Gartner

# Les 10 principales tendances technologiques stratégiques pour 2026

# Maîtriser les enjeux d'un monde où l'IA et l'hyperconnectivité redéfinissent les règles

En 2026, les responsables technologiques devront faire face à une année charnière, dans un contexte où bouleversements, innovation et risques s'intensifient à un rythme inédit. Bien plus que de simples évolutions technologiques, les 10 tendances technologiques stratégiques majeures identifiées par Gartner pour 2026 sont de puissants moteurs de transformation des entreprises, appelant une réponse forte des instances dirigeantes.

Les tendances identifiées cette année reflètent les réalités d'un monde façonné par l'IA et l'hyperconnectivité, où aucune compétence prise isolément ne suffit à répondre à la complexité des enjeux. Regroupées en trois grands axes, elles reflètent les stratégies adoptées par les entreprises leaders pour innover, se démarquer et consolider durablement leur position sur le marché.

## L'architecte

Posez les bases d'un système digital sécurisé, évolutif et résolument adaptatif grâce à des plateformes de développement conçues pour l'IA, aux supercalculateurs dédiés à l'IA et aux technologies de Confidential Computing.

## L'intégrateur

Combinez différentes technologies, systèmes multiagents, modèles de langage spécialisés et IA physique, pour catalyser de nouvelles dynamiques de croissance et de valorisation.

## L'avant-gardiste

Renforcez la confiance, la gouvernance et la sécurité grâce à la cybersécurité préventive, à la traçabilité digitale, aux plateformes de sécurité dédiées à l'IA et à la maîtrise géostratégique des données.

À mesure que vous découvrez ces tendances, vous êtes invités à évaluer comment elles peuvent contribuer à vos ambitions stratégiques et s'intégrer à votre feuille de route pour favoriser une croissance durable et renforcer vos avantages concurrentiels.

**Gene Alvarez**
Vice-président, expert en insights commerciaux et technologiques, Gartner

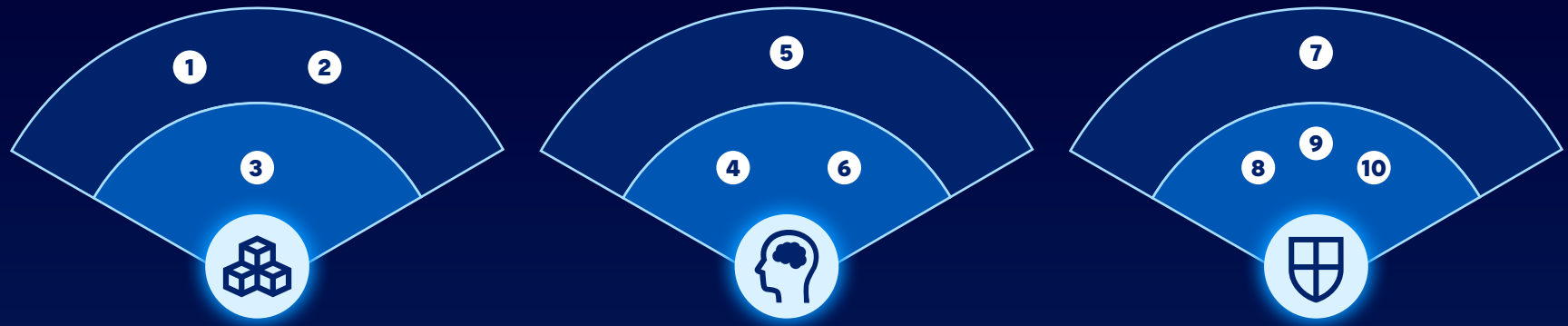
# Principales tendances stratégiques technologiques Gartner pour 2026

Gartner a identifié ces 10 tendances clés pour leur capacité à stimuler l'innovation, renforcer la résilience et instaurer un climat de confiance durable dans un monde hyperconnecté, façonné par l'IA.

Véritables priorités stratégiques, elles exigent des responsables des technologies qui allient vision, discernement et capacité à agir avec détermination.

**Aujourd'hui** (1 à 3 ans)

**À moyen terme** (3 à 5 ans)




## L'architecte

1. Plateformes de développement conçues pour l'IA
2. Supercalculateurs optimisés pour l'IA
3. Confidential Computing

## L'intégrateur

4. Systèmes multi-agents
5. Modèles de langage spécialisés
6. IA physique

## L'avant-gardiste

7. Cybersécurité préventive
8. Provenance des données digitales
9. Plateformes de sécurité dédiées à l'IA
10. Geopatriation (rapatriement des données stratégiques)

# L’architecte

## Posez les fondations d’un système digital sûr, évolutif et résolument tourné vers l’avenir.

Pour favoriser l’innovation et la résilience, les responsables des technologies doivent faire évoluer leurs plateformes et leur infrastructure. Axées sur la mise en place de fondations adaptées à une exploitation optimale de l’IA, les tendances de l’axe Architecte permettent de conjuguer rapidité, sécurité et évolutivité, des leviers indispensables pour réussir dans un monde hyperconnecté où l’IA redéfinit les standards de performance et de compétitivité.

1

# Plateformes de développement conçues pour l'IA

**De quoi parle-t-on exactement ?**
Grâce à l'IA générative, les plateformes de développement conçues pour l'IA permettent d'accélérer et de simplifier la création de logiciels comme jamais auparavant. Ces plateformes s'étendent des outils générant un logiciel complet à partir d'une seule instruction, aux solutions de développement intuitif accessibles aux non-spécialistes, jusqu'aux agents d'IA capables de travailler ensemble pour concevoir des applications de manière autonome.

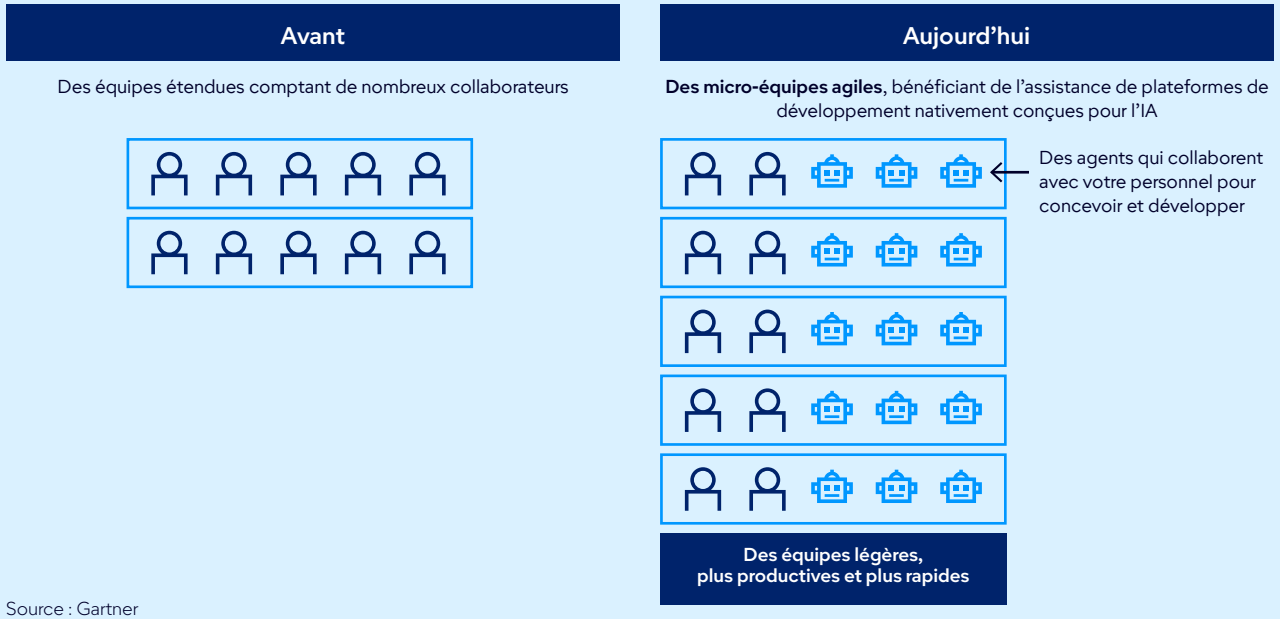
**Pourquoi ces approches s'imposent-elles maintenant ?**
Les DSI se montrent enthousiastes face à l'accélération du développement logiciel et aux gains de productivité, tandis que les dirigeants et les responsables financiers y voient une opportunité stratégique de réduction des coûts. Grâce aux plateformes conçues pour l'IA, de petites équipes peuvent créer plus d'applications sans nécessairement disposer de ressources supplémentaires, cinq binômes peuvent ainsi livrer cinq applications en parallèle. En aidant les DSI à réduire les retards de livraison, cette tendance fait pencher la balance du côté du développement sur mesure plutôt que de l'achat de solutions prêtes à l'emploi.

## Quelles sont les prochaines priorités à envisager ?

**80 %** des entreprises d'ici 2030 auront transformé leurs grandes équipes de développement logiciel en équipes plus réduites, bénéficiant de l'assistance de l'IA.

**40 %** des portefeuilles applicatifs intègreront d'ici 2030 des applications personnalisées développées via des plateformes conçues nativement pour l'IA, une forte progression par rapport aux 2 % observés en 2025.

### Des équipes réduites




Source : Gartner

1

# Générez de meilleurs résultats avec des plateformes de développement pensées pour l'IA

## Un plan d'action pour gagner en rapidité, optimiser les coûts et favoriser l'innovation

| Les différentes étapes | 1 Constituer une équipe dédiée à la gestion des plateformes | 2 Instaurer un cadre de sécurité qui protège sans freiner l'innovation | 3 Lancer un projet pilote avec des outils de développement conçus pour l'IA | 4 Adopter un état d'esprit centré sur l'IA | 5 Accompagner les équipes dans la montée en compétences et l'autonomisation |
|---|---|---|---|---|---|
| **Résultat escompté** | Une coordination centralisée assure l'harmonisation des pratiques et une gouvernance claire et structurée. | Réduction des risques liés à un code non sécurisé ou non conforme. | Des résultats tangibles dès les premières étapes qui prouvent l'utilité de ces outils et renforcent la confiance. | Des livraisons plus rapides et un potentiel d'innovation démultiplié. | Une adoption à plus grande échelle et une collaboration renforcée. |
| **Action** | Mettre en place une équipe spécialisée pour piloter les plateformes IA natives et sélectionner les modèles adaptés. | Intégrer des plateformes de gouvernance de l'IA pour l'examen du code et les contrôles de conformité. | Commencer avec des projets à faible enjeu pour démontrer rapidement les gains de productivité. | Placer les outils nativement conçus pour l'IA au cœur de vos nouveaux projets de développement. | Accompagner développeurs et parties prenantes métier dans l'apprentissage de la rédactique (prompt engineering) et des bonnes pratiques de gouvernance. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Partenaire :** Élaborer une stratégie orientée IA et une structure claire de gouvernance

**Collaboration :** Harmoniser les capacités technologiques avec les enjeux stratégiques de l'entreprise.

**Gouvernance :** Garantir la conformité et mettre en place des mécanismes de sécurité adaptés pour encadrer le développement avec les outils pensés pour l'IA.

### Partenaires au sein des équipes informatiques

**Ingénierie des plateformes :** Assurer la gestion des outils IA natifs, des intégrations et des performances.

**Sécurité :** Déployer une gouvernance IA efficace pour assurer la qualité du code et gérer les risques.

**Passation de marchés :** Évaluer les offres de plateformes IA natives et sélectionner les partenaires technologiques adaptés.

### Partenaires commerciaux

**Responsables produit :** Apporter une expertise métier pour valider l'efficacité des solutions basées sur l'IA.

**Finances :** Adapter les modèles de financement pour accompagner les projets de développement axés sur l'IA.

2

# Supercalculateurs optimisés pour l'IA

**De quoi parle-t-on exactement ?**
Les plateformes de supercalcul dédiées à l'IA fournissent la puissance de traitement massive requise pour entraîner et exécuter des modèles d'IA avancés. Ces systèmes associent calcul haute performance, processeurs spécialisés et architectures évolutives pour répondre aux besoins des charges de travail les plus gourmandes en données.

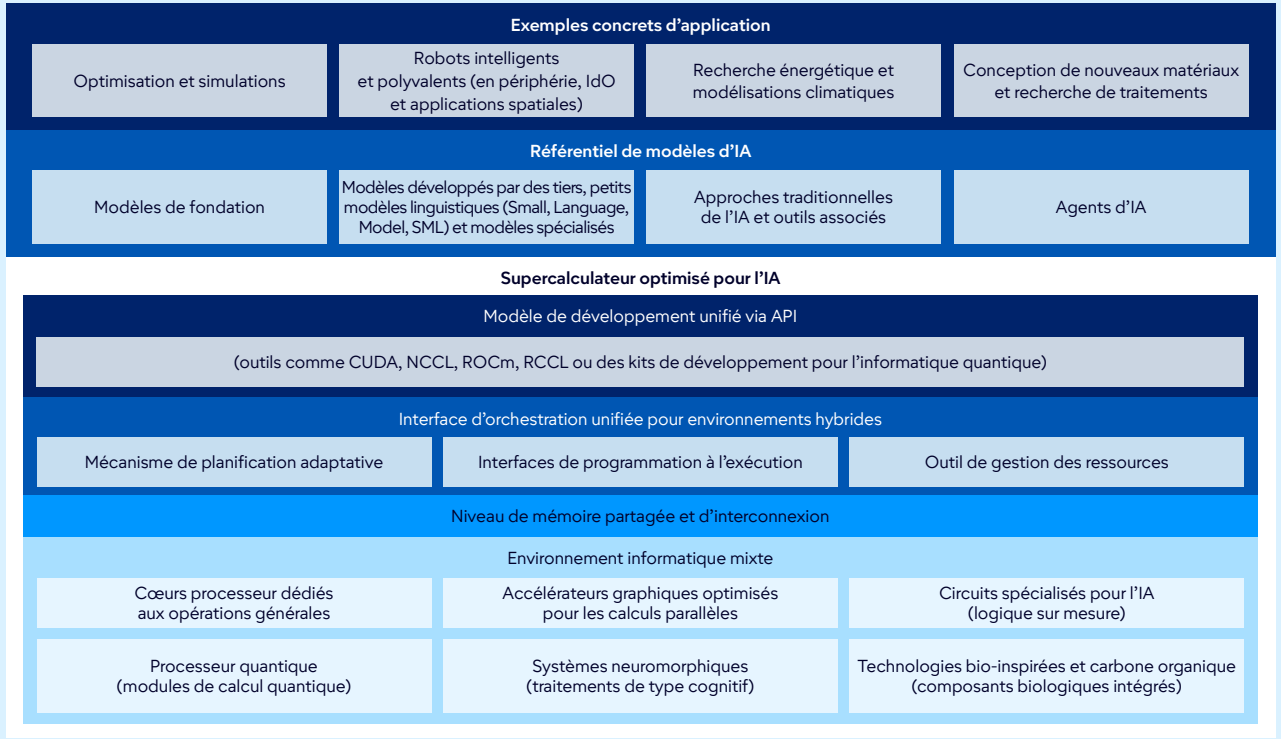
**Pourquoi ces approches s'imposent-elles maintenant ?**
La demande de solutions de supercalcul pour l'IA connaît une forte croissance, les entreprises développant des modèles toujours plus volumineux et complexes qui dépassent les limites des infrastructures traditionnelles.

## Quelles sont les prochaines priorités à envisager ?

**40 %** des entreprises auront adopté d'ici 2028 des architectures de calcul hybrides, contre 8 % aujourd'hui.

**Plus de 20** fournisseurs proposeront d'ici 2028 des environnements unifiés destinés aux développeurs, exploitant toute la puissance du supercalcul.

## Supercalculateur optimisé pour l'IA




Source : Gartner

2

# Produire des résultats concrets avec les plateformes de supercalcul dédiées à l'IA

## Plan d'action pour libérer toute la puissance de calcul disponible

| Les différentes étapes | 1 Cibler les charges de travail à forte valeur stratégique | 2 Miser sur des environnements logiciels cohérents et intégrés | 3 Mettre en place une stratégie d'intégration progressive | 4 Rationaliser le développement entre les différents environnements | 5 Anticiper les exigences de gouvernance et de conformité dès la conception |
|---|---|---|---|---|---|
| **Résultat escompté** | Mise en évidence de la valeur ajoutée et renforcement des compétences en interne. | Une intégration simplifiée et une répartition flexible des charges de travail. | Des infrastructures et du personnel prêts à relever les défis de demain. | Des délais de livraison raccourcis et moins d'obstacles opérationnels. | Des risques maîtrisés et une gouvernance renforcée. |
| **Action** | Expérimenter des projets pilotes avec une orchestration hybride agile et maîtrisée. | Favoriser l'interopérabilité grâce à des standards ouverts, applicables aux systèmes établis comme aux technologies émergentes. | Déployer peu à peu de nouveaux modèles de calcul et accompagner la montée en compétences du personnel informatique. | Mobiliser vos équipes autour de plateformes hybrides et architectures composables. | Intégrer la sécurité et la conformité dès la conception des systèmes. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Élaborer** une stratégie d'orchestration hybride en phase avec les priorités de l'entreprise.

**Veiller** à une bonne gouvernance des charges de travail, de la sécurité et de la conformité.

**Collaborer** avec les responsables métier pour prioriser les charges de travail à forte valeur ajoutée.

### Partenaires au sein des équipes informatiques

**Infrastructures et opérations :** Faire converger les nouvelles technologies d'accélération et les infrastructures en place.

**Sécurité :** Instaurer une gouvernance adaptée aux environnements à architectures multiples.

**DevOps :** Utiliser des environnements logiciels cohérents et des solutions d'orchestration centralisée.

### Partenaires commerciaux

**Produit :** Identifier les utilisations pertinentes du calcul hybride, comme les simulations ou les applications faisant appel à l'IA.

**Finances :** Adapter les budgets aux différentes étapes d'intégration et aux objectifs de durabilité.

**Opérations :** Anticiper l'arrivée de flux de travail pilotés par l'IA dans les processus stratégiques.

3

# Confidential Computing

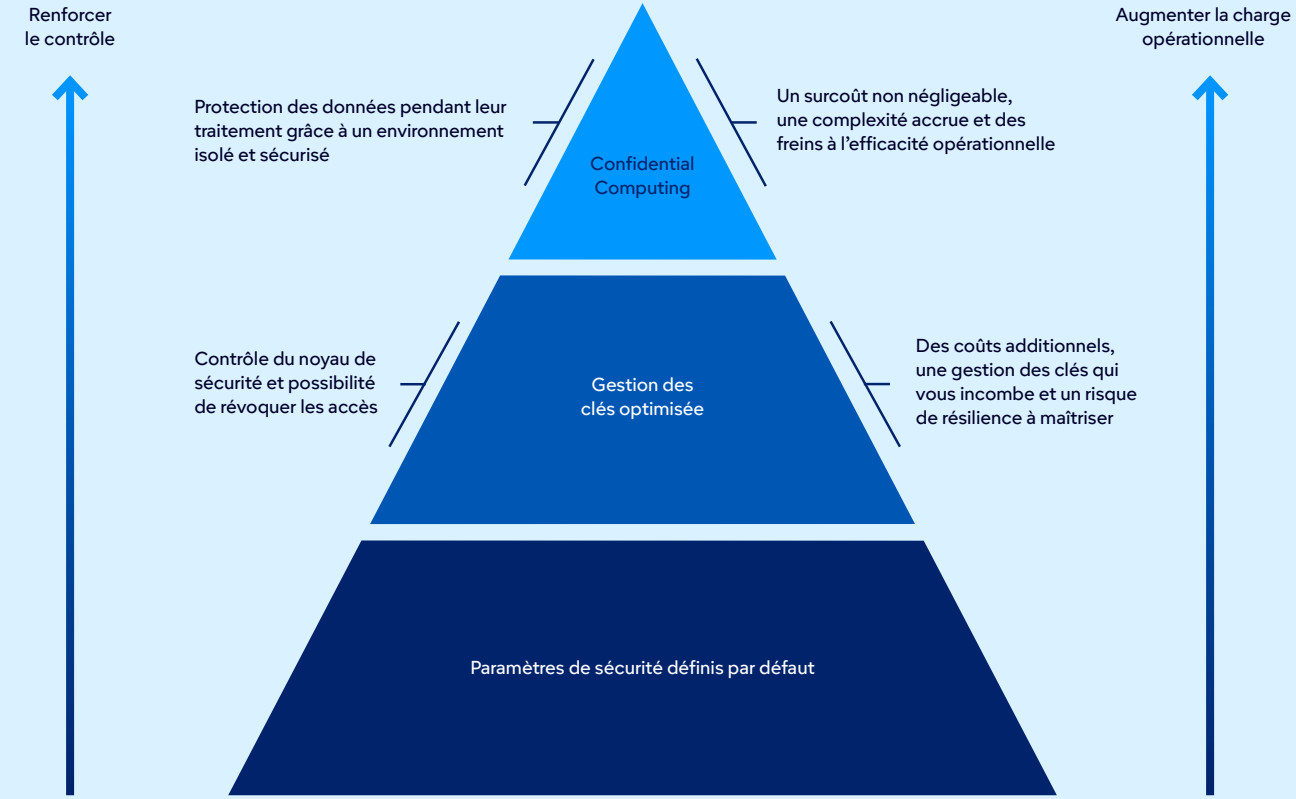
**De quoi parle-t-on exactement ?**
Le Confidential Computing utilise des environnements d'exécution sécurisés au niveau matériel (Trusted Execution Environments, TEE) afin de protéger les données pendant leur traitement et d'empêcher tout accès non autorisé, même de la part des fournisseurs de services cloud.

**Pourquoi ces approches s'imposent-elles maintenant ?**
Entre durcissement des lois sur la confidentialité, contraintes de souveraineté des données et essor de l'IA, la protection des données lors de leur traitement et utilisation devient un impératif. Grâce au Confidential Computing, il est possible d'adopter une stratégie cloud sécurisée et conforme, même pour les charges de travail les plus sensibles.

## Quelles sont les prochaines priorités à envisager ?

**75 %** des traitements sur des environnements non sécurisés seront protégés d'ici 2029 par le Confidential Computing, garantissant l'intégrité et la confidentialité des données.

## Mécanismes de contrôle pour limiter l'accès aux données par le fournisseur de services cloud




Source : Gartner

3

# Tirer parti du Confidential Computing pour produire des résultats tangibles

## Plan d'action pour un traitement des données sûr et conforme, quel que soit l'environnement

| Les différentes étapes | 1 Analyser en profondeur vos charges de travail sensibles | 2 Tester les TEE pour renforcer la protection de vos modèles d'IA | 3 Favoriser une collaboration sécurisée entre équipes et partenaires | 4 Instaurer une gestion autonome des clés de chiffrement | 5 Anticiper les difficultés lors de l'intégration pour garantir une transition sans heurts |
|---|---|---|---|---|---|
| **Résultat escompté** | Identifier les cas où une protection des données en cours d'utilisation est nécessaire. | Renforcer la confidentialité et la protection de la propriété intellectuelle. | Transmettre des analyses et insights sans divulguer les données sources. | Maîtrise complète des accès aux données. | Mise en œuvre sans friction, quel que soit l'environnement. |
| **Action** | Identifier les charges de travail concernées par les exigences en matière de confidentialité ou de souveraineté des données. | Tester les TEE avec des modèles d'IA propriétaires et open source. | Recourir au Confidential Computing dans vos projets d'analyse de données et de veille commerciale. | Déployer des systèmes de gestion de clés cryptographiques contrôlés en interne. | Anticiper l'orchestration de vos environnements sur plusieurs architectures matérielles et fournisseurs. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Élaborer** une stratégie de Confidential Computing cohérente avec vos exigences relatives au cloud, en matière de confidentialité, de conformité et de protection des données.

**Mobiliser** les équipes juridiques et de conformité pour garantir le respect des exigences en matière de localisation et de souveraineté des données.

**Superviser** la gouvernance des TEE et garantir leur intégration aux structures de sécurité existantes.

### Partenaires au sein des équipes informatiques

**Infrastructures et opérations :** Déployer des TEE dans des environnements hybrides et multicloud.

**Sécurité :** Déployer des mécanismes d'attestation et gérer les clés de chiffrement de façon sécurisée.

**Équipes DevOps et gestion de plateforme :** Adapter les charges de travail au Confidential Computing et surveiller les performances.

### Partenaires commerciaux

**Conformité :** Garantir la conformité réglementaire et une préparation optimale aux audits.

**Finances :** Adapter les budgets pour accompagner l'adoption du Confidential Computing et limiter les risques.

**Responsables des données :** Repérer les charges de travail sensibles à protéger lors de leur traitement et fixer des priorités de mise en œuvre.

# L’intégrateur

## Créer de nouvelles sources de valeur en orchestrant des technologies complémentaires.

Pour renforcer leur avantage concurrentiel, les responsables des technologies doivent intégrer des modèles spécialisés, des systèmes multi-agents et l’IA physique dans des solutions sur mesure, adaptées à chaque domaine. L’axe de l’intégrateur ouvre la voie à des écosystèmes intelligents, adaptatifs et interconnectés, en orchestrant des technologies variées pour transformer les processus, réinventer les produits et enrichir les expériences utilisateur.

4

# Systèmes multi-agents

**De quoi parle-t-on exactement ?**
Les MAS mobilisent des agents d'IA spécialisés qui coopèrent pour orchestrer des flux de travail complexes de façon intelligente. En se spécialisant sur des tâches ciblées, chaque agent renforce l'efficacité globale du système et permet une meilleure évolutivité que les modèles d'IA monolithiques.

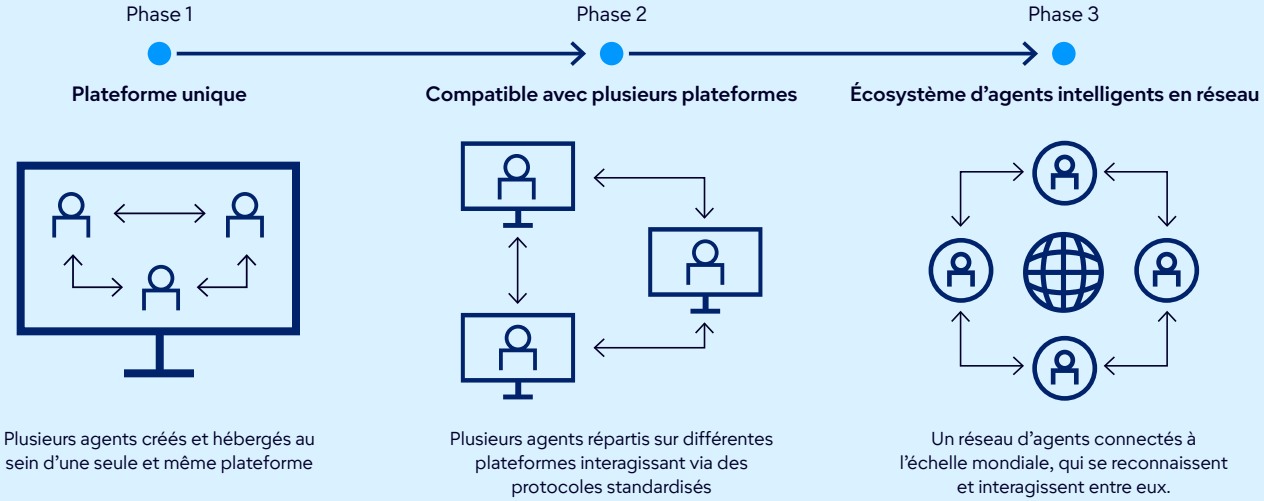
**Pourquoi ces approches s'imposent-elles maintenant ?**
Face aux limites des IA traditionnelles sur les processus complexes, les MAS apportent une réponse agile grâce à une automatisation modulaire et une intégration fluide entre plateformes. Nous enregistrons une augmentation de 1 445 % des demandes liées aux MAS entre le 1er trimestre 2024 et le 2e trimestre 2025, témoignant d'un fort intérêt du monde de l'entreprise.

## Quelles sont les prochaines priorités à envisager ?

**70 %** des systèmes multi-agents (Multiagent Systems, MAS) utiliseront des agents hautement spécialisés d'ici 2027, ce qui améliorera la précision mais complexifiera la coordination.

**60 %** des MAS seront capables d'interagir avec des solutions issues de plusieurs fournisseurs d'ici 2028, stimulant l'innovation et renforçant l'agilité technologique.

## L'évolution des systèmes multi-agents




Source : Gartner

4

# Produire des résultats concrets grâce aux systèmes multi-agents

## Plan d'action pour accélérer l'automatisation modulaire et une intégration harmonieuse entre les systèmes

| Les différentes étapes | 1 Identifier les applications les plus porteuses | 2 Concevoir des agents modulaires | 3 Mettre en place des mécanismes de gouvernance et de suivi en continu | 4 S'appuyer sur des standards ouverts pour l'interopérabilité | 5 Développer les talents et l'expertise de vos équipes |
|---|---|---|---|---|---|
| **Résultat escompté** | Des résultats concrets mesurables et une adoption plus rapide. | Fiabilité renforcée et meilleure évolutivité. | Réduction des risques et contrôle accru. | Des investissements MAS pérennes et évolutifs. | Un déploiement maîtrisé et une gestion efficace des risques. |
| **Action** | Commencer par la mise en place de flux de travail bien définis pour les projets pilotes MAS. | Concevoir des agents spécialisés plutôt que des solutions monolithiques. | Mettre en place une gouvernance rigoureuse des API et des outils de supervision. | Adopter des protocoles émergents pour permettre la collaboration entre agents issus de fournisseurs multiples. | Former le personnel aux structures MAS et à la gestion du changement. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Élaborer une stratégie** MAS autour des processus clés et en cohérence avec les priorités de l'entreprise.

**Définir** des règles de gouvernance pour assurer l'interopérabilité des agents, la sécurité et le respect des normes.

**Communiquer** les plans de gestion du changement afin de répondre aux préoccupations du personnel.

### Partenaires au sein des équipes informatiques

**Équipes DevOps et gestion de plateforme :** Concevoir des agents modulaires et optimiser la gestion des outils d'orchestration.

**Sécurité :** Renforcer la gouvernance des API et contrôler les interactions entre les agents.

**Équipes en charge de l'intégration :** S'appuyer sur des standards pour garantir interopérabilité et suivi continu.

### Partenaires commerciaux

**Responsables métiers :** Repérer les flux de travail adaptés aux projets pilotes MAS et valider les résultats obtenus.

**Finances :** Anticiper les dérives budgétaires et s'équiper d'outils de suivi pour garder le contrôle.

**Opérations:** Favoriser la synergie humain-agent et accompagner les équipes dans leur montée en compétence.

5

# Les modèles de langage spécialisés

**De quoi parle-t-on exactement ?**
Les DSLM sont des modèles d'IA entraînés sur des jeux de données spécifiques à un secteur ou à une fonction métier. Ils offrent une précision accrue et une meilleure conformité par rapport aux grands modèles de langage (Large Language Models, LLM).

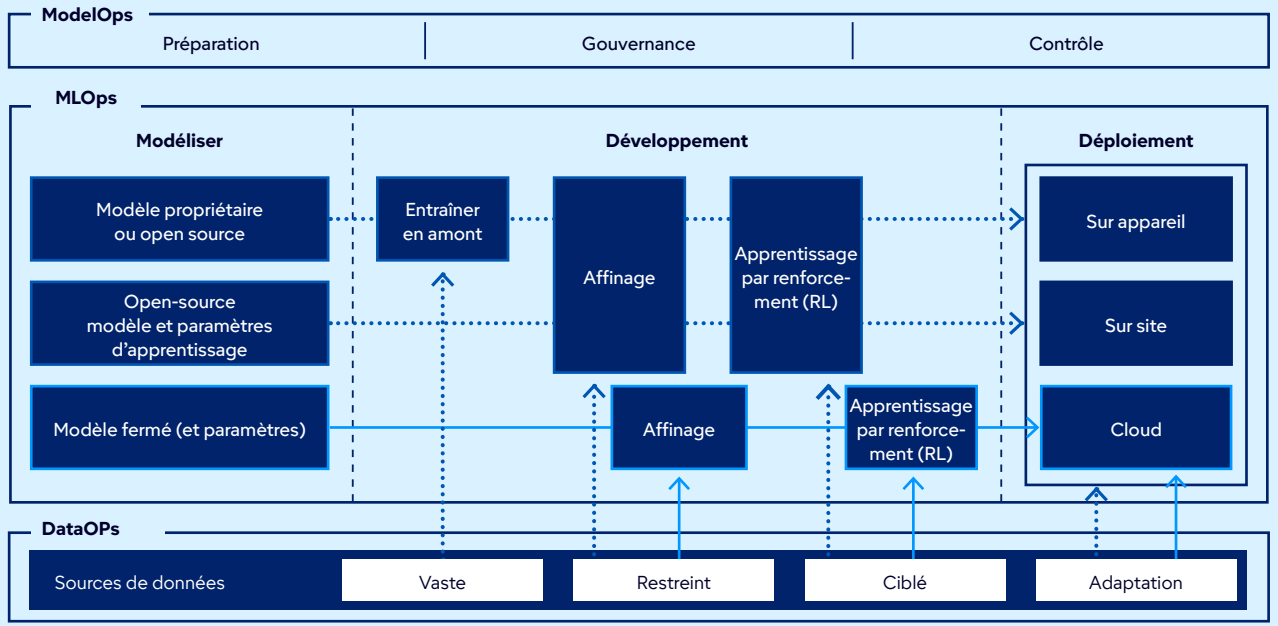
**Pourquoi ces approches s'imposent-elles maintenant ?**
Pour les DSI, l'IA doit produire une valeur commerciale tangible et directement mesurable. En ciblant des domaines clés comme la finance, la santé ou les RH, les DSLM réduisent les erreurs, accélèrent les déploiements et optimisent les coûts sur les flux de travail les plus importants.

## Quelles sont les prochaines priorités à envisager ?

**+de 60 %** des modèles d'IA générative utilisés par les entreprises d'ici 2028 seront adaptés à des domaines spécifiques.

**30 %** des utilisations de l'IA générative s'appuieront sur des modèles de langage spécialisés (Domain-Specific Language Models, DSLM) déployés en local ou directement sur les appareils d'ici 2028.

## Approches de création de modèles DSLM




Source : Gartner

5

# Tirer pleinement parti des DSLM pour générer des résultats tangibles

## Plan d'action pour répondre avec précision aux exigences réglementaires propres à chaque secteur

| Les différentes étapes | 1 Cibler les applications les plus stratégiques | 2 Renforcer la gouvernance des données | 3 Expérimenter les DSLM dans vos fonctions critiques pour en démontrer la valeur | 4 Constituer des équipes interfonctionnelles | 5 Assurer le suivi et améliorer en continu |
|---|---|---|---|---|---|
| **Résultat escompté** | Retour sur investissement accéléré et précision renforcée. | Des résultats fiables et conformes grâce aux modèles DSLM. | Démonstration d'une valeur commerciale mesurable. | Déploiement sans friction et adoption accélérée. | Des performances durables alliées à un contrôle budgétaire optimal. |
| **Action** | Cibler les flux de travail dans lesquels les LLM génériques montrent leurs limites. | Mettre en œuvre des contrôles rigoureux en matière de confidentialité et de qualité. | Démarrer par des processus critiques dans les domaines de la finance, de la santé ou des RH. | Impliquer les équipes informatiques, les experts métier et de la conformité dans les projets DSLM. | Renforcer la transparence et la conformité grâce à des structures adaptées. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Concevoir** une stratégie DSLM ciblée pour les domaines critiques, soumis à des exigences réglementaires élevées.

**Mettre en place** une gouvernance pour assurer la précision, la conformité et la transparence des modèles.

**Adopter les** DSLM en cohérence avec vos objectifs de retour sur investissement et de gestion des risques.

### Partenaires au sein des équipes informatiques

**Analyses de données :** Constituer des jeux de données adaptés à votre secteur et veiller à leur qualité.

**ModelOps :** Superviser l'ajustement des modèles, leur suivi et la gestion de leur cycle de vie.

**Sécurité :** Assurer des déploiements DSLM conformes et sécurisés, dans le respect des exigences de confidentialité.

### Partenaires commerciaux

**Experts en la matière :** Contrôler la qualité des DSLM pour garantir des résultats précis, pertinents et exploitables.

**Finances :** Allouer un budget pour l'adoption des modèles DSLM et assurer l'optimisation des coûts.

**Conformité :** Garantir la conformité avec les exigences réglementaires.

6

# IA physique

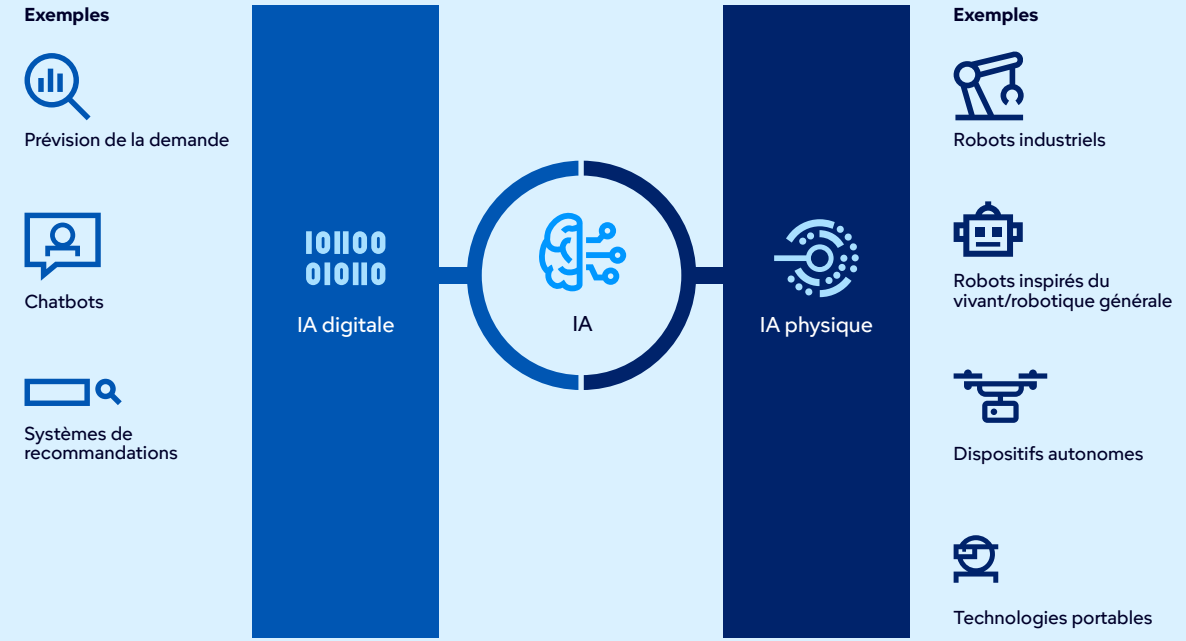
**De quoi parle-t-on exactement ?**
L'IA physique transpose l'IA dans le monde réel avec des robots, des drones, des véhicules et des dispositifs intelligents capables de percevoir leur environnement, de décider et d'agir de manière autonome. Ces systèmes associent capteurs, actionneurs et modèles d'IA pour automatiser des tâches physiques.

**Pourquoi ces approches s'imposent-elles maintenant ?**
Les entreprises veulent exploiter tout le potentiel de l'IA digital pour automatiser et optimiser leurs environnements physiques. En 2028, la moitié des dix plus grands acteurs de l'IA proposeront des solutions d'IA physique.

## Quelles sont les prochaines priorités à envisager ?

**80 %** des entrepôts miseront sur la robotique et l'automatisation pour gagner en efficacité d'ici 2028.

## Types d'IA




Source : Gartner

6

# Exploiter le potentiel de l'IA physique pour transformer vos opérations

## Plan d'action pour automatiser les tâches physiques et stimuler les performances sur l'ensemble de vos sites

| Les différentes étapes | 1 Évaluer les processus opérationnels existants | 2 Lancer des projets pilotes d'IA physique | 3 Constituer des équipes interfonctionnelles | 4 Sensibiliser les parties prenantes | 5 Poser les bases d'une orchestration fluide entre agents autonomes |
|---|---|---|---|---|---|
| **Résultat escompté** | Cibler les leviers d'automatisation à fort potentiel d'économies. | S'assurer de l'efficacité et de la rentabilité des solutions. | Gouvernance et intégration efficaces. | Prévenir les erreurs d'interprétation et les choix d'investissement inadaptés. | Anticipez l'avenir avec des déploiements évolutifs et résilients. |
| **Action** | Cibler les processus logistiques, de maintenance et de sécurité. | Valider vos systèmes avec des jumeaux digitaux avant leur déploiement sur le terrain. | Impliquer les équipes informatiques, opérationnelles et techniques dès la phase de planification. | Clarifier les différences entre IA physique, IA embarquée et IA en périphérie (edge AI). | Adoptez des plateformes d'orchestration pour piloter vos flottes de dispositifs connectés et autonomes. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Élaborer** une stratégie de gestion de l'IA physique en cohérence avec les priorités opérationnelles.

**Mettre en place** une gouvernance pour assurer la sécurité, la robustesse et la transparence des systèmes.

**Travailler main dans la main** avec les opérations et l'ingénierie pour faciliter l'intégration et gérer les risques.

### Partenaires au sein des équipes informatiques

**Infrastructures et opérations :** Intégrer l'IA physique aux IdO connectés et systèmes déjà en place.

**Sécurité :** Prévoir des mécanismes de sécurité pour encadrer les systèmes autonomes.

**Analyses de données :** Accélérer vos validations sur le terrain à l'aide de simulations et de jumeaux digitaux.

### Partenaires commerciaux

**Opérations :** Identifier les applications les plus pertinentes et en tester l'efficacité.

**Finances :** Allouer un budget aux investissements en robotique et en automatisation.

**Conformité :** S'assurer du respect des normes de sécurité et des obligations réglementaires.

# L’avant-gardiste

## Renforcer la confiance, la gouvernance et la sécurité.

Dans un contexte de risques croissants et de contrôle réglementaire accru, la confiance devient un pilier stratégique. Les tendances de l’axe avant-gardiste valorisent une approche proactive de la sécurité, une gouvernance transparente et une intégrité exemplaire dans le digital. Objectif : permettre aux entreprises de préserver leur réputation, de rester en conformité et d’entretenir la confiance de leurs parties prenantes tout en faisant évoluer leur stratégie IA et transformation digitale à grande échelle.

7

# Cybersécurité préventive

**De quoi parle-t-on exactement ?**
La cybersécurité préventive (Preemptive Cybersecurity, PCS) s'appuie sur des technologies d'IA avancées pour détecter les menaces à l'avance, les atténuer et les neutraliser, avant même qu'une attaque ne soit lancée, dépassant les limites des approches réactives traditionnelles.

**Pourquoi ces approches s'imposent-elles maintenant ?**
Les menaces exploitant l'IA progressent à un rythme inédit, mettant en danger réseaux, applications métiers et environnements IdO. D'ici 2029, les solutions technologiques qui n'intègrent pas de cybersécurité préventive seront reléguées au second plan, à mesure que les solutions de défense proactives deviendront une exigence généralisée.

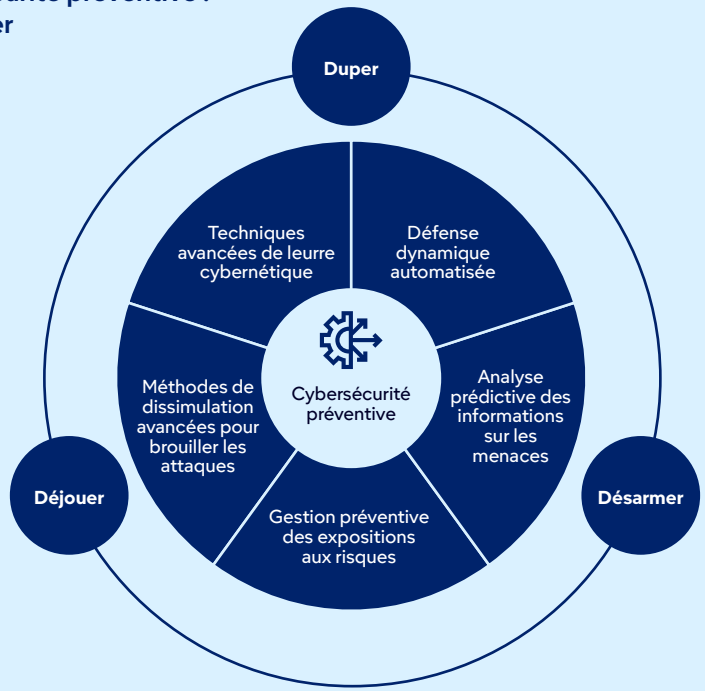
Vous recherchez des analyses et insights adaptés aux organisations technologiques et aux fournisseurs de services ? Consultez notre article sur la cybersécurité préventive à destination des fournisseurs : **Ne remettez pas à demain la mise en place de solutions de cybersécurité préventives.**

## Quelles sont les prochaines priorités à envisager ?

**50 %** des investissements des entreprises et de leur budget cybersécurité seront alloués à des solutions capables d'anticiper les menaces d'ici 2030.

**1 million** 1 million de vulnérabilités identifiées par an d'ici 2030 : un cap symbolique révélateur de l'ampleur des menaces.

## Les 3 « D » de la cybersécurité préventive : Duper, Déjouer, Désarmer




Source : Gartner

7

# Tirer parti de la cybersécurité préventive pour renforcer votre sécurité

## Plan d'action pour protéger vos actifs avant l'apparition des menaces

| Les différentes étapes | 1 Faire un état des lieux de votre système de sécurité actuel | 2 Déployer un projet pilote de PCS sur les domaines à risque élevé | 3 Élaborer des critères de sélection rigoureux pour choisir les bons partenaires de cybersécurité préventive | 4 Faire adhérer les équipes à la stratégie de PCS | 5 Connecter le PCS à votre environnement technologique actuel |
|---|---|---|---|---|---|
| **Résultat escompté** | Cibler les failles critiques et investir intelligemment dans le PCS | Démontrer une réduction des risques quantifiable. | Adopter un PCS pensé pour durer et s'adapter aux menaces de demain. | Obtenir l'adhésion des équipes dirigeantes et des instances décisionnelles. | Optimiser le retour sur investissement et accélérer l'adoption. |
| **Action** | Évaluer les risques et mesurer le niveau de préparation. | Déployer des outils pour anticiper et déjouer les menaces. | Exiger des feuilles de route détaillées pour les capacités préventives. | Démontrer l'impact stratégique et le ROI de PCS auprès des parties prenantes. | Intégrer le PCS aux processus actuels de sécurité et de conformité. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Promouvoir** la transition d'une stratégie de sécurité réactive vers une approche préventive.

**Définir** les critères d'achat des PCS et sensibiliser les autres membres de la direction.

**Assurer** la gouvernance des dispositifs de défense renforcée et la conformité des obligations réglementaires.

### Partenaires au sein des équipes informatiques

**Sécurité :** Mettre en place des technologies pour anticiper les menaces et tromper les attaquants.

**Infrastructures et opérations :** Intégrer le PCS aux environnements cloud, aux technologies opérationnelles et aux systèmes cyber-physiques.

**Risques et conformité :** S'assurer du respect des normes de confidentialité et des obligations réglementaires.

### Partenaires commerciaux

**Finances :** Prévoir des budgets pour tester le PCS et soutenir son déploiement durable.

**Opérations :** Accompagner la transformation digitale en garantissant la sécurité.

**Produit :** Intégrer la cybersécurité préventive aux offres pour se différencier sur le marché.

8

# Provenance des données digitales

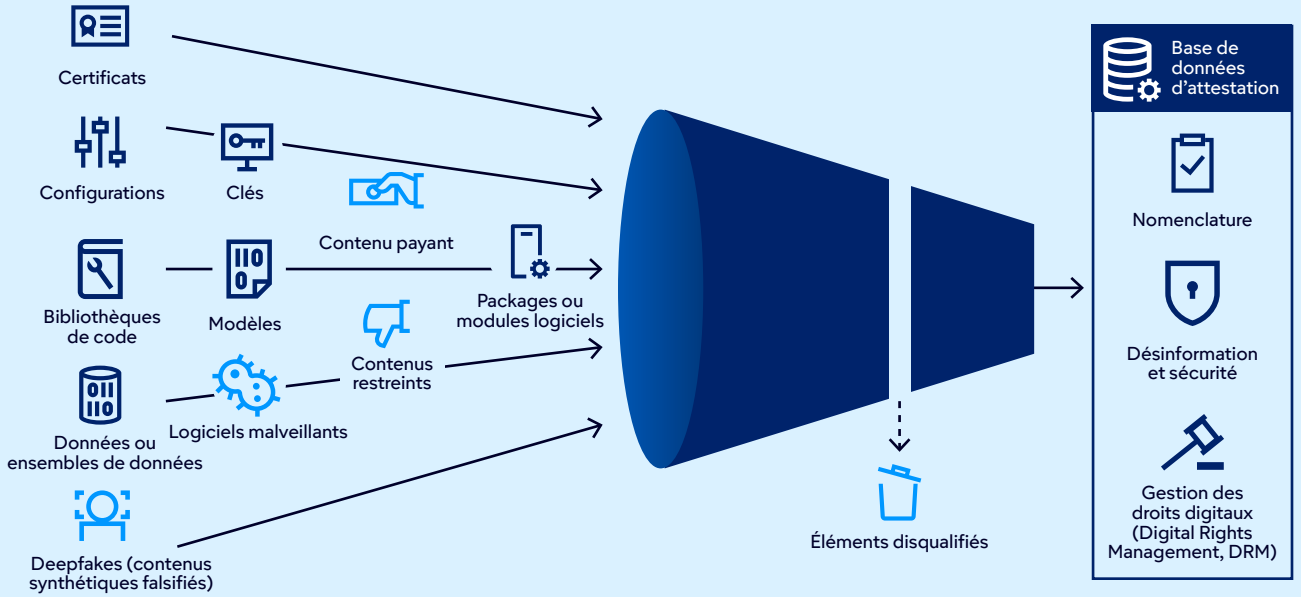
**De quoi parle-t-on exactement ?**
Une solution de détermination de la provenance ou de traçabilité digitale permet de vérifier l'origine et l'intégrité des logiciels, des données et des contenus multimédias à l'aide d'outils tels que les nomenclatures (Bills of Materials, BOM), les bases de données d'attestation et les filigranes. Elle permet d'instaurer transparence et confiance dans les systèmes intégrant des composants tiers et du contenu généré par l'IA.

**Pourquoi ces approches s'imposent-elles maintenant ?**
Les entreprises doivent faire face à des menaces grandissantes : code modifié à leur insu, projets open source laissés sans maintenance et désinformation générée par des deepfakes.

## Quelles sont les prochaines priorités à envisager ?

Avec des réglementations de plus en plus strictes, à l'image de la loi sur l'IA européenne, les contenus générés par l'IA devront intégrer des filigranes et des dispositifs de traçabilité.

## Filtrer en fonction de la provenance des données digitales




Source : Gartner

8

# S’appuyer sur la provenance digitale pour garantir des résultats fiables

## Renforcer la confiance grâce à un plan d’action centré sur la vérification de l’authenticité des données et des contenus

| Les différentes étapes | 1 Déployer des nomenclatures logicielles (BOM) | 2 Mettre en œuvre une base de données d’attestation | 3 Adopter des outils de protection contre la désinformation | 4 Appliquer un filigranage digital | 5 Renforcer la gouvernance |
|---|---|---|---|---|---|
| **Résultat escompté** | Permet d’assurer la traçabilité, la transparence et la sécurité des logiciels. | Registres de provenance centralisés et fiables. | Protection contre l’usurpation d’identité et la fraude. | Conformité avec les réglementations sur les contenus générés par l’IA. | Réduction des risques juridiques et réputationnels. |
| **Action** | Mettre en œuvre des nomenclatures logicielles (SBOM) pour les logiciels et des nomenclatures pour le machine learning (MLBOM) pour les modèles d’IA. | Conserver des preuves d’origine sécurisées grâce à une signature cryptographique. | Intégrer la détection d’identités synthétiques dans les plans de détection et de réponse aux menaces liées à l’identité. | Apposez des balises lisibles par machine pour signaler les contenus générés par l’IA. | Collaborez entre les équipes informatiques, de conformité et de marketing. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Élaborer** une stratégie de traçabilité digitale conforme aux réglementations et adaptée à la gestion des risques.

**Assurer le suivi** du déploiement des nomenclatures logicielles et des bases d’attestation pour garantir transparence et traçabilité.

**Travailler** avec le responsable de la sécurité des systèmes d’information (RSSI) et le directeur général du marketing afin de gérer les risques liés à la désinformation et préserver l’image de marque.

### Partenaires au sein des équipes informatiques

**DevOps :** Intégrer les nomenclatures logicielles (SBOM) et les nomenclatures de machine learning (MLBOM) dans les chaînes de livraison.

**Sécurité :** Déployer des outils de protection contre la désinformation et des systèmes de DRM.

**Données :** Assurer la traçabilité des données d’entraînement des modèles d’IA.

### Partenaires commerciaux

**Conformité :** S’adapter aux nouvelles réglementations en vigueur.

**Juridique :** S’assurer que les droits d’auteur et les licences sont bien respectés.

**Marketing :** Anticiper les risques d’image liés aux deepfakes et aux contenus générés artificiellement.

9

# Plateformes de sécurité dédiées à l'IA

**De quoi parle-t-on exactement ?**
Les plateformes de sécurité pour l'IA (AI Security Platform, AISP) centralisent les mécanismes de contrôle afin de sécuriser à la fois les services IA tiers et les applications IA développées en interne. Elles permettent de traiter des risques propres à l'IA, comme les attaques par injection de prompt (requête), les comportements déviants d'agents autonomes ou les fuites d'information.

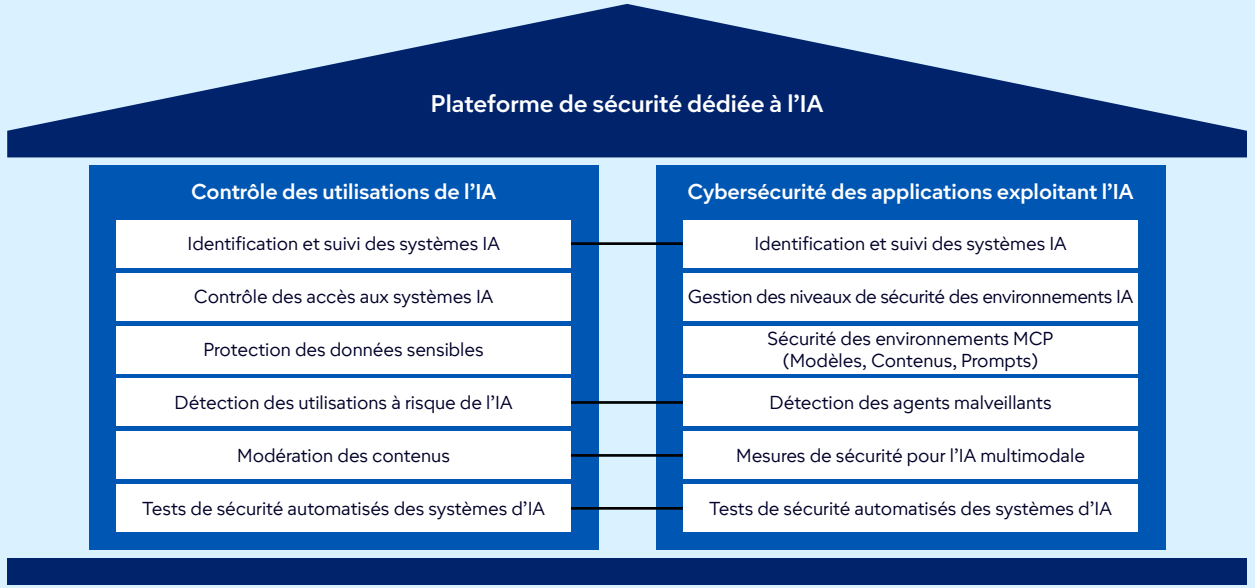
**Pourquoi ces approches s'imposent-elles maintenant ?**
Alors que l'IA se généralise, les solutions de sécurité classiques montrent leurs limites face aux spécificités des environnements et flux de travail exploitant l'IA.

## Quelles sont les prochaines priorités à envisager ?

**+de 50 %** des entreprises auront adopté des plateformes de sécurité pour l'IA (AISP) d'ici 2028.

**80 %** des transactions non autorisées liées à l'IA résulteront de violations internes des politiques, et non d'attaques externes.

## Vue d'ensemble des capacités des plateformes de sécurité dédiées à l'IA




Source : Gartner

9

# Des résultats concrets grâce aux plateformes de sécurité dédiées à l'IA

## Plan d'action pour protéger vos opérations métier en constante évolution à l'ère de l'IA

| Les différentes étapes | 1 Analyser les risques spécifiques à l'IA | 2 Lancer des projets pilotes avec des solutions AISP | 3 Opter pour des solutions intégrées | 4 Inclure des tests de sécurité dans vos processus | 5 Suivre l'évolution des offres et innovations des fournisseurs |
|---|---|---|---|---|---|
| **Résultat escompté** | Repérer les failles de votre dispositif de sécurité. | Mesurer l'efficacité et le retour sur investissement des solutions en place. | Faciliter la gestion tout en limitant la complexité. | Renforcer la résilience face aux attaques par injection de prompts. | Rester proactif face aux nouvelles menaces. |
| **Action** | Identifier les risques propres à l'IA dans l'ensemble des flux de travail. | Commencer par les services IA les plus exposés et les applications développées en interne. | Sélectionner des plateformes AISP capables de gérer les différentes utilisations et sécuriser les applications. | Ajouter des tests de sécurité automatisés aux chaînes de développement. | Assurer une veille active des startups et acteurs établis proposant des fonctionnalités avancées. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Définir** une stratégie de sécurité pour l'IA couvrant à la fois les services tiers et les applications développées en interne.

**Choisir** des partenaires capables de gérer les utilisations de l'IA et la sécurité des applications dans une solution intégrée.

**Communiquer** à la direction les niveaux de risque liés à l'IA ainsi que les exigences en matière de conformité.

### Partenaires au sein des équipes informatiques

**Sécurité :** Mettre en place des mécanismes de protection contre l'injection de prompts et les agents IA non autorisés.

**DevOps :** Sécuriser vos développements dès le départ en intégrant des tests IA dans les chaînes de développement.

**Infrastructures et opérations :** Garantir la compatibilité des solutions avec les environnements cloud et sur site.

### Partenaires commerciaux

**Conformité :** S'assurer que les solutions AISP respectent les réglementations en place, comme la loi de régulation de l'IA européenne.

**Finances :** Allouer un budget à l'intégration des plateformes et à la gestion des risques associés.

**Produit :** Intégrer des fonctions de sécurité dans les produits et services exploitant l'IA.

10

# Géopatriation

**De quoi parle-t-on exactement ?**
Le concept de géopatriation désigne la relocalisation de charges de travail depuis des clouds hyperscales internationaux vers des environnements souverains ou locaux, dans le but de réduire les risques géopolitiques. Cette stratégie, qui peut inclure le rapatriement sur site ou le passage à des clouds souverains, répond à un besoin croissant de sécurité, de conformité et de résilience géopolitique.

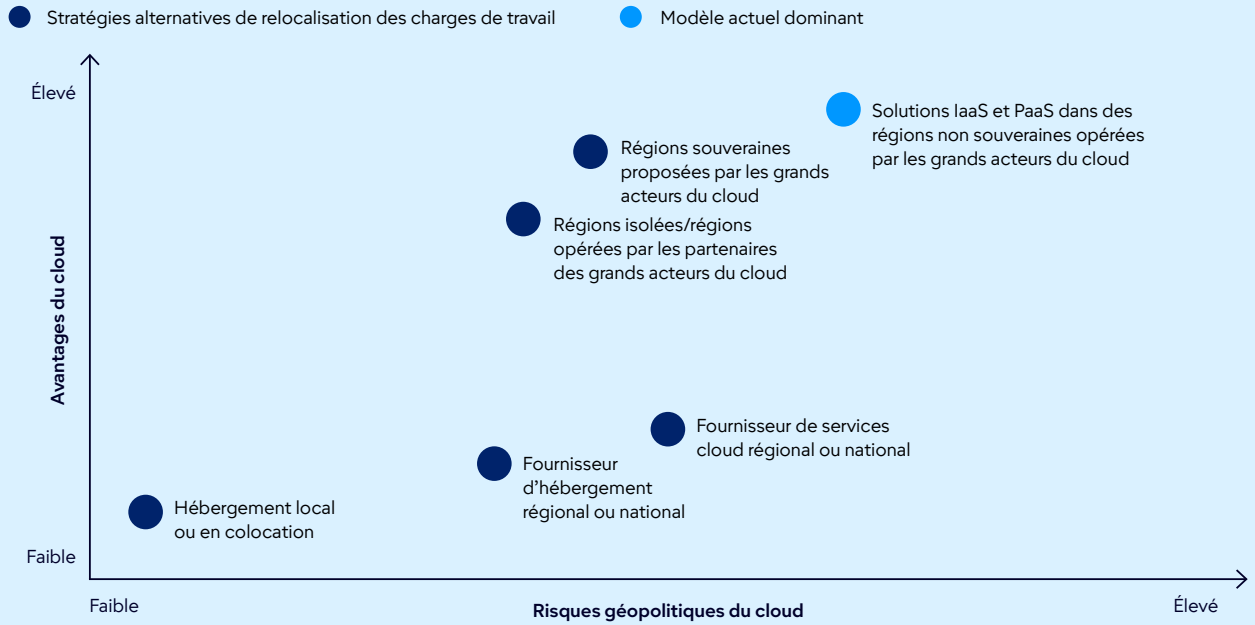
**Pourquoi ces approches s'imposent-elles maintenant ?**
Face aux tensions géopolitiques et aux nouvelles obligations réglementaires, les entreprises réexaminent leur relation au cloud.

## Quelles sont les prochaines priorités à envisager ?

**75 %** des entreprises auront rapatrié certaines charges de travail sur leur territoire pour des raisons géopolitiques et de souveraineté d'ici 2030.

Les offres souveraines, qu'elles viennent d'acteurs mondiaux ou de prestataires locaux, se multiplient rapidement.

## Avantages du cloud et risques géopolitiques associés




Source : Gartner

10

# Reprenez le contrôle avec la géopatriation

## Plan d'action pour réduire les risques en rapatriant les charges de travail digitales stratégiques

| Les différentes étapes | 1 Identifier les charges de travail critiques | 2 Analyser les options souveraines disponibles | 3 Définir des stratégies hybrides adaptées | 4 Mettre en œuvre des dispositifs de gouvernance | 5 Surveiller l'évolution du contexte géopolitique |
|---|---|---|---|---|---|
| **Résultat escompté** | Prioriser la géopatrialisation des actifs à haut risque. | Trouver un équilibre entre agilité opérationnelle et exigences de souveraineté. | Maintenir la résilience et les performances des systèmes. | Réduire les risques liés à la conformité et à la sécurité. | Adapter la stratégie de manière proactive face à l'évolution du contexte. |
| **Action** | Classer vos charges de travail en fonction de leur sensibilité et des risques géopolitiques associés. | Comparer les offres souveraines, grands clouds publics ou fournisseurs locaux. | Combiner cloud souverain, infrastructures sur site et solutions de colocation. | Adopter des cadres de gouvernance intégrant attestation et souveraineté. | Ajuster la stratégie d'hébergement au fil des évolutions géopolitiques. |

## Les acteurs stratégiques pour assurer le succès du déploiement

### DSI

**Définir** une stratégie de géopatriation conciliant souveraineté, agilité et résilience.

**Effectuer** les bonnes concessions et comparer les solutions locales avec les options souveraines proposées par les grands acteurs du cloud.

**Orchestrer** l'évaluation des risques et s'assurer de la conformité des charges de travail critiques.

### Partenaires au sein des équipes informatiques

**Infrastructures et opérations :** Anticiper les étapes de migration et l'interopérabilité avec vos systèmes en place.

**Sécurité :** Valider les mécanismes de contrôle de souveraineté et garantir la conformité réglementaire.

**Architectes cloud :** Optimiser le placement des charges de travail pour maximiser les performances et la résilience.

### Partenaires commerciaux

**Conformité :** Suivre les évolutions réglementaires et les nouvelles obligations de souveraineté.

**Finances :** Anticiper les coûts de migration et les dépenses liées à la maîtrise des risques.

**Opérations:** Assurer la continuité des opérations lors du transfert des charges de travail.

# Des insights à la fois exploitables et objectifs

**Consultez ces ressources connexes et outils gratuits dédiés aux responsables des équipes informatiques :**

Modèle

## Concevoir une planification stratégique pour les services informatiques

Passez de la stratégie aux mesures concrètes grâce à ce modèle de planification d'une page.

Accéder au modèle

Outil

## Outils d'analyse comparative et de diagnostic Gartner

Consultez des benchmarking stratégiques vous permettant d'orienter vos décisions informatiques avec précision et discernement.

En savoir plus

Insights

## Hype Cycle™ de Gartner 2025

Le Hype Cycle pour l'intelligence artificielle 2025 voit plus loin que l'intelligence artificielle générative.

Consulter ce contenu

Insights

## Questions d'actualité sur l'IA et les technologies émergentes

Les experts Gartner apportent des réponses succinctes aux questions récemment posées par nos clients sur certaines technologies émergentes.

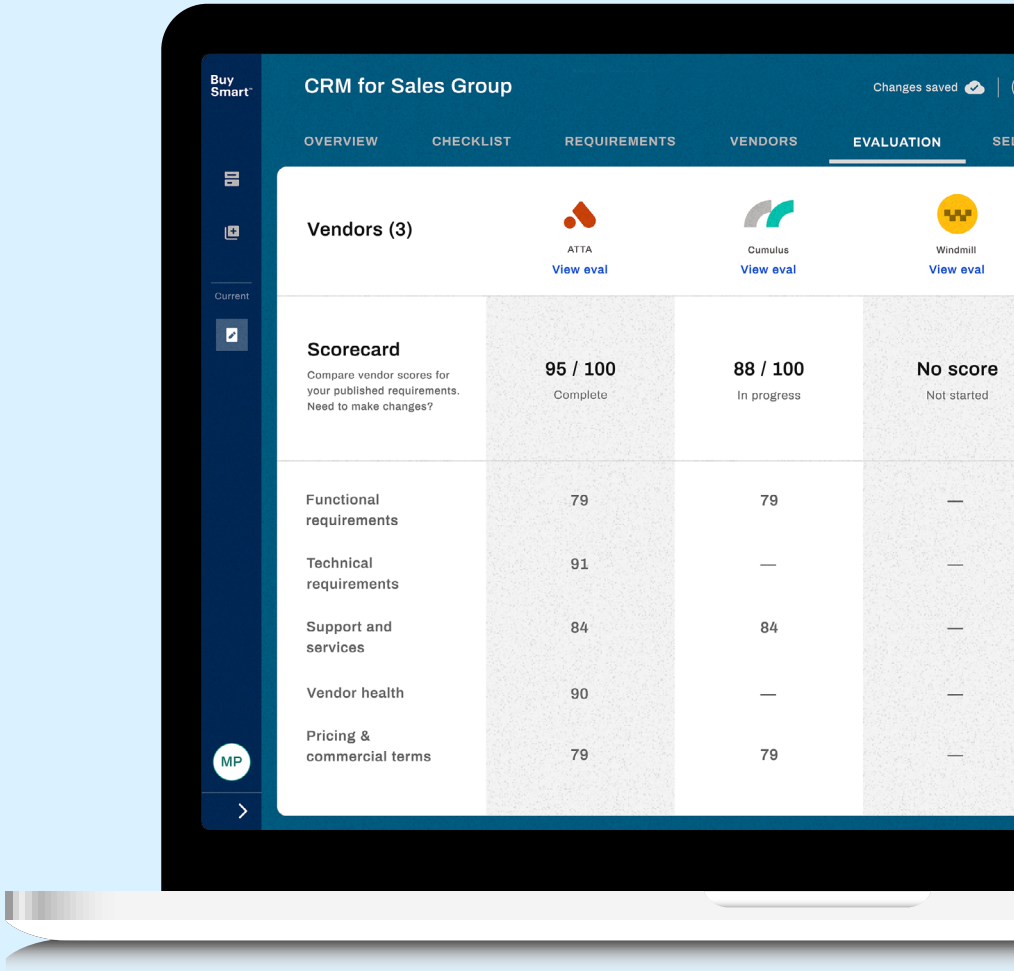
Vérifier les réponses

Déjà client ?
Accédez à d'autres ressources sur votre portail client. **Connexion ↗**

Gartner®

## Gartner BuySmart™

# Rationalisez le processus décisionnel de votre équipe en matière d'achats technologiques




**Ce que vous obtiendrez :**

- Accès à plus de 100 modèles couvrant les principaux marchés du secteur technologique
- Listes de contrôle et exigences prédéfinies et entièrement personnalisables.
- Fonctionnalités de collaboration pour optimiser le flux de travail de votre équipe, le tout réuni au même endroit
- Cotation standardisée pour garantir une sélection rigoureuse des fournisseurs

**En savoir plus ↗** Recherche Liste restreinte Évaluer Négocier

# Contactez-nous

Bénéficiez de connaissances et insights à la fois exploitables et objectifs, qui permettent de prendre des décisions rapides et intelligentes et de mieux répondre aux priorités stratégiques décisives de votre entreprise.

**États-Unis :** 1 855 811 7593

**International :** +44 (0) 3330 607 044

Discuter avec un expert.

**En savoir plus sur Gartner pour les DSI et cadres des équipes informatiques**
https: //www.gartner.fr/fr/directeur-des-systemes-d-information

**Restez connecté pour recevoir les insights les plus récents**

**Participez à une conférence Gartner**
Voir la conférence



Gartner®