SOPHOS

SOPHOS AI DEFENSE

Sortez l'IA de l'ombre.

Adoptez et utilisez l'IA en toute confiance.

Les organisations adoptent l'IA plus vite qu'elles ne peuvent la gérer. Des données sensibles sont partagées, des agents d'IA opèrent sans visibilité, et les équipes de sécurité ne disposent souvent pas d'une vision claire des outils utilisés. Alimenté par Sophos Fusion, Sophos AI Defense vous aide à découvrir, comprendre et contrôler l'utilisation de l'IA dans votre environnement.

69%
des organisations soupçonnent ou disposent de preuves indiquant que des employés utilisent des services d'IA publics interdits[1]

82%
des organisations ont découvert des outils ou des flux de travail d'IA inconnus[2]

90%
des responsables informatiques sont préoccupés par le risque lié au Shadow AI[3]

1,3 milliard
Nombre estimé d'agents d'IA d'ici 2028[4]

CE QUE VOUS OBTENEZ AVEC SOPHOS

Voir l'IA. Contrôler l'IA. Sécuriser l'IA.

Découvrir ce que l'IA fait réellement.

La visibilité commence par ce qui se passe réellement, pas seulement ce qui est approuvé.

- Mettez au jour l'utilisation de l'IA chez vos employés, ainsi que dans vos outils et flux de travail.
- Validez les outils approuvés et découvrez les utilisations non autorisées
- Obtenez une visibilité continue sur les points d'interaction du navigateur, du terminal et du réseau

Identifier les comportements de l'IA qui comptent le plus.

Toutes les activités d'IA n'entraînent pas d'exposition, mais sans contexte, les équipes ne peuvent pas distinguer l'utilisation approuvée du comportement qui justifie une action.

- Évaluez l'utilisation de l'IA, y compris les contextes d'identité, de comportement et des données
- Distinguez l'utilisation acceptable de l'activité non gérée, sur-privilégiée ou risquée
- Concentrez-vous sur les expositions significatives plutôt que de réagir à des événements isolés ou à faible impact

Transformer la politique d'IA en contrôle.

À mesure que l'adoption de l'IA se généralise, les politiques statiques sont dépassées. Les règles doivent être appliquées en continu et pouvoir être imposées.

- Appliquez des garde-fous sur la manière dont l'IA est utilisée, pas seulement sur la manière dont elle est définie dans la politique de sécurité
- Appliquez des contrôles aux points d'interaction clés pour aligner l'utilisation de l'IA et le partage de données sur la politique de sécurité et les réglementations
- Réduisez les utilisations de Shadow AI en guidant les utilisateurs vers des outils approuvés

Intégrer l'IA dans les opérations de sécurité.

L'IA élargit votre surface d'attaque, avec de nouveaux risques concernant les prompts, les données et les actions pilotées par des agents qui nécessitent une gestion active.

- Mettez au jour les usages abusifs, les exploitations malveillantes et les compromissions liés à l'IA dans les flux de travail de détection et d'investigation
- Intégrez l'activité de l'IA dans la télémétrie de sécurité globale
- Appliquez les mêmes playbooks, outils et processus d'escalade que pour les menaces standard.

SOPHOS AI DEFENSE EN BREF

- Découvrez l'utilisation de l'IA chez vos employés, ainsi que dans vos outils et flux de travail — y compris le Shadow AI.
- Identifiez les comportements à risque en utilisant les contextes d'identité, d'exposition des données et d'utilisation.
- Appliquez des garde-fous sur les points d'interaction du navigateur, du terminal et du réseau.
- Empêchez le partage de données sensibles avec les outils d'IA en inspectant les prompts, les téléversements et les interactions avec l'IA en temps réel.
- Intégrez les risques liés à l'IA dans les flux de travail des opérations de sécurité.

À QUI S'ADRESSE SOPHOS AI DEFENSE

- Aux responsables cybersécurité qui ont besoin de visibilité et de contrôle sur l'utilisation de l'IA
- Aux équipes d'opérations de sécurité chargés d'identifier et de répondre aux risques pilotés par l'IA
- Aux organisations cherchant à adopter et à déployer des outils d'IA en toute sécurité
- Aux entreprises cherchant à étendre leurs investissements de cybersécurité existants pour gérer les risques liés à l'IA

LE POINT SUR LES RISQUE RÉELS LIÉS À L'IA

Une sécurité de l'IA conçue pour les utilisations réelles de l'IA.

Répondre aux risques de l'IA actuels, plutôt qu'à des scénarios hypothétiques futurs.

La plupart des solutions sécurisent les modèles ou les applications. Sophos AI Defense aborde ce qui vous met réellement en danger aujourd'hui :

- L'utilisation non administrée de l'IA au sein du personnel
- La visibilité limitée sur les outils, les agents et les flux de travail
- Les données sensibles partagées avec des outils d'IA externes via des prompts et des flux de travail automatisés

Renforcer vos investissements actuels.

Sophos AI Defense s'appuie sur vos contrôles existants — en les coordonnant pour obtenir des résultats immédiats et pratiques.

- Élargissez vos investissements Sophos Workspace Protection, EDR, Firewall, XDR et MDR
- Reliez les points de contrôle au sein d'un cadre unifié de gestion des politiques d'IA.
- Bénéficiez d'une valeur immédiate — aucun nouveau déploiement ou ressource supplémentaire requis

Transformer la visibilité en résultats, pas en données supplémentaires.

La visibilité seule ne suffit pas. Sophos AI Defense transforme les informations en action :

- Combinez visibilité, contexte et contrôle dans un système unifié couvrant l'utilisation de l'IA, les flux de données et l'activité des agents.
- Appliquez la politique de sécurité, priorisez les problèmes et répondez dans les mêmes flux de travail.
- Des résultats sous contrôle, pas une accumulation de tableaux de bord.

RECONNAISSANCE DE L'INDUSTRIE

Une validation par les principaux analystes et les organisations du secteur.

GARTNER 2026

Leader, Endpoint Protection

G2 SUMMER 2026

Solutions XDR et MDR classées #1

ÉVALUATIONS MITRE ATT&CK

Couverture de détection de 100 %

GARTNER PEER INSIGHTS

Un 'Customers' Choice' pour XDR et MDR

Un seul système. Tous les points de contrôle. Une défense unifiée.

Sophos AI Defense fait partie de Sophos Fusion, le système de cyberdéfense le plus complet sur le marché. La solution protège les organisations contre les menaces accélérées par l'IA qui évoluent plus vite que les équipes de défense ne peuvent réagir.

sophos.com/ai-defense →

[1] Gartner, Shadow AI Demands Stricter Endpoint Application Control, 25 mai 2026. [2] CSA, « The Shadow AI Agent Problem in Enterprise Environments », 2025. [3] Komprise IT Survey: AI, Data & Enterprise Risk. [4] IDC Info Snapshot, sponsorisé par Microsoft, 1.3 Billion AI Agents by 2028, #US53361825, mai 2025.

Le contenu de Gartner Peer Insights est constitué d'avis d'utilisateurs individuels basés sur leurs propres expériences et ne doit pas être interprété comme des déclarations de faits et ne représente pas les opinions de Gartner ou de ses affiliés. Gartner ne cautionne aucun fournisseur, produit ou service décrit dans ce contenu et n'offre aucune garantie, explicite ou implicite, quant à l'exactitude ou l'exhaustivité de ce contenu, y compris toute garantie de qualité marchande ou d'adéquation à un usage particulier. GARTNER est une marque déposée et une marque de service de Gartner, Inc. ou de ses filiales aux États-Unis et dans le monde, et PEER Visibilité est une marque déposée de Gartner, Inc. ou de ses filiales et est utilisées ici avec autorisation. Tous droits réservés. Gartner®, Peer Insights™ Voice of the Customer for Extended Detection and Response, Peer Contributors, 23 mai 2025 Gartner®, Peer Insights™ Voice of the Customer for Managed Detection and Response, Peer Contributors, 31 mars 2026.

2026-09-15 SB-FR (MC)

SOPHOS