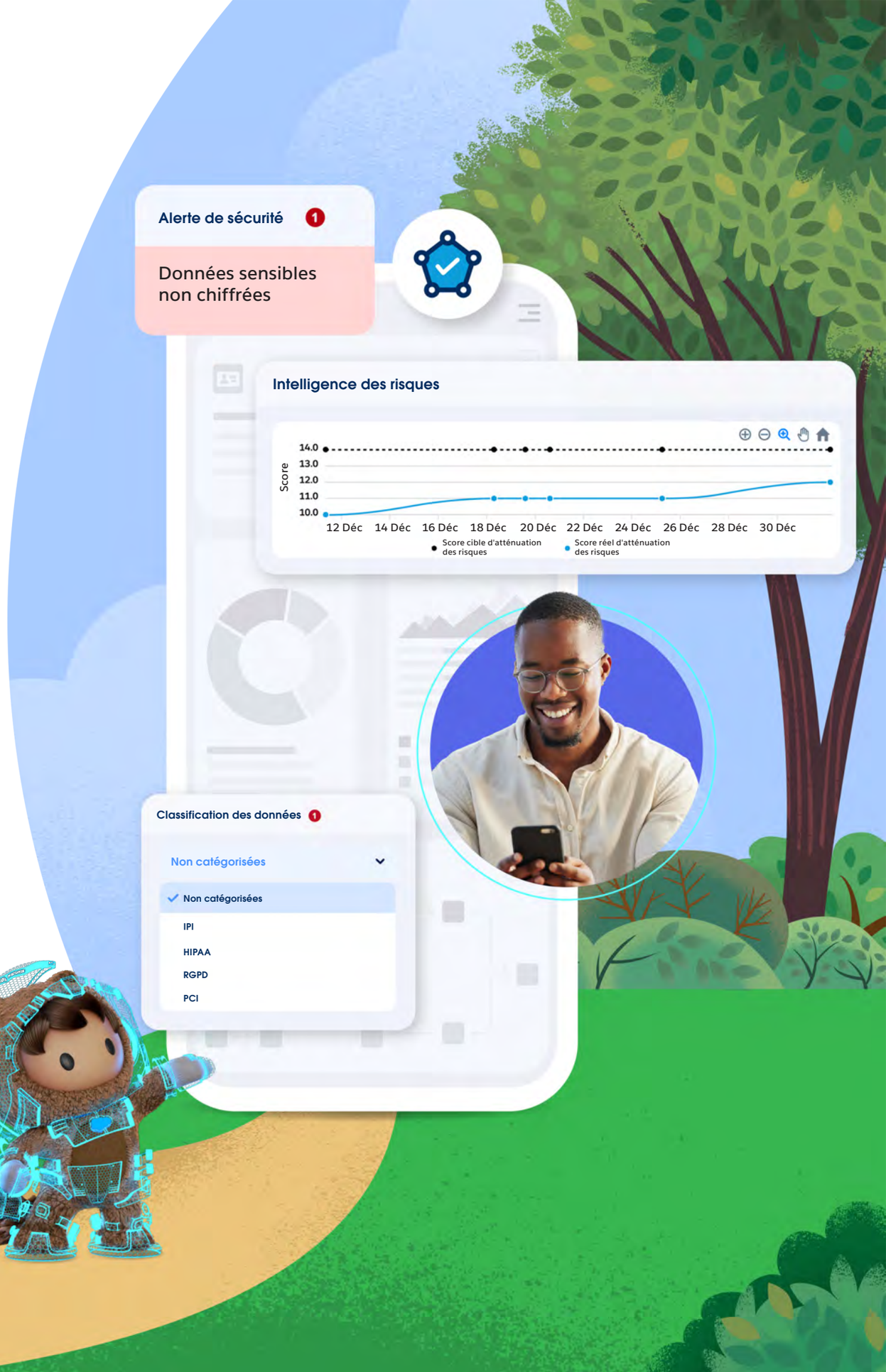
QUATRIÈME ÉDITION

# Focus sur l'IT : Sécurité

Les insights et perspectives de plus de 2 000 responsables de la sécurité, de la confidentialité et de la conformité à l'ère de l'IA agentique.



# Un mot de Salesforce sur la sécurité

La sécurité des données occupe aujourd'hui une place centrale dans le paysage de l'IA, et pas uniquement en raison de la complexification croissante des menaces. Les responsables informatiques et sécurité marchent sur la corde raide : d'un côté, ils doivent protéger l'entreprise contre les ransomwares et l'empoisonnement des données, et de l'autre,ils sont poussés à innover sans relâche dans un contexte où l'IA et l'automatisation sont devenues cruciales pour préserver la compétitivité. Trouver cet équilibre revient à assembler un puzzle dont les pièces changent constamment de place.

Une chose est claire : la sécurité des données n'est pas une simple formalité. Elle est le moteur de la confiance et de l'innovation, tant au sein de l'entreprise qu'avec les clients. Notre enquête menée auprès de plus de 4 000 responsables informatiques dans le monde, dont plus de 2 000 en charge de la sécurité, de la confidentialité et de la conformité, révèle qu'adopter une posture de sécurité solide peut faire bien plus que protéger les données, en ouvrant de nouvelles perspectives. Nous avons recueilli des témoignages d'équipes utilisant l'IA pour détecter les menaces plus tôt, automatiser les tâches de conformité et, in fine, libérer les collaborateurs afin qu'ils puissent se consacrer à des projets stratégiques. Mais nous avons également identifié des défis bien réels : complexité réglementaire, adoption inégale de la gouvernance IA et manque de confiance chez des clients méfiants quant à la gestion de leurs données.

Ce rapport rassemble les perspectives de vos pairs, issus de secteurs et de régions variés, confrontés aux mêmes défis majeurs. Nous espérons que ces insights vous inciteront à envisager la sécurité non pas comme un bouclier défensif, mais comme un tremplin vers l'innovation. Voici donc l'enjeu : protéger l'essentiel tout en ouvrant la voie à de nouvelles opportunités.

# À propos de ce rapport

Salesforce a interrogé plus de 4 000 décideurs informatiques dans le monde, dont plus de 2 000 experts spécialisés en sécurité, protection des données ou conformité, afin de révéler des insights clés sur :

- **L'évolution des menaces et les nouvelles priorités en matière de sécurité :** pourquoi la sécurité et la conformité restent des enjeux majeurs, et comment les entreprises renforcent leurs défenses.
- **Le renforcement de la confiance des clients dans un monde piloté par l'IA :** comment des mesures de sécurité robustes peuvent rassurer les clients et les parties prenantes.
- **L'exploitation de l'IA pour renforcer la posture de sécurité :** comment les agents IA et les technologies avancées améliorent la détection, la réaction et la résilience.

Sauf indication contraire, les données de ce rapport proviennent d'une enquête en double aveugle réalisée entre le 24 décembre 2024 et le 3 février 2025. L'enquête a totalisé 4 275 réponses de responsables informatiques, dont 2 138 spécialisés dans la sécurité, la protection des données ou la conformité, répartis en Amérique du Nord, en Amérique latine, en Asie-Pacifique et en Europe. Consultez la page 25 pour connaître les données démographiques de l'enquête.

Compte tenu des arrondis, les pourcentages ne sont pas tous égaux à 100 %. Tous les calculs de comparaison sont réalisés à partir de chiffres non arrondis.

- Australia‡
- Belgium
- Brazil
- Canada
- Denmark†
- Finland†
- France
- Germany
- India
- Ireland
- Italy
- Japan
- Mexico
- Netherlands
- New Zealand‡
- Norway†
- Portugal
- Singapore
- South Africa
- South Korea
- Spain
- Sweden†
- Switzerland
- United Arab Emirates
- United Kingdom
- United States

**2 138** responsables en sécurité, protection des données et conformité interrogés dans le monde entier

† ‡ Groupes d'échantillon unique

# Sommaire

**Synthèse** . . . . . 05

**Chapitre 1 :** Introduction . . . . . 06

**Chapitre 2 :** La sécurité à l'ère de l'IA agentique . . . . . 11

**Chapitre 3 :** La gouvernance de l'IA agentique . . . . . 15

**Chapitre 4 :** Gagner la confiance des clients à l'ère de l'IA agentique . . . . . 20

**L'avis de Salesforce** . . . . . 23

**Données démographiques** . . . . . 25

# Synthèse

Les responsables informatiques font face à une complexité croissante, entre la montée des cybermenaces, l'essor fulgurant de l'IA et l'évolution constante de la réglementation. Pour faire face à des risques comme les ransomwares ou l'empoisonnement des données, les entreprises investissent davantage dans la sécurité.

Des pratiques de sécurité rigoureuses favorisent l'innovation. Les entreprises qui intègrent la sécurité de manière proactive, par des approches de DevSecOps ou de détection avancée des menaces, se disent plus confiantes dans l'adoption d'agents IA.

Mais les défis en matière de conformité ne cessent de croître à mesure que le contexte réglementaire devient de plus en plus complexe. Nombreuses sont les entreprises qui se disent mal préparées aux évolutions liées à l'IA, d'où le besoin urgent de directives plus claires et d'une gouvernance proactive. L'exigence de transparence des clients sur l'utilisation de leurs données souligne encore davantage l'importance d'avoir une stratégie de sécurité rigoureuse.

L'IA présente à la fois des opportunités et des risques. Si elle améliore la détection des menaces et l'automatisation, elle suscite également des inquiétudes liées à la confidentialité des données et aux biais. Pour tirer parti de l'IA de manière responsable, il faut une gouvernance rigoureuse, une gestion proactive des risques et des processus transparents.

1. **Les budgets consacrés à la sécurité sont en hausse :** 75 % des entreprises prévoient d'augmenter leurs investissements pour contrer l'empoisonnement des données ou la détection avancée.
2. **La confiance est primordiale :** 64 % des clients estiment que les entreprises sont imprudentes avec leurs données, et 61 % pensent que les progrès de l'IA rendent la protection des données plus cruciale que jamais, un signal clair pour faire de la gestion des données une priorité.
3. **La conformité devient plus complexe :** 68 % des responsables sécurité estiment que la conformité est plus difficile à assurer dans un environnement réglementaire en constante évolution, et 43 % se sentent mal préparés aux futures réglementations liées à l'IA.
4. **L'IA peut renforcer les tactiques de défense :** 79 % des responsables sécurité pensent que les agents IA poseront de nouveaux défis en matière de sécurité et de conformité, mais 80 % y voient aussi des leviers d'amélioration.

# 1

# Introduction

01

# Les budgets de sécurité augmentent face à l'évolution des menaces et des tactiques de défense

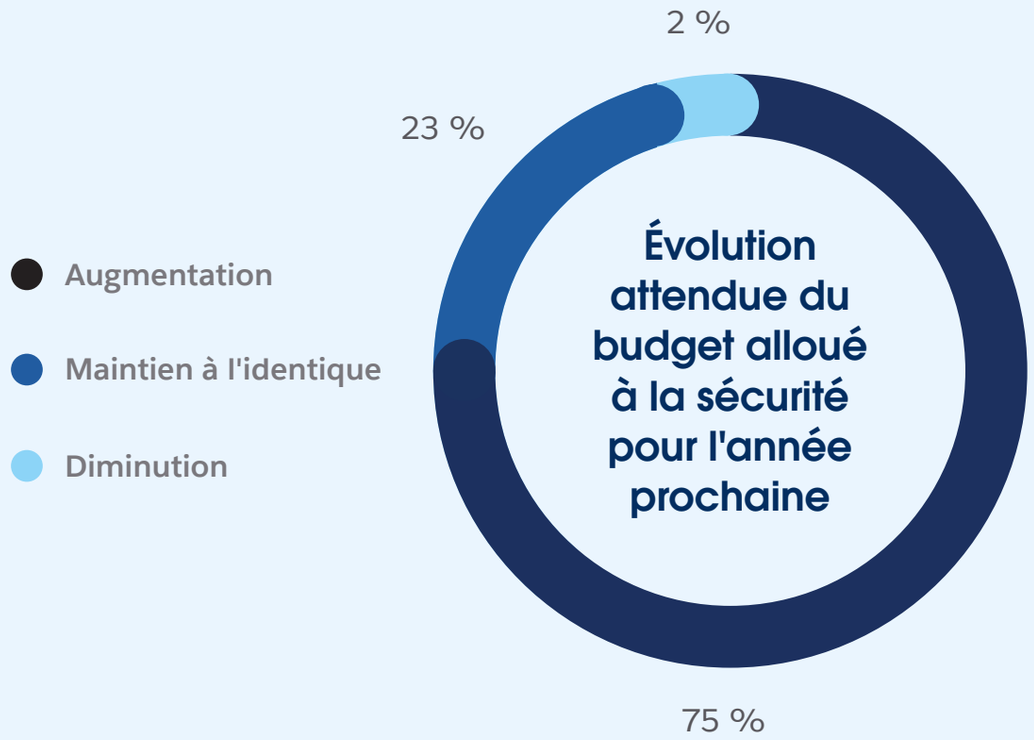
Face à l'intensification des menaces de cybersécurité, de nombreuses entreprises consacrent davantage de ressources à leurs programmes de sécurité. Les attaques deviennent plus sophistiquées (violations dans le cloud, empoisonnement des données) et nécessitent des mesures défensives plus poussées. C'est pourquoi la plupart des services informatiques prévoient une hausse de leur budget sécurité au cours de l'année à venir. En tête des tactiques jugées les plus efficaces : le chiffrement des données, la sauvegarde des données et la gestion des identités et des accès.

## Menaces les plus préoccupantes

1. Menaces de sécurité dans le cloud
2. Empoisonnement des données
3. Logiciels malveillants
4. Hameçonnage
5. Ransomware

## Tactiques de défense les plus efficaces

1. Chiffrement des données
2. Sauvegarde et restauration des données
3. Gestion des accès et des identités
4. Stratégies de confiance zéro
5. Masquage des données



01

# Une posture de sécurité solide favorise l'innovation

Cette hausse des investissements ne vise pas uniquement à limiter les risques : une posture de sécurité robuste permet aux équipes d'innover en toute confiance. Qu'il s'agisse d'adopter des solutions cloud natives ou d'expérimenter des outils alimentés par l'IA, les entreprises se sentent plus sereines pour lancer de nouvelles initiatives lorsqu'elles savent que leur stratégie de défense en profondeur peut suivre le rythme des menaces actuelles.

Concilier sécurité et déploiement de nouvelles technologies peut sembler difficile. Pourtant, les services informatiques les plus visionnaires prouvent que c'est tout à fait possible. Nos recherches montrent que les équipes dotées de protocoles de sécurité et de gouvernance solides se classent également mieux en termes d'innovation, preuve que des défenses structurées et proactives offrent en réalité plus de liberté pour explorer.

Lorsque les bonnes pratiques de sécurité (chiffrement, protocoles de sauvegarde ou formation des employés) sont intégrées aux processus du quotidien, il devient bien plus simple de tester à l'échelle sans compromettre l'intégrité des systèmes ou des données.

## Services informatiques affichant une capacité d'innovation supérieure à la moyenne

**9 % plus** susceptibles d'avoir des politiques et des pratiques de sécurité et de gouvernance supérieures à la moyenne

**19 % moins** susceptibles d'avoir de la difficulté à concilier sécurité et objectifs commerciaux

**6 % plus** susceptibles d'avoir des politiques et des pratiques de confidentialité supérieures à la moyenne

**13 % plus** susceptibles de former activement les employés aux bonnes pratiques de sécurité

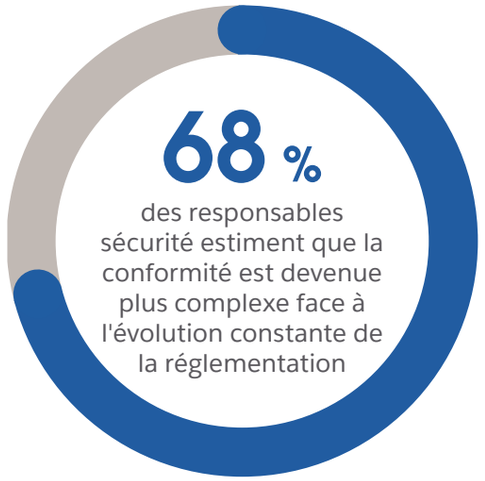
01

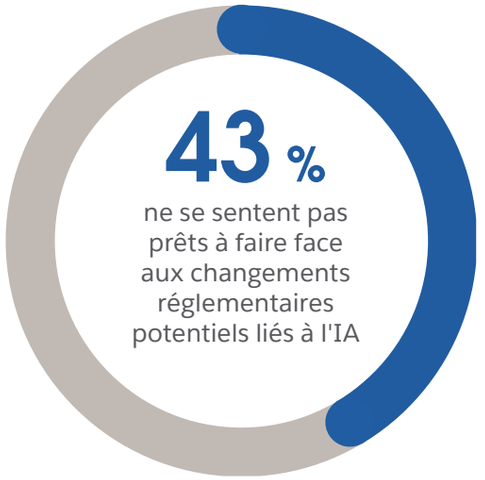
# La conformité devient un défi de plus en plus complexe

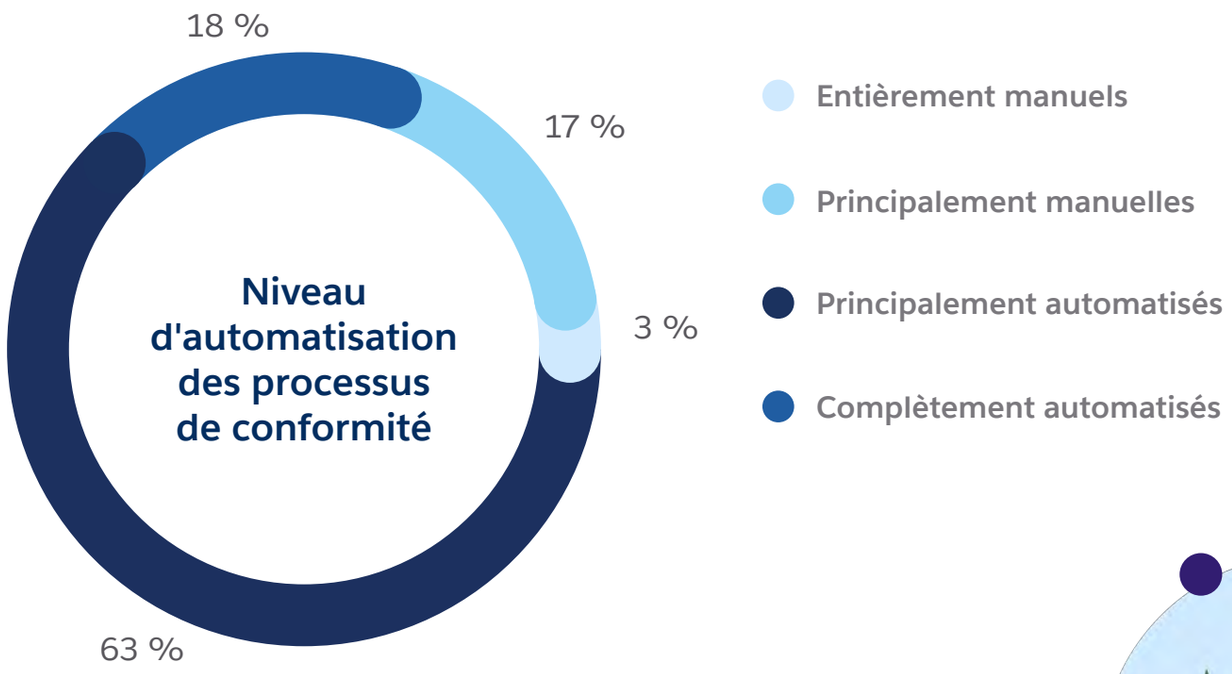
À mesure que les entreprises se développent à l'international et que de nouvelles réglementations voient le jour, la conformité s'alourdit. De nombreux responsables sécurité affirment devoir redoubler d'efforts pour répondre aux exigences, qui varient selon les régions et les secteurs. Si on ajoute à cela de nouvelles règles encadrant l'IA, il n'est pas étonnant que les équipes peinent à suivre.

Mais la conformité ne se résume pas à cocher des cases réglementaires : elle renforce également la crédibilité auprès des clients et des parties prenantes. Si certains processus sont désormais entièrement automatisés, une part importante repose encore sur des actions manuelles, ce qui ouvre la porte aux erreurs et aux incohérences d'un service ou d'un pays à l'autre.

## Préoccupations réglementaires des responsables sécurité




01

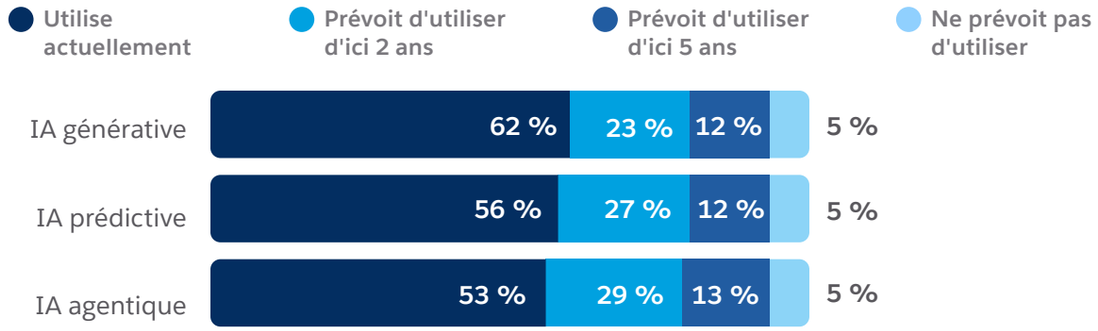
# L'IA, entre opportunités et menaces pour la sécurité

L'IA est déjà très répandue, et tout indique qu'elle le sera encore plus dans les années à venir. La dernière vague d'IA a vu émerger des agents capables de percevoir, de raisonner et d'agir de façon autonome pour accomplir des tâches précises, avec peu voire pas de supervision humaine. Les responsables sécurité reconnaissent que, sans gouvernance adéquate, ces agents pourraient introduire de nouveaux risques en matière de sécurité et de conformité. Il n'est donc pas étonnant que les DSI classent ces deux enjeux au premier rang de leurs préoccupations en matière d'IA, et comme critères de sélection numéro un des fournisseurs d'IA[1].

Mais les responsables sécurité y voient aussi une formidable opportunité. Bien conçus, les agents IA peuvent renforcer la détection des menaces, automatiser la gestion des vulnérabilités et soutenir les efforts de conformité à l'échelle. Cette double réalité impose une stratégie à deux volets : tirer parti de l'IA pour renforcer les défenses, tout en encadrant rigoureusement son usage pour maîtriser les risques.

[1] Étude « CIO Dilemma » de Salesforce, octobre 2024.

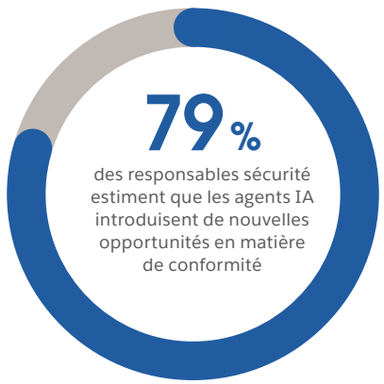
## Utilisation des différentes formes d'IA par les entreprises informatiques[2]




[2] Pourcentage basé sur l'ensemble des répondants à l'enquête « Focus sur l'IT » (comprenant des responsables développement et sécurité).

## Les responsables sécurité voient dans les agents IA à la fois des défis et des leviers d'opportunités




# 2

# La sécurité à l'ère de l'IA agentique

02

# Les équipes se préparent à des menaces d'un nouveau genre avec l'IA

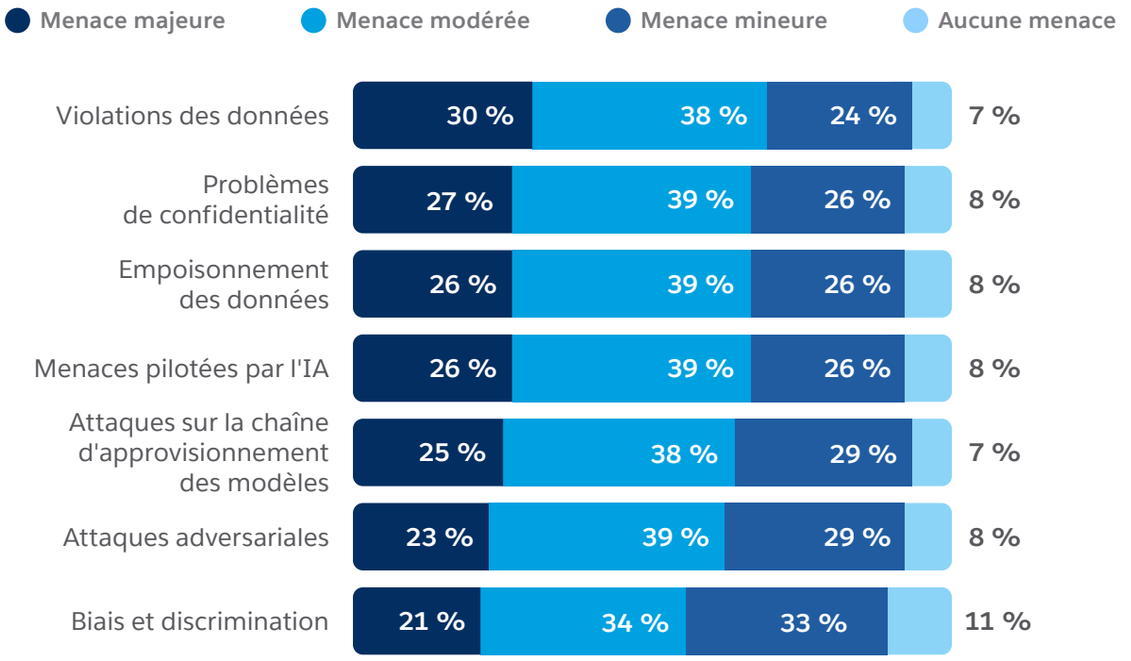
Les équipes de sécurité ont toujours dû faire face à des menaces comme les logiciels malveillants et l'hameçonnage, mais l'IA a changé la donne. Les cybercriminels s'en servent pour automatiser les attaques à grande échelle, tandis que les responsables sécurité doivent protéger un périmètre toujours plus grand, incluant l'infrastructure cloud, le télétravail et les objets connectés. La majorité d'entre eux pensent que les cybermenaces pilotées par l'IA pourraient bientôt dépasser les capacités des défenses traditionnelles, soulignant la nécessité de repenser les tactiques et de maintenir une vigilance constante.

Pour contrer efficacement ces nouvelles menaces, il est essentiel de renforcer la résilience des données à l'échelle de l'entreprise. Cela passe notamment par des contrôles d'accès stricts pour limiter l'exposition et garantir que seules les personnes autorisées accèdent aux informations sensibles. La surveillance proactive des événements, appuyée par l'automatisation, permet également de détecter plus tôt les menaces. Enfin, en cas d'incident, une solution de sauvegarde fiable assure aux utilisateurs un accès continu à des données exactes et à jour.

**75 %** des responsables sécurité estiment que les cybermenaces pilotées par l'IA dépasseront bientôt les capacités des défenses traditionnelles

**79 %** pensent que leurs pratiques de sécurité doivent évoluer avec l'essor de l'IA

## Perception des menaces par les responsables sécurité face à l'essor de l'IA



02

# Comment les agents IA peuvent renforcer la sécurité des données

Les agents IA ne sont pas forcément synonymes de complexité : ils peuvent devenir de précieux alliés en matière de cybersécurité. Capables d'analyser rapidement de grands volumes de données, ils détectent des comportements inhabituels, automatisent les tâches répétitives comme les mises à jour ou les contrôles de conformité, et accélèrent l'analyse des menaces potentielles. De nombreux responsables sécurité estiment que ces agents peuvent ainsi renforcer efficacement leur stratégie de défense en profondeur.

Exemples de l'intérêt des agents IA pour la sécurité et la conformité :

- **Détection des menaces et réponse :** signalement d'activités anormales et coordination de mesures correctives dans les pus brefs délais.
- **Identification des biais dans les modèles :** audits continus pour repérer les biais et les vulnérabilités afin de garantir fiabilité et équité.
- **Automatisation de la conformité :** suivi des politiques sur l'ensemble des systèmes pour réduire le besoin de supervision manuelle.

En confiant aux agents IA les tâches répétitives ou volumineuses, les équipes peuvent recentrer leurs efforts sur des enjeux stratégiques, une nécessité à l'heure où les menaces évoluent plus vite que les capacités d'intervention humaine.

**100 %**

des responsables sécurité estiment que les agents IA peuvent améliorer au moins une problématique de sécurité

### Améliorations attendues en matière de sécurité et de conformité grâce aux agents IA

1. Audit et suivi des performances des modèles d'IA
2. Détection des menaces
3. Identification et atténuation des biais dans les modèles d'IA
4. Surveillance des événements en temps réel
5. Détection des anomalies et analyse comportementale

# Focus : L'approche DevSecOps

Les risques en matière de sécurité ne se limitent pas aux environnements en production. Il est également indispensable de protéger les environnements de développement. Les vulnérabilités introduites en amont peuvent avoir un impact tout aussi important sur la posture de sécurité de l'entreprise, en particulier lorsqu'elle fait évoluer l'IA à grande échelle.

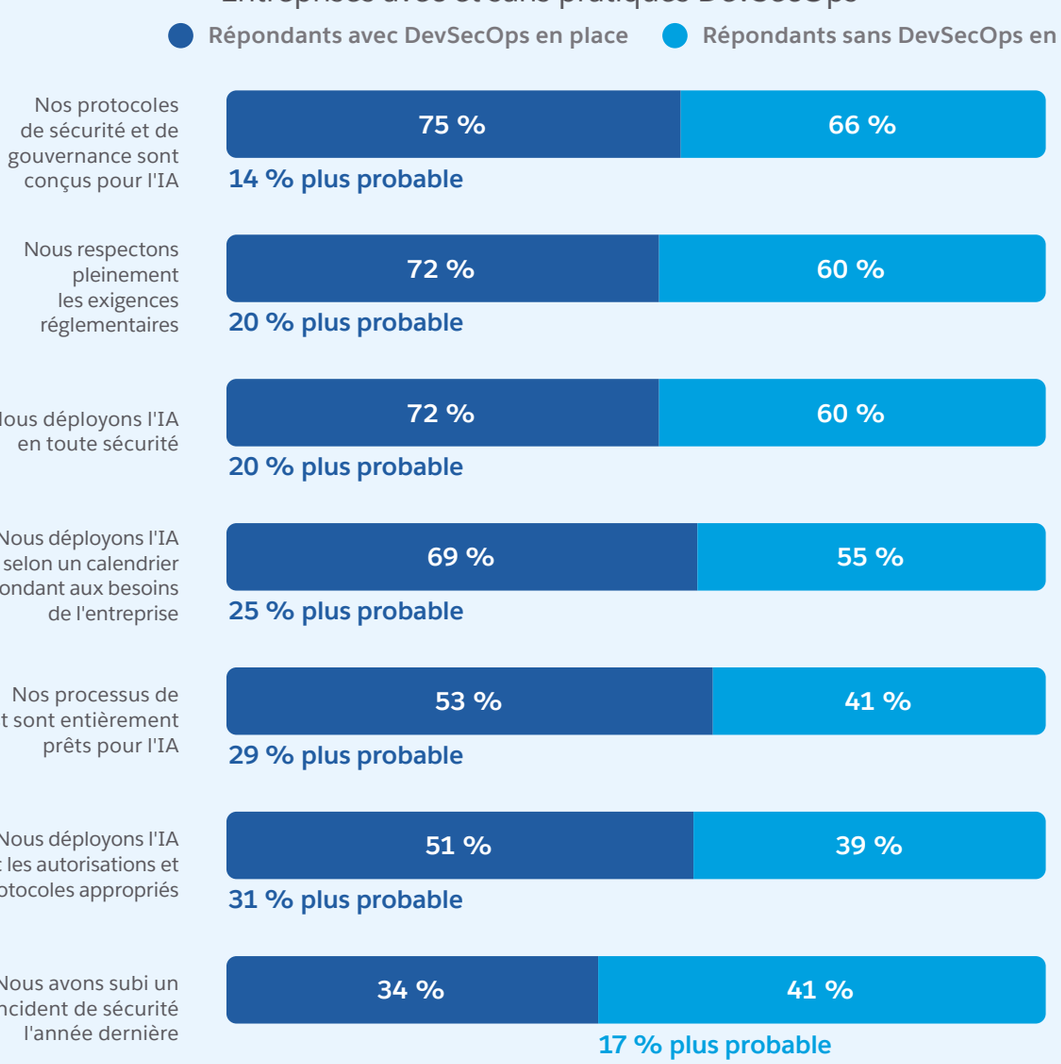
L'approche DevSecOps intègre la sécurité à chaque étape du cycle de développement. Plutôt que d'attendre la dernière minute pour corriger les failles, le DevSecOps intègre les analyses de sécurité, les contrôles de conformité et les processus de remédiation dès la phase de conception, jusqu'au déploiement.

Cette approche proactive est précieuse pour les équipes de sécurité qui font leurs premiers pas avec l'IA. De nombreux responsables informatiques estiment que leur niveau de confiance augmente lorsqu'ils déploient des agents IA ou des solutions d'analyse avancée, car les vulnérabilités sont détectées tôt et régulièrement. Le DevSecOps vise à favoriser la collaboration entre les équipes de développement, de sécurité et d'exploitation, afin de réduire les délais de correction, de limiter les imprévus et de renforcer la confiance envers les systèmes d'IA de l'entreprise.

**85 %** des entreprises informatiques suivent un modèle DevSecOps

## Part des responsables informatiques en accord avec les affirmations suivantes[1]

Entreprises avec et sans pratiques DevSecOps




1 Pourcentages et calculs basés sur l'ensemble des répondants à l'enquête « Focus sur l'IT » (comprenant des responsables développement et sécurité).

# 3

# La gouvernance de l'IA agentique

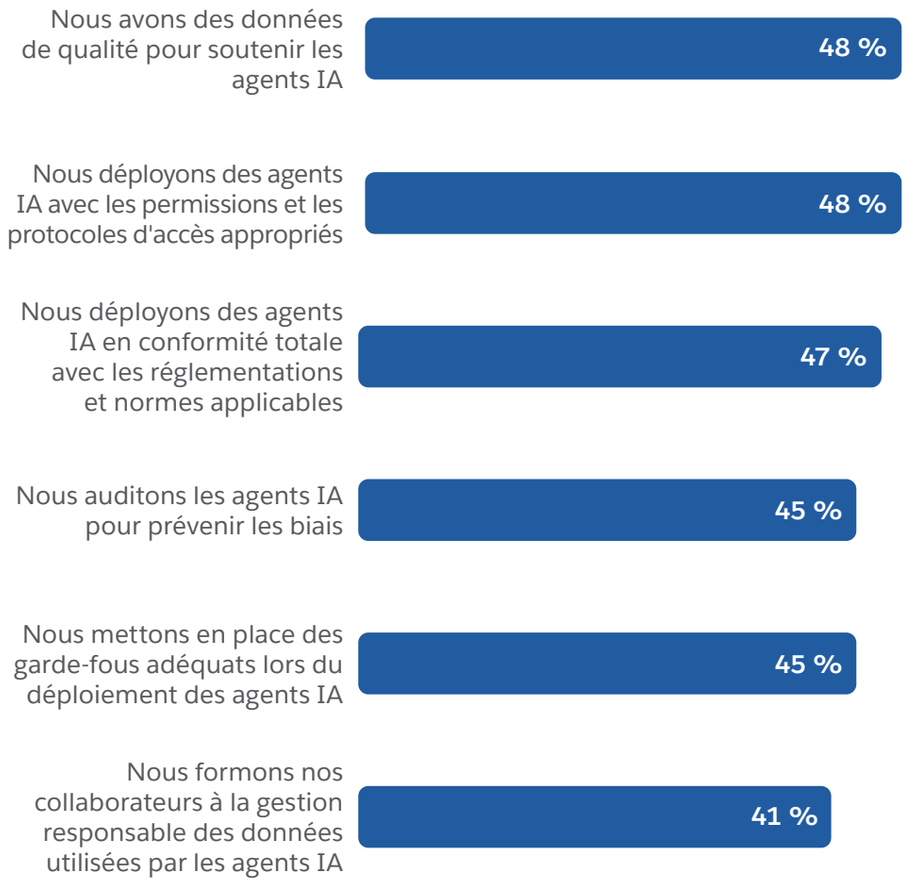
03

# Conformité et gouvernance des agents IA : un chantier en cours

Toute nouvelle technologie, du cloud à l'IA, soulève des questions de gouvernance et de conformité. Si la plupart des entreprises disposent de politiques solides pour leurs infrastructures traditionnelles, peu ont encore mis au point des cadres adaptés aux agents IA. Ce manquement provient souvent de réglementations floues, de systèmes cloisonnés et d'une dépendance aux processus manuels.

Avec 55 % des responsables sécurité qui ne se sentent pas pleinement confiants quant à leur capacité à déployer des agents IA avec des garde-fous adéquats, et 53 % qui doutent de leur conformité aux normes et aux réglementations, beaucoup d'entreprises ont clairement des progrès à faire dans ce domaine.

## La confiance des responsables sécurité dans les domaines suivants

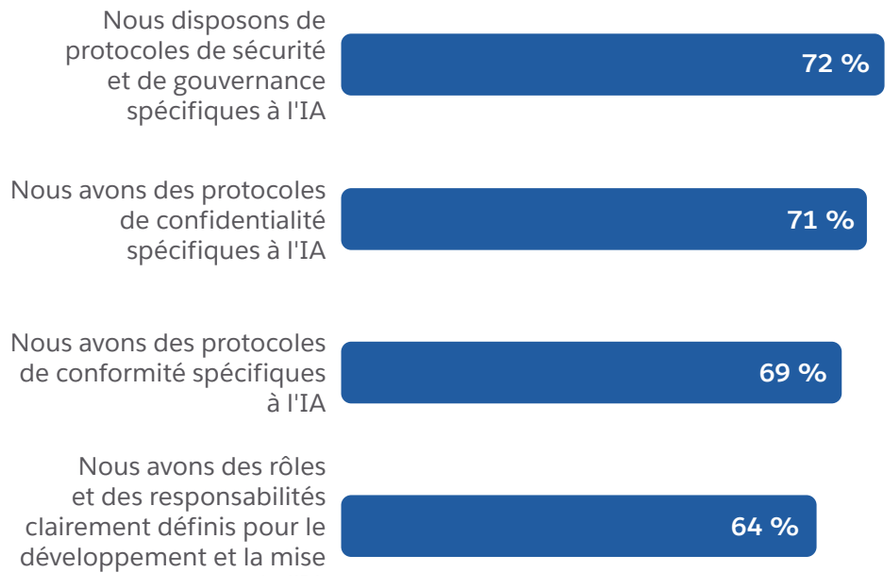



03

# La responsabilité de la gouvernance de l'IA se précise dans les entreprises

Qui supervise l'éthique, la confidentialité, la sécurité et la conformité de l'IA face à des réglementations changeantes et des enjeux majeurs ? Avez-vous mis en place des protocoles de sécurité, de confidentialité et de conformité spécifiques à l'IA ? Ces questions sont essentielles pour les entreprises qui déploient l'IA aujourd'hui. Bien qu'il reste des progrès à faire, plus de 70 % des responsables sécurité affirment déjà disposer de protocoles de sécurité et de confidentialité pour l'IA, et 64 % ont clairement défini les rôles et les responsabilités en matière de développement et de gouvernance de l'IA.

## Responsables sécurité d'accord avec les déclarations suivantes




03

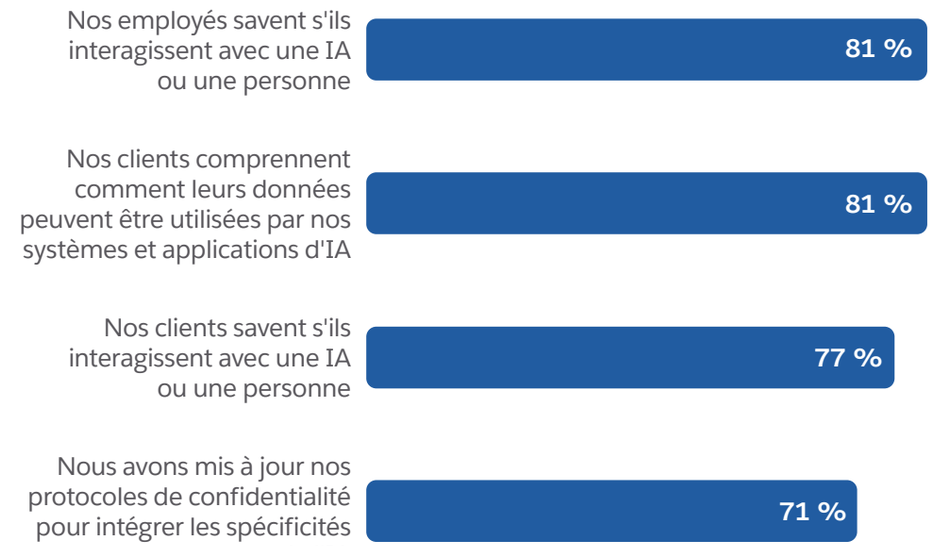
# La transparence, clé de la confiance envers l'IA

Clients et autorités de régulation exigent de plus en plus de comprendre comment les données sont utilisées, surtout lorsque l'IA est impliquée. La transparence n'est pas un luxe, c'est le fondement de la confiance. Selon une étude Salesforce, 42 % des clients affirment qu'une meilleure transparence sur l'utilisation de l'IA renforcerait leur confiance. Par ailleurs, 31 % déclarent que la possibilité d'expliquer les résultats produits par l'IA renforcerait également cette confiance.[1]

La bonne nouvelle, c'est que beaucoup d'entreprises semblent bien s'en sortir sur ce point. Plus des trois quarts (77 %) des responsables sécurité estiment que les clients savent quand ils interagissent avec une IA plutôt qu'avec une personne, et 81 % pensent que les clients comprennent comment leurs données peuvent être utilisées par les systèmes et les applications d'IA de l'entreprise.

[1] Rapport Salesforce « Focus sur le client connecté à l'ère de l'IA », octobre 2024.

## Responsables sécurité d'accord avec les déclarations suivantes[2]




[2] Base : personnes interrogées dans des entreprises utilisant l'IA.

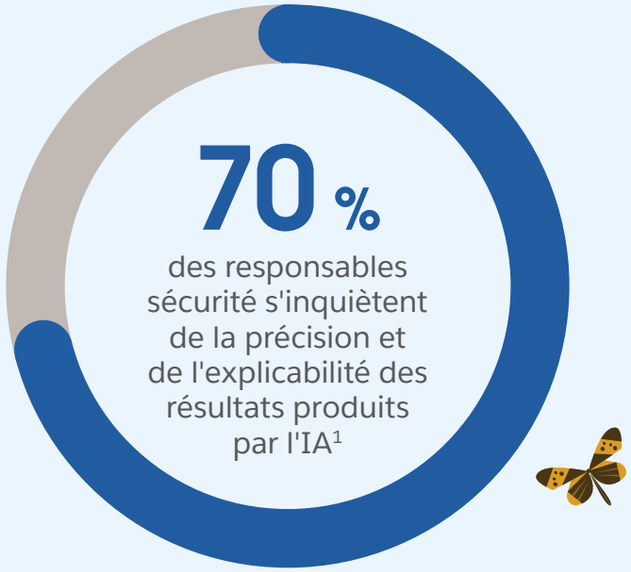
« En donnant la priorité à la sécurité dans nos outils et applications d'IA, nous protégeons non seulement nos systèmes internes, mais nous renforçons aussi la confiance de nos clients. La transparence et des mesures de sécurité solides assurent à nos clients que leurs données sont traitées en toute sécurité, même lorsqu'ils interagissent avec des solutions pilotées par l'IA. »

**ADAM HOOPER**
**RESPONSABLE DES PLATEFORMES CENTRALES, DPD**

03

# L'explicabilité, un enjeu clé dans l'adoption de l'IA

Au-delà de la transparence, l'explicabilité désigne la capacité à expliquer, étape par étape, comment une application ou un agent IA traite les données et produit des résultats. Parmi les entreprises utilisant l'IA, 70 % des responsables sécurité considèrent que la précision et l'explicabilité de l'IA sont des sujets préoccupants, et moins de la moitié se disent pleinement confiants dans leur capacité à expliquer les résultats générés par l'IA.





[1] Base : personnes interrogées dans des entreprises utilisant l'IA.

# 4

# Gagner la confiance des clients à l'ère de l'IA agentique

04

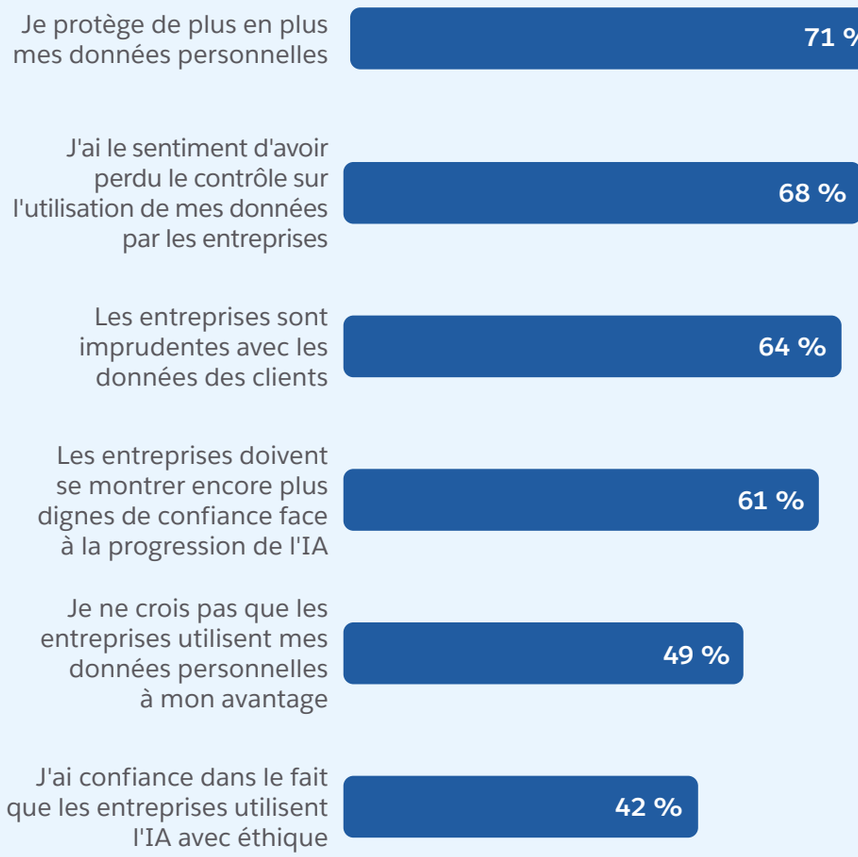
# Les doutes autour des données et de l'IA soulignent l'importance de la confiance

Les clients s'interrogent de plus en plus sur la manière dont leurs données sont collectées, stockées et utilisées, en particulier lorsque l'IA est en jeu. La confiance des clients envers les entreprises ne cesse de faiblir. Plus des deux tiers des clients ont le sentiment de perdre le contrôle sur l'usage de leurs données personnelles par les entreprises, et près de la moitié estiment que ces données ne sont pas exploitées à leur avantage.[1] À mesure que les entreprises développent l'utilisation de l'IA agentique et manipulent les données qui l'alimentent, ce rapport de confiance entre clients et entreprises deviendra encore plus complexe.

Cependant, les équipes informatiques et de sécurité, en première ligne des efforts pour renforcer cette confiance, peuvent agir pour améliorer la situation. Les clients déclarent que leur confiance dans l'IA augmente lorsque les entreprises mettent en place des protections pour l'IA, font preuve de transparence sur son utilisation, améliorent la précision des résultats générés par l'IA et prennent en compte leurs retours[1].

**71 %** des clients déclarent que leur confiance envers les entreprises baisse, contre 52 % en 2023 et 47 % en 2022[1]

## Clients en accord avec les énoncés suivants[1]




[1]Rapport Salesforce « Focus sur le client connecté à l'ère de l'IA », octobre 2024.

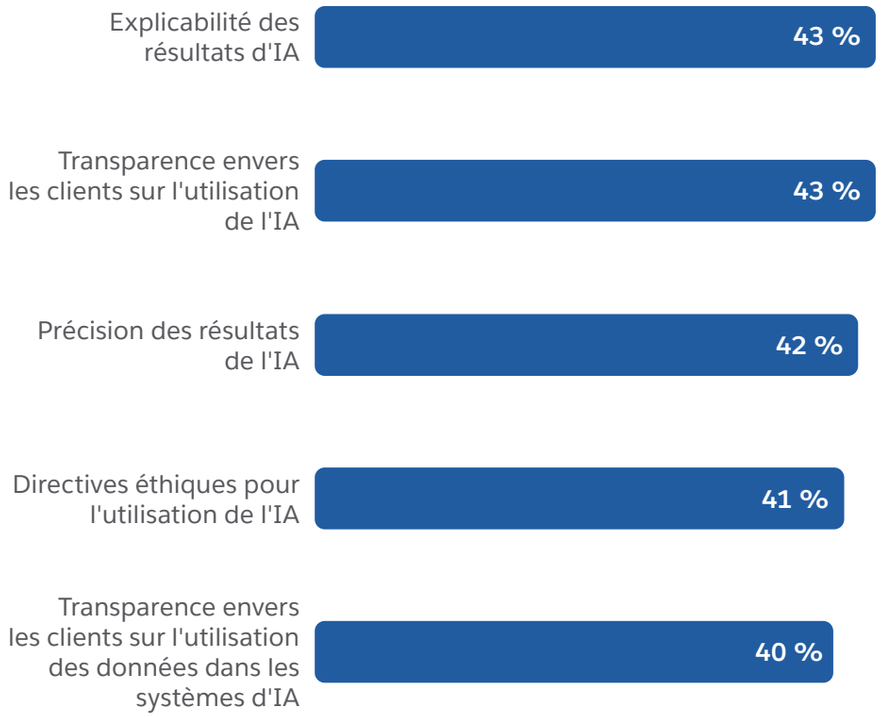
04

# Bilan de l'IA éthique et transparente

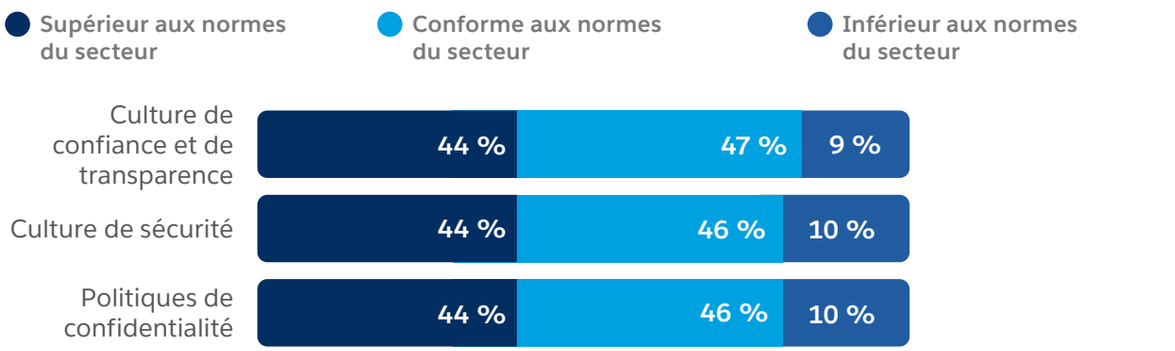
Les responsables sécurité partagent avec les clients l'importance d'une IA transparente et éthique, mais doivent encore améliorer leurs pratiques et leurs capacités. En effet, 64 % d'entre eux estiment que les clients hésitent à adopter l'IA en raison de préoccupations liées à la sécurité ou à la confidentialité.

Comment faire mieux ? Bien que plus de 90 % des responsables sécurité considèrent que leur entreprise respecte ou dépasse les normes du secteur en matière de politiques de confidentialité et de culture de sécurité, de transparence et de confiance, moins de la moitié jugent leur organisation excellente pour expliquer les résultats de l'IA, garantir leur précision et assurer la transparence quant à l'utilisation des données dans les systèmes d'IA.

## Responsables sécurité jugeant excellents dans leur entreprise les éléments suivants[1]




## Auto-évaluation des responsables sécurité sur les éléments suivants



# L'avis de Salesforce

# L'avis de Salesforce

La sécurité est passée d'une fonction réactive à un moteur de croissance stratégique et d'innovation. Avec la progression de l'IA, les responsables informatiques visionnaires conçoivent des infrastructures capables à la fois de contrer les nouvelles menaces et d'introduire de nouvelles possibilités. Qu'il s'agisse de renforcer la détection des menaces ou d'établir des cadres de gouvernance plus solides, les transformations actuelles façonneront la manière dont les entreprises opèrent et rivalisent dans les années à venir.

Plusieurs tendances dessinent déjà ce futur :

1. **Complexité réglementaire croissante :** face à l'émergence de réglementations sur l'IA dans différentes régions du globe, la gestion de la conformité sera un chantier permanent.
2. **Adoption proactive de l'IA :** les entreprises qui verront les agents IA comme des alliés en matière de sécurité, plutôt que comme une menace, découvriront de nouveaux gains d'efficacité et de belles opportunités de différenciation.
3. **Évolution continue des compétences :** les métiers de la sécurité se transformeront, exigeant de nouvelles compétences en supervision de l'IA, en gouvernance des données et en prise de décisions éthiques.

En cette période charnière, aligner les objectifs de sécurité avec les ambitions générales de l'entreprise aidera à maintenir la résilience face aux changements. En misant sur la confiance, la transparence et des mesures de sécurité robustes, les responsables informatiques pourront transformer les vulnérabilités potentielles en avantages compétitifs, ouvrant la voie à un avenir plus sûr, plus agile et plus innovant.

# Données démographiques

# Données démographiques

## Pays

Australie ..... N=64, 3 %
Belgique ..... N=50, 2 %
Brésil ..... N=100, 5 %
Canada ..... N=100, 5 %
France ..... N=100, 5 %
Allemagne ..... N=100, 5 %
Inde ..... N=100, 5 %
Indonésie ..... N=75, 4 %
Irlande ..... N=50, 2 %
Israël ..... N=50, 2 %
Italie ..... N=100, 5 %
Japon ..... N=100, 5 %
Mexique ..... N=100, 5 %
Pays-Bas ..... N=100, 5 %
Nouvelle-Zélande ..... N=36, 2 %
Pays nordiques
(DK, FI, NO, SE) ..... N=100, 5 %
Portugal ..... N=50, 2 %
Singapour ..... N=50, 2 %
Corée du Sud ..... N=100, 5 %
Espagne ..... N=100, 5 %
Suisse ..... N=50, 2 %
Thaïlande ..... N=63, 3 %
Émirats arabes unis ..... N=50, 2 %
Royaume-Uni ..... N=100, 5 %
États-Unis ..... N=250, 12 %

## Secteur d'activité

Architecture, ingénierie
et construction ..... N=112, 5 %
Automobile ..... N=131, 6 %
Communication ..... N=32, 1 %
Biens de consommation ..... N=150, 7 %
Énergie et services publics ..... N=78, 4 %
Services financiers ..... N=163, 8 %
Gouvernement /
Secteur public ..... N=44, 2 %
Santé ..... N=100, 5 %
Sciences de la vie
et biotechnologie ..... N=92, 4 %
Industrie manufacturière ... N=287, 13 %
Médias et divertissement ..... N=57, 3 %
Organismes à but non lucratif N=11, 1 %
Services professionnels
et commerciaux..... N=120, 6 %
Commerce de détail ..... N=268, 13 %
Chaîne d'approvisionnement et
logistique..... N=65, 3 %
Technologie ..... N=372, 17 %
Voyage et hôtellerie ..... N=56, 3 %

## Fonction

Cadre dirigeant ..... N=267, 12 %
Vice-président
ou équivalent ..... N=746, 35 %
Directeur ou équivalent... N=1 125, 53 %

## Taille de l'entreprise

Grande entreprise
(>3 500 collaborateurs) ..... N=466, 22 %
Entreprise intermédiaire
(200-3 500 collaborateurs) N=1 358, 64 %
PME
(<200 collaborateurs) ..... N=466, 15 %

# Envie d'en savoir plus ?


## 6 étapes de sécurité préalables à l'intégration d'Agentforce

Découvrez comment renforcer votre Agentforce grâce à des stratégies de sécurité avancées.

EN SAVOIR PLUS >


## Le guide du DevSecOps par Salesforce

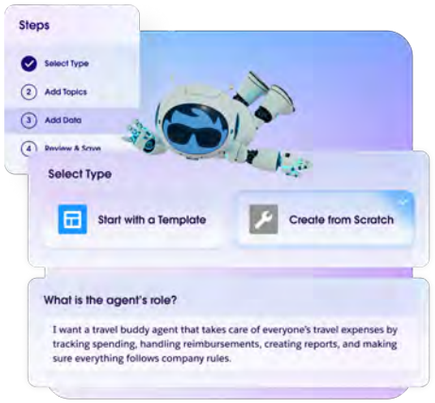
Découvrez comment une solide stratégie de DevSecOps vous permet d'évoluer, de tester en toute sécurité et de déployer rapidement votre Agentforce.

EN SAVOIR PLUS >


## Guide sur les meilleures pratiques en matière de sécurité des données

Apprenez à innover avec l'IA en adoptant les meilleures pratiques de sécurité.

EN SAVOIR PLUS >




## En savoir plus sur Agentforce

Découvrez ce qui distingue Agentforce des autres IA agentiques et ce qu'il peut apporter à votre entreprise.

EN SAVOIR PLUS >