netskope

Cybersecurity INSIDERS

2026

Rapport sur les risques et la maturité face à l'IA

Présentation

Pour la plupart des entreprises, cette année est l'année où l'IA devient une infrastructure. Les agents effectuent désormais des actions de manière autonome : ils modifient des enregistrements, créent des comptes et déploient du code via des appels API qui s'exécutent avant même qu'un humain ne les vérifie. Ce changement fait de chaque déploiement d'IA un risque de sécurité en puissance, quelle que soit la manière dont les entreprises choisissent de l'aborder.

Les infrastructures de sécurité que l'on trouve aujourd'hui dans la plupart des entreprises ont été conçues pour un monde différent : un monde où les humains étaient les seuls acteurs, où les processus étaient définis, où les données gardaient une structure identifiable et où la confiance était vérifiée au niveau du navigateur. Ce monde n'existe plus.

Ce rapport s'appuie sur une enquête approfondie menée auprès de 1 253 professionnels de la cybersécurité. Il analyse comment les entreprises protègent leurs systèmes d'IA, en s'intéressant à la gouvernance, à la visibilité, à la protection des données et au contrôle des agents.

Principales conclusions :

- **L'adoption de l'IA a pris de l'avance sur la gouvernance en matière de sécurité**
  Les outils d'IA sont désormais déployés dans 73 % des entreprises interrogées, mais la mise en place d'une gouvernance garantissant la sécurité et le respect des politiques en temps réel n'atteint que 7 %. Il en résulte un déficit structurel de 66 points, qui ne cesse de se creuser à mesure que l'adoption de l'IA continue de progresser plus rapidement que la mise en place des contrôles.

- **Les dépenses augmentent, mais la confiance diminue**
  90 % des personnes interrogées ont augmenté leur budget consacré à la sécurité de l'IA cette année, mais 29 % d'entre elles se sentent moins en sécurité qu'il y a douze mois. Le problème prend le pas sur les investissements.

- **La plupart des activités liées à l'IA échappent à la vigilance des services de sécurité**
  94 % des personnes interrogées font état d'un manque de visibilité sur les activités liées à l'IA. 88 % ne parviennent pas à distinguer les comptes IA personnels des instances professionnelles. Seules 6 % affirment avoir une vue d'ensemble du pipeline IA de leur entreprise.

- **L'IA rend les solutions traditionnelles de prévention des pertes de données (DLP) inefficaces**
  La DLP trouve des correspondances entre des modèles, tandis que l'IA transforme le sens. Or, seuls 8 % des systèmes sont équipés de contrôles capables d'évaluer le contenu sur le plan sémantique, quelle que soit la manière dont il a été réécrit.

- **Les agents agissent sans aucune restriction**
  Les agents d'IA ont un accès en écriture aux outils de collaboration (53 %), à la messagerie (40 %), aux dépôts de code (25 %) et aux fournisseurs d'identité (8 %). 91 % des entreprises ne prennent connaissance des opérations d'un agent qu'après leur exécution.

- **Une grande partie de la sécurité de l'IA repose sur la confiance**
  31 % des entreprises s'appuient principalement sur des politiques écrites et le respect de celles-ci par les employés pour assurer la conformité. 11 % d'entre elles n'ont mis en place aucune mesure. Seules 23 % déclarent appliquer les mesures de sécurité liées à l'IA en temps réel, au moment même où l'opération se produit.

Les risques de l'IA ne se limitent plus aux dérives liées à l'usage humain. Ils touchent désormais l'autonomie même des machines. Pourtant, les dispositifs de contrôle continuent de se concentrer essentiellement sur le premier aspect. L'enquête souligne quatre priorités architecturales : assurer une visibilité permanente sur toutes les activités de l'IA, notamment le trafic des agents et le trafic M2M ; appliquer les règles en temps réel, sans friction ni latence ; mettre en place des contrôles de données sémantiques, qui analysent le sens plutôt que les modèles ; et étendre le modèle Zero Trust aux identités non humaines (NHI). Les chapitres suivants analysent le niveau de maturité des entreprises et proposent des pistes pour combler le fossé dans la mise en œuvre.

©2026 Cybersecurity Insiders. Tous droits réservés.

La gouvernance de l'IA peine à suivre le niveau d'adoption

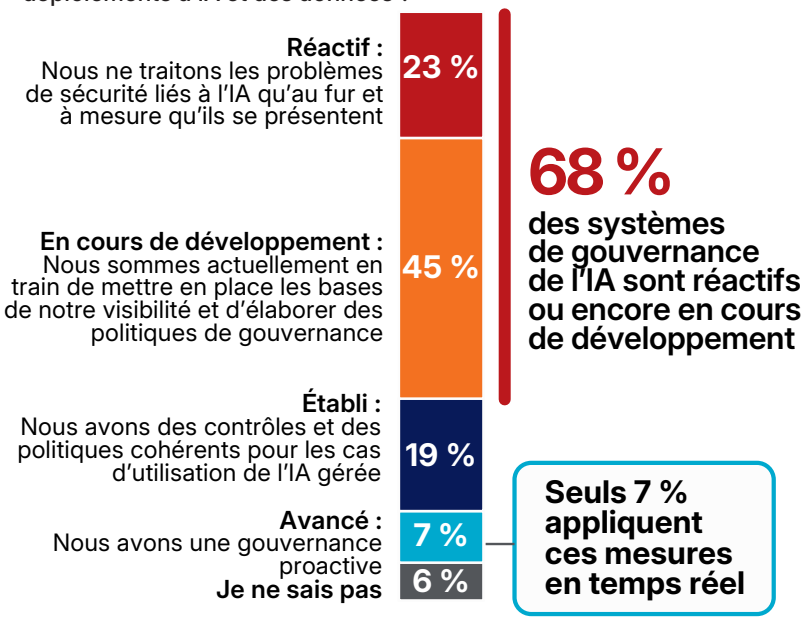
Il y a un an, la plupart des entreprises reportaient à plus tard la gouvernance de l'IA, en attendant que son déploiement se stabilise. Mais son adoption a pris les devants. Les assistants de codage, les outils d'aide à la saisie et les générateurs de contenu se sont multipliés dans tous les services. Quand le service de sécurité a enfin créé un cadre de référence, l'IA était déjà pleinement opérationnelle.

Aujourd'hui, 68 % des entreprises avouent avoir une gouvernance de l'IA réactive, voire en phase de développement. Seules 7 % ont atteint un niveau de maturité avancé, capable d'appliquer les politiques en temps réel. L'écart de 66 points entre les 73 % qui déploient des outils d'IA et les 7 % qui les gèrent en temps réel révèle un décalage structurel : les entreprises connaissent une croissance fulgurante, souvent sans véritable socle en matière de sécurité et de conformité. Et les conséquences commencent à se faire sentir. En effet, 39 % d'entre elles ont déjà évité de justesse un incident lié à l'IA impliquant une exposition involontaire de données. Parmi celles-ci, 17 % n'ont rien changé par la suite.

Que 68 % des entreprises se contentent d'une gouvernance réactive ou en cours de développement peut sembler anodin. Pourtant, cette situation cache une réalité inquiétante : dans de nombreuses entreprises, l'adoption de l'IA reste totalement désorganisée. Plus d'un tiers d'entre elles reconnaissent une adoption fragmentée de l'IA où plusieurs équipes déploient des outils de manière indépendante, sans cadre, normes ou politiques de sécurité communs. Certaines divisions utilisent des agents autonomes avec des directives informelles, tandis que d'autres ignorent même quels outils d'IA leurs employés utilisent. Le débat sur la gouvernance n'a pas pris seulement du retard : dans de nombreuses entreprises, il n'a jamais vraiment commencé. 48 % s'attendent à ce que les prochaines violations majeures liées à l'IA soient provoquées par des failles de gouvernance, qu'il s'agisse de l'utilisation non encadrée de l'IA, la fameuse Shadow AI, ou de droits d'accès trop largement accordés. Les professionnels en première ligne savent bien que l'un de leurs plus grands risques vient des outils que leurs propres équipes ont adoptés il y a à peine un trimestre, sans aucune transparence. Ce déficit de gouvernance fragilise désormais toutes les couches de sécurité.

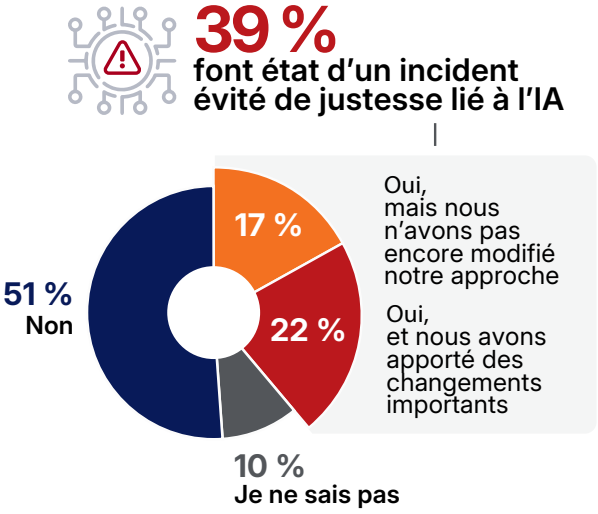
La gouvernance en temps réel est rare

Quelle affirmation décrit le mieux le niveau de maturité de votre entreprise en matière de gouvernance et de sécurisation des déploiements d'IA et des données ?



Les incidents évités de justesse sont déjà une réalité

Avez-vous déjà été confronté à un « incident évité de justesse » lié à l'IA, impliquant la divulgation ou la fuite accidentelle de données sensibles, qui vous a amené à repenser en profondeur votre stratégie de sécurité ?



La solution structurelle la plus simple ? Identifier les trois cas d'utilisation de l'IA à plus haut risque dans votre environnement, intégrer des politiques adaptées à ces cas dans des contrôles techniques et désigner un responsable pour chaque cas.

©2026 Cybersecurity Insiders. Tous droits réservés.

Un budget en hausse, mais une confiance en berne

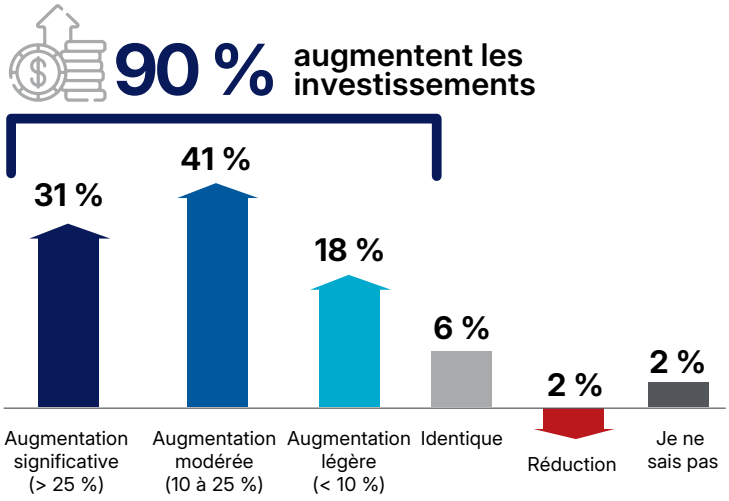
Les entreprises n'ont jamais autant investi dans la sécurité de l'IA… et pourtant, le déficit de gouvernance persiste. Cette année, 90 % d'entre elles ont augmenté leurs dépenses dans le domaine de la sécurité de l'IA, dont près d'un tiers de plus de 25 %. Pourtant, 29 % se sentent aujourd'hui moins en sécurité qu'il y a un an. Les investissements augmentent, mais la confiance, elle, s'effrite.

Les participants à l'étude en ont expliqué les raisons : 34 % d'entre eux considèrent que le principal obstacle réside dans la pression exercée par les entreprises pour adopter l'IA plus vite que la sécurité ne le permet. Le manque de compétences arrive en deuxième position avec 25 %, tandis que les outils hérités, incapables d'interpréter les menaces spécifiques à l'IA, occupent la troisième place avec 21 %. Les contraintes budgétaires arrivent en quatrième position avec 14 %. Si le budget a été débloqué pour beaucoup, l'architecture qu'il finance reflète toujours un modèle de menaces antérieur à l'IA.

Les outils de sécurité actuels ont été conçus pour des formats de fichiers classiques, des flux de données prévisibles et des interactions à rythme humain. Injecter davantage de budget ne résout rien, car cela revient à acheter des solutions qui échouent déjà face aux risques de l'IA. La perte de confiance est flagrante : 51 % estiment leurs contrôles techniques insuffisants, 50 % leur visibilité limitée et 61 % leur gouvernance numérique défaillante.

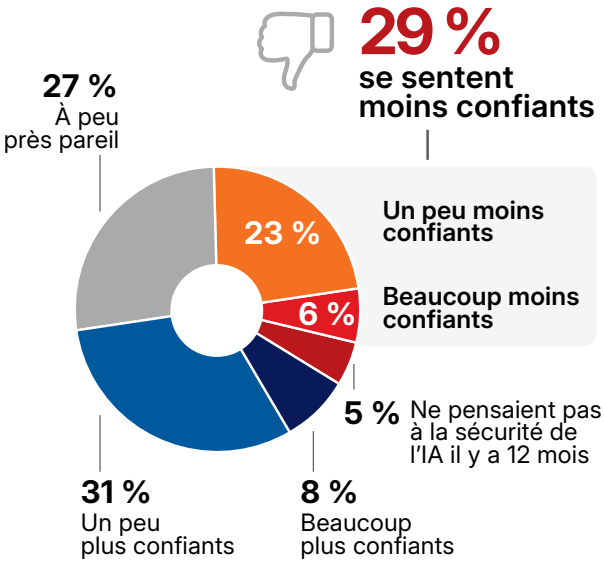
Les dépenses augmentent rapidement

Comment les investissements de votre entreprise dans les mesures de sécurité spécifiques à l'IA vont-ils évoluer au cours des 12 prochains mois ?



La confiance s'effrite

Par rapport à il y a 12 mois, comment a évolué votre confiance dans la capacité de votre entreprise à protéger les systèmes d'IA contre les attaques et les fuites de données ?



Pour réorienter le budget, la première étape consiste à comparer les dépenses actuelles en matière de sécurité de l'IA à trois indicateurs de vulnérabilité (la visibilité, les contrôles techniques et la gouvernance), puis à concentrer les investissements vers les domaines où le décalage entre moyens engagés et capacités réelles est le plus important.

©2026 Cybersecurity Insiders. Tous droits réservés.

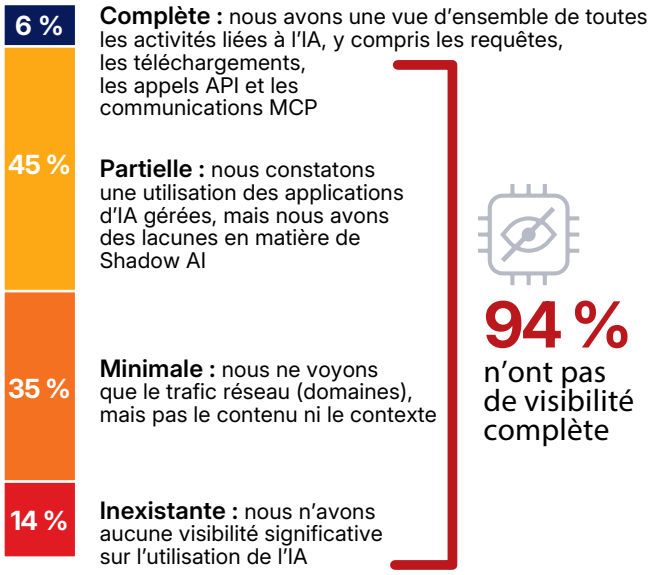
La plupart des activités liées à l'IA échappent à la vigilance des services de sécurité

Vous ne pouvez pas sécuriser ce que vous ne voyez pas. Seules 6 % des entreprises ont une visibilité complète sur l'utilisation de l'IA dans leur environnement. 45 % se contentent d'une visibilité partielle, limitée aux applications gérées, sans aucune visibilité sur ce qui se passe en dehors des outils autorisés. 35 % ne voient que les tendances du trafic au niveau du réseau, ce qui leur permet de savoir qu'il se passe quelque chose, mais pas quoi. Et 14 % n'ont aucune visibilité. 94 % prennent des décisions en matière de sécurité de l'IA sans avoir une vision complète de la situation, et pour la plupart, c'est le mode de fonctionnement par défaut.

Même quand la détection est possible, une question persiste : comment distinguer ce qui est important ? 88 % des entreprises ne parviennent pas à différencier de manière fiable les comptes IA personnels des instances professionnelles sur une même plateforme : le principal angle mort technique révélé par l'enquête. Quand une équipe de sécurité ignore si un employé utilise un abonnement IA autorisé ou un compte personnel sans gouvernance des données, les politiques DLP, les contrôles d'accès et les pistes d'audit ne sont plus fiables. La Shadow AI aggrave encore ces lacunes : 31 % se fient à l'analyse a posteriori des journaux pour repérer les outils d'IA non autorisés, 21 % ne détectent pas du tout la Shadow AI, et seuls 27 % utilisent un CASB ou un SWG pour une détection en temps réel.

La visibilité est incomplète

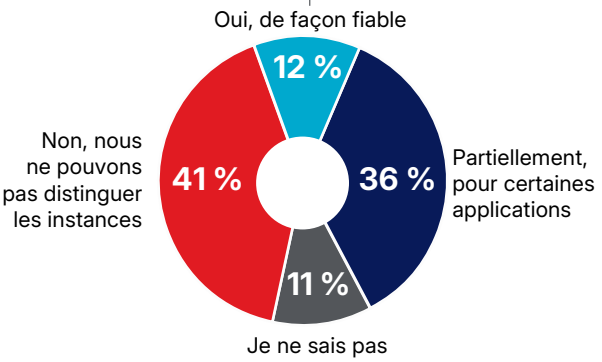
Dans quelle mesure votre équipe de sécurité a-t-elle une vue d'ensemble de l'utilisation de l'IA ?



L'identité de l'instance n'est pas claire

Vos outils de sécurité sont-ils capables de faire la distinction entre les instances personnelles et professionnelles des applications d'IA (par exemple, un compte ChatGPT personnel et un compte ChatGPT professionnel) ?

Seuls 12 % sont capables de distinguer de manière fiable les applications d'IA à usage personnel de celles à usage professionnel



La visibilité est la pierre angulaire de tous les mécanismes de contrôle, car, sans elle, les solutions DLP, les politiques d'accès et l'application des règles d'utilisation acceptable n'ont aucun moyen de réguler une activité invisible. Pire encore, les interactions les plus difficiles à surveiller sont précisément celles qui augmentent le plus vite. En tête des défis figurent les intégrations d'API, les connexions d'agents via MCP et les communications M2M tandis qu'à l'inverse, les conversations directes entre les utilisateurs et l'IA qui sont les moins complexes à suivre ne représentent que 6 % des cas.

Pour combler ce manque de visibilité, il faut d'abord étendre la surveillance des activités à ces canaux en commençant par distinguer clairement les comptes IA personnels des comptes professionnels, car c'est cette distinction qui servira de fondement à toutes les actions suivantes.

©2026 Cybersecurity Insiders. Tous droits réservés.

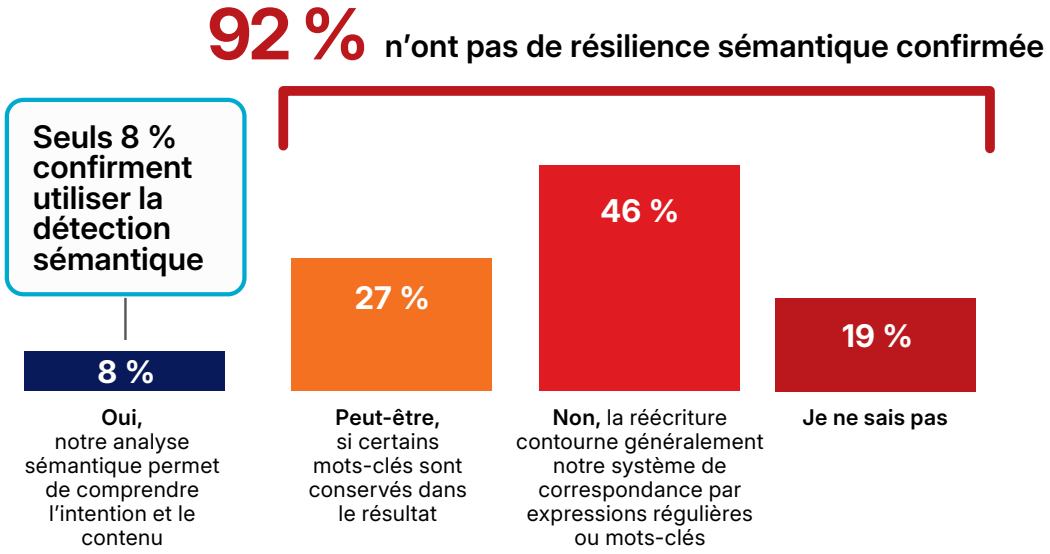
L’IA rend les systèmes DLP traditionnels obsolètes

Même lorsque les entreprises détectent une activité liée à l’IA, leur outil principal de capture des données en mouvement a été conçu pour un type de flux radicalement différent. La DLP a été pensée pour repérer des types de données précis, comme les formats de cartes bancaires, les numéros de sécurité sociale ou les expressions régulières associées à des données sensibles connues. Même si la DLP peut bloquer le téléchargement ou le copier-coller de données sensibles dans les champs de saisie grâce à ces modèles, dès que l’IA accède à ces données, elle reformule le contenu sensible en conservant son sens tout en effaçant toute trace numérique originale.

La distinction est avant tout architecturale. La DLP agit au niveau syntaxique en comparant des séquences de caractères à des règles prédéfinies, tandis que l’IA opère au niveau sémantique en transformant le contenu tout en préservant l’intention. Un simple test de transformation l’illustre parfaitement. Si un employé demande à une IA de résumer la description d’un projet confidentiel dans un e-mail professionnel, celle-ci peut très bien reformuler « Projet X » en « notre prochaine initiative stratégique ». Le problème, c’est qu’un filtre basé sur des expressions régulières laissera passer « initiative stratégique » sans broncher, alors que l’information sensible (le secret lui-même) reste bel et bien présente, simplement habillée autrement. Le même problème apparaît avec la traduction de secrets en anglais dans une autre langue et vice versa. L’IA crée une version où chaque mot-clé original a été remplacé, mais le risque sous-jacent reste, lui, inchangé. Les solutions DLP traditionnelles échouent aussi face à l’inférence. Prises séparément, deux listes, l’une de noms, l’autre de pathologies, peuvent sembler parfaitement anodines. Mais, une IA est capable de reformuler le document de manière à relier explicitement les deux, créant ainsi une violation de la loi HIPAA qu’un filtre DLP classique, fondé sur des modèles de détection, serait incapable de repérer. 46 % reconnaissent que leurs contrôles ne détecteraient pas ce type de violation, puisque la réécriture contourne systématiquement les expressions régulières et la correspondance de mots-clés. 27 % ont également souligné que la détection repose entièrement sur la persistance de mots-clés spécifiques après la transformation : un mécanisme qui, en pratique, ne fonctionne que si l’adversaire veut bien jouer le jeu. Si on ajoute les 19 % qui ne sont pas sûrs de leur couverture, nous constatons que 92 % des entreprises n’ont pas de système DLP dont l’efficacité est prouvée une fois que l’IA a reformulé le contenu.

La réécriture empêche le contrôle des modèles

Le test de transformation : si un employé demande à une IA de « réécrire ce document sous la forme d’un article de blog générique », vos mesures de sécurité sont-elles en mesure de détecter les données sensibles dans le résultat obtenu ?



La DLP continue de détecter les violations basées sur des modèles, mais le contenu transformé par l’IA passe inaperçu. Le problème s’est en effet déplacé vers une couche que la DLP n’a jamais été conçue pour analyser. Voici une méthode simple pour évaluer votre exposition : testez la transformation sur votre infrastructure. Prenez un document confidentiel. Demandez à un outil d’IA de le reformuler, puis vérifiez si vos contrôles signalent le résultat. Cette opération servira de référence pour déployer une inspection sensible au contenu qui soit capable d’évaluer le sens au moment du transfert.

©2026 Cybersecurity Insiders. Tous droits réservés.

Les agents d'IA s'exécutent sans aucune supervision

Si la fuite de données via des outils d'IA est le risque le plus souvent identifié par les entreprises, la menace la plus préoccupante est ailleurs : les systèmes d'IA fonctionnent désormais de façon autonome, et bon nombre d'entre eux opèrent dans l'ombre, en dehors de la portée des équipes de sécurité.

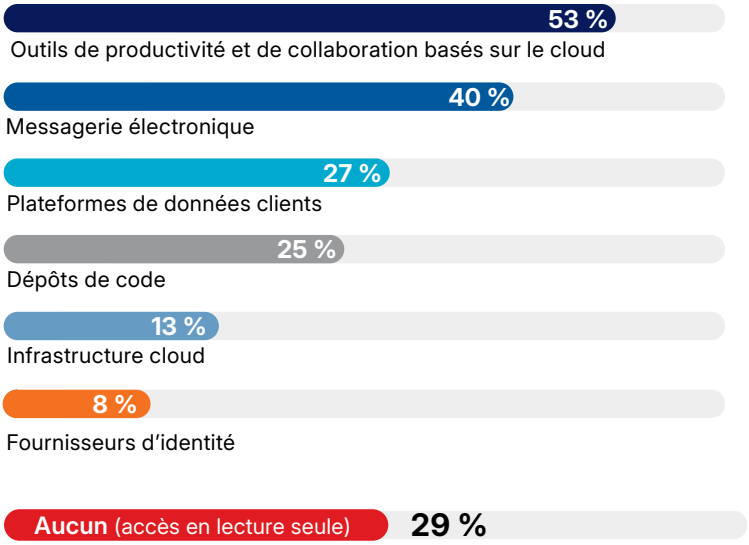
L'enquête permet de quantifier l'ampleur de ce phénomène. 56 % des répondants déclarent être exposés à de réels risques liés à l'IA agentique : 24 % dans le cadre d'une production limitée, 9 % à grande échelle pour la gestion de la logique métier fondamentale, et 23 % via des déploiements parallèles dont le service IT n'a pas connaissance. 32 % n'ont aucune visibilité sur les actions des agents, et 36 % ignorent tout du trafic IA M2M.

Les entreprises qui ne peuvent pas voir les agents ne peuvent pas savoir qu'elles ont des agents fantômes. 10 % déclarent avoir interdit l'IA agentique. Pourtant, sur l'ensemble des entreprises interrogées, 23 % signalent une utilisation clandestine. Dans la pratique, les interdictions poussent souvent ces activités dans la clandestinité, ce qui rend leur gestion plus difficile et leur contrôle encore plus compliqué en cas de problème.

L'étendue des droits d'écriture est plus importante que ne le pensent la plupart des équipes de sécurité. 53 % accordent aux outils d'IA des droits d'écriture sur les suites de productivité et de collaboration dans le cloud, 40 % sur la messagerie électronique, 25 % sur les dépôts de code et 13 % sur l'infrastructure cloud. Mais ce sont les cas suivants qui modifient la nature même du risque : 8 % accordent des droits d'écriture aux fournisseurs d'identité. Un agent ayant un accès en écriture à la couche d'identité peut créer des comptes de service, élever des privilèges sur l'ensemble des systèmes fédérés et s'octroyer un accès externe via des appels API qui ne franchissent jamais le périmètre du réseau.

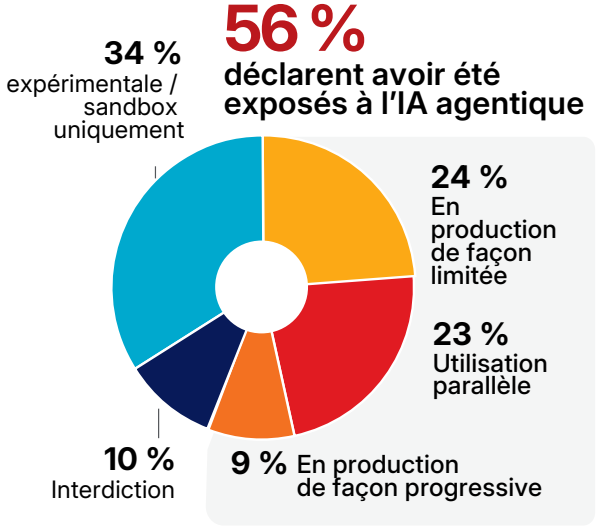
Les agents ont déjà des droits d'écriture

À quels systèmes internes vos outils ou agents d'IA ont-ils un accès en écriture ?



Le déploiement parallèle est courant

Comment décririez-vous votre adoption de l'IA agentique (une IA qui poursuit des objectifs de manière autonome) ?



Seules 29 % des entreprises limitent l'accès aux outils d'IA à la lecture seule. Pour les 71 % restants, la marche à suivre est claire : vérifier quels outils d'IA ont actuellement un accès en écriture et mettre en place des procédures d'approbation pour toute action visant à créer des comptes, à modifier des autorisations ou à transférer des données en dehors des murs de l'entreprise.

©2026 Cybersecurity Insiders. Tous droits réservés.

Quand les agents agissent, personne ne les arrête

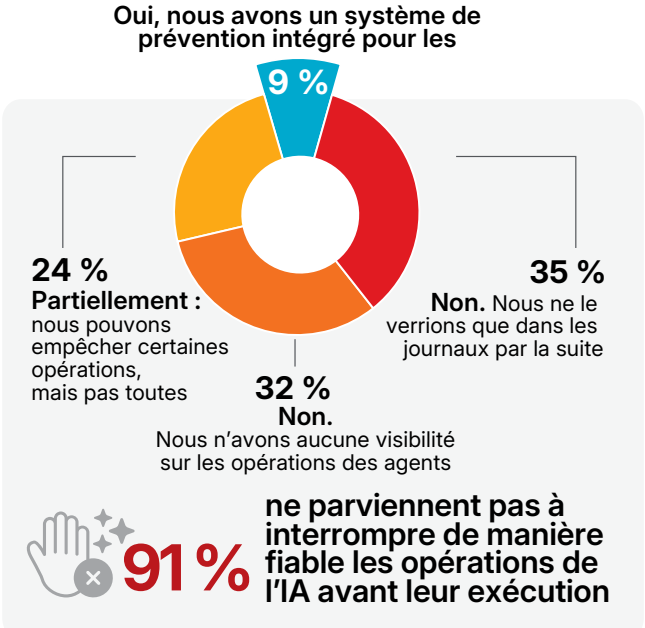
Les agents ont un large accès à l'ensemble des systèmes professionnels, et pratiquement aucune de leurs actions ne peut être interceptée. Une fois qu'un agent lance une action malveillante, seules 9 % des entreprises parviennent à intervenir avant qu'elle ne soit exécutée. Les 91 % restants se répartissent selon différents degrés d'impuissance : 24 % peuvent bloquer certaines actions des agents, mais pas toutes ; 35 % ne découvrent l'action qu'après coup, dans les journaux ; et 32 % n'ont absolument aucune visibilité sur les actions des agents. Parmi les entreprises qui déploient une IA agentique, moins d'une sur dix est en mesure de bloquer un agent avant qu'il ne supprime un dépôt de code, ne modifie une fiche client ou ne s'octroie des privilèges supplémentaires.

Les conséquences se font déjà sentir. 37 % des entreprises ont rencontré des problèmes opérationnels causés par des agents d'IA au cours des douze derniers mois, dont 8 % étaient suffisamment graves pour entraîner des pannes ou une corruption des données. 38 % citent le transfert autonome de données par un agent vers un emplacement non fiable comme leur principale crainte en matière de défaillance, et 24 % redoutent qu'un agent ne supprime des configurations ou du code critiques. Ces préoccupations se reflètent dans les incidents signalés de manière indépendante pour la période 2025-2026. Au milieu de l'année 2025, la vulnérabilité EchoLeak (CVE-2025-32711, CVSS 9.3) a démontré une injection de prompt sans clic contre Microsoft 365 Copilot, qui a permis l'exfiltration de données d'une entreprise sans intervention d'un utilisateur. Début 2026, des chercheurs ont révélé l'attaque Reprompt, qui enchaînait trois techniques pour transformer Copilot Personal en un canal d'exfiltration de données en un seul clic.

Parmi les 32 % qui n'ont aucune visibilité sur les agents d'IA, il y a un analyste SOC qui, un lundi matin, remontera la piste d'une élévation de privilèges suspecte jusqu'à un compte de service créé par un agent trois jours plus tôt, avant de réaliser que cet agent a écrit dans les systèmes de production pendant tout le week-end. Les journaux consigneront chaque action. Aucune alerte n'a été déclenchée, car aucune règle de détection n'existait pour ce type de comportement initié par un agent.

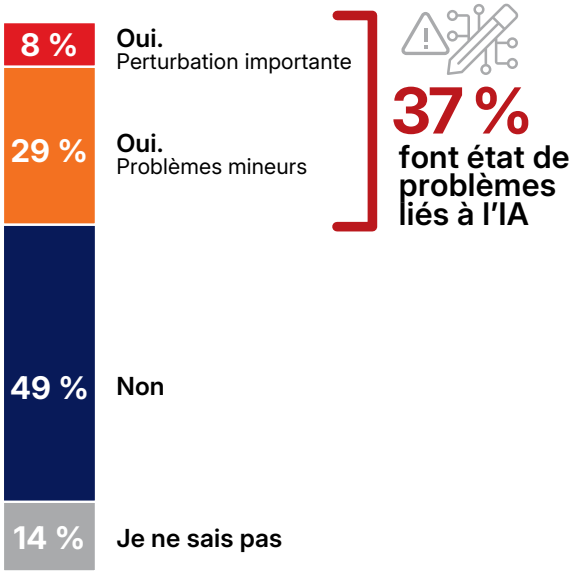
La prévention est l'exception

Votre entreprise est-elle en mesure d'empêcher une opération risquée générée par l'IA (par exemple, la suppression d'un dépôt par un agent) avant qu'elle ne se produise ?



Les répercussions opérationnelles commencent à se faire sentir

Au cours de l'année passée, un outil d'IA a-t-il causé un problème opérationnel ?



Il existe une solution à ce problème : définissez ce qui constitue un comportement anormal pour les actions des agents dans votre environnement, élaborez des règles de détection pour ces types de comportements et imposez une validation humaine pour les opérations à haut risque des agents, telles que la création de comptes, la modification des autorisations et les transferts de données vers l'extérieur. L'interception automatisée au niveau de la couche des requêtes est l'objectif visé à mesure que les outils gagnent en maturité.

©2026 Cybersecurity Insiders. Tous droits réservés.

Le Zero Trust s'arrête au niveau de la machine

91 % des entreprises sont incapables de bloquer un agent avant qu'il n'agisse. La raison est d'ordre architectural, car le modèle Zero Trust a été conçu autour d'un utilisateur doté d'un appareil, d'un emplacement, d'un profil de comportement et d'un score de risque. Or un agent d'IA se limite à des identifiants, un périmètre d'action et une tâche. 62 % appliquent les principes Zero Trust à la sécurité de l'IA sous une forme ou une autre, ce qui en fait l'approche la plus adoptée. Pourtant, 65 % reconnaissent que leurs contrôles Zero Trust actuels échouent à sécuriser les identités non humaines (NHI).

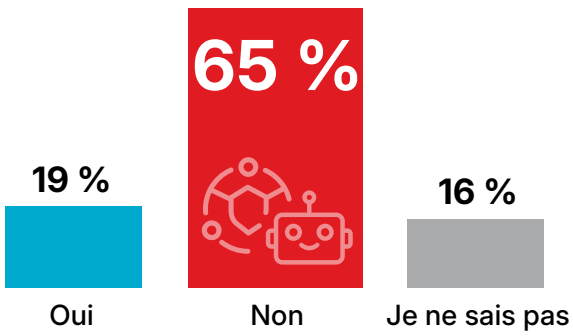
La gouvernance des identités non humaines (NHI) obtient les scores les plus bas dans tous les domaines évalués, 61 % des personnes interrogées la jugeant insuffisante, alors que 78 % s'attendent à ce que la croissance des NHI dépasse celle des identités humaines au cours de l'année à venir. Chaque nouvel agent, microservice et processus d'automatisation crée des comptes de service et des clés API que la gouvernance traditionnelle des identités n'a jamais été conçue pour gérer. Ces cadres ont été conçus pour des entités qui persistent au-delà des trimestres financiers. Une identité d'agent peut, quant à elle, ne durer que quelques minutes.

Les protocoles utilisés par les agents pour communiquer créent un deuxième problème. Le MCP s'est imposé comme un connecteur courant entre les agents d'IA et les outils d'entreprise. Dans de nombreuses implémentations actuelles, l'interopérabilité a pris le pas sur la vérification d'identité intégrée, l'application du principe du moindre privilège ou la visibilité d'audit indépendante. L'enquête montre que seules 8 % des entreprises ont mis en place des politiques pour encadrer le MCP. Les 92 % restantes ne le surveillent pas ou n'en ont jamais entendu parler. En ce qui concerne le trafic IA M2M, 36 % des répondants n'ont aucune visibilité à ce sujet, tandis que 28 % s'en remettent entièrement à la sécurité de la plateforme du fournisseur, sans vérification indépendante. Seuls 14 % inspectent le trafic API avec la même rigueur que celle appliquée au trafic utilisateur.

Les entités non humaines ne sont pas couvertes

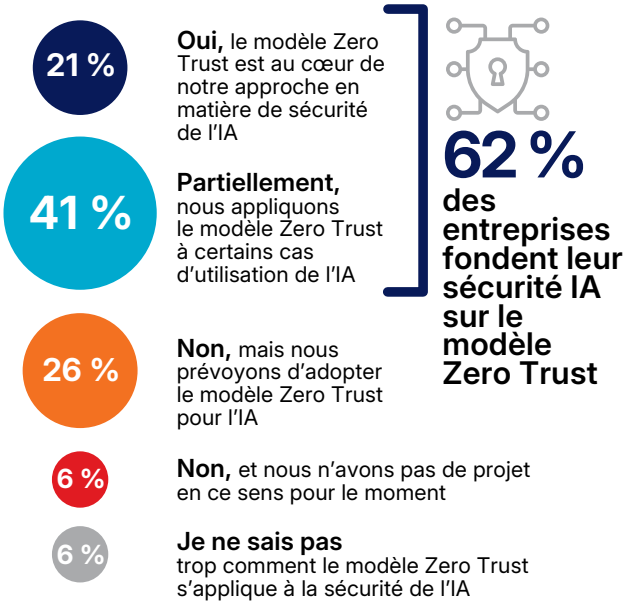
Vos contrôles d'accès Zero Trust actuels permettent-ils à votre entreprise de sécuriser les identités non humaines ?

La plupart des programmes Zero Trust ne s'étendent pas aux identités non humaines



Le Zero Trust est toujours notre stratégie

Votre stratégie de sécurité en matière d'IA repose-t-elle sur les principes du Zero Trust (vérification de chaque requête, surveillance de chaque flux de données, octroi d'accès en



Pour combler cette lacune, l'entreprise doit rapprocher la couche protocolaire de la couche d'identité afin que les identifiants, les périmètres d'accès et les autorisations des agents soient soumis au même niveau d'exigence que ceux des utilisateurs humains.

©2026 Cybersecurity Insiders. Tous droits réservés.

La plupart des systèmes de sécurité basés sur l'IA reposent sur la confiance

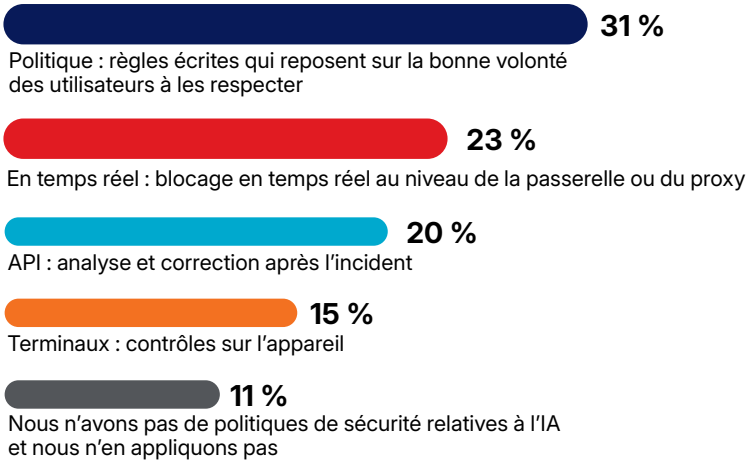
Le modèle Zero Trust couvre les identités humaines, mais laisse les agents d'IA et les NHI largement hors de tout cadre réglementaire. La question qui se pose concernant cette lacune est d'ordre pratique : lorsqu'un outil d'IA enfreint une règle ou qu'un agent prend une décision risquée, quel mécanisme de contrôle intervient concrètement ? Cette enquête dresse un tableau complet des mesures de contrôle. 31 % des entreprises assurent la sécurité de l'IA en s'appuyant sur des politiques écrites et sur leur respect par les employés. 20 % d'entre elles complètent cette approche par une analyse a posteriori des API, ce qui permet de détecter les violations une fois les opérations terminées. Les contrôles basés sur les terminaux représentent 15 %, et les mesures d'application des règles en temps réel 23 %. Les 11 % restantes n'ont aucune politique de sécurité en matière d'IA. La principale catégorie de mesures coercitives est celle du système fondé sur la confiance. La deuxième étape consiste à analyser ce qui s'est déjà passé, a posteriori.

Un examen plus approfondi des données laisse penser que même les 23 % d'entreprises qui déclarent appliquer des mesures de contrôle en temps réel utilisent probablement des outils peu adaptés. 42 % appliquent une logique du tout ou rien face aux applications d'IA : elles sont soit bloquées, soit autorisées sur l'ensemble des plateformes. Impossible, dans ce cadre, d'autoriser un compte professionnel tout en bloquant un compte personnel, ou encore de permettre une simple recherche tout en interdisant le téléchargement d'un modèle financier. Seules 19 % disposent de contrôles suffisamment fins pour distinguer les différentes actions réalisées au sein d'une application autorisée. Quand des contrôles en temps réel existent, ils ciblent avant tout les interventions humaines : le blocage des téléchargements de fichiers (48 %) et la détection des copier-coller (37 %) dominent, alors que la surveillance des publications de contenu (29 %) et le contrôle des envois de fichiers (25 %) sont à la traîne. Les appels d'API lancés par des agents, les échanges de jetons OAuth et les flux de données M2M ne sont pratiquement pas pris en compte.

Ce décalage dans l'exécution révèle un manque de cohérence. Lorsque le CASB, le moteur DLP et la politique d'accès fonctionnent chacun de leur côté, avec une vision fragmentée, aucun d'entre eux ne peut réellement appliquer la stratégie de sécurité telle qu'elle a été pensée. Voici un bon indicateur : quand une seule décision stratégique vous force à naviguer entre plus de deux consoles pour croiser les données, c'est le signe que la fragmentation empêche toute application efficace des règles. Pour y remédier, ces différents niveaux doivent être harmonisés de sorte qu'une seule évaluation puisse intégrer à la fois la classification du contenu, l'identité de l'utilisateur et le type d'instance d'IA, et ce, avant toute exécution d'une opération.

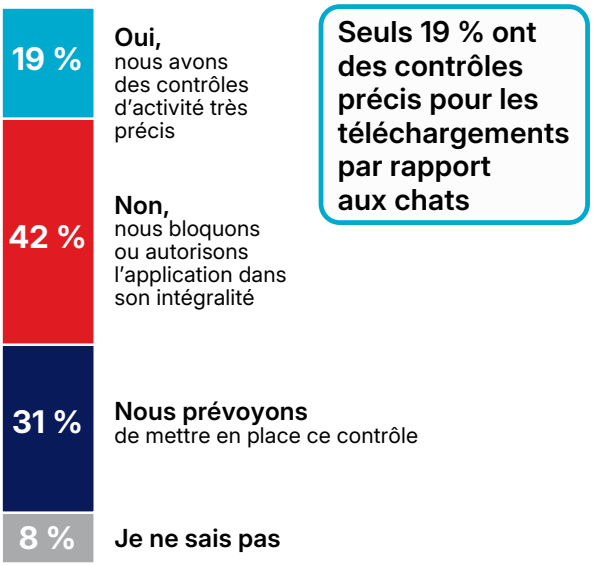
L'application des règles se fait principalement après coup

Comment vos politiques de sécurité en matière d'IA sont-elles principalement mises en œuvre ?



Les contrôles manquent encore de précision

Appliquez-vous des règles différentes pour les « téléchargements » et le « chat » ?



Seuls 19 % ont des contrôles précis pour les téléchargements par rapport aux chats

Les approches classiques de sécurité périmétrique ne suffisent plus, car la sécurité de l'IA doit être pensée en profondeur, et non simplement plaquée sur des modèles existants. Elle repose sur l'application, en temps réel, de règles cloud natives qui évaluent l'identité, le contenu et le contexte dans un point de décision unique, avant toute exécution.

©2026 Cybersecurity Insiders. Tous droits réservés.

Quel est votre niveau de maturité en matière de sécurité de l'IA ?

Toutes ces lacunes se renforcent mutuellement. En effet, sans une visibilité claire, la prévention des pertes de données devient inefficace ; les agents livrés à eux-mêmes passent entre les mailles des contrôles d'accès ; et une mise en œuvre morcelée fragilise l'ensemble du dispositif, couche après couche. Le modèle de maturité présenté ci-dessous s'articule autour de six domaines essentiels de la sécurité de l'IA, déclinés en trois niveaux de préparation. Chaque cellule décrit les fonctionnalités à ce stade. Recherchez dans chaque ligne la description qui correspond à votre entreprise. Le domaine où le niveau de maturité est le plus bas représente votre maillon faible, et c'est là que le risque de défaillance est le plus élevé. C'est là que les investissements doivent être prioritairement orientés.

DOMAINES DE LA SÉCURITÉ DE L'IA	RÉACTIF	GÉRÉ	ADAPTATIF
Alignement de la gouvernance et des risques	Politiques sur papier. Application inégale.	Politiques appliquées aux outils d'IA gérés. Shadow AI hors de contrôle.	Politique intégrée aux contrôles techniques, en temps réel.
Visibilité et suivi de la situation	Visibilité partielle ou inexistante. Impossible de distinguer les instances personnelles des instances professionnelles.	Suivi de l'activité sur l'ensemble des solutions SaaS et des API gérées. Distinction entre les instances personnelles et les instances professionnelles.	Visibilité en temps réel sur l'ensemble des processus d'IA, qu'il s'agisse d'interactions entre agents ou de communications entre machines.
Protection des données et des actifs	Les contrôles basés sur des modèles échouent face à la transformation induite par l'IA.	La DLP a été étendue au trafic lié à l'IA, y compris les discussions et les requêtes. Détection sémantique en phase pilote.	Inspection sémantique de l'ensemble des flux de données d'IA.
Contrôle de l'accès et de l'exécution	Application des règles après exécution. Système basé sur la confiance pour l'application des règles.	Application en temps réel pour l'IA pilotée par l'humain. Les actions de l'agent sont enregistrées, non bloquées.	Application dynamique avant l'exécution, humaine et non humaine.
Détection et réponse	Surveillance basée sur les journaux. Aucune logique de détection spécifique au comportement guidé par l'IA.	Règles de détection des types connus d'utilisation abusive de l'IA. Confinement manuel.	Surveillance continue avec confinement automatisé pour l'ensemble des activités liées à l'IA.
Intégration architecturale et résilience opérationnelle	Fragmentée. Visibilité, protection et application des règles en silo.	Contrôles intégrés pour les solutions SaaS gérées. Lacunes dans le trafic des API et des agents.	Infrastructure unifiée capable de résister à l'automatisation et à la mise à l'échelle.

Interrogés sur leurs regrets concernant l'adoption de l'IA, 38 % des répondants auraient souhaité que la mise en place d'un cadre de gouvernance précède l'adoption de l'IA à grande échelle, et 25 % auraient souhaité investir plus tôt dans des mesures de contrôle de la visibilité. Seuls 7 % se déclarent satisfaits de leur approche actuelle, ce qui constitue l'indicateur de confiance le plus bas de l'ensemble de l'enquête.

Le changement est motivé par la pression

52 %
affirment que la réglementation impose des changements

47 %
déclarent qu'une violation entraîne des changements

©2026 Cybersecurity Insiders. Tous droits réservés.

Combler le fossé en matière d'exécution

Le modèle de maturité des fonctionnalités met en évidence les lacunes. Les paragraphes suivants détaillent les mesures les plus efficaces pour renforcer chaque vecteur de risque, en commençant par la visibilité, socle sur lequel reposent tous les autres contrôles.

1. **Comblez les lacunes en matière de visibilité de l'IA :** 94 % ont signalé des lacunes, et 88 % ne parviennent pas à distinguer les comptes personnels des comptes professionnels.
   Étendez la surveillance aux activités liées au trafic SaaS, API et M2M en commençant par distinguer clairement, au niveau des comptes, les comptes IA personnels des comptes professionnels, car c'est la condition préalable à toute mise en place de mesures fiables de protection des données (DLP), de contrôles d'accès et de pistes d'audit.

2. **Transformez les politiques en directives ayant force obligatoire :** 68 % agissent de manière réactive ; seuls 7 % interviennent en temps réel.
   Identifiez les trois cas d'utilisation de l'IA à plus haut risque dans votre environnement, intégrez des politiques applicables à ces cas dans les contrôles techniques et désignez un responsable pour chacun d'entre eux avant d'étendre la couverture à tous les autres cas d'utilisation de l'IA.

3. **Mettez en œuvre la protection sémantique des données :** 46 % échouent au test de transformation du contenu.
   Testez la transformation de contenu avec votre propre système DLP : prenez un document confidentiel, demandez à un outil d'IA de le reformuler, puis vérifiez si vos contrôles signalent le résultat. Cette opération sert de référence pour déployer une inspection sensible au contenu qui soit capable d'évaluer le sens au moment du transfert.

4. **Appliquez les règles avant l'exécution :** 23 % appliquent les règles en temps réel ; 9 % peuvent bloquer à l'avance une action risquée d'un agent.
   Vérifiez quels agents disposent actuellement d'un accès en écriture et mettez en place des procédures de validation pour toute opération impliquant la création de comptes, la modification des autorisations ou le transfert de données vers des systèmes externes.

5. **Modernisez la détection et le confinement :** 67 % s'appuient sur les journaux ou n'ont aucune visibilité sur les actions des agents ; 37 % ont déjà rencontré des problèmes opérationnels liés à l'IA.
   Définissez ce qui constitue un comportement anormal pour les actions des agents dans votre environnement et créez des règles de détection pour ces modèles. Mettez en place des procédures de confinement permettant d'intervenir au niveau de la couche de requête avant qu'une action ne soit menée à bien, plutôt que de créer un ticket une fois que le mal est fait.

6. **Réduisez la fragmentation des contrôles :** 42 % utilisent des contrôles binaires de type « tout ou rien » sans distinction selon le niveau d'activité ; seuls 14 % inspectent le trafic API avec la même rigueur que celle appliquée au trafic utilisateur.
   Harmonisez les solutions CASB, DLP et les politiques d'accès afin qu'une seule évaluation tienne compte de la classification du contenu, de l'identité de l'utilisateur et du type d'instance d'IA. Quand une seule décision stratégique vous force à naviguer entre plus de deux consoles pour croiser les données, c'est le signe que la fragmentation empêche toute application efficace des règles.

La sécurité de l'IA est désormais une discipline opérationnelle à part entière. Les dimensions de maturité sont définies, la séquence des dépendances est claire et les actions à mener sont concrètes. Il ne reste plus qu'à passer à l'action.

La gouvernance est en retard

68 %
réagissent ou créent des politiques de gouvernance et de sécurité pour les déploiements d'IA et les données

La visibilité est incomplète

94 %
n'ont pas une visibilité complète sur l'utilisation de l'IA

Les contrôles de données ne sont pas appliqués après la réécriture

Seulement 8 %
confirment avoir une détection sémantique de l'intention / du contenu

Les interceptions sont rares

Seulement 9 %
disposent d'une prévention intégrée pour les actions des API et des agents

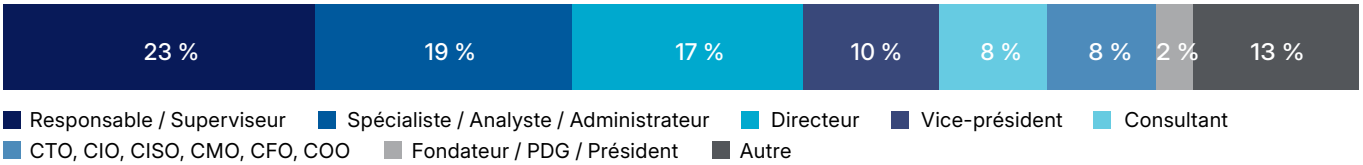
©2026 Cybersecurity Insiders. Tous droits réservés.

Méthodologie et données démographiques

Ce rapport s'appuie sur une enquête menée début 2026 auprès de 1 253 professionnels de la cybersécurité et de l'informatique. Les personnes interrogées sont des professionnels de la sécurité, des architectes et des responsables technologiques chargés de protéger les infrastructures d'entreprise, les environnements cloud et les applications basées sur l'IA dans un grand nombre de secteurs et d'entreprises de toutes tailles.

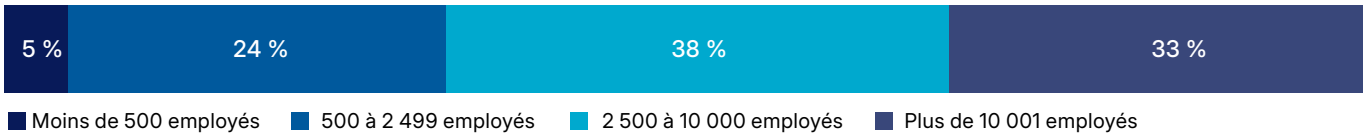
Cette étude examine la manière dont les entreprises sécurisent leurs déploiements d'IA. Elle analyse notamment la maturité de la gouvernance, la visibilité sur les activités d'IA, la protection des données, la gestion des identités non humaines et le contrôle des agents autonomes. Grâce à une méthode d'échantillonnage stratifié, l'enquête a atteint un niveau de confiance de 95 % avec une marge d'erreur de +/- 2,8 %.

NIVEAU DE CARRIÈRE

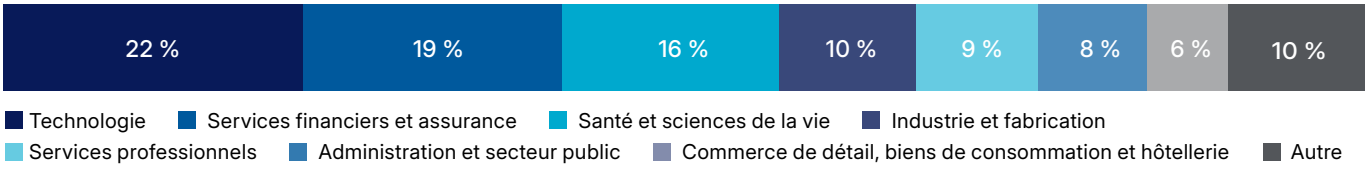


DÉPARTEMENT

TAILLE DE L'ENTREPRISE



SECTEUR D'ACTIVITÉ



©2026 Cybersecurity Insiders. Tous droits réservés.

Une citation rédactionnelle limitée (100 mots maximum et un graphique non modifié) est autorisée, à condition de mentionner clairement la source « **Cybersecurity Insiders, Rapport 2026 sur les risques et la maturité face à l'IA »** et d'inclure un lien visible vers cybersecurity-insiders.com.

Le sponsor du rapport est autorisé à citer les conclusions et à utiliser des graphiques ou des données spécifiques dans ses présentations et ses supports marketing à condition d'en mentionner explicitement la source. Le rapport complet, les données sous-jacentes ainsi que la méthodologie de recherche restent la propriété intellectuelle exclusive de Cybersecurity Insiders et ne peuvent être reproduits, redistribués ou intégrés à des travaux dérivés sans autorisation écrite préalable.

Ce rapport a été rédigé par Cybersecurity Insiders avec le soutien de **Netskope**. Autorisations : info@cybersecurity-insiders.com

À propos de Netskope

Netskope (NASDAQ : NTSK), leader dans le domaine de la sécurité et des réseaux modernes à l'ère du cloud et de l'IA, répond aux besoins des équipes chargées de la sécurité et des réseaux en offrant un accès optimisé et une sécurité en temps réel, basée sur le contexte, pour l'écosystème de l'IA. Sa solution couvre en outre l'ensemble des composants : agents, applications, outils, grands modèles de langage (LLM), employés, appareils et données.

Des milliers de clients, notamment plus de 30 entreprises du Fortune 100, font confiance à la plateforme Netskope One, son moteur Zero Trust et son puissant réseau NewEdge pour réduire les risques et obtenir une visibilité et un contrôle absolus sur les applications cloud, SaaS, web et privées. Cet outil permet d'assurer la sécurité tout en optimisant les performances, sans aucun compromis.

Pour en savoir plus, consultez :

netskope.com/fr/products/ai-security

©2026 Netskope, Inc. Tous droits réservés. Netskope, NewEdge, SkopeAI et le logo stylisé « N » sont des marques déposées de Netskope, Inc. Netskope Active, Netskope Cloud XD, Netskope Discovery, Cloud Confidence Index et SkopeSights sont des marques de Netskope, Inc. Toutes les autres marques appartiennent à leurs propriétaires respectifs. 03/2026 RR-971-2-FR

Cybersecurity
INSIDERS

ÉVALUEZ VOTRE NIVEAU DE MATURITÉ EN MATIÈRE DE SÉCURITÉ

Une étude indépendante révèle les lacunes qui influencent les stratégies de cybersécurité

Cybersecurity Insiders mène des études indépendantes fondées sur des enquêtes auprès de responsables et de professionnels de la cybersécurité dans le monde entier. Nos rapports révèlent les points faibles des stratégies de sécurité sur le terrain. Ils permettent ainsi aux entreprises d'évaluer leur maturité, d'identifier leurs lacunes et de hiérarchiser les mesures nécessaires pour y remédier.

Pour en savoir plus, consultez

cybersecurity-insiders.com

©2026 Cybersecurity Insiders. Tous droits réservés.

Avril 2026 // Version 1.7