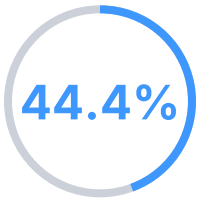
jamf

ENQUÊTE DE JAMF SUR LA GOUVERNANCE DE L'IA :

les révélations de 687 responsables informatiques et de la sécurité sur la gouvernance de l'IA

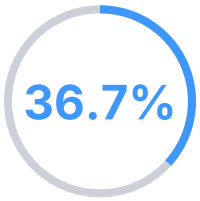
Résumé des conclusions

687 responsables informatiques et de la sécurité au sein d'entreprises utilisant des produits Apple nous ont donné un aperçu de l'ampleur, des objectifs et de la sécurité de leur déploiement de l'IA. Voici ce que nous avons découvert.



Automatisation

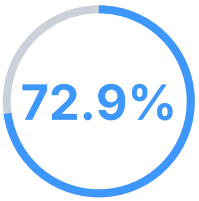
Déploiement



Gouvernance

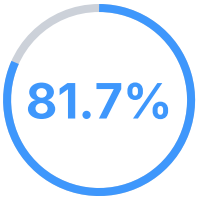
Trois grandes priorités en matière d'IA émergent

Les personnes interrogées ont cité l'automatisation des opérations informatiques (44,4 %), le déploiement d'outils de productivité basés sur l'IA (41,0 %) et la mise en place d'une gouvernance de l'IA (36,7 %) **comme leurs principales priorités dans ce domaine**.



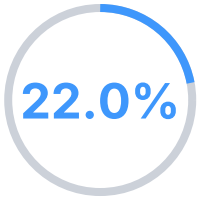
des organisations ont déployé l'IA

Près des trois quarts des entreprises ont déployé l'IA sous une forme ou une autre. Le stade de l'adoption est dépassé. La gouvernance est incontournable.



des organisations sont exposées à des risques liés à l'IA

22,0 % ont déjà été victimes d'un incident lié au coût de l'IA ou à la sécurité. Elles sont 59,7 % de plus à y voir un risque à court terme. Quand ils ne sont pas déjà une réalité, les risques liés à l'IA sont activement anticipés.



des organisations ont connu un incident lié au coût de l'IA ou à la sécurité

Plus d'une entreprise sur cinq a déjà été confrontée à un incident lié au coût de l'IA, à la sécurité ou aux deux. Les répercussions se font sentir à la fois sur le budget et sur l'équipe de sécurité.

d'augmentation du taux d'incidents

Parmi les organisations qui ont largement intégré l'IA, 27,1 % ont connu un incident lié à l'IA, contre 19,4 % de celles qui en sont encore au stade de l'exploration. L'exposition augmente mécaniquement avec l'adoption.

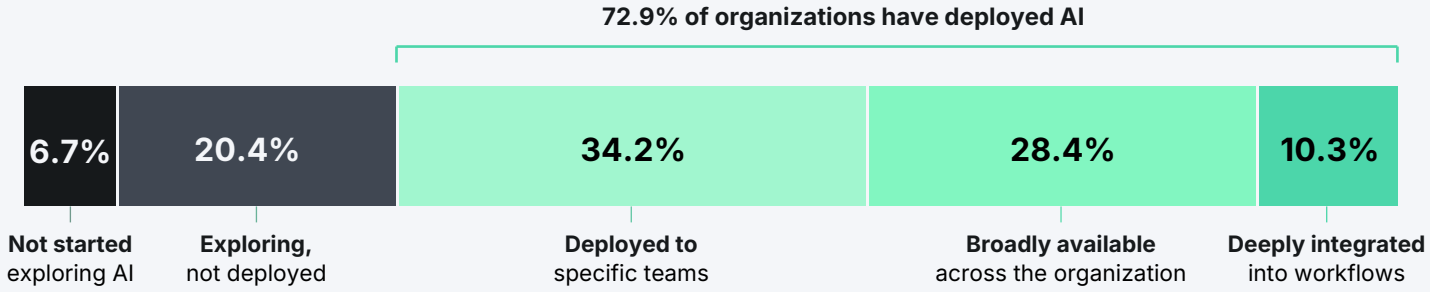
Plus vous utilisez l'IA, plus le risque augmente.

La plupart des entreprises encouragent l'adoption de l'IA, mais les risques augmentent mécaniquement. L'IA de l'ombre, les fonctionnalités discrètement intégrées aux logiciels, les assistants sur mobile et les outils agentiques sont autant d'angles morts difficiles à contrôler et plus difficiles encore à auditer. Plus l'IA s'ancre dans les usages, plus l'exposition augmente. La question n'est plus de savoir si un incident va se produire, mais quand.

GRAPHIQUE 1

Les entreprises Apple et l'adoption de l'IA

Point clé : près des trois quarts des entreprises utilisant les produits Apple ont déployé l'IA sous une forme ou une autre, qu'il s'agisse de projets pilotes au niveau d'une équipe ou d'une intégration poussée dans les workflows quotidiens. La question de l'adoption n'est plus d'actualité.



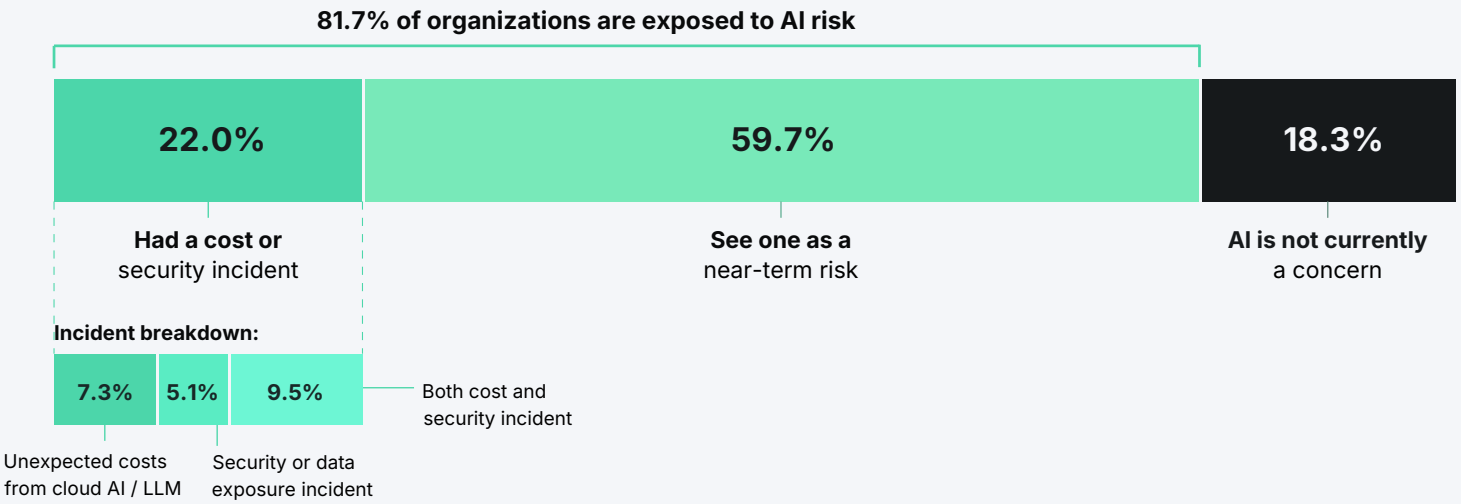
Note : n = 687 responsables informatiques et de la sécurité. 2e trimestre 2026.

Même si près de trois organisations sur quatre ont adopté l'IA, son déploiement à grande échelle ne réduit pas les risques. Au contraire, il ne fait qu'aggraver la situation. 22,0 % des entreprises ont déjà été confrontées à un incident : 7,3 % ont subi des coûts imprévus liés à l'utilisation de l'IA ou de grands modèles de langage (LLM) dans le cloud, 5,1 % à la suite d'un incident de sécurité ou d'une fuite de données, et 9,5 % pour les deux raisons combinées. Parmi celles qui sont encore indemnes, 59,7 % s'attendent tout de même à faire face à un tel incident.

GRAPHIQUE 2

Incidents et préoccupations liés à l'IA au cours des 12 derniers mois

Point clé : 22,0 % des entreprises ont déjà été confrontées à un incident lié à l'IA. Elles sont 59,7 % de plus à en anticiper un. 18,3 % seulement des personnes interrogées affirment que l'IA ne représente pas une source de préoccupation actuellement.



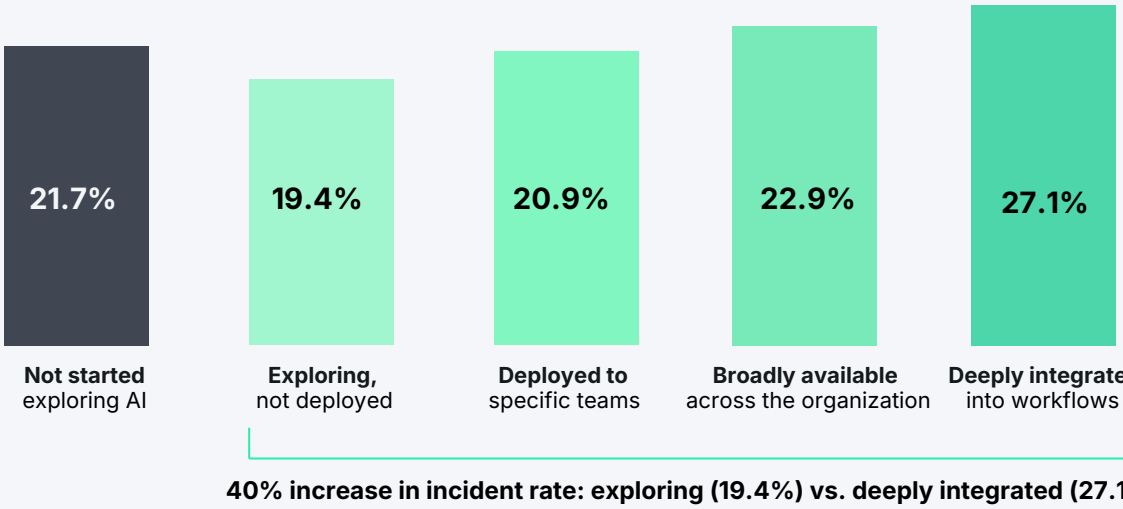
Note : *n = 681. Cette tendance se confirme indépendamment dans les deux échantillons de l'enquête.*

Cependant, les données révèlent un phénomène contre-intuitif : ce sont les organisations les plus avancées en matière d'IA qui enregistrent le plus grand nombre d'incidents.

GRAPHIQUE 3

Taux d'incidents en fonction du niveau d'adoption de l'IA

Point clé : les entreprises Apple qui ont déployé l'IA à un niveau poussé signalent un nombre d'incidents plus élevé. Parmi les entreprises qui l'utilisent le plus, 27,1 % ont déjà été confrontées à un incident, contre 19,4 % de celles qui en sont encore au stade de l'exploration.



Note : n = 683 responsables informatiques et de la sécurité. 2e trimestre 2026.

Dès que les équipes commencent à explorer l'utilisation de l'IA au sein de leur organisation, le risque d'incident augmente. Chez les organisations qui ont largement intégré l'IA, les incidents sont 40 % plus fréquents que chez celles qui en sont encore au stade de l'exploration (27,1 % contre 19,4 %).

⚠ Les défis de l'IA s'articulent autour de thèmes communs

Les réponses libres des personnes interrogées évoquant la prévention des incidents s'articulaient autour de quatre thèmes.

IA de l'ombre

Avec les promesses de gain de productivité, l'essor des outils d'IA et les incitations à l'intégration de l'IA dans l'entreprise, les employés ont de plus en plus souvent recours à l'IA. Ces pratiques échappent souvent au regard du service informatique ; les employés créent des comptes personnels et peuvent y saisir des données sensibles. Le service informatique ne sait pas quels systèmes d'IA sont utilisés dans l'entreprise, et ne peut donc ni contrôler ni bloquer les plateformes d'IA. Le manque de visibilité complique encore la sécurité et la gouvernance, quand elles ne deviennent pas simplement impossibles.

Prolifération des fournisseurs

Outre l'essor des nouveaux logiciels d'IA, de nombreuses applications intègrent désormais l'intelligence artificielle à leurs produits existants. L'évaluation et le déploiement de chaque outil d'IA demandent beaucoup de temps et d'efforts aux équipes informatiques, surtout quand on pense à la rapidité avec laquelle évolue cette technologie. Les personnes interrogées indiquent qu'elles ont du mal à savoir quelles plateformes d'IA seraient les plus utiles à leurs employés et à les inciter à utiliser les outils d'IA approuvés. La multiplication des points d'entrée rend l'IA difficile à sécuriser.

IA agentique et outils pour développeurs

Les défis liés à l'IA agentique et aux outils pour développeurs se manifestent dans plusieurs domaines clés : déploiement sécurisé et visibilité, fonctionnalités d'IA et formation des utilisateurs. Les personnes interrogées se plaignent de difficultés à trouver un moyen de déployer de l'IA agentique qui facilite la tâche des utilisateurs sans compromettre la sécurité des données. Les problèmes liés à la visibilité sur les outils en ligne de commande, les paquets tiers, les extensions d'IDE, les LLM intégrés et bien d'autres éléments sont également fréquents. Lorsqu'elle dispose des autorisations appropriées, l'IA agentique fait courir de graves risques aux bases de code : elle peut en effet ajouter du code non sécurisé ou problématique, ou supprimer du code indispensable. Les problèmes liés au développement ne touchent pas seulement les développeurs : les utilisateurs non techniques créent aussi leurs propres applications sans procéder aux vérifications ni aux contrôles de qualité adéquats.

Surprises au niveau des coûts

Chargées de concilier les coûts, les initiatives de l'entreprise et la sécurité, les équipes informatiques sont mises à rude épreuve. La tarification à l'utilisation des API d'IA et de LLM cloud rend les dépenses imprévisibles ; quand chaque service de l'entreprise adopte de nouveaux outils, les licences payantes se recoupent et s'accumulent. Sans savoir exactement ce qui est réellement utilisé, les équipes informatiques ne disposent d'aucun critère clair pour déterminer quels outils regrouper.

La gouvernance et la productivité vont de pair.

Dans les entreprises qui ont adopté l'IA, plus celle-ci est profondément intégrée, plus le taux d'incidents est élevé.

Les défis communs à toutes les personnes interrogées concernent la visibilité, le déploiement, la multiplication des fournisseurs et les coûts.

Toutes ces observations font émerger une réalité : **l'IA se déploie plus rapidement qu'on ne peut l'encadrer.**

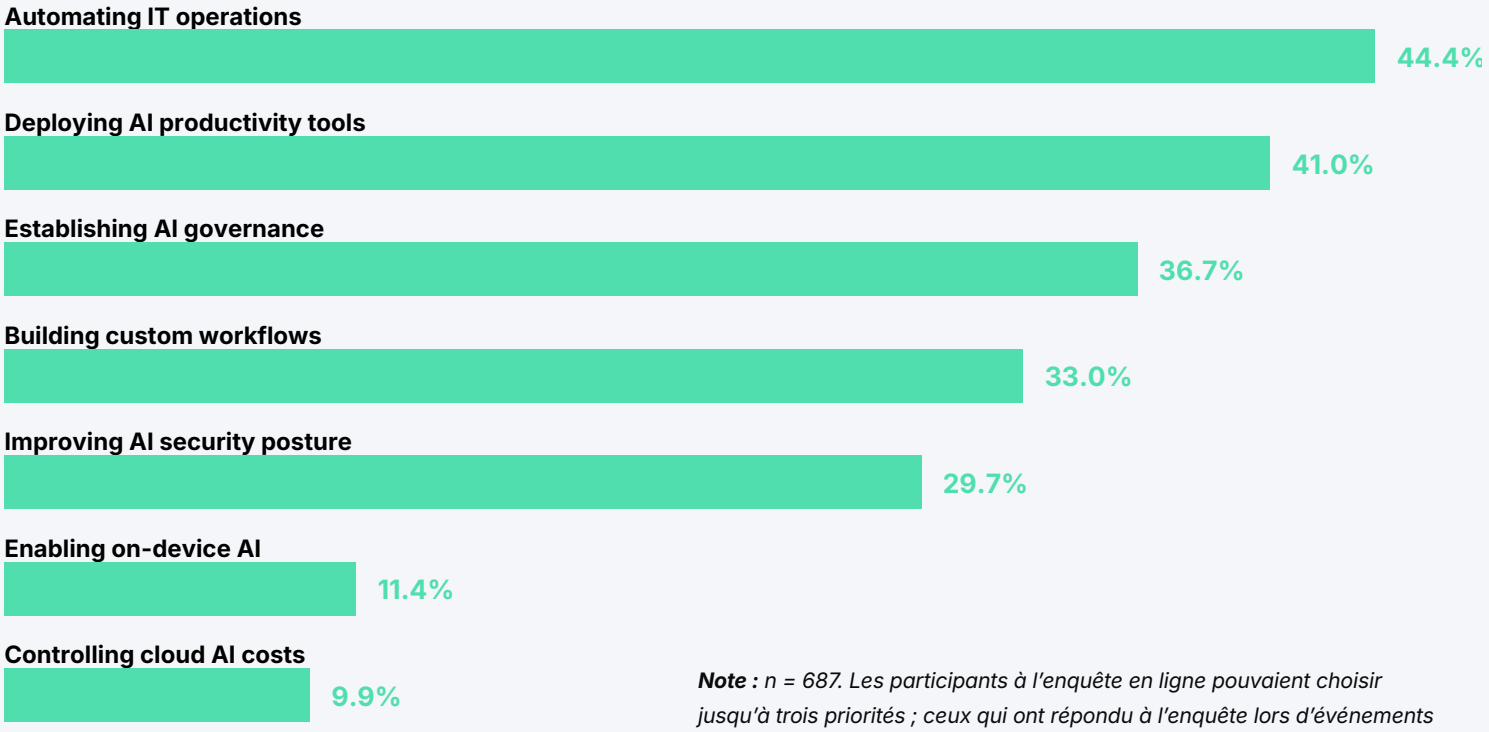
Les symptômes de ce mal sont nombreux : IA de l'ombre, exposition de points d'accès aux données ou aux systèmes de l'entreprise, adoption de plateformes redondantes (et coûteuses). Et à cela s'ajoutent des risques difficiles à évaluer, car ils échappent à la vigilance du service informatique.

Les équipes informatiques doivent donc revoir leurs priorités à l'heure où l'IA transforme les méthodes de travail de chacun.

GRAPHIQUE 4

Les grandes priorités en matière d'IA pour les 12 prochains mois

Point clé : l'automatisation des opérations informatiques, le déploiement d'outils de productivité et la mise en place de la gouvernance sont tout aussi prioritaires. La gouvernance ne suit pas l'autonomisation, elle évolue de pair avec elle.



Note : *n = 687. Les participants à l'enquête en ligne pouvaient choisir jusqu'à trois priorités ; ceux qui ont répondu à l'enquête lors d'événements en présentiel en ont choisi une. Pour plus de détails, voir la méthodologie.*

La gouvernance et l'autonomisation peuvent sembler se contredire. Plus il y a d'outils d'IA, plus il est difficile de les encadrer. Les équipes informatiques jonglent depuis toujours entre des priorités contradictoires, et l'IA ne fait pas exception. Mais sa rapidité d'adoption, ses caractéristiques et ses risques font entrer les équipes en terre inconnue.

C'est pour cette raison que les équipes poursuivent toutes ces priorités de front. Si vous allez trop vite, le risque d'incident augmente. Si vous allez trop lentement, les solutions que trouveront vos employés compromettront votre sécurité.

🗨 Dans vos propres termes : les défis que l'IA pose à vos collègues

Grâce aux 178 réponses ouvertes, l'enquête a permis d'obtenir des informations détaillées qui replacent les résultats dans leur contexte. Huit témoignages tirés des réponses ouvertes que nous avons reçues* :

Les utilisateurs veulent un accès immédiat, et les équipes de sécurité qui tentent de les ralentir subissent de fortes pressions. Le problème fondamental reste entier : **un contrôle total tend à nuire à la productivité, mais le laxisme entraîne un risque réel de non-conformité.**

Tous les fournisseurs intègrent l'IA à leurs solutions, que vous le vouliez ou non. La désactivation complète des systèmes permet de gagner du temps, mais cette approche n'est pas viable à long terme. La question la plus préoccupante concerne le traitement des données dans le cloud et le contrôle que nous avons sur leur destination.

Bloquer les sites d'IA connus reste la partie la plus facile. Les outils en ligne de commande, les extensions pour IDE, les extensions de navigateur et les paquets extraits sur GitHub **passent généralement inaperçus** ; et lorsqu'un chemin est bloqué, les utilisateurs en trouvent une autre.

Dans les secteurs réglementés et certaines juridictions, des cadres de conformité spécifiques doivent être mis en place avant toute mise en service. Et à l'heure actuelle, les **outils et les cadres disponibles ne répondent pas aux exigences.**

L'IA de l'ombre et l'exécution de scripts en boîte noire arrivent en tête de la liste des risques. Juste derrière, on retrouve les utilisateurs non techniciens qui codent leurs propres applications à l'instinct et créent des choses qu'ils ne comprennent pas entièrement, sans se rendre compte qu'ils exposent leurs données.

Il y a un fossé entre l'idée que tout le monde doit utiliser l'IA et la volonté de financer les licences. Les équipes qui l'ont adoptée rapidement se retrouvent désormais avec une multiplicité d'agents redondants **qui coûtent cher, sans cadre précis** pour déterminer lesquels méritent d'être conservés.

Il est difficile de convaincre les gens de donner aux agents d'IA l'accès aux infrastructures de développement et de production. Beaucoup craignent qu'un agent fasse exactement l'inverse de ce que vous voulez, puis vous annonce que vos données ont disparu. **Il n'existe pas encore de moyen fiable de déployer des capacités agentiques de manière contrôlée et gérée.**

Lorsque des résultats fantaisistes sont traités comme des faits et que l'IA s'intègre de plus en plus profondément dans notre quotidien, les **risques progressent plus vite que la maîtrise de l'outil.**

* Les témoignages ci-dessus ont été synthétisés par Jamf à partir des tendances observées dans 178 réponses ouvertes. Chacun d'entre eux reflète un thème récurrent plutôt que les propos exacts d'un participant donné.

Passer à l'action : quatre principes de gouvernance

1.

Gagnez en visibilité.

Comme l'ont mentionné de nombreux participants, il est primordial de gagner en visibilité. On ne peut pas encadrer ce qu'on ne voit pas. Mais c'est bien là que réside toute la difficulté. En procédant à des audits réguliers des applications installées et en surveillant le trafic, vous pourrez identifier les interactions avec les plateformes d'IA. Mais si les utilisateurs s'appuient sur des plateformes d'IA locales et que des applications approuvées intègrent tout à coup de l'IA dans leurs fonctionnalités, il faut aller plus loin dans la détection de l'IA en temps réel.

2.

Contrôlez l'outil, pas l'utilisateur.

De nombreuses équipes informatiques ont le sentiment que leur entreprise a rapidement édicté des règles en matière d'IA sans les consulter. Et ces règles sont conçues pour encourager et accélérer l'utilisation de l'IA. Les utilisateurs reçoivent des directives, cela ne signifie pas pour autant qu'elles sont obligatoires. C'est là qu'émerge l'IA de l'ombre.

Au contraire, la gouvernance doit être définie en fonction de la tolérance au risque et des directives de sécurité de l'organisation, qui doivent se refléter dans les paramètres de partage des données des outils d'IA. La gouvernance détermine quelles données il peut consulter, comment il les traite et ce qu'il peut modifier. Avec l'IA de l'ombre, l'utilisateur n'est pas toujours visible ; en revanche, le trafic, les données et les appels API le sont. On ne peut encadrer que ce que l'on voit.

3.

Intégrez la gouvernance dans le processus de déploiement.

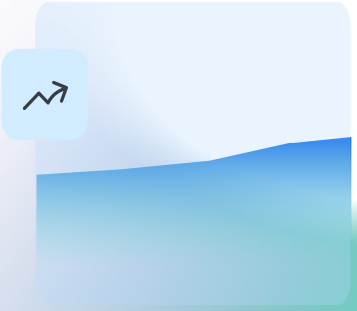
Les organisations qui ont déployé l'IA dans la précipitation se sont exposées à des risques d'incident. Il faut faire les choses dans l'ordre : la gouvernance doit accompagner le déploiement des applications, et non y répondre a posteriori. Certes, c'est plus facile à dire qu'à faire, et vous avez peut-être déjà du retard à rattraper. Cependant, en identifiant les outils présents, en les mettant à la disposition des utilisateurs et en définissant des politiques d'accès, vous pourrez plus facilement sécuriser l'adoption de l'IA.

4

Utilisez des outils conçus dès le départ pour Apple.

Les outils basés sur le réseau vous permettent de visualiser le trafic et de savoir quels services d'IA cloud vos utilisateurs consultent, à quel moment et à quelle fréquence. C'est un signal essentiel, mais il s'arrête à la périphérie du réseau. Même lorsque l'IA est exécutée dans le cloud, c'est sur l'appareil que s'effectuent les opérations : il reste crucial de savoir quels outils y sont installés, quels processus ils lancent et à quels fichiers ils accèdent. Rien de tout cela n'apparaît dans un journal DNS. Les outils natifs d'Apple comblent cette lacune : consultez la liste des outils, des processus et des accès aux fichiers, et définissez ceux qui sont autorisés.

Gouvernez ce que vous autorisez. Autorisez ce que vous gouvernez.



La vitesse d'évolution de l'IA dépasse les capacités de la plupart des cadres de gouvernance mis en place pour la gérer. Mais les difficultés que vous avez déjà rencontrées ne doivent pas nécessairement déterminer votre approche du déploiement. Vous n'avez pas à choisir entre donner aux utilisateurs les outils d'IA dont ils ont besoin et sécuriser les pratiques.

Les équipes qui s'en sortent le mieux ne sont pas celles qui vont le plus vite ni celles qui verrouillent le plus. Elles envisagent la gouvernance et l'autonomisation comme un seul et même projet, en intégrant dès le départ des mécanismes de visibilité et de contrôle d'accès au déploiement de l'IA. Pour les entreprises Apple, il faut des outils qui comprennent l'environnement d'exécution que vous gérez : le trafic cloud, les modèles d'appareils et les processus agentiques génèrent des signaux différents, et les solutions de supervision qui ne sont pas conçues pour Apple en ignorent la plupart. La solidité de vos mesures de gouvernance dépend entièrement de ce que vos outils sont capables de détecter.

On ne peut pas freiner l'adoption de l'IA. Mais vous pouvez le maîtriser ; c'est même tout l'enjeu de votre mission.

Méthodologie

Les données ont été recueillies en deux temps. La première vague de collecte a été menée auprès de la communauté des clients Jamf en mars et en avril 2026 (338 répondants). La deuxième vague a pris la forme d'une enquête en présentiel lors des événements Jamf Nation Live organisés dans six villes d'Amérique du Nord (349 personnes interrogées). Échantillon total : 687 responsables informatiques et de la sécurité. Tous les participants travaillent au sein d'organisations qui gèrent et sécurisent des appareils Apple à grande échelle, et sont clientes de Jamf.

Pour les questions portant sur les priorités, les personnes interrogées ont été invitées à indiquer leurs principales priorités en matière d'IA pour les 12 prochains mois. Les sondages de mars et d'avril permettaient de cocher jusqu'à trois réponses ; celui de Jamf Nation Live n'en autorisait qu'une seule. Les pourcentages indiqués pour cette question correspondent à la part des 687 personnes interrogées qui ont inclus la priorité en question dans leur sélection. Ces deux critères de sélection sont présentés ici par souci de transparence.

Les analyses statistiques confirment que ces deux vagues ont donné lieu à des populations distinctes ; les participants des Jamf Nation Live affichant en moyenne un stade plus avancé de maturité en matière d'IA. Ces orientations s'appliquent indépendamment aux deux échantillons. Toutes les données des personnes interrogées ont été recueillies et analysées de manière anonyme ; aucune réponse individuelle n'est attribuée à des personnes ni à des organisations spécifiques. Les participants n'ont reçu aucune rémunération pour leur participation.