LAZAR SOFT

Expert Partner
ManageEngine

FICHE SOLUTION · GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

ManageEngine SecureAI

Chaque agent IA gouverné, chaque appel sécurisé.

SecureAI découvre vos agents IA, modèles et serveurs MCP, donne un responsable à chaque agent, certifie ses accès et fait appliquer vos règles d'accès et de protection des données à chaque appel, via une passerelle MCP.

Copilot Studio · Microsoft Foundry · Gemini Enterprise · Zia · Anthropic Claude · GitHub Copilot · Serveurs MCP

TROIS ÉDITIONS · SUR SITE

Évaluation · Gratuite · Licence annuelle

Tarif éditeur **de 50 € à 21 € par agent et par an**, selon le palier. Détail en page 5.

45 jours
D'ESSAI COMPLET, SANS CARTE BANCAIRE

10 agents
COUVERTS PAR L'ÉDITION GRATUITE

Agent · MCP
CHAQUE APPEL CONTRÔLÉ ET JOURNALISÉ

DLP
BLOCAGE OU MASQUAGE DES DONNÉES SENSIBLES

LAZAR SOFT
Distributeur & intégrateur ManageEngine en France

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com

Un agent IA qui a des accès est une identité. Gouvernez-le comme tel.

Ce qu'est SecureAI

SecureAI est la plateforme de sécurité et de gouvernance des agents IA de ManageEngine. Elle recense les agents, modèles et serveurs MCP présents sur vos plateformes d'IA, rattache chaque agent à un responsable humain, certifie ce qu'il peut atteindre et fait respecter ces décisions à chaque appel, grâce à une passerelle MCP. ManageEngine la présente comme le composant de sécurité et de gouvernance de l'IA agentique d'AD360, sa suite de gestion des identités et des accès.

Les risques qu'elle traite

- **Exposition de données invisible :** des données sensibles transitent sans protection dans les échanges avec l'IA.
- **Prolifération des privilèges :** des agents aux accès excessifs élargissent le rayon d'impact potentiel.
- **Accès aux outils non surveillés :** des appels d'outils non gouvernés peuvent déclencher des actions non autorisées.
- **Agents orphelins :** un agent sans responsable crée des angles morts de supervision et de responsabilité.
- **Erreurs de configuration :** des failles de configuration fragilisent la posture de sécurité de l'IA.

> **94 % des répondants voient dans l'IA le principal moteur de changement en cybersécurité. 87 % citent les vulnérabilités liées à l'IA comme le risque cyber qui a le plus progressé.**
>
> World Economic Forum, Global Cybersecurity Outlook 2026

PLATEFORMES DÉCOUVERTES

Copilot Studio · Microsoft Foundry · Gemini Enterprise Agent Platform · Zia · Microsoft 365 · Google Workspace

ÉVALUATION DES RISQUES

Anthropic Claude · Google Gemini · GitHub Copilot

MODE DE DÉPLOIEMENT

Sur site — SERVEUR WINDOWS

Web — CONSOLE

PRÉREQUIS SYSTÈME

Installeur Windows 64 bits
Windows Server 2012 et versions ultérieures
Windows 10 et versions ultérieures
Navigateurs Mozilla Firefox, Google Chrome, Microsoft Edge

Le périmètre couvert — trois temps, une seule console

DÉCOUVRIR

- Découverte multiplateforme des agents, modèles et serveurs MCP
- Évaluation des risques IA (AI-SPM)

GOUVERNER

- Un responsable pour chaque agent
- Graphe des accès
- Habilitations et certification des accès

PROTÉGER

- Passerelle MCP
- Protection des données sensibles (DLP)
- Visibilité en exécution et audit

02 — LES FONCTIONNALITÉS

Découvrir, gouverner, protéger : ce que fait SecureAI.

Découverte multiplateforme des agents IA

Agents, modèles et serveurs MCP sont recensés dans un même inventaire : Copilot Studio, Microsoft Foundry, Gemini Enterprise Agent Platform et Zia. Les fournisseurs d'identité Microsoft 365 et Google Workspace sont aussi analysés. Les agents sans responsable, très privilégiés ou hors du registre MCP approuvé sont signalés.

Un responsable pour chaque agent

Chaque agent IA est rattaché à un responsable humain qui en répond. Des politiques d'attribution désignent automatiquement un responsable pour chaque nouvel agent découvert.

Graphe des accès

Tout ce qu'un agent peut atteindre, dans une seule vue : identités, rôles, permissions, politiques, mémoire, garde-fous, outils, sources de connaissance, rôles IAM et autres agents qu'il contrôle. Les réviseurs voient le chemin d'accès complet avant de valider ou de révoquer.

Habilitations et certification des accès

Les habilitations des agents sont gouvernées et le périmètre de revue est défini par des modèles d'accès. Demandes de revue et campagnes de certification permettent aux réviseurs d'approuver ou de révoquer, avec un historique conservé pour les audits.

Évaluation des risques IA (AI-SPM)

Les comptes d'entreprise Anthropic Claude, Google Gemini et GitHub Copilot sont évalués sur la sécurité des clés d'API, les identités et accès, la journalisation, les accès réseau, les intégrations tierces et les données. Le score de risque (faible, moyen ou élevé) se suit dans le temps et s'exporte.

Passerelle MCP

Un point de contrôle unique entre les agents et les serveurs MCP. Les politiques s'appliquent selon l'identité, l'horaire, l'adresse IP et la localisation, le serveur, l'outil ou le type d'outil. Plusieurs passerelles peuvent coexister, chacune avec son URL, sur un registre de serveurs partagé.

Protection des données sensibles (DLP)

Les entrées et sorties des outils MCP sont inspectées. Le contenu qui correspond à vos règles est bloqué, ou masqué par un texte de remplacement pendant que le reste de la requête continue. Les règles se ciblent par identité, serveur, outil, horaire ou localisation.

Visibilité en exécution et audit

Chaque appel MCP est journalisé : heure, agent, outil, décision. Les rapports montrent l'usage des agents et des outils MCP, la latence des serveurs, les serveurs inactifs, les erreurs et les décisions de politique.

Une console pour chaque acteur, de la direction à l'exploitation

RSSI

- Réduire le risque lié à l'IA et renforcer la supervision sécurité à mesure que l'adoption de l'IA s'étend.

ADMINISTRATEURS

- Découvrir les agents, désigner leurs responsables et appliquer les politiques, quel que soit le fournisseur d'IA.

ÉQUIPE SECOPS

- Repérer les agents à haut risque et suivre les violations de politique ainsi que l'activité MCP.

Cadres de référence : l'éditeur indique des contrôles alignés sur l'OWASP, MITRE ATLAS, le règlement européen sur l'IA (EU AI Act), le NIST AI RMF et AI TRiSM.

Trois raisons de choisir SecureAI

01 · VISIBILITÉ SUR LE PARC IA

- Savoir où se situe le risque IA dans votre environnement et prioriser ce qui doit être traité.

02 · DES ACCÈS IA ATTRIBUÉS

- Des accès d'agents qui ont un responsable, sont revus et restent alignés sur les besoins de l'entreprise.

03 · DES ÉCHANGES PROTÉGÉS

- Moins d'accès non autorisés et d'exposition de données sensibles dans les échanges entre agents et serveurs MCP.

Chaque appel contrôlé avant d'atteindre vos outils.

La passerelle MCP de SecureAI se place entre vos agents IA et les serveurs MCP qu'ils appellent. Chaque requête est confrontée à vos politiques d'accès et de DLP avant d'atteindre le serveur, et le résultat est consigné pour l'audit.

AUTORISER

La requête respecte la politique. Elle atteint le serveur MCP et la décision est enregistrée.

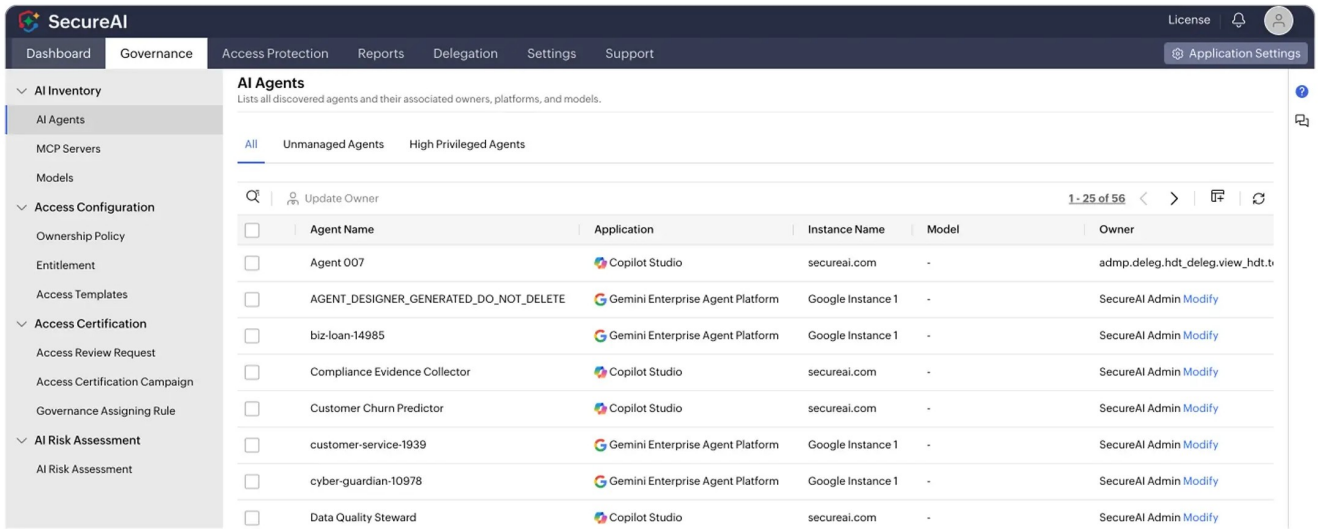
MASQUER

Des données sensibles sont détectées. Elles sont remplacées par un texte de masquage dans l'entrée ou la sortie de l'outil, et le reste de la requête continue.

BLOQUER

La requête sort du cadre de la politique. Elle est arrêtée à la passerelle et n'atteint jamais le serveur.

Conditions disponibles : identité, horaire, adresse IP et localisation, serveur MCP, outil et type d'outil. Plusieurs passerelles peuvent coexister, chacune avec sa propre URL, sur un registre de serveurs partagé.



Console SecureAI : inventaire des agents IA, avec leur application, leur instance, leur modèle et leur responsable. Onglets dédiés aux agents non gérés et aux agents fortement privilégiés.

SECUREAI ET AD360

Une brique d'AD360

ManageEngine présente SecureAI comme le composant de sécurité et de gouvernance de l'IA agentique d'AD360, sa suite de gestion des identités et des accès. LAZAR SOFT vous aide à définir le bon périmètre selon les produits ManageEngine déjà en place chez vous.

ManageEngine édite SecureAI. LAZAR SOFT le déploie chez vous.

AVANT-VENTE GRATUITE

- POC dans votre environnement, pas sur une démo générique.

DÉPLOIEMENT CLÉ EN MAIN

- Plateformes d'IA, annuaires, passerelles MCP, règles DLP, campagnes de certification.

SUPPORT EN FRANÇAIS

- Un ingénieur certifié qui connaît votre configuration.

ESCALADE DIRECTE

- Accès prioritaire aux équipes R&D de l'éditeur via le canal Expert Partner.

04 — ÉDITIONS ET TARIFS

Une licence au nombre d'agents. On vous aide à la dimensionner.

LICENCE ANNUELLE · PAR AGENT IA	PRIX PAR AGENT ET PAR AN
Palier 100 agents	50 €
Palier 500 agents	38 €
Palier 1 000 agents	31 €
Palier 1 500 agents	28 €
Palier 2 000 agents	26 €
Palier 3 000 agents	23 €
Palier 5 000 agents	21 €
Au-delà, ou déploiement sur mesure	Sur devis

ÉVALUATION

- Toutes les fonctionnalités pendant 45 jours
- Sans carte bancaire
- Bascule automatique en édition gratuite à l'issue

GRATUITE

- Jusqu'à 10 agents IA
- Inventaire IA
- Graphe des accès
- Rapports

LICENCE ANNUELLE

- Licence par agent, facturation annuelle
- Prix par agent dégressif selon le palier
- Devis LAZAR SOFT selon votre parc d'agents réel

Tarifs publics éditeur, licence annuelle, prix par agent et par an : source ManageEngine, page de tarification SecureAI (manageengine.com/secure-ai/pricing-details.html), consultée le 17/11/2026. Éditions Évaluation et Gratuite : même source ; essai sans carte bancaire : page de téléchargement SecureAI, consultée le 17/11/2026. Prix indicatifs et non contractuels (la source ne précise pas s'ils s'entendent hors taxes) : le montant applicable dépend du nombre d'agents et du périmètre retenu. Devis personnalisé LAZAR SOFT sur demande.

Contactez-nous.

Une question, un POC dans votre environnement ou un chiffrage précis : un #RocketExpert vous répond sous 24 h ouvrées.

TÉLÉPHONE
+33 (0)1 76 21 60 43

E-MAIL
sales@lazarsoft.com