Zscaler AI Security : Les fondamentaux de la sécurité à l'ère de l'IA

L'ESSENTIEL

Les avantages de la sécurité de l'IA

DÉCOUVRIR LES ACTIFS ET LES RISQUES LIÉS À L'IA
Découvrez et cartographiez l'ensemble de votre écosystème d'IA, des outils d'IA fantômes et des applications à risque aux modèles et pipelines d'IA, entre autres.

IDENTIFIER LES VULNÉRABILITÉS DE L'IA
Testez vos systèmes d'IA avec une approche Red Team continue et automatisée afin d'identifier leurs vulnérabilités et leurs risques.

SÉCURISER L'ACCÈS À L'IA
Tirez parti de garde-fous IA intégrés aux flux pour appliquer en temps réel des mesures de protection contre les menaces, les fuites de données et les usages à risque.

GARANTIR LA CONFORMITÉ DES USAGES DE L'IA
Gérez votre empreinte IA et vos déploiements à l'aide de référentiels de gouvernance de l'IA afin de maîtriser les risques et de garantir la conformité

Une sécurité IA de bout en bout avec Zscaler

Zscaler propose des solutions basées sur l'IA conçues pour aider les entreprises de tirer pleinement parti de son potentiel de transformation tout en maîtrisant les risques associés.

Ces solutions couvrent l'ensemble du cycle, de l'identification des usages de l'IA à risque à la sécurisation du développement et à la protection des versions sensibles grâce à des mécanismes de défense avancés directement intégrés aux flux.

Zscaler redéfinit ce que signifie sécuriser l'innovation en IA. Libérez tout le potentiel de l'IA et innovez sans crainte avec Zscaler.



Pourquoi Zscaler pour la sécurité de l'IA ?

CYCLE DE VIE COMPLET DE L'IA
Sécurité de l'IA, de la découverte au déploiement

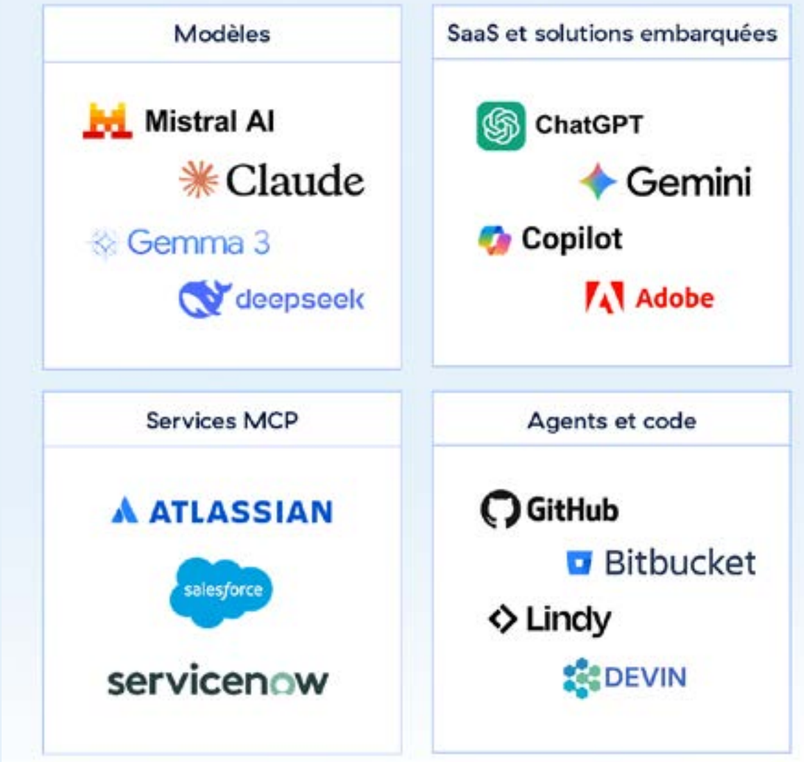
PLATEFORME UNIFIÉE
Plateforme éprouvée qui associe sécurité de l'IA et Zero Trust

PARTENAIRE RECONNU
Expertise en matière de réussite et de transformation client

Découverte des actifs avec AI SPM

Identifier son empreinte IA dans un environnement qui évolue à un rythme effréné est un véritable défi. Sans visibilité claire sur l'IA fantôme, les modèles, les services, les serveurs MCP et les pipelines, les entreprises peinent à détecter les risques et à y répondre efficacement.

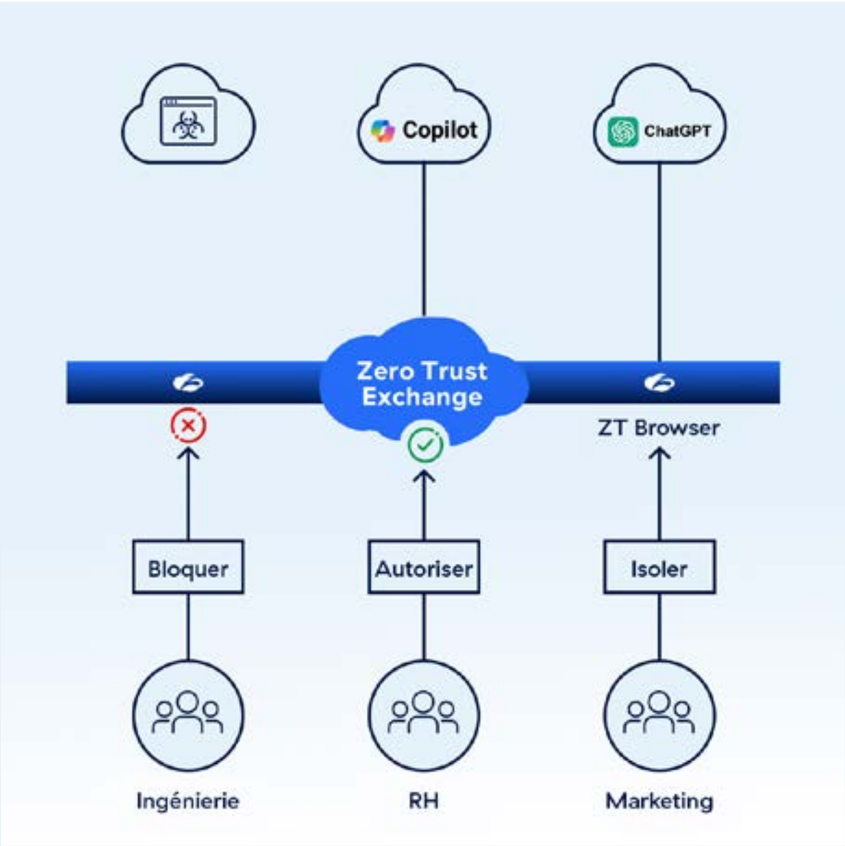
Avec Zscaler AI SPM, les entreprises bénéficient d'une visibilité complète sur leurs écosystèmes d'IA. La solution offre une visibilité sur l'ensemble de votre empreinte, des applications d'IA générative aux LLM, modèles, serveurs MCP et pipelines, et vous aide ainsi à identifier les expositions à risque et les vulnérabilités susceptibles de compromettre vos données et votre activité.



Sécurité des accès pour l'IA

Contrôler les accès aux applications SaaS d'IA générative et en garantir la sécurité devient de plus en plus complexe. Face à la généralisation incontrôlée de l'IA fantôme et à l'augmentation des risques de fuite de données ou d'usages non conformes, les entreprises ont besoin de solutions efficaces pour répondre à ces menaces.

Zscaler AI Access Security permet d'encadrer l'utilisation des applications d'IA afin de garantir des usages sûrs, conformes et responsables. Appliquez des contrôles d'accès précis pour déterminer les utilisateurs ou applications qui peuvent interagir avec les outils d'IA. Exploitez la protection DLP ou l'isolation pour empêcher les fuites de données via les prompts, et appliquez une modération des contenus pour garantir le respect des politiques d'utilisation acceptable de l'entreprise.



©2026 Zscaler, Inc. Tous droits réservés.

Tests avec Red Teaming automatisé

Tester les systèmes d'IA pour détecter leurs vulnérabilités est souvent un processus complexe et chronophage. Réaliser des évaluations approfondies peut sembler quasiment impossible aux entreprises qui ne disposent pas de ressources Red Team dédiées.

Le Red Teaming automatique et continu de Zscaler répond à ces difficultés grâce à son moteur innovant de Red Teaming automatisé. SPLX propose plus de 25 tests prédéfinis, ainsi que la possibilité de créer des tests entièrement personnalisés et de charger des jeux de données, afin d'adapter les scénarios de test à vos domaines d'activité, à vos environnements réglementaires et à vos cas d'usage.



Protection inline avec AI Guard

Les LLM sont rapidement devenus un vecteur particulièrement dangereux de menace et de perte de données. Sans inspection inline performante de ces connexions, les entreprises s'exposent à des fuites de données, à la compromission de leurs systèmes d'IA et à des menaces malveillantes.

Zscaler AI Guard assure une inspection inline performante des prompts et des interactions avec les systèmes d'IA. Détectez les menaces telles que les injections de prompts et les tentatives de jailbreak, empêchez les fuites de données sensibles et modérez les contenus afin de garantir des usages sûrs et conformes aux politiques d'utilisation acceptable. S'appuyant sur son expertise reconnue en matière d'inspection inline, Zscaler assure une protection robuste de vos flux d'IA critiques.

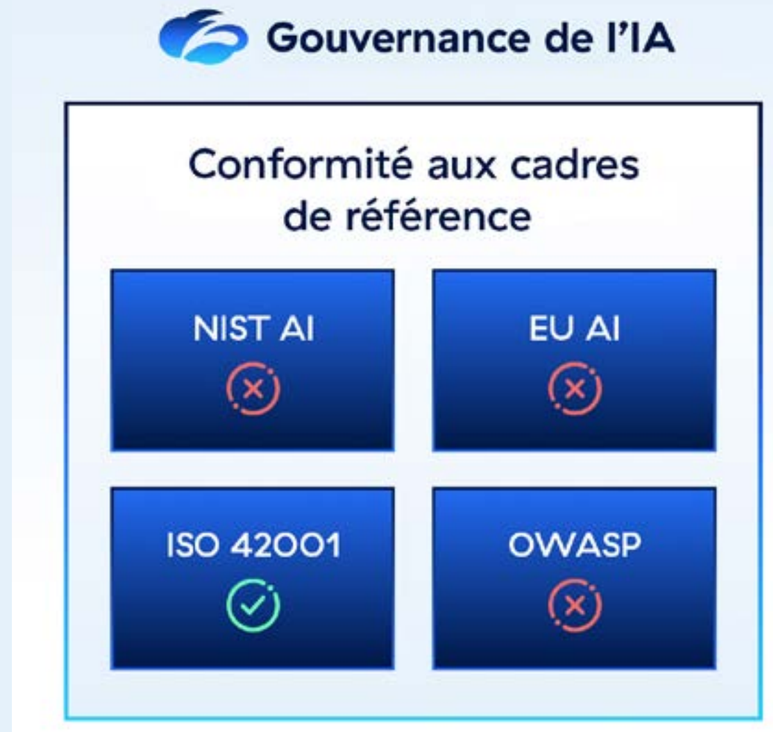


©2026 Zscaler, Inc. Tous droits réservés.

Gouvernance de l’IA avec AI SPM

À mesure que les entreprises étendent leur utilisation de l’IA, assurer la conformité et la gouvernance des systèmes d’IA devient de plus en plus complexe. Sans contrôle rigoureux du respect des politiques et des référentiels de gouvernance de l’IA, les entreprises s’exposent à des risques juridiques, financiers et de réputation.

L’approche de Zscaler en matière de gouvernance de l’IA permet d’automatiser le suivi de la conformité et de simplifier les processus de reporting. Surveillez en continu la conformité des systèmes d’IA avec les politiques internes et les normes réglementaires, tout en réunissant les éléments de preuve nécessaires aux audits et au respect des exigences. Veillez à ce que les usages de l’IA soient conformes aux référentiels de gouvernance, afin de réduire les risques et de préserver l’intégrité de vos opérations.



À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation numérique pour améliorer l’agilité, l’efficacité, la résilience et la sécurité de ses clients. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et la perte de données, en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quel que soit leur emplacement. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange™, basé sur SSE, constitue la plus vaste plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur **zscaler.com/fr** ou suivez-nous sur X (ex-Twitter) **@zscaler**.

© 2026 Zscaler, Inc. Tous droits réservés. Zscaler™ et les autres marques commerciales répertoriées sur **zscaler.com/fr/legal/trademarks** sont soit 1) des marques déposées ou des marques de service, soit 2) des marques commerciales ou des marques de service de Zscaler, Inc. aux États-Unis et/ou dans d’autres pays. Toutes les autres marques sont la propriété de leurs détenteurs respectifs.

+1 408 533 0288 **Zscaler, Inc. (siège) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/fr**

Zero Trust Everywhere