Rapport

Les PME à l'ère de l'IA : naviguer dans la complexité cybernétique et renforcer la résilience

Avec les travaux d'étude et d'analyse de

Sage

IDC

Méthodologie et contexte de l'enquête

Joel Stradling
Senior Research Director,
European Security, IDC

Ce rapport s'appuie sur les résultats d'une étude mondiale menée par IDC, à la demande de Sage, auprès de 2 210 petites entreprises réparties sur huit marchés.

L'étude publiée dans l'InfoBrief IDC intitulé Les PME à l'ère de l'IA : naviguer dans la complexité cybernétique et renforcer la résilience (mars 2026 ; IDC no EUR254487126) et rédigée par Joel Stradling, analyste chez IDC, évalue la façon dont les PME répondent aux défis actuels et émergents en matière de cybersécurité.

Elle explore leurs principales préoccupations et leur posture en matière de sécurité par rapport à l'IA et aux solutions de fournisseurs tiers, et identifie les changements stratégiques nécessaires pour passer d'une défense réactive à une sécurité proactive et à une cyberrésilience durable qui prend en compte les risques.

L'étude a porté sur les secteurs suivants : services financiers, soins de santé, télécommunications, énergie, fabrication, ressources, commerce de détail, logiciels et services d'information, transports et voyages, services aux entreprises et aux particuliers, éducation, gouvernement, organisations à but non lucratif, audit et fiscalité, construction, et hôtellerie et loisirs.

Source : IDC InfoBrief, « Les PME à l'ère de l'IA : naviguer dans la complexité cybernétique et renforcer la résilience », sponsorisé par Sage, avril 2026, IDC Doc n° EUR254487126.

Pays faisant partie de l'enquête

- Canada
- Espagne
- États-Unis
- Portugal
- France
- Royaume-Uni
- Allemagne
- Afrique du Sud

Taille de l'entreprise

1 à 9
Micro-entreprise

10 à 99
Petite entreprise

100 à 499
Moyenne entreprise

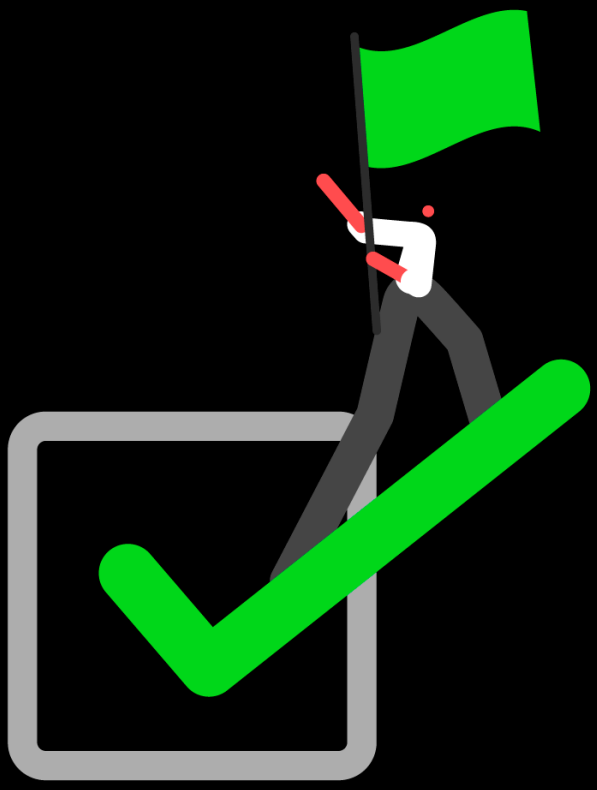
« L'IA devrait être une opportunité de croissance pour toutes les PME, et pas seulement pour celles qui disposent des ressources les plus solides en matière de sécurité. Les petites entreprises restent plus prudentes, car l'adoption sécurisée de la cybersécurité reste difficile dans la pratique. Si nous voulons que davantage de PME profitent de l'IA, nous devons simplifier l'adoption de la cybersécurité grâce à des mesures de protection intégrées, des orientations plus claires et un soutien pratique. »

Gustavo Zeidan
Chief Information Security Officer, Sage

Sage

Table des matières

Résumé



Les PME investissent de plus en plus dans la cybersécurité tout adoptant l'IA à un rythme croissant. Mais pour beaucoup d'entre elles, leurs pratiques en matière de sécurité n'ont pas évolué aussi rapidement, ce qui les laisse plus exposées à des risques qui se développent plus rapidement que la résilience.

S'appuyant sur une enquête menée auprès de 2 210 PME sur huit marchés, ce rapport examine la manière dont les petites et moyennes entreprises répondent à l'évolution des défis en matière de cybersécurité, en mettant l'accent sur l'adoption de l'IA et le risque lié aux fournisseurs tiers. La cybersécurité est désormais une priorité essentielle pour les petites et moyennes entreprises.

Dans le cadre de cette enquête, 52 % des PME ont déclaré qu'assurer la cybersécurité et la protection des données est l'une de leurs principales priorités pour les 12 prochains mois, juste derrière la croissance de l'entreprise (59 %) et bien avant l'intensification de l'utilisation de l'IA (33 %). Dans le même temps, 60 % prévoient d'augmenter leurs dépenses dans la cybersécurité, ce qui montre une intention claire d'agir.

Mais pour de nombreuses PME, les initiatives menées ne sont toujours pas à la hauteur du risque. Près de la moitié d'entre elles déclarent subir un cyberincident chaque année, et les pratiques de sécurité proactives restent limitées, en particulier dans les petites entreprises. Seuls 13 % des micro-entreprises et 21 % des petites entreprises qualifient leur approche de proactive, contre 48 % des entreprises de taille moyenne.

L'IA amplifie les risques. Elle ne crée pas un ensemble de risques entièrement nouveaux, mais elle rend les menaces connues plus rapides, plus convaincantes et plus difficiles à gérer. De nombreuses PME ne sont pas du tout prêtes à faire face aux menaces liées à l'IA, en particulier les petites entreprises. 84 % des micro-entreprises et 65 % des petites entreprises affirment qu'elles ne sont pas préparées ou qu'elles n'en sont qu'aux premières étapes.

Dans le même temps, 22 % déclarent n'avoir mis en place aucune mesure de sécurité spécifique pour les applications d'IA, ce chiffre atteignant 44 % dans les micro-entreprises.

Les risques liés aux SaaS tiers et à la chaîne d'approvisionnement représentent un angle mort majeur. Alors que les outils SaaS sont omniprésents dans les écosystèmes des PME, 43 % des micro-entreprises n'effectuent pas de contrôle régulier ou continu de leurs fournisseurs tiers, et préfèrent faire confiance uniquement à des certifications statiques ou des vérifications ponctuelles. Cela limite la visibilité en temps réel des risques liés aux fournisseurs et augmente la probabilité que les failles de sécurité ne soient pas détectées jusqu'à ce qu'une perturbation se produise.

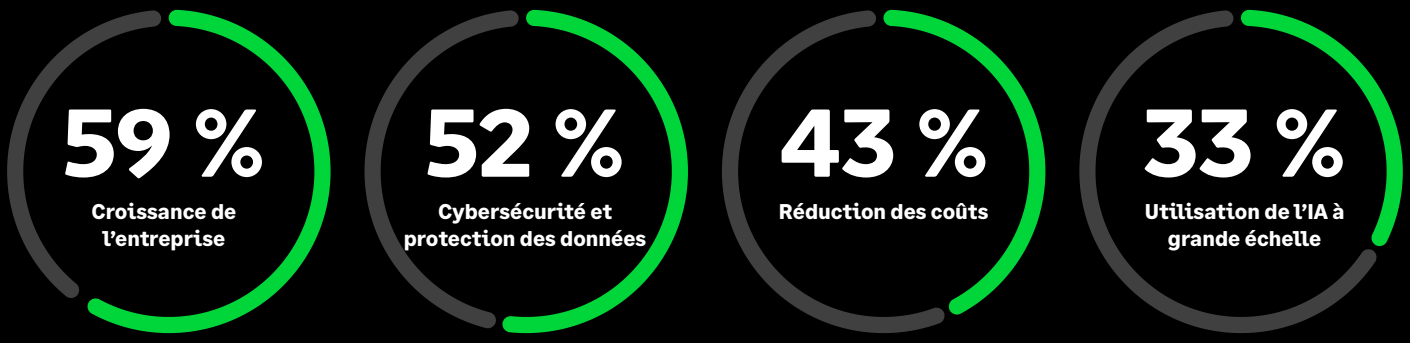
Les conclusions de l'étude mettent en évidence un impératif clair : les PME on besoin d'outils plus simples et plus pratiques permettant de dépasser le stade de la posture réactive pour intégrer la gestion des risques dans leurs activités quotidiennes.

Cela signifie qu'il faut intégrer la sécurité dès le départ, renforcer la discipline au quotidien et se concentrer sur une appropriation claire, un contrôle régulier et une sensibilisation des employés en fonction de la taille de l'entreprise. Une bonne gestion des risques n'est pas seulement importante pour ces entreprises, mais aussi pour la confiance des clients, les chaînes d'approvisionnement et la résilience de l'écosystème numérique au sens large.

La cybersécurité est désormais au cœur des priorités des PME, mais les demandes concurrentes en matière d'informatique pèsent sur les budgets

Interrogées sur leurs principales priorités pour les 12 prochains mois, plus de la moitié des PME (52 %) citent la cybersécurité et la protection des données, juste après la croissance de l'entreprise (59 %) et avant la réduction des coûts (43 %). Cela témoigne d'un net changement d'état d'esprit. Le risque cybernétique n'est plus considéré comme une question purement technique, compte tenu de ses répercussion majeure sur les activités de l'entreprise.

Priorités des entreprises pour l'année :



Prévoient une augmentation du budget de la sécurité au cours des 12 prochains mois :

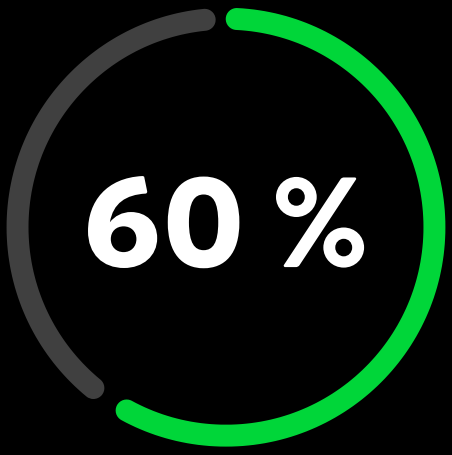
51 % **1 à 9** Micro-entreprise

59 % **10 à 99** Petite entreprise

65 % **100 à 499** Moyenne entreprise

Les investissements prévus confirment ces priorités. Six PME sur dix (60 %) déclarent qu'elles prévoient d'augmenter leurs dépenses dans la cybersécurité au cours des 12 prochains mois, ce qui témoigne à la fois d'une reconnaissance du problème et d'une volonté d'agir. Cependant, d'autres priorités concurrentes, notamment la maîtrise des coûts et l'accélération de l'adoption de l'IA (33 %), empêchent ces entreprises de progresser comme elles le devraient. Bien que la cybersécurité soit clairement en tête de liste des priorités, l'augmentation des dépenses ne leur permet pas toujours de pouvoir se préparer, ce qui explique en partie pourquoi il existe toujours des lacunes en matière de fiabilité, de gouvernance et d'exécution sur le marché des PME.

Les données indiquent qu'il existe un écart croissant entre l'intention et l'exécution. La cybersécurité est plus importante que jamais, mais de nombreuses PME peinent à la rendre opérationnelle de manière cohérente.



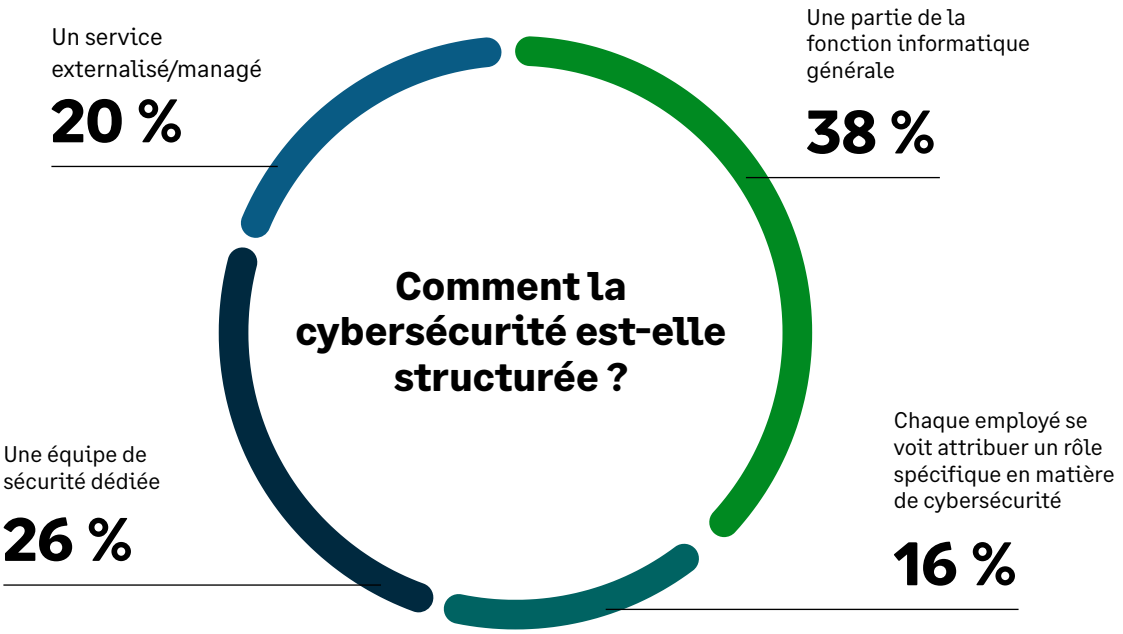
des PME déclarent qu'elles prévoient d'augmenter leurs dépenses en matière de cybersécurité au cours des 12 prochains mois

La gouvernance de la sécurité reste informelle pour la plupart des PME, ce qui limite l'impact des investissements croissants

Pour la majorité des PME (38 %), les responsabilités en matière de cybersécurité restent vaguement définies et intégrées dans la fonction informatique au sens large, plutôt que d'être soutenues par une appropriation claire, des cycles d'examen formels ou des processus documentés.

En conséquence, les activités en matière de sécurité sont souvent réactives, consécutives à des incidents, plutôt que gérées comme une discipline de routine.

Cette lacune en matière de gouvernance contribue à expliquer pourquoi l'augmentation des dépenses en matière de cybersécurité ne se traduit pas toujours par une meilleure préparation. Sans une responsabilité plus claire, une surveillance de routine et une discipline opérationnelle, même les investissements, aussi pertinents soient-ils, peinent à contribuer à une réduction cohérente des risques, en particulier à mesure que l'IA et les outils tiers exposent les entreprises à des risques croissants.



Pour remédier à ces insuffisances, les **PME doivent faire de la sécurité un élément plus cohérent de leur activité quotidienne**, avec une responsabilité claire, des examens réguliers et des processus pratiques qui peuvent s'adapter au fil du temps.

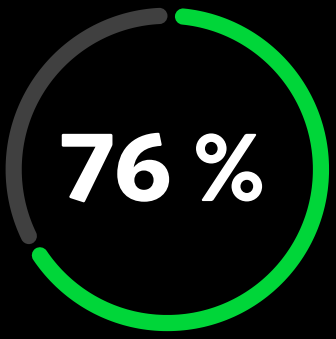
La plupart des PME disposent des bons outils de sécurité, mais peinent à les appliquer de manière cohérente

Les contrôles techniques de base sont désormais la norme dans la plupart des PME, mais il reste des défis à relever dans des domaines tels que la gestion des outils, la formation du personnel et la planification de la réponse aux incidents.

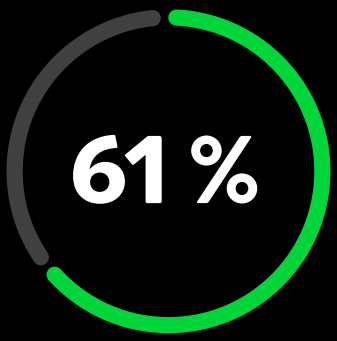
Par conséquent, la maturité en matière de sécurité dépend moins de l'introduction de nouveaux contrôles que de l'intégration de la discipline opérationnelle nécessaire pour maintenir l'efficacité des mesures de protection existantes au fur et à mesure de l'évolution de l'entreprise.

Pour renforcer leur posture en matière de cybersécurité, les PME devraient mettre davantage l'accent sur la gouvernance des données, les contrôles de sécurité et la transparence. À mesure qu'elles évoluent, elles doivent mettre en place des cycles de révision plus formels, définir clairement les responsabilités et documenter les processus de manière cohérente dans l'ensemble de l'organisation.

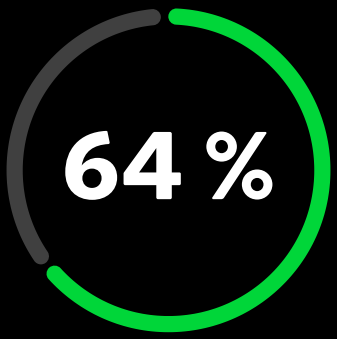
Indicateurs de confiance opérationnels :



examinent régulièrement leur cybersécurité

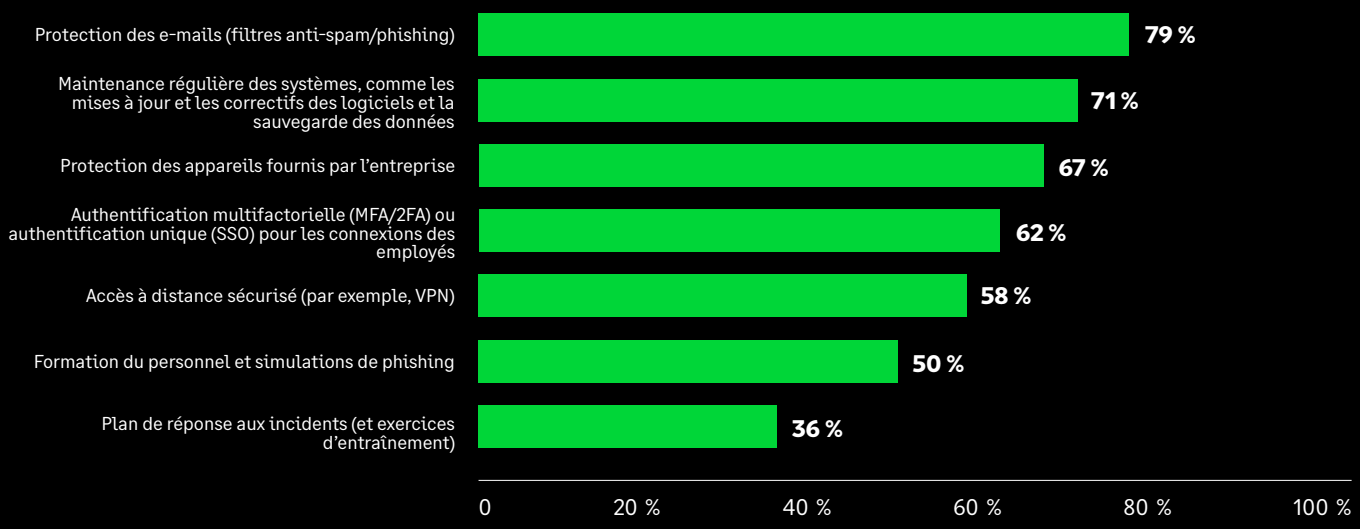


affirment que les employés sont formés à l'identification des cyberrisques



examinent rigoureusement la sécurité liée aux tiers avant de conclure un contrat

Quelles sont les mesures de cybersécurité actuellement en place ?



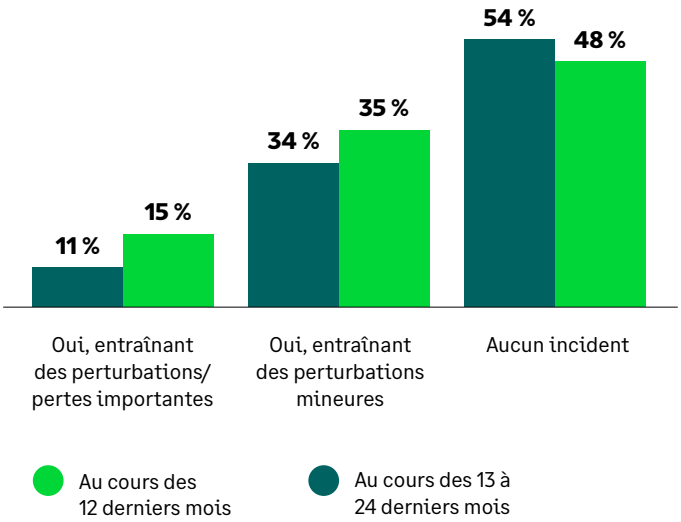
Lorsque la sécurité reste informelle, les incidents deviennent perturbateurs

Pour les PME, le cyberrisque n'implique plus des perturbations occasionnelles. Il s'agit d'un défi permanent pour l'entreprise, façonné par un ensemble de menaces plus large et moins prévisible, allant du phishing et de l'ingénierie sociale aux risques internes, à l'exposition de tiers et aux vulnérabilités de la chaîne d'approvisionnement.

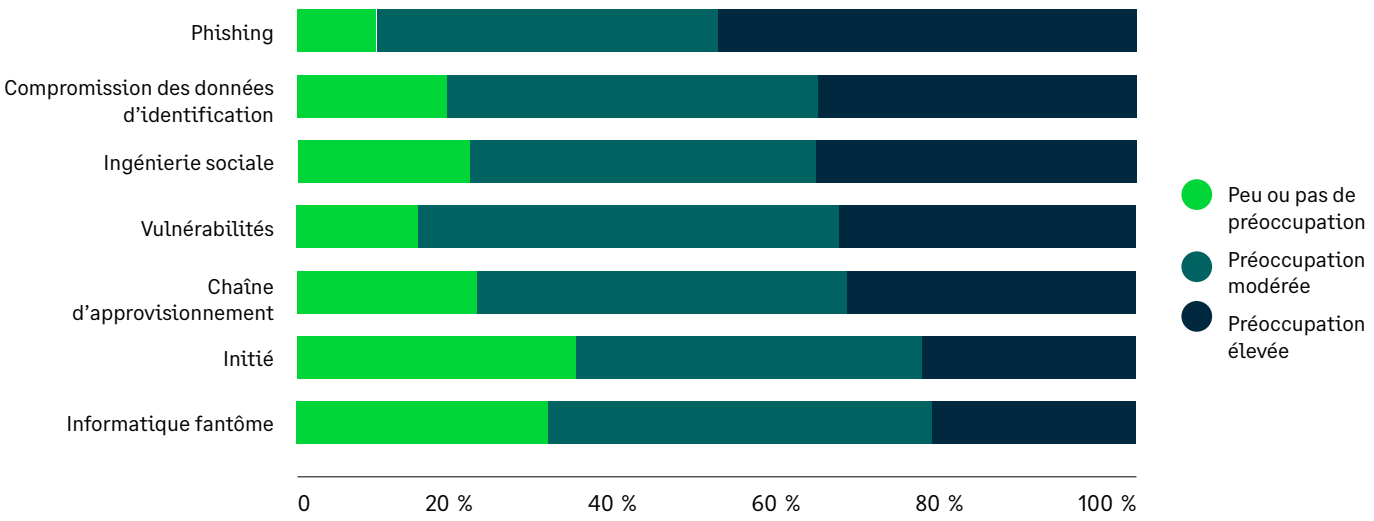
Alors que les entreprises sont de plus en plus exposées, la résilience dépend moins de la prévention de chaque incident que de la capacité à bien gérer les perturbations.

L'accent n'est donc plus mis uniquement sur les incidents, mais sur la qualité de la réponse : la rapidité avec laquelle les problèmes sont identifiés, l'efficacité avec laquelle ils sont maîtrisés et la capacité de l'entreprise à rétablir efficacement ses activités, en préservant la confiance placée en elle, ainsi que sa trésorerie et la continuité de ses activités

Incidents de cybersécurité ou violations de données



Préoccupation concernant chacun des risques suivants



Pour les PME, cela signifie qu'il faut mettre en place des **moyens simples et reproductibles visant à détecter rapidement les problèmes**, réagir rapidement, limiter les répercussions et continuer à faire fonctionner l'entreprise en cas de perturbation.

L’évolution rapide des menaces et une visibilité limitée exposent davantage les PME aux risques de cybersécurité

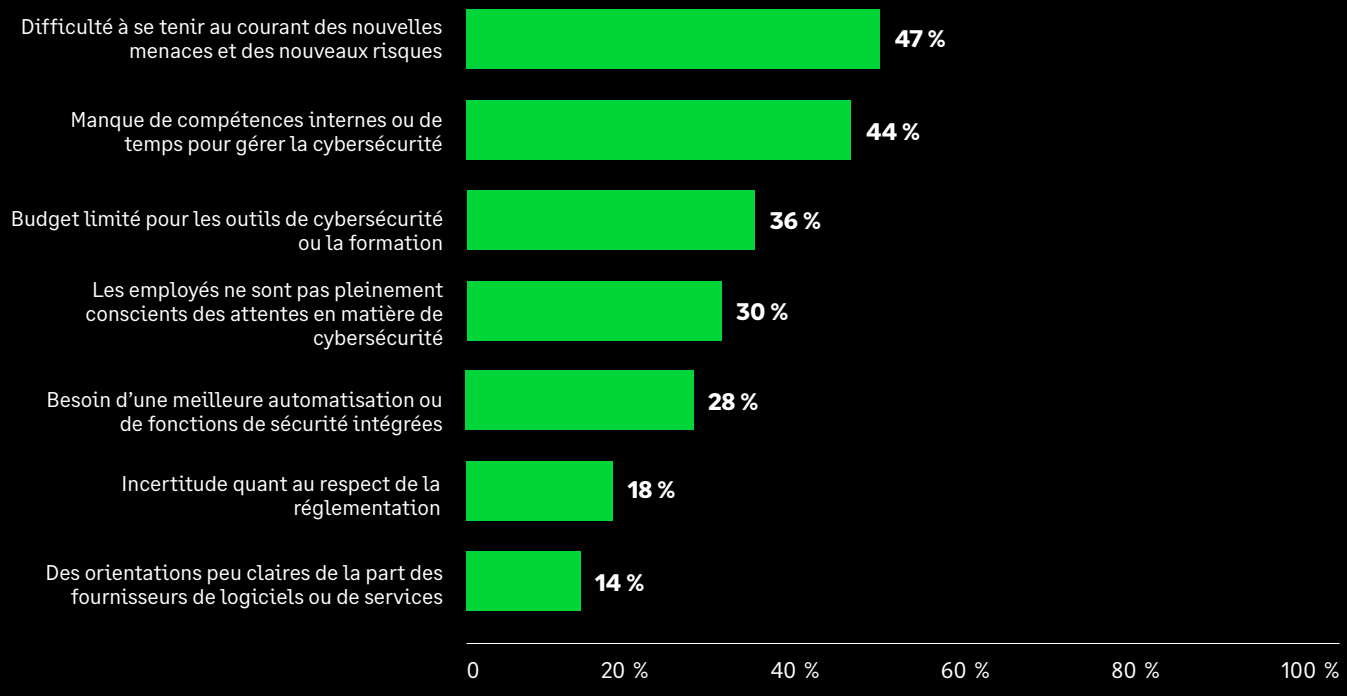
Près de la moitié des PME (47 %) considèrent que se tenir au courant des nouvelles menaces et des nouveaux risques est le principal défi à relever en matière de cybersécurité.

Les attaques basées sur l’IA, le phishing plus sophistiqué et l’utilisation croissante des services cloud et SaaS augmentent à la fois la vitesse et la complexité des cybermenaces, et les entreprises parviennent rarement à s’adapter par manque de capacités.

Dans le même temps, de nombreuses PME ne disposent pas d’une visibilité claire et permanente sur les points les plus exposés. Des compétences spécialisées limitées, des priorités opérationnelles concurrentes et des contraintes budgétaires rendent difficile le maintien d’une surveillance continue ou d’une évaluation structurée des risques. En conséquence, le cyberisque est souvent compris dans ses grandes lignes, mais n’est pas géré activement au jour le jour.

Cette combinaison d’une évolution rapide des menaces et d’une visibilité incomplète augmente considérablement la probabilité que les problèmes soient détectés tardivement, qu’ils soient mal priorisés ou qu’ils ne soient traités à postériori. Pour les PME dont la gouvernance est informelle et la discipline opérationnelle inégale, cela crée un écart persistant entre le risque perçu et l’exposition réelle.

Lesquels des éléments suivants décrivent le mieux les principaux défis auxquels votre entreprise est confrontée en matière de gestion de la cybersécurité ?



Pour progresser plus rapidement, les PME devraient privilégier les solutions qui réduisent les frais généraux opérationnels, notamment les solutions d’automatisation, de protections intégrées et d’assistance externe, adaptées à leurs ressources limitées.

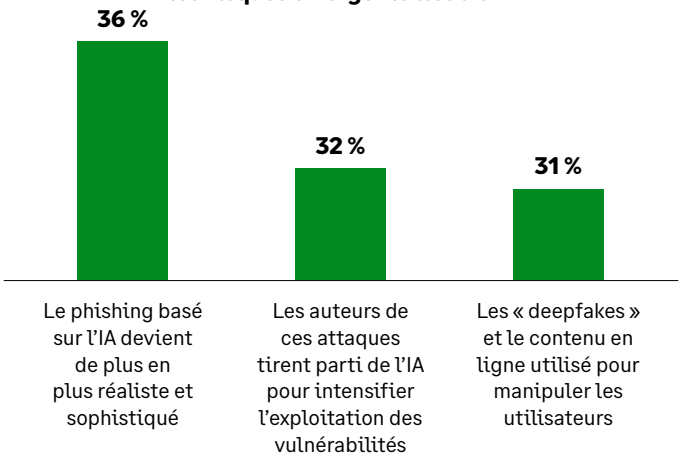
Les menaces liées à l'IA évoluent plus rapidement que les pratiques de sécurité des PME

L'intelligence artificielle vient exacerber les défis d'un environnement cyber déjà exigeant, alors que les PME sont les moins armées pour faire face à cette évolution.

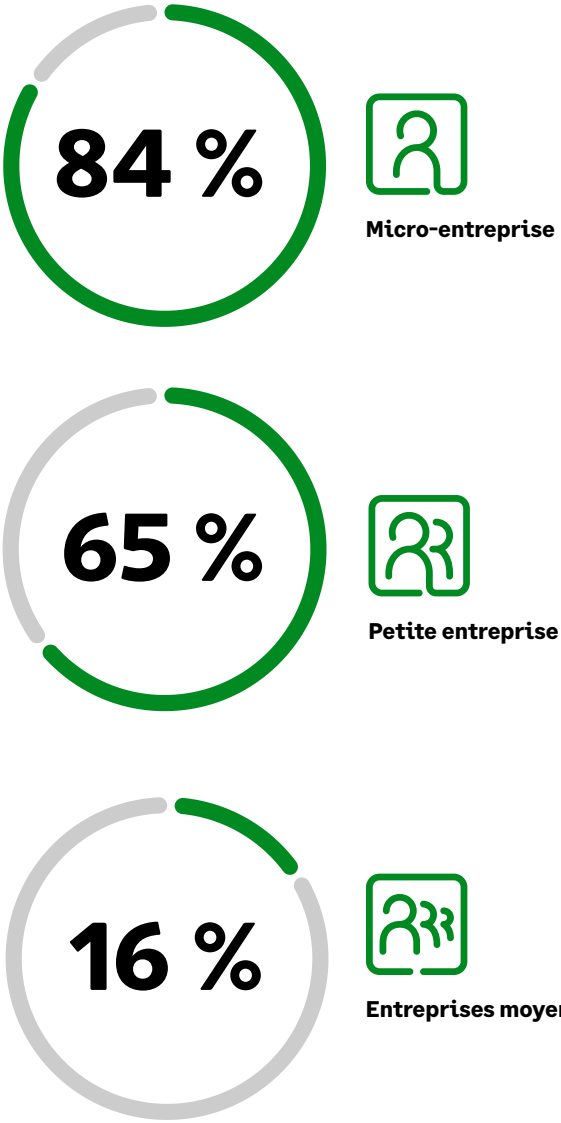
Les micro-entreprises et les petites entreprises souffrent des plus grandes lacunes, avec une surveillance quotidienne plus faible, un contrôle moins cohérent et un personnel moins sensibilisé à la cybersécurité, alors que l'IA est utilisée pour augmenter à la fois la vitesse et l'ampleur des attaques. Les pratiques en matière de sécurité qui ont pu suffire dans le passé deviennent moins efficaces à mesure que les menaces évoluent.

Pour les PME, la réponse doit commencer par les bases : une plus grande sensibilisation, des mesures de protection concrètes et des moyens plus clairs de détecter et de gérer les risques à un stade précoce. Mais ce n'est qu'une partie de la réponse. À mesure que les menaces liées à l'IA évoluent, les entreprises auront également besoin de moyens plus simples d'automatiser les tâches de sécurité de routine, de réduire les tâches manuels, et de développer des capacités informatiques et de sécurité actuellement limitées pour se concentrer sur les domaines présentant le plus de risques.

Les trois principales préoccupations concernant les risques émergents liés à l'IA



Pas préparées ou aux premières étapes de préparation pour faire face aux menaces liées à l'IA :



Pour les **PME moins matures en particulier, la formation et la sensibilisation restent essentielles.** Les responsables de la sécurité devraient donner la priorité à des mesures pratiques faciles à adopter qui aident les équipes à reconnaître et à réduire les risques liés à l'IA sans ajouter de complexité inutile.

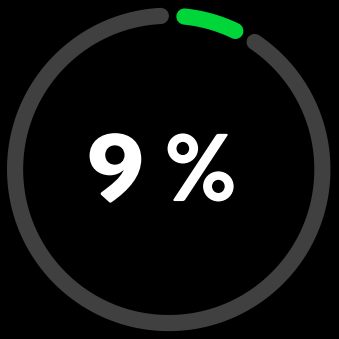
Sage

Les PME recherchent de nouvelles possibilités d'utiliser l'IA, alors même que les risques de sécurité augmentent

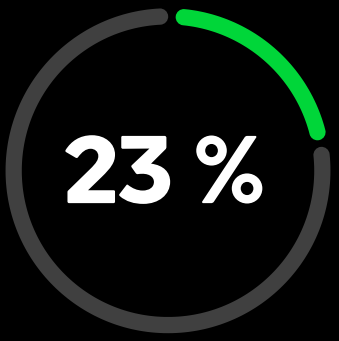
Une part importante des PME voit des opportunités dans l'IA, tandis qu'une proportion encore plus importante pense que l'IA augmente les risques de cybersécurité. Cette perception varie selon la taille de l'entreprise. Les entreprises de taille moyenne sont plus susceptibles de considérer l'IA comme une opportunité.

Les micro-entreprises et les PME abordent l'IA avec plus de prudence. Cela traduit des disparités en matière de confiance dans les contrôles de sécurité et la gouvernance, plutôt qu'un manque d'ambition.

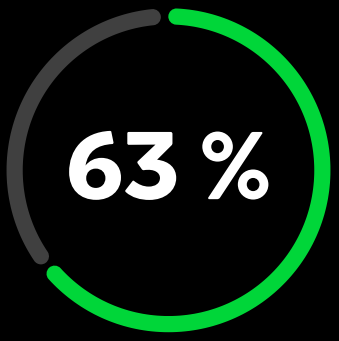
L'IA est perçue comme une opportunité de croissance :



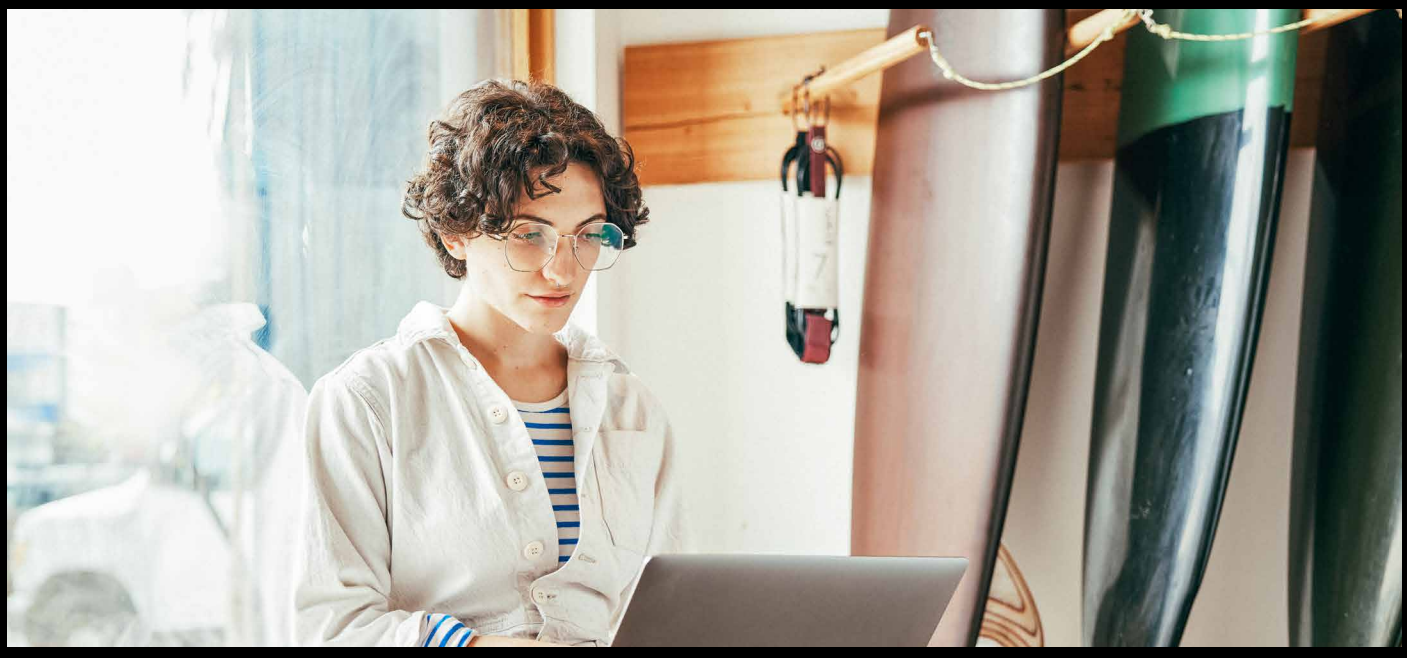
Micro-entreprise



Petite entreprise

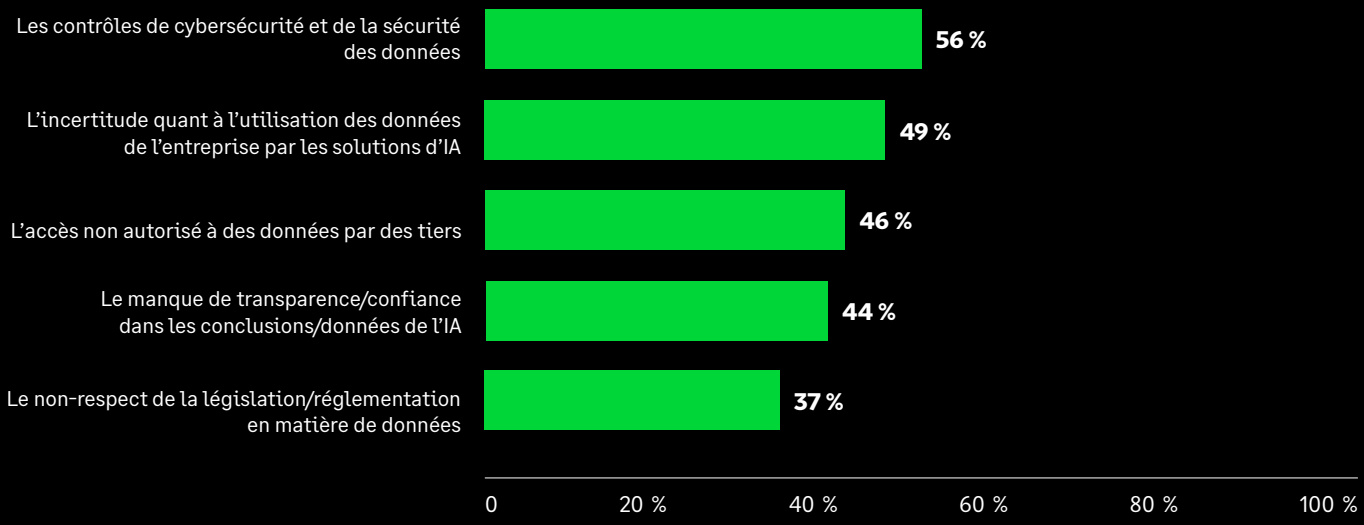


Entreprises de taille moyenne



La sécurité des données, la gouvernance et la transparence dans l'adoption de l'IA suscitent des inquiétudes. Sans visibilité claire sur la manière dont les données sont utilisées et protégées, de nombreuses PME restent prudentes quant au déploiement de l'IA à grande échelle.

Parmi les propositions suivantes, quelle est votre plus grande préoccupation concernant l'adoption ou l'utilisation de l'IA au sein de votre entreprise ?



À mesure que l'IA s'intègre dans les activités quotidiennes, les PME ont besoin d'une visibilité claire sur l'endroit et la manière dont elle est utilisée, ainsi que d'une gouvernance bien définie pour gérer les risques associés. Il s'agit notamment d'identifier les outils et systèmes d'IA dans l'ensemble de l'entreprise et de mettre en place des mécanismes de surveillance, ainsi que des politiques et une responsabilité appropriées au niveau de la direction. Sans cela, le rythme d'adoption de l'IA risque d'introduire des risques que l'entreprise ne sera pas en mesure de gérer, augmentant ainsi son exposition au lieu de créer de la valeur.

Les PME posent déjà les bases de la conformité réglementaire en matière d'IA

Parallèlement à l'émergence de nouvelles réglementations et normes en matière d'IA, de nombreuses PME entament leurs travaux de mise en conformité.

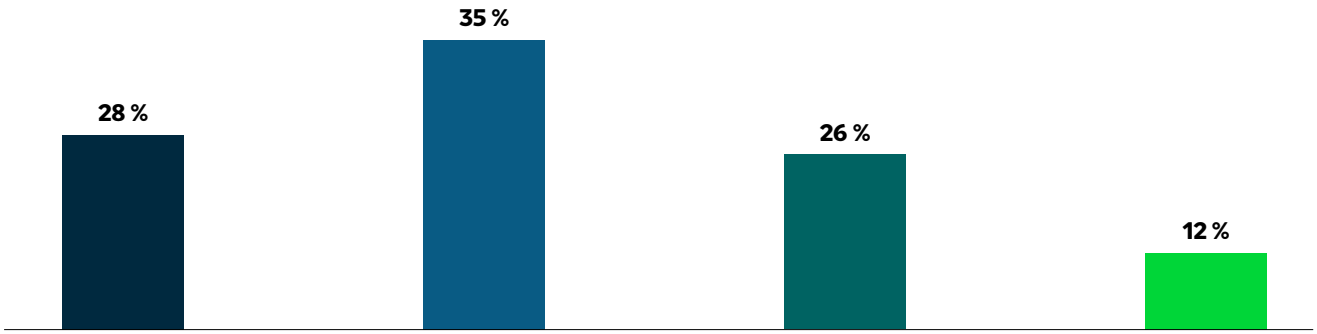
Les cadres de référence, tels que les réglementations nationales en matière d'IA et les codes de pratique non obligatoires, sont destinés à aider les entreprises à traduire les politiques de haut niveau en mesures pratiques de sécurité et de gouvernance au quotidien. Un nombre croissant de gouvernements reconnaissent que les pratiques de base en matière de sécurité logicielle et de l'IA doivent être largement adoptées tout au long de la chaîne d'approvisionnement, et pas seulement par les grandes entreprises. Des pays comme le Royaume-Uni se concentrent sur des approches pratiques et proportionnées.

Le code de pratique sur la sécurité des logiciels (Software Security Code of Practice) et le programme connexe des ambassadeurs de la sécurité des logiciels (Software Security Ambassadors Scheme), lancés dans le cadre du plan d'action sur le cyberespace du gouvernement britannique, en sont un exemple. Ces programmes rassemblent des organisations des secteurs public et privé, dont Sage, afin de promouvoir l'adoption des principes fondamentaux de la sécurité logicielle, de partager des expériences pratiques de mise en œuvre et de promouvoir le renforcement de la résilience dans l'ensemble de l'économie.

« Les PME sont l'épine dorsale de l'économie britannique, mais nous savons que nombre d'entre elles ont du mal à investir dans la cybersécurité, alors que les cybermenaces se multiplient. L'amélioration de la cyberrésilience au Royaume-Uni est une priorité pour le gouvernement. C'est pourquoi notre Centre national de cybersécurité a développé la boîte à outils Cyber Action pour aider les PME à renforcer leurs cyberdéfenses. Nous recommandons à toutes les entreprises d'adopter notre programme Cyber Essentials, très efficace, qui les aide à se protéger contre les menaces en ligne les plus courantes et réduit les risques d'être victimes d'une cyberattaque coûteuse et déstabilisante. »

La très honorable Liz Kendall MP, secrétaire d'État britannique à la science, à l'innovation et à la technologie

Préparation des PME à se conformer aux réglementations sur l'IA et aux normes d'assurance



Non préparée
Peu ou pas de sensibilisation ou de planification pour les réglementations ou les normes en matière d'IA

Commence à peine
Consciente des exigences à venir ; premières discussions ou planification en cours

En cours
Développe activement les politiques, le contrôle et la gouvernance pour se conformer aux exigences de l'UE

Bien préparée
Processus et garanties déjà en place pour répondre aux nouvelles exigences

Pour les PME, des initiatives de ce type mettent en évidence une voie pragmatique à suivre : se conformer à des cadres reconnus, choisir des partenaires engagés dans le développement sécurisé et intégrer des pratiques de sécurité de base dès le début, à mesure que l'adoption de l'IA s'accélère.

Sage

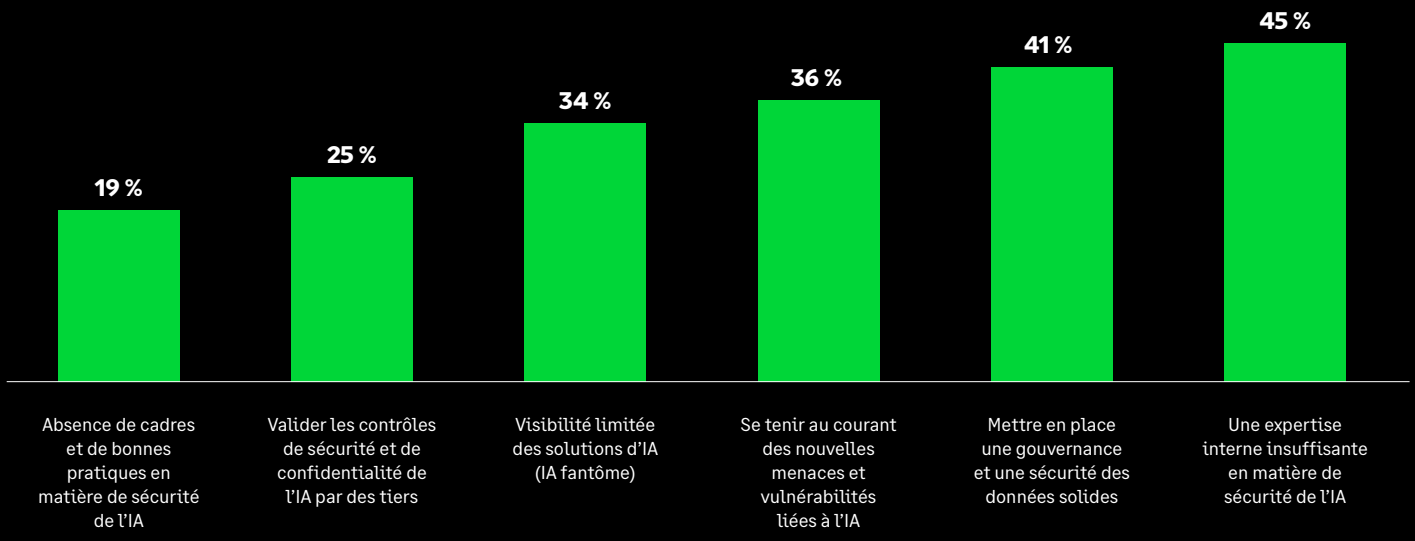
Les défis de sécurité de l'IA pour les PME concernent essentiellement les lacunes de compétences, la protection des données et l'évolution rapide des menaces

L'IA est le révélateur d'un déficit de capacités pour les PME, et pas seulement un déficit technologique. De nombreuses entreprises adoptent l'IA plus rapidement qu'elles ne peuvent en appréhender les risques, évaluer leur exposition à ces risques ou juger de la fiabilité de leurs prestataires tiers en matière de sécurité.

La situation est particulièrement difficile pour les petites entreprises, où la responsabilité repose souvent sur un seul spécialiste informatique ou sur une équipe généraliste

La protection des données et l'évolution rapide des menaces aggravent la situation. Comme les outils d'IA ont besoin d'accéder aux données de l'entreprise et des clients, une faible visibilité et une surveillance relâchée peuvent rapidement exposer l'entreprise à des risques. Dans le même temps, l'IA rend les attaques connues plus rapides, plus convaincantes et plus difficiles à gérer, ce qui fait que de nombreuses PME ont du mal à s'adapter.

Principaux défis liés à la protection des applications et des infrastructures d'IA et de GenIA



Pour les PME disposant de ressources spécialisées limitées, la priorité est de rester pragmatique : limiter l'utilisation de l'IA aux outils approuvés, établir des règles simples permettant de savoir quelles données peuvent être utilisées, examiner régulièrement comment l'IA est utilisée, et s'appuyer sur des fournisseurs de confiance ou des partenaires externes lorsque l'expertise interne est limitée. Cela contribuera davantage à réduire les risques que d'ajouter de la complexité.

La surveillance limitée des fournisseurs de SaaS laisse de nombreuses PME exposées

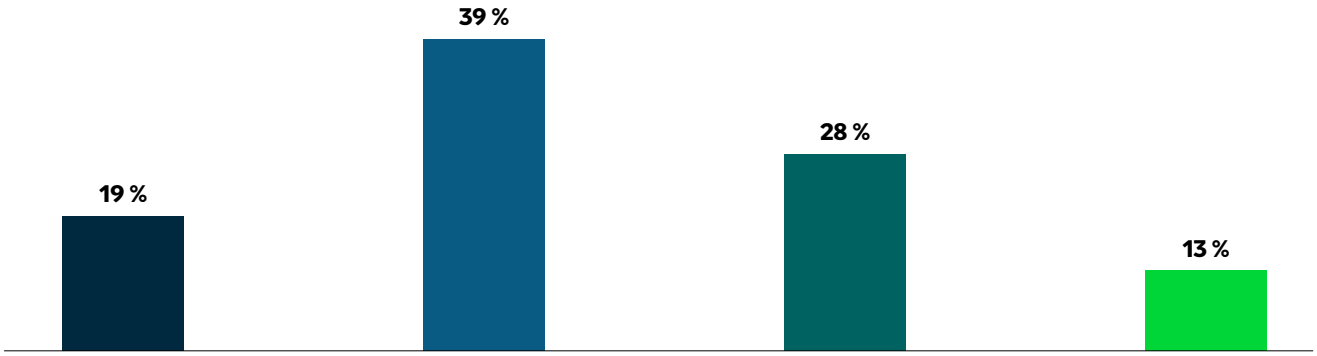
Les applications SaaS et les plateformes tierces sont désormais au cœur des activités de nombreuses PME, mais la surveillance de la sécurité reste souvent intermittente.

Pour de nombreuses entreprises, les risques liés aux fournisseurs sont examinés uniquement au début d'une relation ou lors du renouvellement d'un contrat, et ne font pas l'objet d'un suivi continu. Il en résulte une visibilité insuffisante, une plus grande exposition aux risques et la possibilité que des problèmes ne soient pas identifiés avant qu'une perturbation intervienne.

Les micro-entreprises et les petites entreprises sont particulièrement exposées, une grande partie d'entre elles affirmant ne pas effectuer de contrôle régulier des services tiers. Par conséquent, les problèmes potentiels peuvent passer inaperçus jusqu'à ce qu'une perturbation se produise.

Les PME plus matures adoptent des contrôles d'accès centralisés, une gestion plus claire du cycle de vie des utilisateurs et des examens plus réguliers des fournisseurs, ce qui améliore leur capacité à identifier les anomalies et à réagir plus rapidement. Une gestion de la sécurité liée aux tiers en tant que processus continu et non ponctuel devient indispensable à mesure que les écosystèmes SaaS se développent et que des outils basés sur l'IA sont introduits par l'entremise de fournisseurs externes.

Fréquence à laquelle les PME contrôlent la sécurité liée aux fournisseurs tiers de solutions SaaS ?



Pas de surveillance
Sécurité examinée uniquement au début

Contrôles périodiques
Examens effectués occasionnellement ou lorsque des problèmes surviennent

Examens réguliers
Réévaluations annuelles ou semestrielles

Surveillance continue
Outils automatisés ou contrôles réguliers intégrés dans les processus de sécurité

Pour les PME, l'amélioration de la sécurité des solutions SaaS vendues par des fournisseurs tiers commence par une meilleure discipline au quotidien : savoir quels outils sont utilisés, contrôler qui peut y accéder, supprimer rapidement les comptes inutilisés et surveiller les applications non autorisées ou les activités inhabituelles. Pour les petites équipes en particulier, une approche simple et cohérente soutenue par des fournisseurs de confiance ou des services gérés sera plus efficace que d'essayer d'élaborer par elles-mêmes un modèle de surveillance complexe.

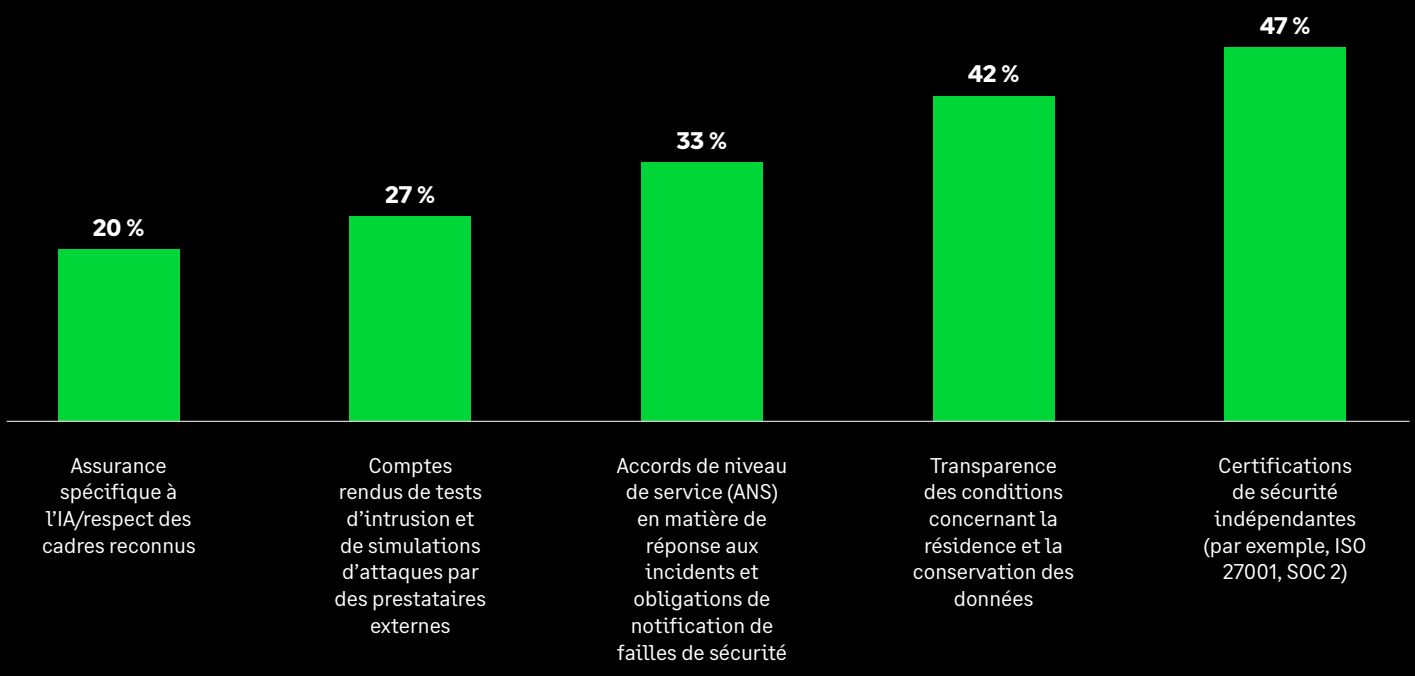
Pour évaluer des fournisseurs tiers, les PME se fient à des preuves concrètes et vérifiables

À mesure que les services SaaS basés sur l'IA s'intègrent davantage dans les opérations des PME, celles-ci ont besoin d'évaluer la fiabilité des fournisseurs en se basant sur des preuves claires, compréhensibles et faciles à vérifier.

Les PME accordent la plus grande importance aux certifications indépendantes, à la transparence du traitement des données et aux engagements clairs en matière de réponse aux incidents, car ces facteurs leur donnent l'assurance pratique que des mesures de sécurité fondamentales sont en place. Les arguments plus techniques spécifiques à l'IA peuvent sembler plus développés et pointus, mais il est souvent plus difficile pour les petites entreprises de les évaluer clairement.

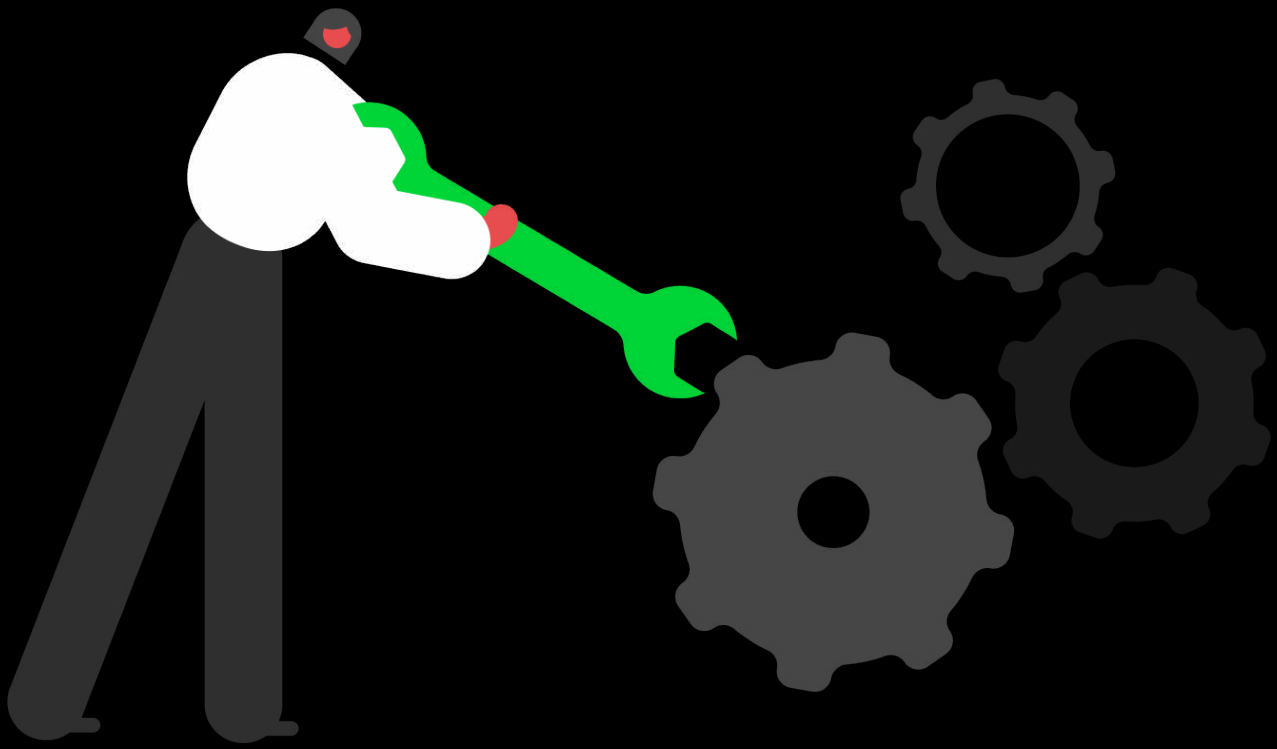
Les fournisseurs ont donc tout intérêt à faire preuve de clarté. Ceux qui sont capables d'expliquer, en termes simples, comment les données des clients sont protégées, où elles sont stockées et ce qui se passe en cas de problème auront plus de faciliter à convaincre leurs clients.

Preuves de confiance dans la sécurité des systèmes d'IA et les pratiques responsables des fournisseurs tiers



Les PME devraient privilégier les fournisseurs qui apportent des preuves claires et vérifiables de la manière dont ils gèrent la sécurité, et réévaluer régulièrement la sécurité.

Transformer les insights en action



Micro-entreprises : renforcer la résilience par des mesures simples et évolutives

À mesure de l'adoption de l'IA, il est essentiel de responsabiliser les acteurs, et de renforcer les cycles d'examen ainsi que la gouvernance de base. Les mesures à mettre en place doivent rester peu coûteuses et faciles à mettre en œuvre, en privilégiant la simplicité et une charge de gestion minimale.

Mesures à court terme

Posture en matière de cybersécurité
Assigner une responsabilité : désigner un responsable de la sécurité et établir une liste de contrôle simple pour la réponse aux incidents, couvrant l'escalade, les sauvegardes et l'assistance externe.

Sécurité de l'IA
Sécuriser l'accès aux systèmes d'IA : restreindre l'accès aux systèmes d'IA au personnel autorisé, permettre un enregistrement simple des activités et imposer des mots de passe robustes pour réduire les risques à mesure que l'utilisation de l'IA se développe.

Plans à moyen terme

Posture en matière de cybersécurité
Instaurer une discipline de routine : introduire un examen régulier de la sécurité couvrant les droits d'accès et les mises à jour des logiciels. Sauvegardes et outils tiers.

Sécurité de l'IA
Définir des règles et former le personnel : formaliser les règles de traitement des données et les protocoles d'accès, assurer la formation du personnel et jeter les bases d'une sécurité de l'IA évolutive.

Points à prendre en compte pour le long terme

Posture en matière de cybersécurité
Réduire la dépendance à l'égard des talents internes : consolider et normaliser les contrôles, en donnant la priorité aux services à faible coût, groupés ou gérés, afin de réduire les frais généraux opérationnels et financiers.

Sécurité de l'IA
Mettre en œuvre des pratiques de surveillance : mettre en place une surveillance continue de base et procéder à des contrôles élémentaires de la sécurité des systèmes d'IA chez les prestataires. Sélectionner des applications dignes de confiance qui s'engagent à mettre l'accent sur la sécurité.

Sage

Petites entreprises : renforcer la sécurité par la structure et la discipline

Les petites entreprises doivent structurer les processus de sécurité et la gouvernance de l'IA. À mesure de l'adoption de l'IA, la formalisation et l'application cohérente des pratiques de sécurité deviennent essentielles pour réduire les risques non gérés.

Mesures à court terme

Posture en matière de cybersécurité
Formaliser la visibilité des risques : rendre les rapports de sécurité réguliers, confirmer qui est responsable des décisions clés, et s'assurer que les incidents et les examens d'accès sont discutés au niveau de la direction.

Sécurité de l'IA
Visibilité des actifs d'IA : maintenir un inventaire à jour des modèles, agents, ensembles de données et services d'IA. Surveiller l'utilisation non autorisée ou fantôme des applications d'IA.

Plans à moyen terme

Posture en matière de cybersécurité
Professionnaliser les opérations de sécurité : appliquer les politiques de manière cohérente pour toutes les équipes, vérifier les risques liés aux tiers avant d'engager des fournisseurs, et rationaliser les outils existants pour réduire la complexité des opérations.

Sécurité de l'IA
Sécuriser les interactions avec l'IA : procéder à une validation des flux entrants et sortants pour prévenir les injections de commandes (prompt injection), les contournements de sécurité (jailbreaks) et les fuites de données.

Points à prendre en compte pour le long terme

Posture en matière de cybersécurité
Intégrer la sécurité dans les décisions stratégiques : intégrer la sécurité dans les décisions d'approvisionnement, les initiatives numériques et les plans de développement afin que la gestion des risques évolue en parallèle de la croissance de l'entreprise.

Sécurité de l'IA
Préparation aux incidents liés à l'IA : documenter et tester le plan de réponse aux incidents en cas de défaillance ou de violation de l'IA. Introduire une gestion structurée des risques liés aux fournisseurs.

Entreprises de taille moyenne : étendre la sécurité à l'ensemble de l'entreprise de manière cohérente

Les entreprises de taille moyenne disposent d'une sécurité bien structurée, avec des rôles dédiés, une gestion proactive et une surveillance formelle par des tiers. L'étape suivante consiste à s'assurer que ce dispositif évolue de manière cohérente à mesure que l'exposition au menaces numériques et à l'IA s'accroît.

Mesures à court terme

Posture en matière de cybersécurité
Renforcer les contrôles existants : mapper les actifs essentiels et les fournisseurs clés, examiner les droits d'accès au sein des équipes et identifier les outils de sécurité qui se chevauchent ou qui sont sous-utilisés.

Sécurité de l'IA
Gestion des risques liés à l'IA : formaliser un framework de sécurité de l'IA qui intègre la visibilité de l'IA et des données, la surveillance continue des anomalies du système et la gestion structurée des risques liés aux fournisseurs.

Plans à moyen terme

Posture en matière de cybersécurité
Normaliser les pratiques en matière de sécurité : appliquer les mêmes contrôles et règles dans tous les services, introduire des examens structurés des fournisseurs, communiquer régulièrement les indicateurs de risque clés à la direction.

Sécurité de l'IA
Conformité réglementaire : veiller à ce que l'utilisation de l'IA respecte les réglementations relatives à la protection de la vie privée et à l'IA. Inclure les spécificités de l'IA dans les cadres de contrôle de sécurité en vigueur.

Points à prendre en compte pour le long terme

Posture en matière de cybersécurité
Intégrer la sécurité dans la gouvernance de l'entreprise : intégrer la cybersécurité dans l'approvisionnement, la continuité des activités et la planification stratégique afin que la protection évolue au rythme de la croissance de l'entreprise.

Sécurité de l'IA
Tests de robustesse : tester la résilience des systèmes d'IA face aux attaques antagonistes ou aux simulations d'attaques de l'équipe rouge.

Sage

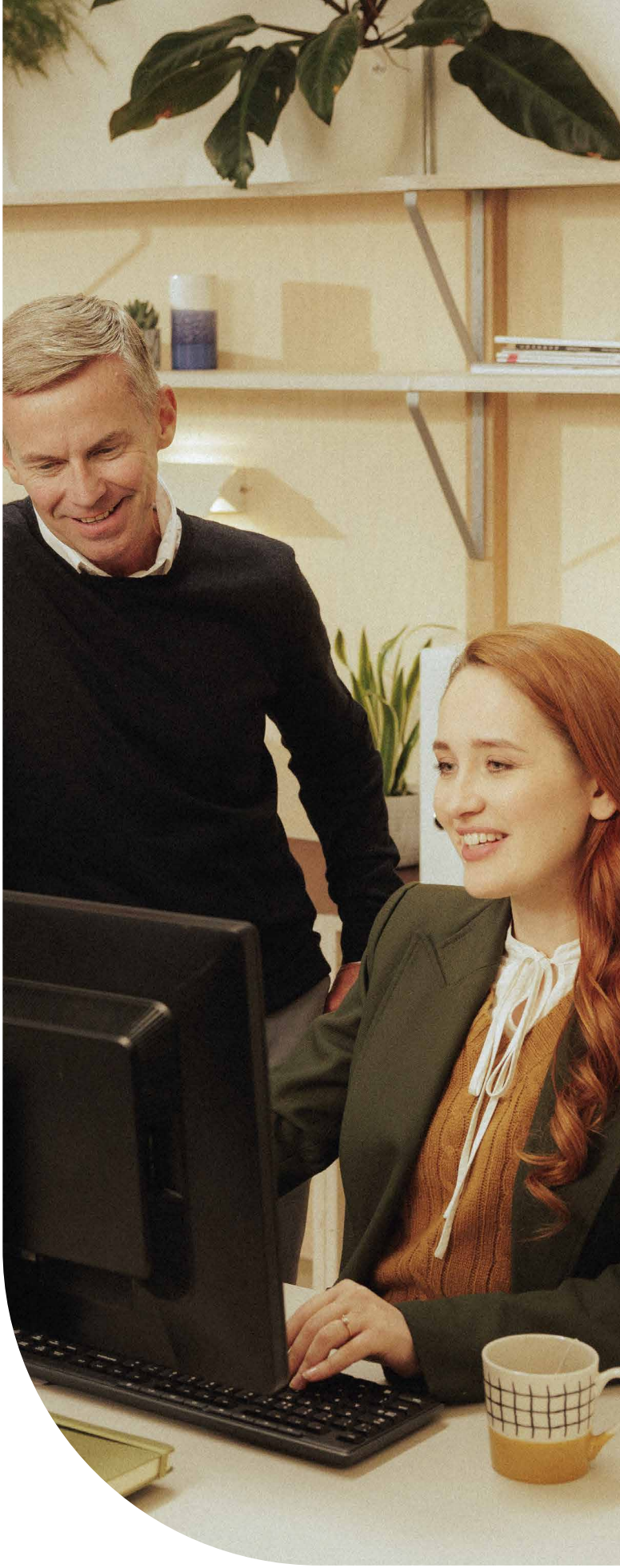
Message de Sage

Sage travaille depuis longtemps au service des petites et moyennes entreprises, et comprend les opportunités et les pressions auxquelles elles sont confrontées. Ce rapport montre que la cybersécurité est désormais au cœur des priorités des PME. Elle se situe juste après la croissance dans l'agenda des entreprises, ce qui montre à quel point la cyberrésilience est désormais étroitement liée à la confiance, à la continuité et à la réussite à long terme.

De nombreuses PME doivent composer avec des cyberrisques croissants, mais disposent de peu de temps, de ressources de personnel et de moyens financiers, alors que l'IA et les technologies tierces s'intègrent de plus en plus dans les activités quotidiennes. Elles ne devraient pas avoir à gérer cela seules.

Chez Sage, nous nous attachons à aider les PME à mettre en pratique une bonne sécurité grâce à des conseils clairs, des principes de sécurité pris en compte dès la conception et une transparence sur la façon dont les données sont protégées et dont l'IA est utilisée. L'objectif est de permettre aux PME d'atténuer les risques tout en utilisant la technologie pour alimenter la croissance.

Les gouvernements, les organisations sectorielles, les éditeurs de logiciels et les fournisseurs devraient collaborer étroitement pour donner aux PME des orientations plus claires, des mesures de protection plus simples à mettre en œuvre, ainsi qu'un soutien pratique adapté aux réalités auxquelles elles sont confrontées chaque jour.



Sage

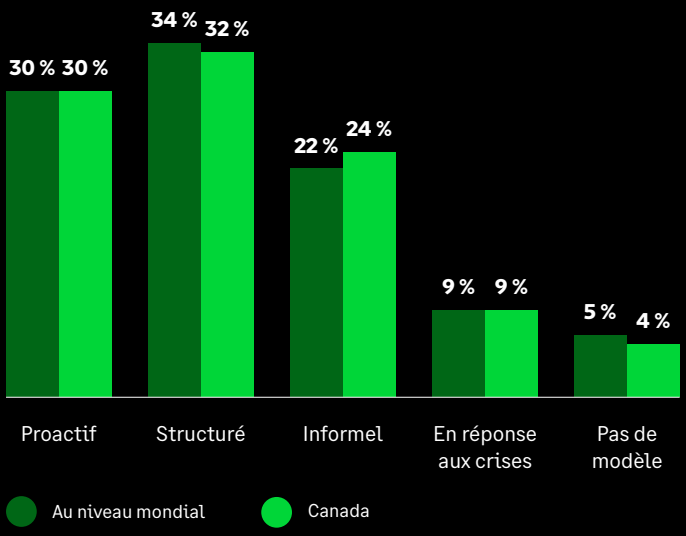
Annexe : Perspectives par pays

Canada

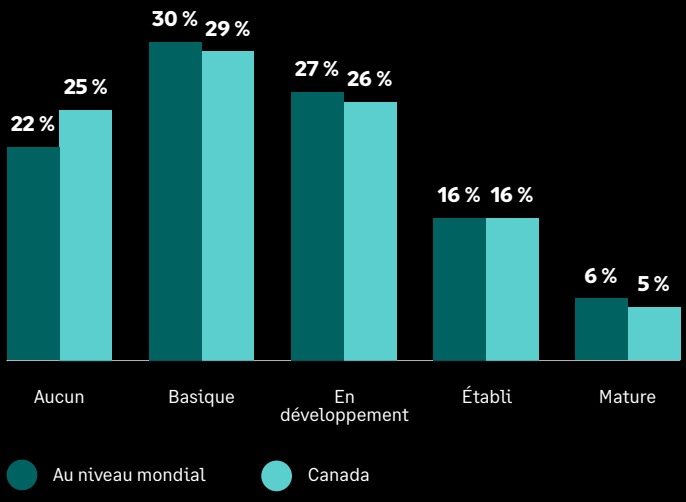
Le Canada est en avance sur la moyenne mondiale en ce qui concerne les mesures de sécurité de base, ce qui lui donne une base solide pour la protection quotidienne et contribue à maintenir les niveaux d'incidents proches de la moyenne mondiale.

Le pays est toutefois en retard dans sa préparation à l'IA. Il semble moins bien préparé à transformer cette base solide en une sécurité efficace, avec une adoption plus faible des mesures de protection pratiques, une préparation à la conformité plus faible et un manque d'expertise plus prononcé dans le domaine de la sécurité liée à l'IA. L'accent doit désormais être mis sur le renforcement des compétences, la surveillance et la mise en place de garde-fous pour gérer plus efficacement les risques liés à l'IA.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

Canada	55 % Aucun incident	33 % Incidents mineurs rapidement résolus	10 % Incidents entraînant des perturbations importantes
Au niveau mondial	54 % Aucun incident	34 % Incidents mineurs rapidement résolus	11 % Incidents entraînant des perturbations importantes

Des mesures de sécurité de haut niveau sont en place

Canada	86 % Protection des e-mails	82 % Maintenance (mises à jour, correctifs et sauvegardes)	77 % MFA/SSO
Au niveau mondial	79 % Protection des e-mails	71 % Maintenance (mises à jour, correctifs et sauvegardes)	67 % Protection des terminaux

Principaux défis liés à la sécurisation des applications d'IA

Canada	48 % Expertise insuffisante en matière de sécurité liée à l'IA	38 % Mettre en place une sécurité des données forte	41 % Suivre le rythme des nouvelles menaces liées à l'IA
Au niveau mondial	45 % Expertise insuffisante en matière de sécurité liée à l'IA	41 % Mettre en place une sécurité des données forte	36 % Suivre le rythme des nouvelles menaces liées à l'IA

Principales mesures de protection contre les risques et les menaces liés à l'IA

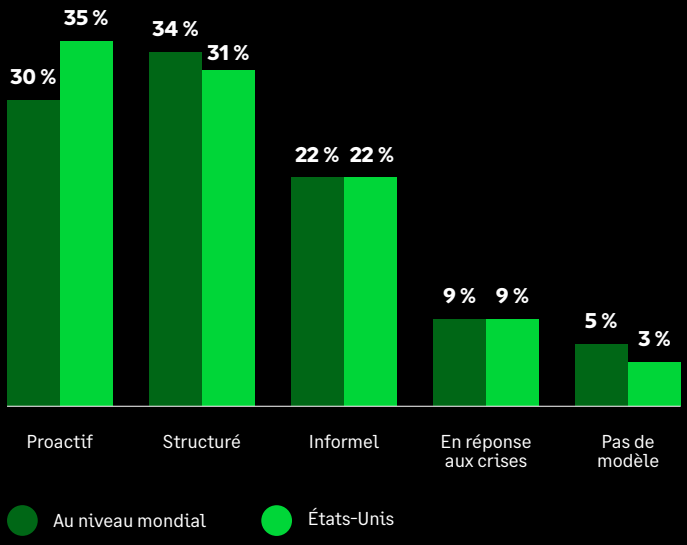
Canada	35 % Politique claire en matière d'utilisation de l'IA	34 % Outils d'IA approuvés avec contrôles administratifs	32 % Tester les outils d'IA avant leur déploiement
Au niveau mondial	41 % Politique claire en matière d'utilisation de l'IA	38 % Outils d'IA approuvés avec contrôles administratifs	33 % Tester les outils d'IA avant leur déploiement

États-Unis

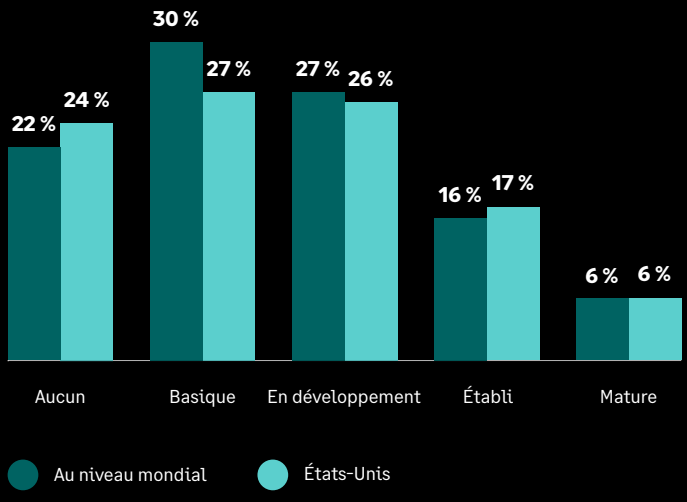
Les États-Unis sont en avance sur la moyenne mondiale pour ce qui est de passer de la sensibilisation à la cybersécurité à une pratique quotidienne plus structurée. Ils disposent ainsi d'une base plus solide comparativement à d'autres pays, à l'heure où l'IA s'intègre de plus en plus dans les activités des entreprises.

La part plus élevée d'incidents plus graves suggère que la résilience doit être renforcée dans la pratique, en particulier en ce qui concerne la sécurité des données, la surveillance et la capacité à répondre à l'évolution plus rapide des menaces.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

	Aucun incident	Incidents mineurs rapidement résolus	Incidents entraînant des perturbations importantes
États-Unis	55 %	32 %	13 %
Au niveau mondial	54 %	34 %	11 %

Des mesures de sécurité de haut niveau sont en place

	Protection des e-mails	Maintenance (mises à jour, correctifs et sauvegardes)	Protection des terminaux
États-Unis	85 %	71 %	69 %
Au niveau mondial	79 %	71 %	67 %

Principaux défis liés à la sécurisation des applications d'IA

	Expertise insuffisante en matière de sécurité liée à l'IA	Mettre en place une sécurité des données forte	Suivre le rythme des nouvelles menaces liées à l'IA
États-Unis	43 %	38 %	38 %
Au niveau mondial	45 %	41 %	36 %

Principales mesures de protection contre les risques et les menaces liés à l'IA

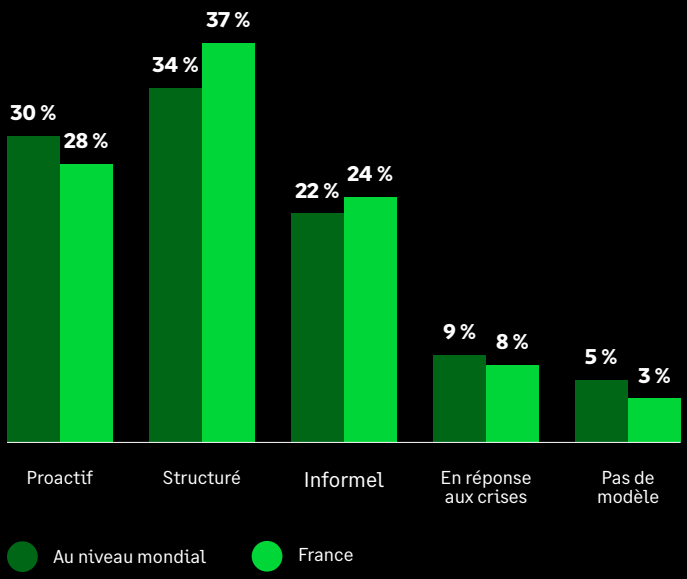
	Politique claire en matière d'utilisation de l'IA	Outils d'IA approuvés avec contrôles administratifs	Tester les outils d'IA avant leur déploiement
États-Unis	40 %	39 %	34 %
Au niveau mondial	41 %	38 %	33 %

France

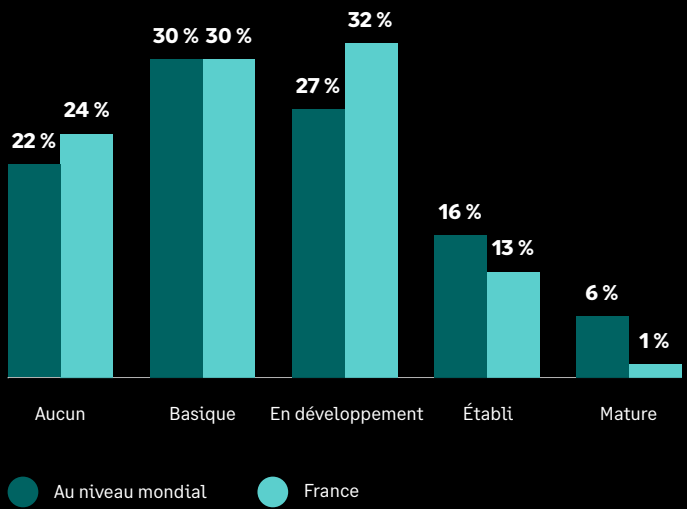
La France subit une pression accrue en matière de cybersécurité, dépassant la moyenne mondiale. On observe une adoption plus restreinte des mesures de sécurité essentielles, un taux plus important de perturbations significatives et une maturité limitée en matière de sécurité de l'IA, seule une minorité d'entreprises atteignant les niveaux de préparation les plus avancés. Cela témoigne d'une certaine disparité en ce qui concerne les bases de la sécurité, et des répercussions plus importantes que la moyenne des menaces de sécurité.

La prochaine étape doit consister à renforcer à la fois les bases et la capacité à gérer les risques liés à l'IA dans la pratique. Une meilleure visibilité, une protection renforcée des données et une préparation à une réponse plus structurée seront essentielles, en particulier sur un marché où la confiance semble dépendre fortement de la capacité des entreprises à réagir en cas de problème.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

France	**51 %** Aucun incident	**33 %** Incidents mineurs rapidement résolus	**15 %** Incidents entraînant des perturbations importantes
Au niveau mondial	**54 %** Aucun incident	**34 %** Incidents mineurs rapidement résolus	**11 %** Incidents entraînant des perturbations importantes

Des mesures de sécurité de haut niveau sont en place

France	**77 %** Protection des e-mails	**60 %** Maintenance (mises à jour, correctifs et sauvegardes)	**69 %** Protection des terminaux
Au niveau mondial	**79 %** Protection des e-mails	**71 %** Maintenance (mises à jour, correctifs et sauvegardes)	**67 %** Protection des terminaux

Principaux défis liés à la sécurisation des applications d'IA

France	**48 %** Expertise insuffisante en matière de sécurité liée à l'IA	**43 %** Mettre en place une sécurité des données forte	**35 %** Visibilité limitée sur les outils d'IA utilisés
Au niveau mondial	**45 %** Expertise insuffisante en matière de sécurité liée à l'IA	**41 %** Mettre en place une sécurité des données forte	**36 %** Suivre le rythme des nouvelles menaces liées à l'IA

Principales mesures de protection contre les risques et les menaces liés à l'IA

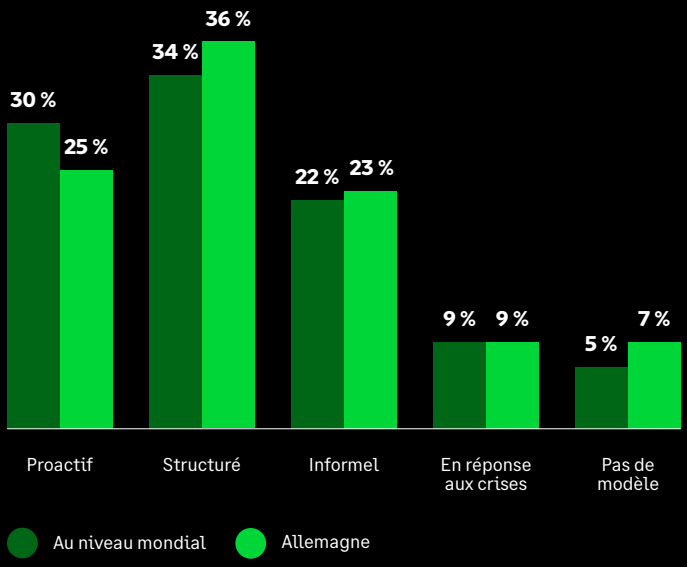
France	**42 %** Politique claire en matière d'utilisation de l'IA	**38 %** Outils d'IA approuvés avec contrôles administratifs	**34 %** Tester les outils d'IA avant leur déploiement
Au niveau mondial	**41 %** Politique claire en matière d'utilisation de l'IA	**38 %** Outils d'IA approuvés avec contrôles administratifs	**33 %** Tester les outils d'IA avant leur déploiement

Allemagne

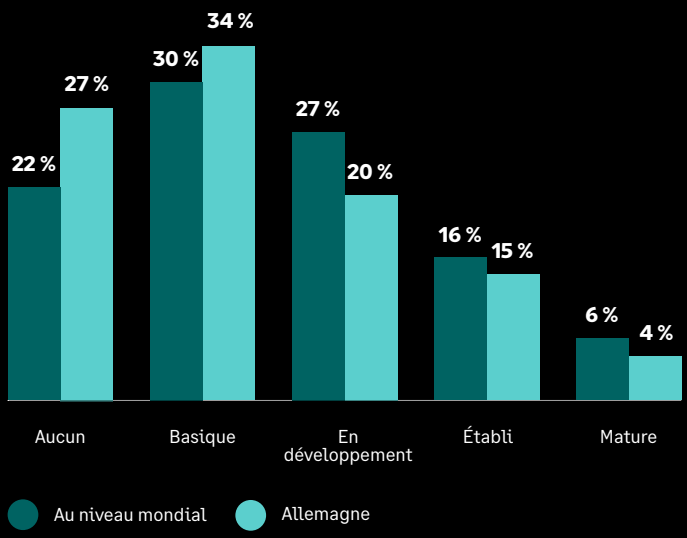
L'Allemagne présente un profil plus prudent et davantage axé sur la conformité que la moyenne mondiale. L'adoption des mesures de base est moins généralisée, la gestion proactive est moins répandue et le niveau de maturité pour la sécurité liée à l'IA reste plus faible, un plus grand nombre d'entreprises se situant aux premiers stades. Les niveaux d'incidents sont proches des normes mondiales, de sorte que la pression est moins visible aujourd'hui, mais les fondements de la gestion des risques liés à l'IA sont encore sous-développés.

La priorité de l'Allemagne est de passer de la prudence à la préparation pratique. Les fortes inquiétudes concernant l'utilisation des données et la visibilité limitée sur les outils d'IA mettent en évidence un marché axé sur le contrôle et la conformité. La prochaine étape consistera à renforcer les garanties pratiques, à améliorer la visibilité sur l'utilisation de l'IA et à veiller à ce que la prudence se traduise par une plus grande résilience au fur et à mesure de l'adoption de l'IA.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

	Aucun incident	Incidents mineurs rapidement résolus	Incidents entraînant des perturbations importantes
Allemagne	54 %	36 %	10 %
Au niveau mondial	54 %	34 %	11 %

Des mesures de sécurité de haut niveau sont en place

Allemagne	77 % Protection des e-mails	68 % Maintenance (mises à jour, correctifs et sauvegardes)	61 % MFA/SSO
Au niveau mondial	79 % Protection des e-mails	71 % Maintenance (mises à jour, correctifs et sauvegardes)	67 % Protection des terminaux

Principaux défis liés à la sécurisation des applications d'IA

Allemagne	43 % Expertise insuffisante en matière de sécurité liée à l'IA	39 % Mettre en place une sécurité des données forte	37 % Visibilité limitée sur les outils d'IA utilisés
Au niveau mondial	45 % Expertise insuffisante en matière de sécurité liée à l'IA	41 % Mettre en place une sécurité des données forte	36 % Suivre le rythme des nouvelles menaces liées à l'IA

Principales mesures de protection contre les risques et les menaces liés à l'IA

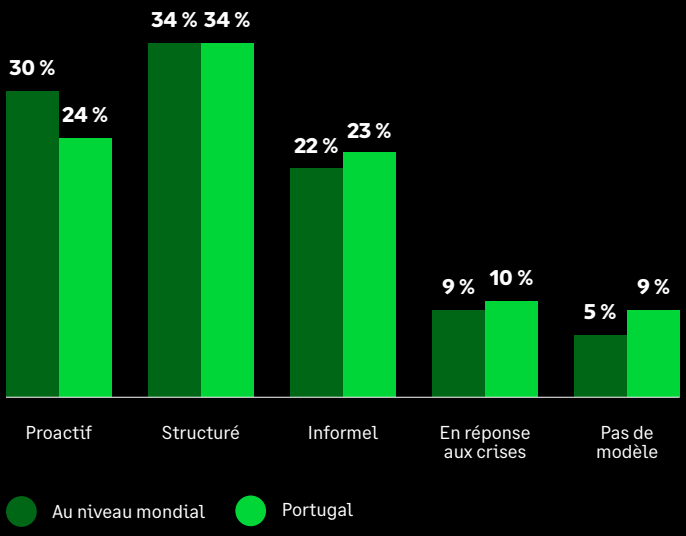
Allemagne	42 % Politique claire en matière d'utilisation de l'IA	32 % Outils d'IA approuvés avec contrôles administratifs	26 % Contrôles de la protection des données sensibles
Au niveau mondial	41 % Politique claire en matière d'utilisation de l'IA	38 % Outils d'IA approuvés avec contrôles administratifs	33 % Tester les outils d'IA avant leur déploiement

Portugal

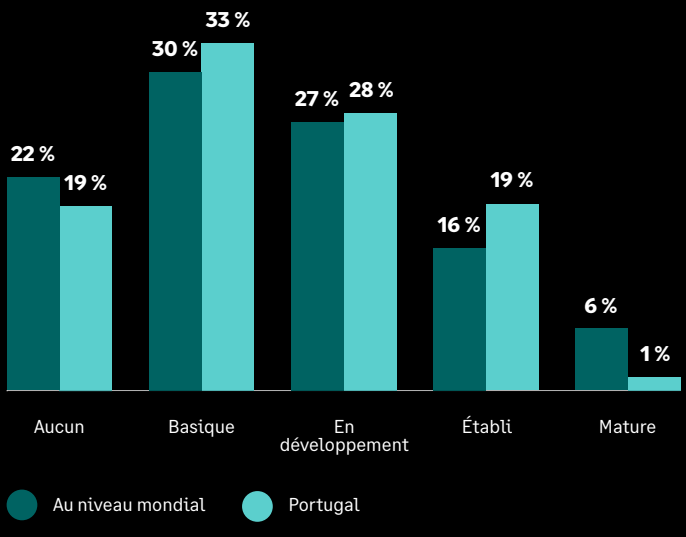
Le Portugal présente un profil de sécurité moins mature que la moyenne mondiale. Les mesures de sécurité de base sont moins largement adoptées, les niveaux d'incidents sont plus élevés et les perturbations importantes sont plus fréquentes. En ce qui concerne la sécurité liée à l'IA, les niveaux de maturité sont inégaux, un plus grand nombre d'entreprises se situant au tout premier stade et très peu atteignant un bon niveau de maturité.

Pour le Portugal, le défi réside dans l'exécution. La priorité est désormais de renforcer les bases, de réduire l'incertitude autour du traitement des données liées à l'IA et de mettre en place des pratiques de sécurité quotidiennes plus cohérentes afin que les risques soient gérés avec moins de perturbations. La confiance accrue dans les certifications indépendantes montre également que ce marché est à la recherche de preuves claires pour accorder sa confiance à des parties externes au fur et à mesure de l'adoption de l'IA.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

	Aucun incident	Incidents mineurs rapidement résolus	Incidents entraînant des perturbations importantes
Portugal	43 %	39 %	16 %
Au niveau mondial	54 %	34 %	11 %

Des mesures de sécurité de haut niveau sont en place

	Protection des e-mails	Maintenance (mises à jour, correctifs et sauvegardes)	Protection des terminaux
Portugal	65 %	65 %	61 %
Au niveau mondial	79 %	71 %	67 %

Principaux défis liés à la sécurisation des applications d'IA

Portugal	44 % Expertise insuffisante en matière de sécurité liée à l'IA	40 % Mettre en place une sécurité des données forte	34 % Visibilité limitée sur les outils d'IA utilisés
Au niveau mondial	45 % Expertise insuffisante en matière de sécurité liée à l'IA	41 % Mettre en place une sécurité des données forte	36 % Suivre le rythme des nouvelles menaces liées à l'IA

Principales mesures de protection contre les risques et les menaces liés à l'IA

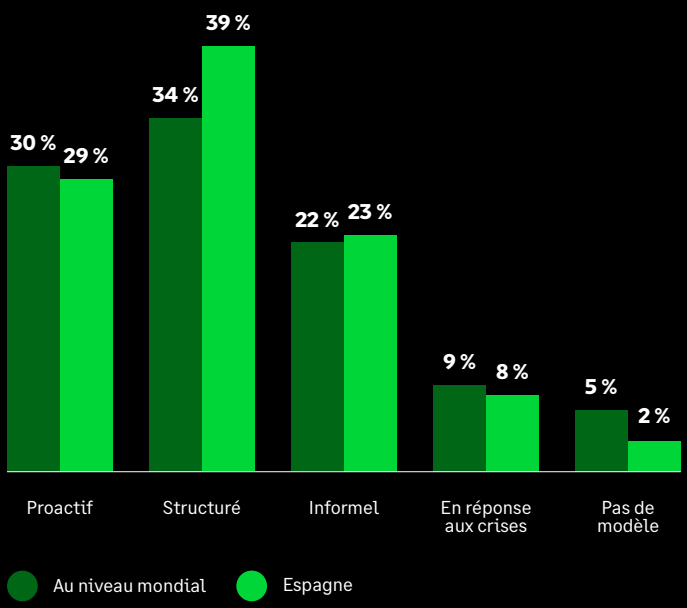
Portugal	43 % Politique claire en matière d'utilisation de l'IA	34 % Outils d'IA approuvés avec contrôles administratifs	33 % Tester les outils d'IA avant leur déploiement
Au niveau mondial	41 % Politique claire en matière d'utilisation de l'IA	38 % Outils d'IA approuvés avec contrôles administratifs	33 % Tester les outils d'IA avant leur déploiement

Espagne

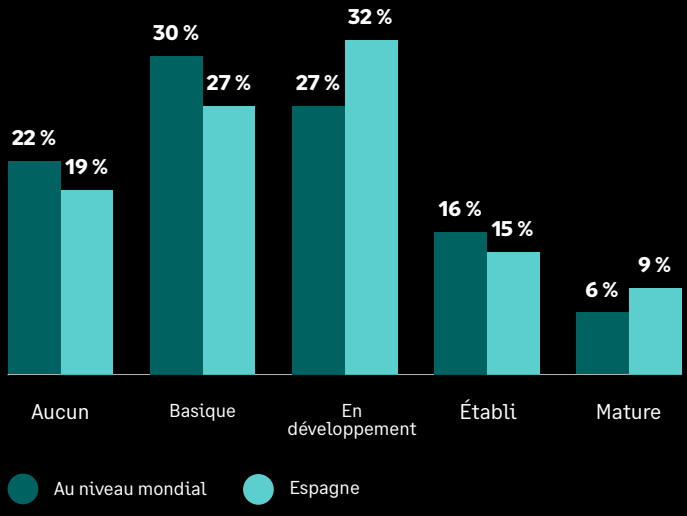
L'Espagne présente un profil de sécurité plus mature que la moyenne mondiale. Les niveaux d'incidents sont plus bas, la gestion structurée de la sécurité est plus répandue et la maturité de la sécurité liée l'IA se situe à un stade plus avancé, avec un plus grand nombre d'entreprises ayant dépassé les premiers stades pour atteindre un bon niveau de maturité.

Pour l'Espagne, le défi consiste à conserver cette posture au fur et à mesure de l'adoption de l'IA. La priorité est désormais de renforcer la protection contre les risques liés au facteur humain, d'améliorer la visibilité sur l'utilisation de l'IA et de combler les lacunes dans la surveillance continue des tiers, afin que les bases solides mises en place ne soient pas compromises par des angles morts face à des menaces en mutation.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

Espagne	60 % Aucun incident	29 % Incidents mineurs rapidement résolus	10 % Incidents entraînant des perturbations importantes
Au niveau mondial	54 % Aucun incident	34 % Incidents mineurs rapidement résolus	11 % Incidents entraînant des perturbations importantes

Des mesures de sécurité de haut niveau sont en place

Espagne	75 % Protection des e-mails	72 % Maintenance (mises à jour, correctifs et sauvegardes)	62 % Protection des terminaux
Au niveau mondial	79 % Protection des e-mails	71 % Maintenance (mises à jour, correctifs et sauvegardes)	67 % Protection des terminaux

Principaux défis liés à la sécurisation des applications d'IA

Espagne	42 % Expertise insuffisante en matière de sécurité liée à l'IA	36 % Mettre en place une sécurité des données forte	34 % Visibilité limitée sur les outils d'IA utilisés
Au niveau mondial	45 % Expertise insuffisante en matière de sécurité liée à l'IA	41 % Mettre en place une sécurité des données forte	36 % Suivre le rythme des nouvelles menaces liées à l'IA

Principales mesures de protection contre les risques et les menaces liés à l'IA

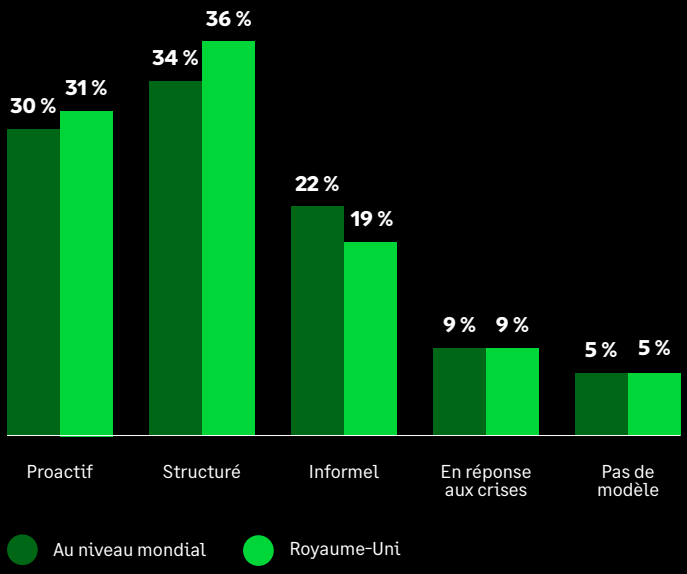
Espagne	43 % Politique claire en matière d'utilisation de l'IA	38 % Outils d'IA approuvés avec contrôles administratifs	32 % Tester les outils d'IA avant leur déploiement
Au niveau mondial	41 % Politique claire en matière d'utilisation de l'IA	38 % Outils d'IA approuvés avec contrôles administratifs	33 % Tester les outils d'IA avant leur déploiement

Royaume-Uni

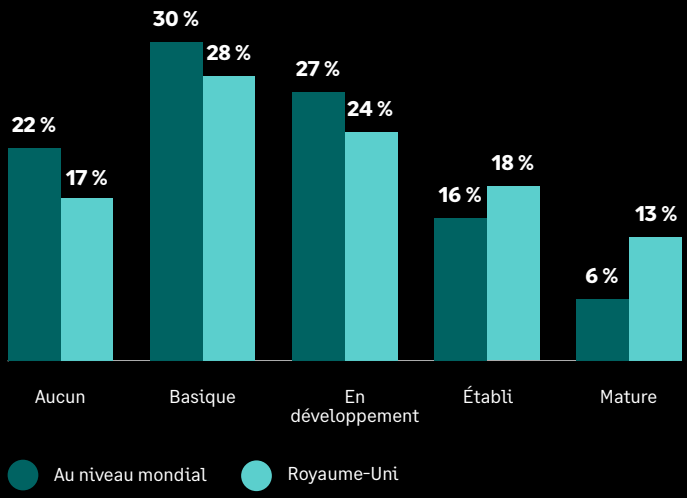
Le Royaume-Uni se distingue par des progrès plus importants et plus rapides que la moyenne mondiale en matière de sécurité liée à l'IA. Les entreprises sont plus avancées dans la mise en place de mesures de protection pratiques, plus susceptibles d'utiliser des outils approuvés et des politiques formelles, et plus avancées dans la construction d'une posture de sécurité de l'IA mature. Cela indique un marché qui n'attend pas de réagir, mais adopte une approche plus volontaire pour se préparer aux risques liés à l'IA au fur et à mesure de son adoption.

La priorité est désormais de renforcer le contrôle à mesure que l'utilisation de l'IA se développe, en particulier en ce qui concerne la protection des données, les menaces qui évoluent rapidement et la capacité à faire en sorte qu'une posture solide en matière de sécurité liée à l'IA puisse se traduire en pratique par de la résilience. Le taux légèrement supérieur de perturbations graves prouve que les efforts de préparation doivent encore se traduire par une réponse opérationnelle efficace lors des incidents.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

	Aucun incident	Incidents mineurs rapidement résolus	Incidents entraînant des perturbations importantes
Royaume-Uni	55 %	32 %	13 %
Au niveau mondial	54 %	34 %	11 %

Des mesures de sécurité de haut niveau sont en place

	Protection des e-mails	Maintenance (mises à jour, correctifs et sauvegardes)	Protection des terminaux
Royaume-Uni	75 %	79 %	67 %
Au niveau mondial	79 %	71 %	67 %

Principaux défis liés à la sécurisation des applications d'IA

	Expertise insuffisante en matière de sécurité liée à l'IA	Mettre en place une sécurité des données forte	Suivre le rythme des nouvelles menaces liées à l'IA
Royaume-Uni	44 %	46 %	37 %
Au niveau mondial	45 %	41 %	36 %

Principales mesures de protection contre les risques et les menaces liés à l'IA

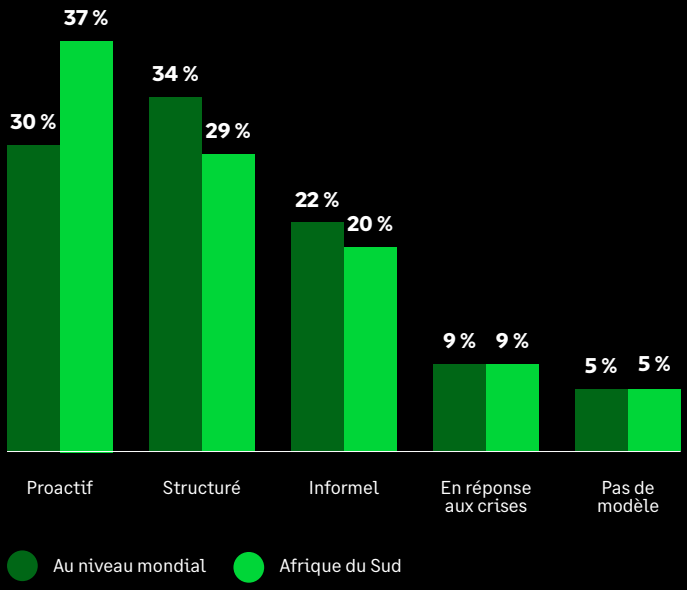
	Politique claire en matière d'utilisation de l'IA	Outils d'IA approuvés avec contrôles administratifs	Tester les outils d'IA avant leur déploiement
Royaume-Uni	43 %	45 %	38 %
Au niveau mondial	41 %	38 %	33 %

Afrique du Sud

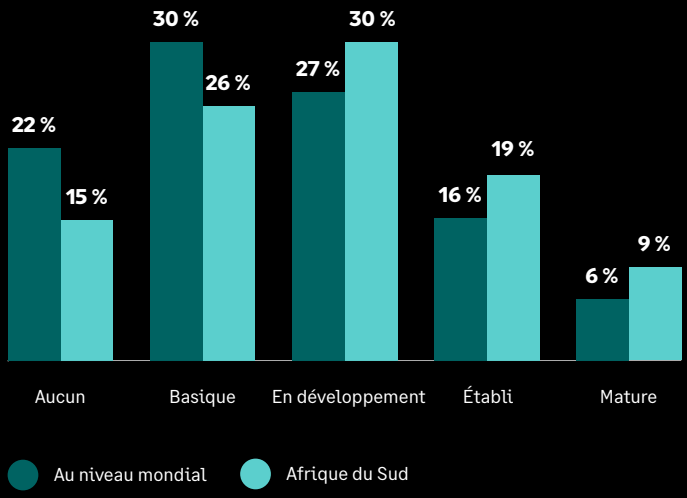
L'Afrique du Sud est en avance sur la moyenne mondiale en ce qui concerne la sécurité liée à l'IA. Les entreprises sont plus susceptibles de remettre en question leur approche de l'IA, plus évoluées dans leur posture de sécurité pour les applications utilisant l'IA, et plus performantes lorsqu'il s'agit d'assurer une surveillance continue des tiers. Cela indique que le marché estime que la sécurité liée à l'IA est un sujet prioritaire et met en place des mesures de protection plus concrètes au fur et à mesure de l'adoption de l'IA.

Le défi consiste à rationaliser toutes ces avancées. L'adoption des mesures de sécurité fondamentales reste inégale, et les inquiétudes concernant la protection des données et les menaces en mutation rapide restent vives. La priorité est désormais de combler ces lacunes afin qu'une posture renforcée en matière d'IA s'accompagne de pratiques de sécurité quotidiennes plus résilientes.

Modèle de gestion de la cybersécurité



Niveau actuel de sécurité des applications tirant parti de l'IA



Cyberincidents ou violations intervenus au cours de l'année écoulée

Afrique du Sud	55 % Aucun incident	35 % Incidents mineurs rapidement résolus	9 % Incidents entraînant des perturbations importantes
Au niveau mondial	54 % Aucun incident	34 % Incidents mineurs rapidement résolus	11 % Incidents entraînant des perturbations importantes

Des mesures de sécurité de haut niveau sont en place

Afrique du Sud	75 % Protection des e-mails	74 % Maintenance (mises à jour, correctifs et sauvegardes)	70 % Protection des terminaux
Au niveau mondial	79 % Protection des e-mails	71 % Maintenance (mises à jour, correctifs et sauvegardes)	67 % Protection des terminaux

Principaux défis liés à la sécurisation des applications d'IA

Afrique du Sud	45 % Expertise insuffisante en matière de sécurité liée à l'IA	44 % Mettre en place une sécurité des données forte	37 % Suivre le rythme des nouvelles menaces liées à l'IA
Au niveau mondial	45 % Expertise insuffisante en matière de sécurité liée à l'IA	41 % Mettre en place une sécurité des données forte	36 % Suivre le rythme des nouvelles menaces liées à l'IA

Principales mesures de protection contre les risques et les menaces liés à l'IA

Afrique du Sud	45 % Politique claire en matière d'utilisation de l'IA	39 % Outils d'IA approuvés avec contrôles administratifs	36 % Contrôles de la protection des données sensibles
Au niveau mondial	41 % Politique claire en matière d'utilisation de l'IA	38 % Outils d'IA approuvés avec contrôles administratifs	33 % Tester les outils d'IA avant leur déploiement

sage.com