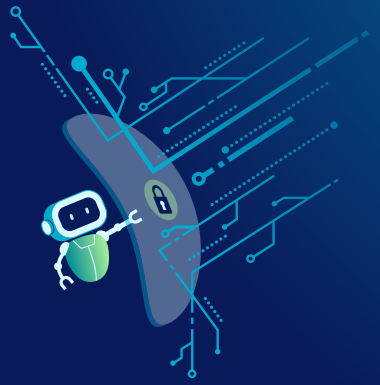
netskope

# Checklist des bonnes pratiques pour la sécurité de l'IA

Un guide pratique pour les RSSI et les équipes de sécurité assurant la sécurisation de l'utilisation de l'IA

# Checklist des bonnes pratiques pour la sécurité de l'IA



Les entreprises adoptent rapidement l'IA, ce qui met les équipes de sécurité sous pression pour s'assurer qu'elles disposent des bases nécessaires à un déploiement sécurisé. Mais dans la course pour tirer parti des avantages de l'IA, il est essentiel que les organisations ne négligent aucune étape.

Cette checklist répertorie les questions essentielles à vous poser lorsque vous examinez votre environnement, vos politiques et vos contrôles. Elle a pour objectif d'aider les responsables de la sécurité à évaluer rapidement la situation actuelle et à déterminer les prochaines étapes. Vous pourrez ainsi repérer plus facilement les lacunes, hiérarchiser les actions et avoir une meilleure idée des domaines sur lesquels concentrer vos efforts.

# Découvrez

## Identifiez toutes les utilisations de l'IA dans l'ensemble de l'organisation

On assiste depuis peu à une explosion du nombre d'outils d'IA au sein des entreprises, dont tous ne sont pas forcément connus des professionnels de la sécurité. L'utilisation du Shadow AI reste un problème récurrent : 47 % des utilisateurs d'IA continuent d'utiliser des applications d'IA personnelles au travail (rapport Netskope 2026 sur le cloud et les menaces). Il est également possible que votre écosystème d'applications SaaS intègre des fonctionnalités d'IA susceptibles d'accroître les risques liés aux données. Les équipes chargées de la sécurité doivent donc examiner minutieusement chaque outil afin d'évaluer son impact pour l'IA.

### Éléments à considérer

**Avons-nous une visibilité sur les outils d'IA managés et non managés ?**

**Pouvons-nous identifier les fonctionnalités d'IA intégrées aux applications SaaS ?**

**Comprenons-nous comment les utilisateurs et les agents interagissent avec les modèles d'IA aujourd'hui ?**

# Analysez

## Comprenez l'exposition de vos données liée à l'IA et les facteurs de risque

Toutes les données n'ont pas la même valeur. Ce principe guide depuis longtemps les politiques de sécurité des entreprises. Mais il n'a jamais été aussi important qu'à l'ère de l'IA, où les équipes de sécurité s'efforcent de trouver le juste équilibre entre l'accélération de l'innovation et la maîtrise des risques. Une compréhension plus approfondie de la manière dont les outils d'IA sont utilisés et du type de données qui y transitent peut aider les organisations à prendre des décisions plus éclairées et à mobiliser leurs ressources de manière plus efficace.

### Éléments à considérer

**Savons-nous quels types de données sont partagés avec les outils d'IA ?**

**Pouvons-nous faire la différence entre les interactions à faible risque et à haut risque ?**

**Pouvons-nous repérer des facteurs indiquant un risque émergent ?**

# Appliquez

## Appliquez des contrôles d'utilisation sûrs dans toutes les interactions avec l'IA

Comprendre que les besoins en matière d'accès dépendent du contexte est au cœur de la méthodologie Zero Trust. L'octroi d'un accès approprié se complique avec l'IA, car des outils peuvent, par inadvertance, transmettre des informations confidentielles à un collègue qui interroge un outil d'IA interne. À cette complexité s'ajoute le déploiement continu d'agents d'IA, qui introduisent de nouveaux vecteurs d'attaque, notamment des actions autonomes non sécurisées et de nouvelles voies d'exfiltration des données.

### Éléments à considérer

**Pouvons-nous contrôler l'utilisation de l'IA et l'accès aux données en fonction de l'identité de l'utilisateur ou de l'agent, de la sensibilité des données ou du risque ?**

**Les contrôles sont-ils cohérents entre les différents outils et environnements d'IA ?**

**Nos modèles d'IA privés sont-ils protégés contre le jailbreaking ou les tentatives de prompt engineering malveillant ?**

# Gouvernez

## Assurez-vous que l'utilisation de l'IA est conforme, traçable et gérée de manière responsable

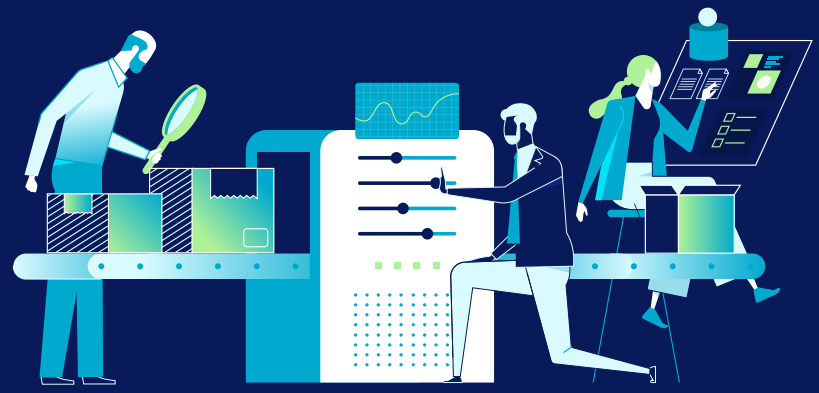
Les professionnels de la sécurité savent que le respect des normes du secteur est essentiel. Cependant, la réglementation en matière d'IA évolue constamment pour suivre le rythme des avancées technologiques. Il est donc important d'adapter les politiques de sécurité en conséquence et d'avoir à tout moment des pistes d'audit claires. Cette exigence est particulièrement importante dans des secteurs tels que les services financiers et la santé, où la réglementation joue un rôle stratégique.

### Éléments à considérer

**Pouvons-nous démontrer comment l'utilisation de l'IA est réglementée aujourd'hui ?**

**Les interactions avec l'IA sont-elles vérifiables et traçables ?**

**Les responsabilités liées à l'utilisation de l'IA sont-elles clairement définies ?**



Vous souhaitez en savoir plus ? Cliquez ici pour en découvrir l'approche de Netskope pour sécuriser l'IA.

## À propos de Netskope

Netskope, leader dans le domaine de la sécurité et des réseaux modernes à l'ère du cloud et de l'IA, répond aux besoins des équipes chargées de la sécurité et des réseaux en offrant un accès optimisé ainsi qu'une sécurité en temps réel et contextuelle pour les employés, les appareils et les données, où qu'ils se trouvent. Des milliers de clients, notamment plus de 30 entreprises du Fortune 100, font confiance à la plateforme Netskope One, son moteur Zero Trust et son puissant réseau NewEdge pour réduire les risques et obtenir une visibilité et un contrôle absolus sur les applications cloud, SaaS, web et privées. Cet outil permet d'assurer la sécurité tout en optimisant les performances, sans aucun compromis.

netskope



**Vous souhaitez en savoir plus ?**

Planifier un démo