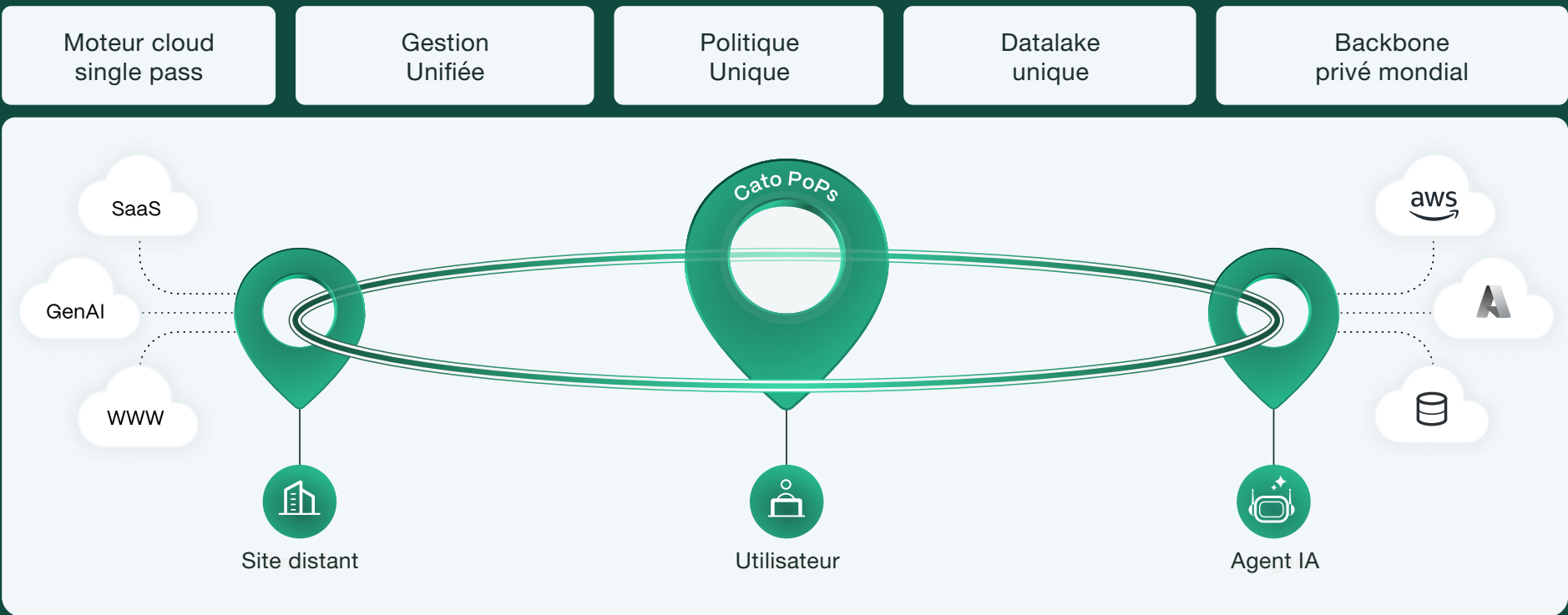
TRISM IA agentique
(Septembre 2025)

Gartner®

Gartner® Magic Quadrant™
2025 pour les plateformes SASE

La plateforme SASE de Cato

Commencez la transformation de votre réseau et de votre sécurité là où les besoins sont les plus urgents. Vous exploiterez ensuite toute la puissance du Cato SASE Cloud : conçu nativement pour le SASE auto-optimisé avec un moteur single pass, un datalake unique et une application uniforme des politiques.



À propos de Cato Networks

Cato Networks, leader du SASE et de la sécurité de l'IA, fournit un accès sécurisé et Zero Trust partout à des milliers de clients dans le monde. Conçue pour les organisations fonctionnant sur tous les environnements cloud et hybrides, la plateforme Cato unifie le réseau, la sécurité et l'accès, fournissant cela comme des capacités élastiques et modulaires que les organisations peuvent facilement adopter et développer au fil du temps. Cato combine le Cato Cloud, un réseau mondial conçu nativement pour le SASE, avec une expérience opérationnelle simplifiée, le tout livré via une plateforme robuste et assistée par l'IA. Avec Cato, les organisations se modernisent en toute confiance, opèrent avec une plus grande résilience et innovent plus rapidement, sans complexité ni risque supplémentaires.