

Proofpoint AI Security

Visibilité unifiée, application des règles en temps réel et pistes d'audit défendables pour les applications d'IA, les agents et les serveurs MCP



Principaux avantages

- **Visibilité sur chaque type d'IA d'entreprise**, y compris les outils des collaborateurs, l'IA intégrée aux applications, les agents autonomes et les serveurs MCP
- **Application des règles en temps réel**, avec blocage, masquage, restriction ou escalade en fonction du déroulement de l'interaction
- **Pistes d'audit défendables** pour toutes les parties prenantes : reconstitution complète des transactions depuis la demande de l'utilisateur jusqu'à l'action de l'agent et le résultat
- **Télémetrie de l'IA adaptée au SOC** grâce à l'intégration SIEM et SOAR native, qui sépare les incidents de sécurité des violations de la gouvernance

Le problème

De nombreuses entreprises n'ont aucune visibilité sur les outils d'IA présents dans leurs environnements, les personnes qui les utilisent ou les données exposées. Ces défis fondamentaux en matière de sécurité de l'IA se complexifient à mesure que la technologie gagne en maturité.

Les outils d'IA ne sont plus uniquement disponibles par le biais des navigateurs Web. Ils sont désormais intégrés dans de nombreuses applications de type logiciel en tant que service (SaaS). De plus en plus, ils exécutent des workflows autonomes sur les systèmes d'entreprise et se connectent aux ressources d'entreprise via des serveurs MCP (Model Context Protocol). De nombreuses équipes de sécurité manquent de visibilité sur les outils d'IA utilisés par les collaborateurs et sur ce à quoi ces outils peuvent accéder.

Les produits de sécurité traditionnels ne peuvent pas détecter quand un agent prend des mesures qui sortent du cadre de la tâche qui lui a été confiée. Cette menace, connue sous le nom d'élévation sémantique des privilèges, survient lorsque l'agent passe les vérifications des autorisations avec succès, mais que ses actions entraînent tout de même un incident de sécurité.

Les autorisations peuvent être valides, mais l'intention détournée. De même, l'intention peut être respectée, mais les comportements peuvent s'écarter de ceux attendus. La sécurisation de l'IA implique d'évaluer simultanément l'accès, l'intention et le comportement et de les faire concorder.

L'approche de Proofpoint : assurer l'intégrité de l'IA

La plupart des éditeurs de solutions de sécurité de l'IA se concentrent sur une seule dimension : la détection de l'intention, le contrôle des accès ou la surveillance des comportements. Ces approches présentent toutefois les problèmes suivants :

- L'accès seul vous montre ce à quoi un agent a accès, mais ne vous indique pas s'il devrait y avoir accès pour une tâche donnée.
- L'intention seule vous indique ce qu'un utilisateur ou un agent avait l'intention de faire, mais pas si les actions en aval concordaient toujours avec cette intention.
- Le comportement seul vous indique ce qui s'est passé, mais pas si c'était autorisé ou conforme à la demande initiale.

En revanche, Proofpoint AI Security observe, évalue et vérifie que l'accès, l'intention et le comportement sont alignés. Lorsqu'ils le sont, l'intégrité de l'IA est assurée. Lorsqu'ils divergent, les entreprises connaissent des incidents de sécurité, et ce même si toutes les vérifications des autorisations individuelles réussissent. Cette différence fondamentale est ce qui distingue l'intégrité de l'IA de la sécurité de l'IA.

Sécurisez chaque couche de votre IA

Sécurisez la manière dont les collaborateurs utilisent l'IA

Proofpoint identifie les outils d'IA non approuvés (Shadow IA) dans les applications installées sur les terminaux, les services cloud et les serveurs MCP. Les équipes de sécurité disposent ainsi d'une visibilité sur les outils d'IA utilisés par les collaborateurs et les endroits où les données sensibles sont susceptibles d'être exposées. Des modèles de détection propriétaires analysent le contenu et le comportement de chaque invite et réponse.

Les modèles de détection évaluent également chaque interaction afin d'identifier les risques en fonction de la sensibilité des données, de la posture de l'éditeur de solutions et de la fréquence d'utilisation. Lorsque les interactions enfreignent les règles, des contrôles d'utilisation acceptable configurables les bloquent ou les signalent par catégorie d'utilisateurs. Cette approche favorise une adoption sûre, plutôt que de reléguer l'utilisation de l'IA dans la clandestinité.

Sécurisez l'utilisation de l'IA par les agents

Proofpoint offre une visibilité complète et assure la sécurité en temps réel des agents sans nécessiter de modifications de code, que ce soit en mode visibilité ou d'application en ligne. Le contrôle d'accès basé sur l'intention (IBAC) évalue si les actions des agents sont conformes à leur objectif initial. Cela permet de détecter toute élévation sémantique des privilèges avant qu'elle ne se traduise par des actions inappropriées. L'intégralité de la chaîne d'exécution est capturée lors d'investigations numériques avec annotations de sécurité qui retracent chaque étape, appel d'outil et interaction avec les données jusqu'à la demande d'origine.

Sécurisez les interactions entre l'IA et les systèmes d'entreprise

La passerelle MCP sert de point de contrôle unique pour tout le trafic MCP. Aucun grand modèle de langage (LLM) ne peut se connecter aux sources de données d'entreprise sans passer par elle. Un registre de plus de 800 serveurs MCP sécurisés avec vérification de la chaîne logistique peut sécuriser tout nouveau serveur à partir de la source en moins de 15 minutes. Toutes les connexions sont authentifiées et inspectées afin de détecter les données sensibles, les tentatives d'injection d'invites et les violations des règles.

Conséquences pour l'entreprise

Accélération de l'adoption de l'IA

Les équipes de sécurité peuvent adopter l'IA en toute confiance, car la gouvernance est intégrée au déploiement. Les programmes d'IA passent de la phase pilote à la production en quelques semaines, plutôt qu'en plusieurs mois.

Réduction de l'exposition aux risques

La surface d'attaque est réduite à ce qui est connu, gouverné et activement surveillé. Cela s'applique à toutes les formes d'IA d'entreprise, des chatbots aux agents autonomes.

Audits défendables sans reconstitution manuelle

Chaque interaction avec l'IA produit les preuves requises pour un audit défendable. La préparation à la conformité devient un état continu, et non une course trimestrielle.

Des opérations de sécurité qui évoluent

L'intégration native avec les plates-formes de gestion des informations et des événements de sécurité (SIEM) et d'orchestration, d'automatisation et de réponse en matière de sécurité (SOAR) fournit une télémétrie spécifique à l'IA qui offre un contexte complet. Les équipes de sécurité peuvent étendre la couverture à l'IA sans faire appel à des experts en IA.

Fonctionnalités de Proofpoint AI Security

FONCTIONNALITÉ	RÔLE	CE QUI DISTINGUE PROOFPOINT
Contrôle de l'utilisation de l'IA	Découverte de l'utilisation de l'IA par les applications SaaS, les extensions IDE, les applications de bureau, les outils CLI, les plug-ins de navigateur et les modèles locaux. Évaluation des risques contextuels en fonction de la sensibilité des données, de la posture des éditeurs de solutions et de la fréquence d'utilisation.	Gouvernance de l'utilisation de l'IA au niveau sémantique, et non par un simple filtrage des URL. Évaluation des risques liés à chaque interaction, au lieu de se limiter à déterminer si un outil est autorisé.
Gestion du niveau de sécurité de l'IA	Inventaire complet des applications d'IA, des agents, des outils, des intégrations, des services externes et des serveurs MCP. Évaluation continue du niveau de sécurité tout au long du cycle de vie de l'IA.	La découverte s'étend aux chaînes d'outils des agents et à l'inventaire des serveurs MCP – en cartographiant l'ensemble du graphe d'exécution, et pas seulement les interfaces de chat.
Défense en temps réel de l'IA	Inspection en temps réel des interactions avec l'IA avec évaluation en ligne des invites, des sorties et du comportement des modèles. 18 détecteurs intégrés à travers les modalités.	L'évaluation au niveau sémantique distingue les comportements légitimes des activités inhabituelles ou malveillantes – réduisant ainsi les faux positifs qui érodent la confiance du centre des opérations de sécurité (SOC).
Sécurité de l'écosystème d'IA agentique	Prévention de l'élévation sémantique des privilèges grâce au contrôle d'accès basé sur l'intention (IBAC). Capture de l'intention de l'utilisateur et propagation à l'ensemble du workflow de l'agent.	L'IBAC valide l'alignement à chaque action. Détection des anomalies comportementales, manifestes des agents pour les règles en tant que code, et investigation numérique complète des transactions à travers les chaînes d'agents.
Sécurité de la chaîne logistique de l'IA	Authentification et inspection du contenu imposées par la passerelle MCP pour tous les accès aux outils. Découverte et enregistrement de tous les serveurs MCP en cours d'utilisation.	L'application en temps réel gouverne les données qui traversent les frontières MCP et les actions autorisées via les connexions du protocole.

Demander une démonstration

Contactez l'équipe Proofpoint responsable de votre compte pour planifier une démonstration de Proofpoint AI Security, ou visitez le site proofpoint.com/fr pour en savoir plus.

proofpoint.

Proofpoint est une marque déposée ou un nom commercial de Proofpoint, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.