# État du secteur sans-fil 2026

## Exploiter l'effet démultiplicateur : Comment les investissements stratégiques dans le sans-fil stimulent la croissance des entreprises à l'ère de l'IA

France

© 2026 Cisco and/or its affiliates. All rights reserved.

# Sommaire exécutif

En 2026, le Wi-Fi a dépassé son simple rôle de commodité pour devenir un levier de croissance stratégique. À l'échelle mondiale, les entreprises qui investissent de manière holistique dans le sans-fil ont quatre fois plus de chances d'obtenir un retour sur investissement élevé et des gains mesurables dans toutes leurs activités – de l'efficacité opérationnelle à la croissance du chiffre d'affaires. Cet effet démultiplicateur distingue le secteur du sans-fil d'autres investissements dans les TI, générant des rendements cumulés à l'échelle de l'entreprise.

Pourtant presque toutes les entreprises (98%) rapportent que la complexité s'est intensifiée, les menaces pour la sécurité se sont multipliées et les compétences nécessaires pour relever ces défis se font de plus en plus rares. Les entreprises doivent s'adapter à divers besoins en connectivité et porter assistance à un éventail toujours plus large d'utilisateurs et d'appareils – des employés et sous-traitants aux robots autonomes, capteurs intelligents et applications intégrant l'IA.

Ce rapport inaugural révèle un paradoxe IA sans-fil: l'IA est à la fois le principal levier de rentabilité pour le sans-fil et la principale source de risques croissants. Bien que les opérations gérées par IA permettent de libérer des centaines d'heures pour les services informatiques chaque année, elles accentuent les besoins en infrastructure, les menaces pour la sécurité et la pénurie de main-d'œuvre qualifiée. Le rapport est fondé sur l'utilisation du WI-FI comme principal mode de connexion pour les entreprises, tout en considérant les possibilités offertes par le système sans fil dans son ensemble, notamment les applications basées sur l'IA, les environnements IoT et OT, et les cas d'utilisation émergents pour les entreprises.

Notre recherche met en évidence l'infrastructure obsolète et trois obstacles interdépendants qui empêchent les entreprises de tirer pleinement parti du retour sur investissement dans le sans-fil: la complexité opérationnelle, l'intensification des menaces sur la sécurité et le manque de main-d'œuvre qualifiée. Ces défis se renforcent mutuellement, ce qui multiplie les risques.

Les entreprises qui s'attaquent à ces barrières opérationnelles, de sécurité et de talents de façon holistique obtiennent un retour sur investissement 63% plus élevé que celles qui ne le font pas. Ce qui démontre que les investissements stratégiques dans le sans-fil génèrent des rendements mesurables et cumulatifs sur plusieurs plans. Cela explique pourquoi la dynamique d'investissement dans le sans-fil continue de s'accélérer, d'autant plus avec l'augmentation de l'utilisation de l'IA et les avancées en matière d'innovation.

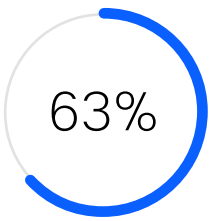
Dans l'ensemble, les résultats montrent que lorsque les entreprises en France priorisent stratégiquement le sans-fil, des résultats mesurables sont obtenus à plusieurs niveaux. Plus de 76% rapportent des améliorations de la productivité des employés, de la productivité des opérations (74%), et de l'engagement client (72%), tandis que 60% rapportent des impacts positifs sur leur chiffre d'affaires. Cela montre qu'une infrastructure sans fil moderne se traduit directement en croissance des activités.

Le moment pour tirer parti de cet avantage concurrentiel est maintenant. Les entreprises en France qui agissent de manière décisive en 2026 – en simplifiant les opérations, modernisant la sécurité des réseaux sans fil, et développant une expertise certifiée – vont positionner le Wi-Fi comme un vecteur de croissance stratégique pour la prochaine décennie.

**Les entreprises multinationales qui investissent de façon holistique dans l'IA, l'automatisation, des mesures de sécurité modernes et une expertise certifiée ont un avantage sur celles qui ne le font pas :**

+4x

plus de chance de générer des rendements élevés sur les investissements dans le sans-fil




Un retour sur investissement plus élevé de 63% en moyenne dans le sans-fil.

© 2026 Cisco and/or its affiliates. All rights reserved.

# La stratégie du sans-fil face dans cette tempête: Naviguer le paradoxe IA et les barrières qui limitent la croissance du retour sur investissement

## Définir le paradoxe IA sans-fil et pourquoi il importe

Le paradoxe IA sans-fil met en lumière le principal enjeu stratégique pour les dirigeants d'entreprise en 2026 — et l'opportunité pour ceux qui agissent en premier. L'IA est simultanément le catalyseur principal du retour sur investissement dans le sans-fil et la source de ses plus grands défis. À l'échelle mondiale, les entreprises qui déploient l'IA sont plus susceptibles de considérer le sans-fil comme stratégique et d'obtenir des rendements nettement supérieurs lorsqu'elles intègrent l'optimisation de leurs réseaux sans fil à leurs stratégie d'intégration de l'IA. Or, cette même IA entraîne une complexité opérationnelle sans précédent, contribuant à l'émergence de nouvelles menaces à la sécurité et intensifie la concurrence dans le recrutement de personnel qualifié.

**Le paradoxe IA sans-fil**
L'IA est à la fois la solution et le problème

**Solution**
- Les opérations dirigées par l'IA simplifient la complexité des réseaux sans fil
- L'automatisation libère les équipes informatiques afin qu'elles se concentrent sur des activités à plus forte valeur ajoutée.
- La gestion des demandes (tickets) est simplifiée et accélérée.

**Problème**
- Les cyberattaques générées par IA constituent une menace majeure pour la sécurité. La pénurie de professionnels compétents en sans-fil et en IA s'accentue.
- Les professionnels de l'informatique se détournent du sans-fil au profit de l'IA.

L'IA est un levier majeur pour améliorer le retour sur investissement du sans-fil - mais aussi une source importante de risques.

© 2026 Cisco and/or its affiliates. All rights reserved.

## L'IA pose des défis complexes aux équipes du sans-fil

| Principales menaces à la sécurité | Principaux domaines qui détournent les talents informatiques du sans-fil | Principaux obstacles au recrutement de talents en sans-fil |
|---|---|---|
| **#1** Les cyberattaques générées par l'IA ou automatisées / outils automatisés d'intrusion. | **#1** Cybersécurité | **#1** Manque de candidats possédant des compétences avancées dans le sans-fil ou en intégration de l'IA. |
| **#2** Travail à distance et hybride : surface d'attaque accrue / points d'accès non gérés | **#2** IA / apprentissage automatique | **#2** Contraintes budgétaires internes ou gel des embauches |
| **#3** Contraintes budgétaires ou ressources limitées freinant les améliorations en matière de sécurité. | **#3** Infrastructure cloud / DevOps. | **#3** Limitations géographiques ou difficultés associées au travail à distance. |

Les entreprises en France confiant des tâches à l'IA perçoivent l'importance du sans-fil différemment des autres. Parmi les responsables des réseaux sans fil au sein des entreprises qui confient des tâches à l'IA, 56 % considèrent le sans-fil comme étant d'une importance stratégique comparé comparativement à 46 % chez celles qui ne le font pas.

La raison est simple: les tâches confiées à l'IA nécessitent des réseaux sans-fil plus performants et plus résilients. Les entreprises qui intègrent l'optimisation de leurs réseaux sans-fil à leur stratégie de déploiement de l'IA obtiennent des rendements nettement supérieurs. En France, plus de sept entreprises sur dix font état d'impacts positifs de leurs investissements en réseaux sans fil sur l'efficacité opérationnelle, l'engagement client, la productivité des employés et l'augmentation du chiffre d'affaires.

Quels liens existent entre ces opportunités, défis et risques liés aux avancées dans l'IA?

Alors que l'IA est souvent présentée comme un moyen de simplifier l'exploitation des réseaux sans-fil et de résoudre des problèmes complexes, les cyberattaques générées par l'IA ou automatisées représentent la principale source de menaces à la sécurité pour ces réseaux. Par ailleurs, l'IA figure parmi les domaines qui attirent le plus les talents, au détriment du sans-fil en France.

### **1ère barrière**: La complexité opérationnelle dépasse les capacités actuelles.

La première barrière qui empêche les entreprises de résoudre le paradoxe de l'IA est la complexité opérationnelle croissante. Presque tous les dirigeants dans le sans-fil (96%) en France rapportent que l'exploitation des réseaux sans fil devient plus complexe. Cette situation alimente une posture réactive: elle mobilise les ressources, freine le travail stratégique et compromet directement les AIOps et les initiatives d'automatisation censées réduire la complexité. Il s'ensuit un cercle vicieux: la complexité entraîne un mode réactif; le mode réactif limite la modernisation; l'absence de modernisation renforce la complexité.

Les entreprises en France citent trois facteurs principaux à l'origine de cette complexité grandissante: la nécessité d'atténuer les nouveaux risques liés à la sécurité (44%); la multiplication des charges de travail critiques TI, IoT et OT – incluant de plus en plus d'applications gérées par l'IA (40%) – et la demande accrue de bande passante liée à de nouveaux usages (35%).

Cette complexité entraîne des contraintes opérationnelles bien concrètes: 31% rapportent que leur équipe

© 2026 Cisco and/or its affiliates. All rights reserved.

informatique reçoit au moins 50 demandes de soutien par semaine liées au sans-fil. Cela représente des centaines d'heures par mois consacrées à la gestion de ces demandes.

Un indicateur préoccupant de ce mode réactif: 57% disent consacrer la majeure partie de leur temps à la résolution de problèmes et à la gestion d'incidents. Les activités proactives – notamment les projets stratégiques, la formation, les certifications et l'optimisation du réseau – passent alors au second plan.

Cette posture va à l'encontre des efforts de modernisation. Les équipes mobilisées par la résolution de problèmes détournent des ressources qui pourraient être consacrées à la planification stratégique des réseaux sans-fil, à la formation et aux certifications, ou à la mise en place de processus d'automatisation.

Un facteur qui aggrave ce défi est le manque de visibilité. 81% des entreprises rapportent un manque de visibilité qui compromet leur capacité à résoudre efficacement les problèmes de Wi-Fi. Les enjeux les plus fréquents concernent la visibilité sur les clients, les applications et l'infonuagique, ainsi que sur les paquets.

Sans visibilité de bout en bout, les équipes ne peuvent pas isoler rapidement la source des problèmes. Cela alimente une dynamique particulièrement risquée: les réseaux sans-fil deviennent des boucs émissaires pour des problèmes dont l'origine est ailleurs. 45% des répondants indiquent que plus de 10% des incidents sont attribués à tort au sans-fil.

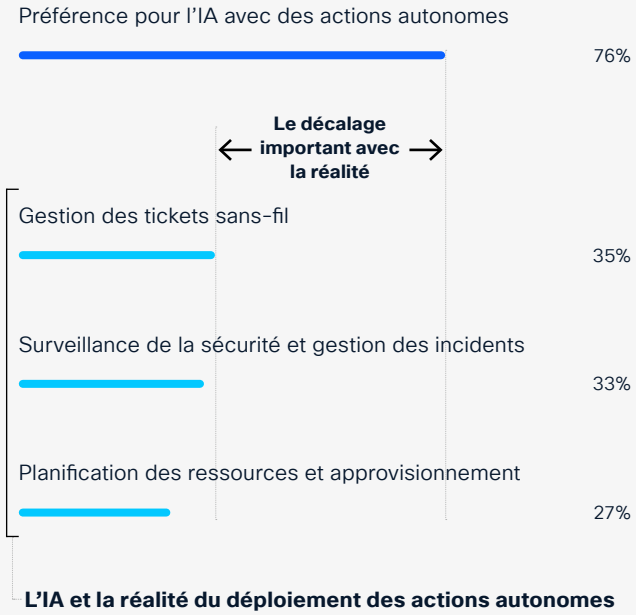
Dans un contexte de transformation organisationnelle accélérée par l'IA, les dirigeants du sans-fil sont nettement convaincus que l'IA représente la solution la plus prometteuse pour surmonter ces défis – avec des bénéfices mesurables: gains de temps, simplification de l'exploitation des réseaux et réduction du temps de résolution des demandes.

Cependant, un écart significatif existe en France entre les attentes et la réalité en ce qui concerne les capacités IA pour le sans-fil.

## 94% signalent un manque de visibilité, notamment:

| | |
|---|---|
| Manque de visibilité sur les clients | 34% |
| Manque de visibilité sur les applications cloud | 32% |
| Manque de visibilité sur les paquets | 31% |

## Le décalage entre attentes et réalité quant à l'IA




**L'IA et la réalité du déploiement des actions autonomes**

© 2026 Cisco and/or its affiliates. All rights reserved.

La complexité opérationnelle à elle seule représente un obstacle majeur à la résolution du paradoxe IA sans-fil et à l'amélioration du retour sur investissement, des solutions sans fil. Combinée à l'intensification des menaces à la sécurité (la deuxième barrière), elle amplifie les impacts sur la résilience organisationnelle et la performance financière.

## **2ème barrière:** La sécurité du sans-fil en péril - la prolifération de l'IoT face aux attaques générées par IA

La sécurité du sans-fil représente la deuxième barrière critique, empêchant les entreprises françaises de résoudre le paradoxe IA et d'obtenir un retour sur investissement significatif. Les entreprises ne peuvent pas déployer le Wi-Fi en toute confiance comme plateforme de charge de travail stratégique, alors que les menaces sur la sécurité s'intensifient et que les pertes financières ne cessent d'augmenter.

84% des entreprises françaises ont connu au moins un incident lié au sans-fil au cours des 12 derniers mois. De plus, 34% rapportent des menaces de plus en plus graves sur le sans-fil au cours des deux dernières années, affirmant qu'elles sont devenues plus fréquentes, préjudiciables, et plus difficiles à détecter et à corriger.

Les dirigeants responsables du sans-fil sont nombreux à citer les cyberattaques générées par l'IA ou automatisées parmi les trois principaux facteurs expliquant la hausse des menaces de cybersécurité visant les réseaux sans-fil. Ces attaques peuvent repérer des vulnérabilités, adapter leurs stratégies selon les mesures de défense en place et opérer à une échelle et à une vitesse qui dépassent largement les capacités d'attaque humaines. De plus, l'IA abaisse la barrière d'entrée pour attaquer les réseaux Wi-Fi, permettant à des acteurs malveillants de déployer des attaques plus sophistiquées et plus rapides qu'auparavant, avec des ressources moindres.

Parallèlement, la surface d'attaque continue de s'étendre. Parmi les entreprises touchées par ces incidents, 26% signalent des perturbations causées par des appareils IoT ou OT compromis. Cela représente une menace importante pour le Wi-Fi, puisqu'il demeure la technologie de connectivité la plus répandue pour l'IoT. La prolifération des appareils connectés – particulièrement lorsqu'ils ne sont pas gérés – augmente la vulnérabilité: les failles individuelles s'additionnent et peuvent exposer l'ensemble du réseau.

### Principaux facteurs à l'origine de la hausse du niveau de menace pour les réseaux sans-fil

| | |
|---|---|
| Les cyberattaques générées par IA ou automatisées / outils automatisés de piratage | 32% |
| Le travail à distance et hybride augmentent la surface d'attaque / les points d'accès non gérés | 29% |
| Contraintes budgétaires ou de ressources qui limitent les améliorations en matière de sécurité | 28% |
| Mauvaises pratiques des utilisateurs, erreurs humaines ou risques liés au personnel interne | 27% |
| Hausse de l'utilisation de l'IoT et des appareils connectés (croissance rapide du nombre d'appareils) | 25% |

L'impact financier de ces incidents est considérable. En France, 49% des entreprises rapportent avoir subi des pertes financières à la suite d'incidents liés à la sécurité du sans-fil. Parmi elles, 40% indiquent des pertes de plus de 1 million de dollars américains au cours de la dernière année – un impact qui, à lui seul, justifie des investissements accrus dans la sécurité du Wi-Fi.

Les répercussions ne se limitent pas aux coûts directs associés aux incidents. En plus de l'impact financier, 30% des entreprises rapportent une perte de confiance de la part de leurs clients tandis que 30% disent avoir fait face à des sanctions réglementaires ou à des conséquences en matière de conformité.

Paradoxalement, la plupart des entreprises demeurent confiantes quant à la sécurité de leur réseau sans fil. 79% estiment que leur organisation en fait suffisamment pour protéger ses réseaux sans-fil, alors que 81% s'attendent aussi à une augmentation des défaillances de sécurité au cours des deux prochaines années.

© 2026 Cisco and/or its affiliates. All rights reserved.

Les entreprises citent trois principaux obstacles à l'amélioration de la sécurité du réseau sans fil: la complexité de mise en œuvre, l'infrastructure existante et les enjeux de performances. Ces obstacles ne sont pas isolés, ils reflètent des enjeux plus larges – pénurie de professionnels qualifiés, manque de visibilité et pressions opérationnelles – qui limitent la capacité des entreprises à moderniser leur posture de sécurité.

Il en résulte une augmentation des vulnérabilités: alors même que les risques s'intensifient, les entreprises sont limitées par des systèmes obsolètes, de la complexité et des contraintes de performance, ralentissant la transformation et érodant leur résilience.

Cependant, la recherche montre que les entreprises qui adoptent des systèmes d'authentification modernes, fondés sur des certificats ou des profils, affichent de meilleurs résultats en matière de sécurité, et des performances bien supérieures à celles qui n'en utilisent pas. Elles subissent également, en moyenne, des pertes financières moins importantes que celles qui n'utilisent pas de protocoles d'authentification modernes.

Cependant, la mise en œuvre de protocoles de sécurité modernes nécessite des experts spécialisés, qui sont de plus en plus difficiles à trouver. Cela nous amène au troisième obstacle: la concurrence pour attirer les talents dans le secteur du sans-fil.

## **3ème barrière**: Le sans-fil perd la course aux talents contre l'IA

La pénurie de main-d'œuvre qualifiée constitue le troisième obstacle. Combinée à la complexité opérationnelle et à l'intensification des menaces à la sécurité, elle entraîne un ralentissement qui limite la capacité des entreprises à optimiser le retour sur investissement de leurs solutions sans fil.

Le manque de professionnels compétents ne freine pas seulement la modernisation; il accentue directement les contraintes opérationnelles et les risques liés à la sécurité, tout en rendant plus difficile la mise en œuvre d'AIOps. Cela contribue à créer un cercle vicieux: les entreprises en manque de professionnels mettent plus de temps à se moderniser, la complexité et les risques liés à la sécurité s'aggravent, les coûts augmentent, et les meilleurs professionnels partent vers des entreprises plus avancées.

En France, 89% des entreprises font état de difficultés de recrutement, les professionnels des TI se dirigeant vers d'autres domaines technologiques plus valorisés, comme l'IA et la cybersécurité. Cette situation accentue la pénurie de main-d'œuvre qualifiée, qui se traduit par une hausse des coûts d'exploitation (33%), une baisse du moral (30%) et une capacité d'innovation réduite (24%).

Le lien entre les enjeux de talents et les résultats négatifs est clair. Les entreprises qui éprouvent des difficultés importantes à recruter des spécialistes des réseaux sans-fil consacrent davantage de temps à des tâches réactives. Et l'impact ne se limite pas aux opérations: elles font état de coûts annuels plus élevés liés aux incidents de sécurité que celles qui ne rencontrent pas de difficultés de recrutement.

Les entreprises confrontées à des enjeux de recrutement doivent aussi composer avec d'autres effets: des coûts opérationnels plus élevés, une augmentation des risques liés à la sécurité, moins d'automatisation et moins de capacité pour se mettre à niveau. Les entreprises qui investissent tôt dans les compétences et les certifications ont un avantage concurrentiel, la complexité augmentant et que les compétences spécialisées deviennent essentielles à la mise en œuvre opérationnelle, en particulier dans un contexte de concurrence croissante pour attirer les professionnels qualifiés.

© 2026 Cisco and/or its affiliates. All rights reserved.

La pénurie de main-d'œuvre qualifiée met en évidence l'interdépendance du paradoxe IA sans-fil. Si les entreprises ne placent pas l'IA au cœur de leurs activités liées au des réseaux sans fil, elles risquent de continuer à perdre leurs meilleurs professionnels. Sans les compétences requises, il devient plus difficile de mener à bien les projets stratégiques comme la modernisation des systèmes de sécurité.

Or, sans systèmes de sécurité à jour, les coûts liés aux incidents augmentent, ce qui rend plus difficile l'investissement en parallèle dans les talents et les technologies. Cette combinaison explique pourquoi les entreprises doivent s'attaquer simultanément à ces trois barrières pour sortir de ce paradoxe.

## Lien entre l'IA, la « fuite des cerveaux » du sans-fil et la pénurie de main-d'œuvre qualifiée

**Figurant parmi les trois principaux secteurs qui attirent les talents au détriment du secteur sans-fil**

| | |
|---|---|
| Cybersécurité | 62% |
| IA / Apprentissage automatique | 53% |
| Infrastructure cloud / DevOps | 37% |

**Principales raisons de la difficulté à recruter des professionnels du secteur sans-fil**

| | |
|---|---|
| Manque de candidats ayant des compétences avancées dans le sans-fil ou en intégration de l'IA | 48% |
| Contraintes budgétaires internes ou gel des embauches | 32% |
| Limitations géographiques ou difficultés associées au travail à distance | 30% |

© 2026 Cisco and/or its affiliates. All rights reserved.

# Méthodologie

Cette étude a été réalisée à partir d'entretiens menés auprès de 6,098 entreprises sur 30 marchés, dont 308 entreprises en France. Elle a été réalisée en novembre 2025 par Sandpiper Research and Insights.

**Profil des personnes interrogées:** les entretiens ont été menés auprès de 6,098 décideurs et spécialistes techniques du secteur sans-fil issus d'entreprises comptant au moins 250 employés. Six répondants sur dix (61%) travaillent dans des entreprises dont le chiffre d'affaires annuel est d'au moins 100 millions de dollars américains.

Amériques — 22%

Europe, Moyen-Orient et Afrique — 28%

Asie-Pacifique — 50%

**Couverture géographique:** La recherche a couvert 30 marchés, dont ceux des pays suivants : Afrique du Sud, Arabie saoudite, Australie, Brésil, Canada, Corée du Sud, Espagne, France, Allemagne, Hong Kong, Inde, Indonésie, Italie, Japon, Malaisie, Mexique, Nouvelle-Zélande, Pays-Bas, Philippines, Pologne, Singapour, Suisse, Taïwan, Thaïlande, Émirats arabes unis, Royaume-Uni, États-Unis et Vietnam.

**Représentation des secteurs:** Les répondants proviennent d'un large éventail de secteurs, notamment les services aux entreprises, la construction, l'éducation, l'ingénierie, le design et l'architecture, les services financiers, le gouvernement et les services publics, la santé, l'industrie, les médias et la communication, les ressources naturelles, l'immobilier, la restauration, la vente au détail, les services informatiques et technologiques, le transport, les agences de voyage et le commerce de gros.

**Date:** L'étude a été menée en novembre 2025

© 2026 Cisco and/or its affiliates. All rights reserved.

**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)