Liste de contrôle : comment détecter et protéger votre entreprise de l’IA fantôme

L’IA générative (GenAI) transforme la façon de travailler de vos collaborateurs et élargit la surface d’attaque de l’entreprise. Des outils tels ChatGPT, Gemini ou Claude boostent certes la productivité, mais utilisés sans autorisation (IA fantôme), ils exposent l’entreprise à de sérieux risques de sécurité et de conformité.

De plus en plus d’employés s’appuient sur ces systèmes pour rédiger des e-mails, résumer des documents ou générer du code. Sans supervision informatique, ils risquent d’envoyer par mégarde des données sensibles (informations personnelles identifiables (PII), dossiers financiers ou propriété intellectuelle) vers des modèles d’intelligence artificielle (IA) externes qui ne peuvent être ni contrôlés ni audités. La perte de données n’est plus seulement une possibilité, mais une probabilité.

Plutôt que de bloquer complètement les outils IA générative, ce qui freinerait la productivité, de nombreux responsables informatiques recherchent les moyens d’adopter une IA sécurisée qui protège les données sans créer de frictions. Voici six étapes proactives pour détecter l’IA fantôme dans votre environnement, évaluer les risques et mettre en place des contrôles techniques et organisationnels, tout en conservant les bénéfices de ces applications.

01

Auditer votre exposition à l’IA fantôme

Avant de pouvoir sécuriser IA générative, vous devez comprendre ce qui se passe dans votre environnement. Commencez par effectuer un audit global des applications d’IA tierces qu’utilisent vos employés, puis identifiez celles qui n’ont pas été approuvées par le service informatique. Suivez le trafic vers les outils d’IA générative, contrôlez-en l’accès depuis les appareils non gérés et évaluez le volume ainsi que la nature des données que partagent vos collaborateurs.

02

Évaluer les risques liés à vos données

Les employés utilisent souvent l’IA générative pour sa rapidité et sa commodité, sans en mesurer les conséquences. Comprendre les types de données que vos employés partagent avec ces outils, et pourquoi, est essentiel pour hiérarchiser vos efforts de réponse. Vérifiez si vos équipes transmettent des données sensibles (informations personnelles, propriété intellectuelle, dossiers financiers) et identifiez les flux de travail où ces données entrent dans les outils. Déterminez également si vos équipes informatiques peuvent contrôler ou rappeler les données partagées et si des risques de conformité sont impliqués.

03

Mettre en place des garde-fous pour l’usage de l’IA générative

Des règles claires d’utilisation de l’IA posent les bases d’une adoption responsable dans toute l’entreprise. Précisez quelles applications d’IA générative sont autorisées et donnez des consignes claires sur ce qu’il faut faire — ou éviter — lors du partage de données de l’entreprise. Établissez d’emblée des règles de gestion des données propres à l’IA. Intégrez-les dans l’onboarding et la formation à la sécurité, et exigez de chaque employé qu’il les accepte et les respecte. Ces garde-fous protègent les données sans brider la productivité.

04

Renforcer la sécurité à la périphérie

- Des politiques solides exigent des contrôles concrets. Surveillez et maîtrisez les flux de données vers les outils d'IA générative grâce à une architecture moderne comme le Zero Trust. Les plateformes Zero Trust intègrent plusieurs outils pour limiter l'exposition des données : un CASB (Cloud Access Security Broker) pour détecter l'usage d'applications d'IA non autorisées, la protection contre la perte de données (DLP) inline pour empêcher la saisie de données sensibles dans les champs de requête, l'isolation du navigateur pour bloquer l'IA fantôme sans perturber la navigation web, l'analyse du comportement des utilisateurs et des entités (UEBA) pour détecter les anomalies dans l'usage des outils d'IA.

05

Instaurer une culture d'IA responsable

- La technologie et la politique ne sont qu'une partie de l'équation. Il est tout aussi important de sensibiliser vos collaborateurs. Formez vos équipes aux risques inhérents au partage d'informations sensibles avec l'IA générative et donnez-leur des exemples d'utilisation sûre et appropriée. Expliquez comment exploiter les applications approuvées pour gagner en productivité et encouragez-les à signaler les outils non approuvés ou les comportements douteux. Créer une culture de responsabilité fera de votre personnel une extension de votre équipe de sécurité.

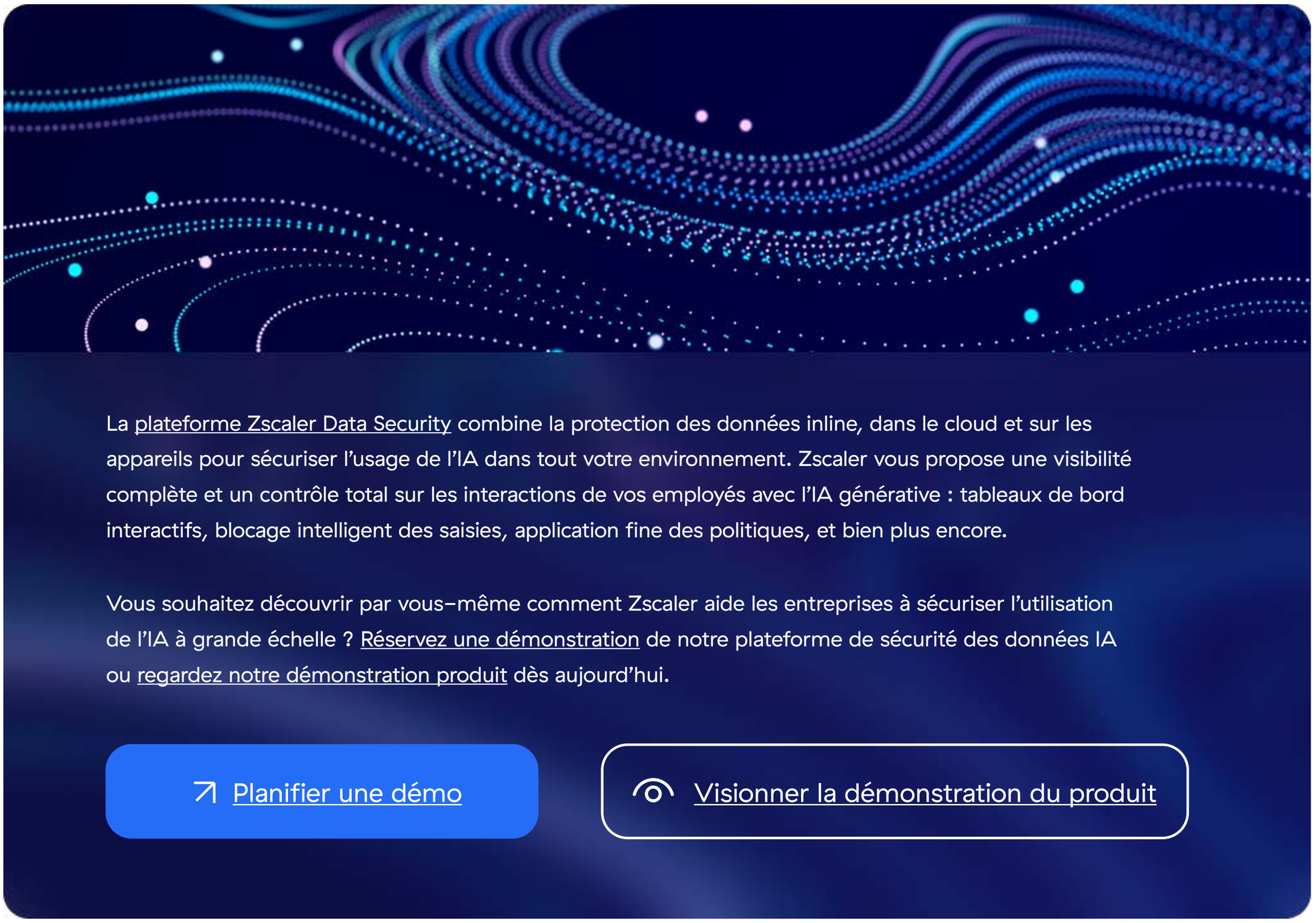
06

Faire de la gestion de l'IA fantôme un processus continu

- Sécuriser l'utilisation de l'IA n'est pas un projet ponctuel, mais un programme continu qui doit évoluer avec les menaces. Maintenez vos défenses à jour, surveillez en permanence l'apparition de nouveaux outils d'IA générative, suivez les tendances d'utilisation et actualisez régulièrement vos formations et vos politiques pour anticiper les risques émergents. Alignez la gestion de l'IA fantôme sur l'approche Zero Trust et la stratégie DLP de votre entreprise pour en faire un effort durable et non une solution provisoire.

Zscaler : la sécurité de l’IA générative qui coche toutes les cases

En appliquant les mesures de cette liste de contrôle, vous créez une base solide qui permet à votre entreprise d’adopter sereinement l’IA générative, sans compromettre la sécurité. Cette approche progressive donne à vos équipes informatiques la maîtrise de tous les aspects de l’usage de l’IA générative, des saisies aux applications autorisées, afin que vos collaborateurs en tirent parti en toute sécurité.



La plateforme Zscaler Data Security combine la protection des données inline, dans le cloud et sur les appareils pour sécuriser l’usage de l’IA dans tout votre environnement. Zscaler vous propose une visibilité complète et un contrôle total sur les interactions de vos employés avec l’IA générative : tableaux de bord interactifs, blocage intelligent des saisies, application fine des politiques, et bien plus encore.

Vous souhaitez découvrir par vous-même comment Zscaler aide les entreprises à sécuriser l’utilisation de l’IA à grande échelle ? Réservez une démonstration de notre plateforme de sécurité des données IA ou regardez notre démonstration produit dès aujourd’hui.

Planifier une démo

Visionner la démonstration du produit

zscaler™ | **Explorez votre monde, en toute sécurité.™**

À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale 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, quelle que soit leur localisation. Adossé à plus de 150 data centers dans le monde, Zero Trust Exchange, basé sur le SASE, est la plus importante plateforme de sécurité cloud inline au monde. Pour en savoir plus, rendez-vous sur zscaler.com/fr

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.com/fr