Microsoft Security

Indice de la sécurité des données

Tendances, informations et stratégies de sécurisation des données et d'exploitation de l'IA générative

Rapport de 2024

Avant-propos

Alors que nous entamons notre seconde année d'exploration dans le domaine en pleine mutation de la sécurité des données, les défis que nous affrontons et les occasions qui se présentent n'ont jamais été aussi intenses et cruciaux. L'année écoulée a révélé une recrudescence marquée des incidents liés à la sécurité des données. Dans cette ère dominée par la donnée, les stratégies et les outils mis en place pour en assurer la protection se transforment à un rythme effréné.

Cette année, notre étude se penche sur une nouvelle dimension : le rôle et l'influence de l'IA générative sur les stratégies de sécurité des données.

L'IA suscite un intérêt considérable à l'échelle mondiale, notamment pour ses capacités inédites à stimuler l'innovation et à optimiser l'efficacité. Face à ce potentiel immense, les entreprises expriment cependant des inquiétudes, notamment quant aux risques pour la sécurité des données et les nouvelles responsabilités qu'elles imposent aux équipes dédiées à cette mission. Nous pensons que l'IA offre aux entreprises la possibilité de renforcer rapidement les pratiques essentielles en matière de sécurité des données, ce qui aide à limiter les risques de partage excessif, de fuites d'information, et à développer des processus soutenant une adoption prudente et réfléchie de l'IA. L'IA permet également d'approfondir les pratiques de sécurité des données en détectant les risques cachés et les failles potentielles dans la protection, tout en proposant des stratégies de prévention et en accélérant la détection et la résolution des incidents de sécurité.

Notre recherche vise à fournir aux responsables de la sécurité des données des analyses et des conseils utiles, afin qu'ils puissent accompagner leurs équipes dans une adaptation sereine de leur stratégie, pour protéger l'usage de l'IA et l'intégrer dans leurs plans de sécurité de manière cohérente. Aussi impressionnante que soit son ampleur et son potentiel, l'IA s'inscrit dans la lignée des transformations qui ont marqué les entreprises au cours des dernières années. Le travail hybride, le nuage et la mobilité ont eux aussi révélé l'impérieuse nécessité d'une visibilité accrue pour réduire les risques et optimiser l'effet de l'organisation. À la lumière de ces enseignements, garantir la protection adéquate des données en interaction avec l'IA et employer celle-ci pour renforcer la sécurité des données permettra aux équipes de gagner en productivité, en résilience et en agilité face aux défis de demain.

Nous vous invitons à découvrir nos dernières analyses, avec l'espoir que celles-ci contribueront à renforcer votre posture de sécurité, à favoriser l'intégration de l'IA, et à définir une stratégie de protection des données exhaustive, ouvrant ainsi la voie à une innovation accrue et à un avenir plus sécurisé pour tous.

Rudra Mitra
vice-président
Sécurité et conformité des données Microsoft

Présentation

Chaque année, les entreprises enregistrent en moyenne 156 incidents relatifs à la sécurité des données. L'effet de ces événements demeure une préoccupation constante pour les décideurs en matière de sécurité. Et cela avec raison : car un seul incident peut causer des dégâts substantiels, tant financiers que réputationnels, dans un paysage où les menaces évoluent sans cesse, avec des attaquants déterminés à exploiter la moindre faille. Ce risque s'amplifie avec l'essor rapide de l'IA. En effet, sans les protections et les mesures de sécurité adéquates, les utilisateurs peuvent, sciemment ou non, exposer des données sensibles de l'entreprise – qu'il s'agisse d'informations relatives aux employés et aux clients, de propriété intellectuelle, de prévisions financières ou de données opérationnelles. Alors que les entreprises explorent de nouvelles manières de préserver la confidentialité de leurs données sensibles, nombre de décideurs s'orientent vers l'essor impressionnant de l'intelligence artificielle.

Le défi que représente l'IA est d'une double nature. Près de deux tiers des entreprises admettent que leurs employés recourent à des outils d'IA non autorisés; il devient dès lors crucial de veiller à ce que ces instruments soient employés dans des conditions de sécurité optimales. Par ailleurs, l'IA peut devenir un atout précieux dans le cadre d'une stratégie de protection des données sophistiquée.

Les solutions de sécurité des données, renforcées par l'IA, jouent d'ores et déjà un rôle central dans la détection des menaces et la réponse en temps réel, optimisant la vitesse et la précision des programmes de sécurité, tout en permettant de prévenir les incidents de sécurité avant même qu'ils ne surviennent. En plus de s'appuyer sur la puissance de l'IA, les entreprises doivent s'attacher à maîtriser les risques inhérents à cette technologie afin de repérer, à la vitesse de la machine, des schémas complexes parfois difficiles à saisir et à interpréter par l'humain, et pour contrer des cyberattaques d'une sophistication croissante.

En 2023, Microsoft a mandaté une agence de recherche indépendante, Hypothesis, pour réaliser une étude internationale auprès de plus de 800 professionnels de la sécurité des données. Cette initiative visait à lancer un indice de sécurité des données, répondant aux attentes de nos partenaires et clients, et aidant les dirigeants à bâtir leurs propres stratégies de sécurité.

En 2024, ce rapport s'enrichit de nouvelles analyses issues d'une enquête internationale élargie, menée auprès de plus de 1 300 experts en sécurité des données. Si les données dévoilent des tendances familières dans les marchés observés, elles nous révèlent aussi de nouvelles perspectives sur les pratiques et les dynamiques mondiales en matière de sécurité et d'IA.

hypothesis Microsoft Security

Principaux constats

1

Le paysage de la sécurité des données demeure fragmenté, renforçant le besoin de stratégies cohérentes en dépit des risques – anciens et nouveaux – induits par l'utilisation de l'IA

Les entreprises déclarent une confiance et une satisfaction élevées envers leurs dispositifs de sécurité des données. Néanmoins, la gravité des incidents liés à la sécurité continue de croître, exacerbée par l'écart persistant entre leurs politiques actuelles et l'adoption croissante d'applications basées sur l'IA. Face à ces défis, de nombreuses entreprises continuent de recourir à une pluralité d'outils de sécurité, augmentant ainsi leur exposition et leur vulnérabilité globales.

2

À mesure que les utilisateurs finaux adoptent toujours plus d'applications IA, la protection des données sensibles devient plus cruciale, nécessitant une visibilité accrue et des contrôles renforcés

Les outils d'IA s'ancrent dans les opérations quotidiennes, poussant les entreprises à reconsidérer leurs préoccupations en matière de sécurité. Elles prennent acte de la nécessité de renforcer leurs défenses et s'engagent à anticiper les incidents suscités par l'IA; néanmoins, l'usage non autorisé de ces outils souligne l'urgence d'une vigilance accrue.

3

Les décideurs conservent une vision optimiste du potentiel de l'IA pour renforcer leurs dispositifs de sécurité

Les entreprises investissent activement dans des technologies de sécurité intégrant l'IA afin d'améliorer leurs capacités de détection et de réaction. L'IA se montre apte à repérer les données non sécurisées, à proposer des solutions de protection, et à analyser et résoudre plus promptement les incidents de sécurité, offrant ainsi aux équipes la possibilité de se concentrer davantage sur des missions stratégiques. L'intégration de l'intelligence artificielle renforce la confiance des entreprises dans leur stratégie globale de sécurité des données, en accroissant leur capacité à répondre rapidement et avec précision aux incidents.

1

Le paysage de la sécurité des données demeure fragmenté, renforçant le besoin de stratégies cohérentes en dépit des risques – anciens et nouveaux – induits par l'utilisation de l'IA

Cependant, un décalage persiste entre la confiance des décideurs en matière de sécurité des données et le niveau réel de protection offert par leurs pratiques

Comme indiqué en 2023, la majorité des décideurs se montrent optimistes quant à leurs stratégies de sécurité : en 2024, 74 % se déclarent satisfaits de leurs solutions. Ils se disent rassurés par leur aptitude à suivre et à gérer les informations sensibles : 88 % affirment connaître l'emplacement de la majorité de leurs données sensibles, et 85 % estiment que celles-ci sont correctement classifiées et étiquetées. Nombreux sont ceux qui expriment également leur confiance dans leurs dispositifs de défense : 79 % se disent capables de prévenir l'exfiltration de données, et 76 % adoptent une approche proactive, plutôt que réactive, en matière de sécurité.

Toutefois, cette assurance vacille à mesure que la gravité des incidents s'accentue. **Le nombre moyen d'incidents de sécurité annuels reste élevé, bien qu'il soit passé de 166 en 2023 à 156 en 2024, tandis que la gravité des incidents a crû, avec 27 % d'incidents graves en 2024, contre 20 % l'année précédente.**

156

incidents liés à la sécurité des données

27 %

des incidents considérés comme graves (hausse de 20 % en 2023)

63 %

des alertes sont examinées chaque jour

« L'emplacement de la plateforme logicielle, les sites de stockage de données et les personnes autorisées compliquent la sécurité et la gestion des informations de nos outils d'IA et de nos prestataires. Nous avons pour mission de protéger et de régir plus d'un siècle de données, conformément aux exigences légales de chaque juridiction où nous sommes présents », déclare un responsable de la gouvernance de l'information au sein d'un fabricant d'équipements lourds.

La montée en gravité des incidents a provoqué une hausse du volume d'alertes de sécurité. **Les entreprises doivent désormais traiter en moyenne 66 alertes par jour, contre 52 en 2023.** Ce chiffre fluctue selon la taille des organisations : les entreprises de taille moyenne (500 à 999 employés) et les grandes entreprises (1 000 à 4 999 employés) reçoivent en moyenne 56 alertes quotidiennes, contre 80 pour les très grandes entreprises (plus de 5 000 employés).

Face à un tel flux d'alertes, la plupart des entreprises peinent à suivre le rythme. En moyenne, les équipes de sécurité examinent 63 % des alertes quotidiennes, parmi lesquelles 35 % s'avèrent être des faux positifs. Ce décalage entre le contrôle perçu et la réalité opérationnelle entraîne un épuisement des équipes, contraintes de vérifier et d'améliorer sans cesse leurs protections, tout en redoutant que des incidents graves ne passent inaperçus.

Pour contrer les risques, anciens et nouveaux, associés à l'usage croissant d'outils d'IA, les entreprises ont besoin de stratégies de sécurité plus robustes et cohérentes

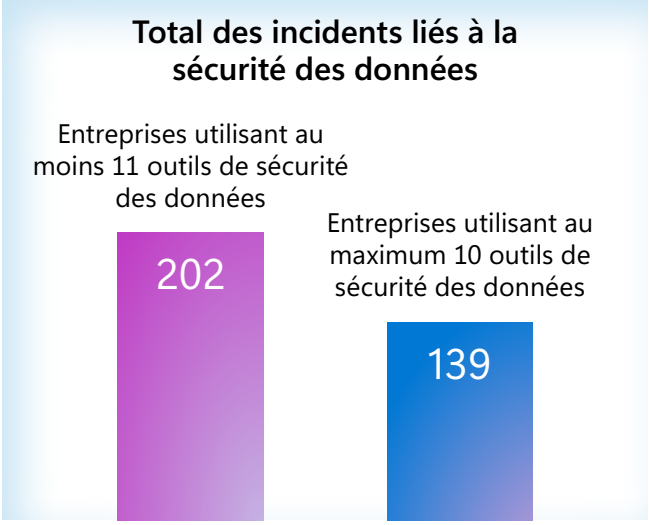
Malgré la multiplication des outils disponibles, de nombreux décideurs admettent que l'abondance n'est pas toujours synonyme d'efficacité. Ainsi, 21 % d'entre eux identifient leur principal défi dans le manque de visibilité intégrale et de compréhension partagée des risques, résultant de l'utilisation d'outils épars[1].

La plupart des décideurs (82 %) s'accordent à dire qu'une plateforme complète et totalement intégrée est supérieure à la gestion de plusieurs outils isolés. **En moyenne, ils jonglent avec une douzaine de solutions de sécurité des données, ce qui intensifie une complexité qui expose davantage à la vulnérabilité.** Cela est particulièrement vrai pour les plus grandes entreprises : en moyenne, les entreprises de taille moyenne utilisent 9 outils et les grandes entreprises 11, contre 14 pour les très grandes entreprises.

Les données révèlent une forte corrélation entre la multiplication des outils de sécurité et la recrudescence des incidents liés à la sécurité des données. Les moyennes et grandes entreprises signalent environ 89 incidents par an, tandis que les très grandes entreprises en rapportent jusqu'à 248. Cette disparité frappante souligne le risque élevé auquel sont confrontées les grandes structures, bien que celles-ci affichent une confiance déclarée dans l'efficacité de leurs mesures de sécurité.

En 2024, les entreprises utilisant un nombre plus élevé d'outils de sécurité (onze ou plus) ont enregistré en moyenne 202 incidents, contre 139 pour celles qui en comptent dix ou moins.

1. Enquête de septembre 2024 sur les décideurs chargés de la sécurité, de la gouvernance, de la conformité et de la confidentialité des données, commandée par Microsoft à l'agence MDC Research



La fragmentation des solutions complique la compréhension globale du niveau de sécurité des données d'une entreprise : les données restent cloisonnées et les flux de travail disjoints, rendant difficile une visibilité complète des risques. Lorsque les équipes de sécurité des données recourent à des outils non intégrés, elles se voient dans l'obligation de mettre en place des processus pour corréler les données et obtenir une vue d'ensemble cohérente des risques, créant ainsi des zones d'ombre et rendant plus ardues la détection et l'atténuation efficaces des risques.

La hausse des incidents de sécurité liés aux applications d'intelligence artificielle suscite une inquiétude grandissante : ces incidents ont presque doublé, passant de 27 % en 2023 à 40 % en 2024. Cette progression est alimentée par une augmentation des attaques de logiciels malveillants et de rançongiciels, qui sont passées de 50 % en 2023 à 59 %. Les attaques liées aux applications d'IA mettent en péril non seulement les données sensibles, mais compromettent également la robustesse des systèmes d'IA eux-mêmes, accentuant la complexité d'un paysage de sécurité déjà fragmenté. En somme, il devient impérieux d'adopter des stratégies de sécurité des données plus cohérentes et renforcées, capables d'anticiper et de contenir les risques, tant anciens qu'émergents, notamment ceux associés aux outils d'IA.

La voie à suivre

Face à l'ampleur croissante des incidents de sécurité des données, l'IA pourrait jouer un rôle décisif en offrant des réponses adaptées à ces nouveaux enjeux. Les entreprises les plus avancées intègrent des systèmes de sécurité des données fondés sur l'IA, favorisant la hiérarchisation des incidents, l'automatisation de la classification des données et l'optimisation des politiques de protection existantes. L'IA peut analyser et synthétiser en temps réel la gravité potentielle des alertes, offrant aux équipes de sécurité des informations clés pour une réaction rapide et une réduction du temps consacré aux faux positifs. Ce processus de simplification des flux de travail permet aux équipes de sécurité de se concentrer sur des améliorations stratégiques de la sécurité et des actions proactives.

2

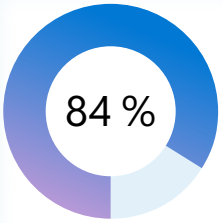
À mesure que les utilisateurs finaux adoptent toujours plus d'applications IA, la protection des données sensibles devient plus cruciale, nécessitant une visibilité accrue et des contrôles renforcés

L'IA devient ainsi un outil incontournable des opérations quotidiennes, et les entreprises doivent s'adapter à cette nouvelle réalité avec anticipation

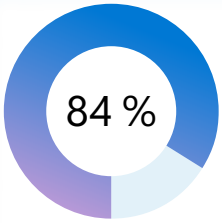
L'adoption rapide des outils d'IA par les employés a redéfini la manière dont les entreprises envisagent la sécurité des données. Bien que l'IA transforme la productivité et les flux de travail, elle peut, à l'instar de toute technologie émergente, amplifier les risques existants ou en introduire de nouveaux, nécessitant une approche renouvelée de la protection des informations sensibles. Ainsi, les entreprises continuent de chercher un équilibre subtil dans ce paysage en perpétuelle mutation. Un responsable en ingénierie et analyse de données dans le secteur des transports résume : « Nous surveillons les données avec une attention accrue dans le cadre de l'IA. Il nous faut trouver un juste milieu entre productivité et sécurité, précision et confidentialité. »

La confiance dans une utilisation sécurisée de l'IA par les employés demeure mitigée. La majorité (84 %) des entreprises souhaiterait ressentir une plus grande assurance dans la maîtrise et l'exploration de la saisie de données. Alors que seuls 22 % des organisations se disent pleinement confiantes dans leurs capacités de sécurisation des données, la plupart (59 %) n'expriment qu'une « grande confiance », révélant ainsi un potentiel d'amélioration considérable. Une grande partie des entreprises (86 %) admettent qu'elles aimeraient entretenir un sentiment plus favorable vis-à-vis de la gestion et de la découverte des données générées par les outils d'IA.

À mesure que l'IA prend une place centrale dans la productivité quotidienne, son usage intensif s'accompagne d'inquiétudes croissantes quant aux incidents de sécurité des données. **Près d'un tiers (31 %) des organisations anticipent une recrudescence des incidents liés à la sécurité des données en raison de l'utilisation de l'IA par leurs employés, et 84 % reconnaissent la nécessité de renforcer leur protection contre ces risques.** Ces inquiétudes sont particulièrement élevées au sein des plus grandes entreprises : alors que seulement 26 % des entreprises de taille moyenne, et 29 % des grandes entreprises s'attendent à une augmentation des incidents de sécurité des données liés à l'IA, une part nettement plus élevée, c'est-à-dire 36 % des très grandes entreprises, prévoit cette augmentation.



aimeraient se sentir davantage confiants quant à la gestion et la découverte des saisies de données dans les applications et outils d'IA



reconnaissent qu'elles doivent en faire plus pour se protéger contre l'utilisation risquée des applications et des outils d'IA par les employés

L'utilisation non autorisée de l'IA est largement répandue

40 % des entreprises rapportent que leurs applications d'IA ont déjà été compromises lors d'incidents de sécurité. Encore une fois, cette part est plus élevée au sein des plus grandes entreprises : les entreprises de taille moyenne signalent un taux d'incidents de 36 % et les grandes entreprises de 38 %, mais les très grandes entreprises sont celles qui en signalent le plus (44 %).

Cette utilisation non autorisée survient souvent lorsque des employés se connectent avec des informations d'identification personnelles ou utilisent des appareils personnels pour des tâches professionnelles. **En moyenne, 65 % des entreprises reconnaissent que leurs employés se tournent vers des outils d'IA non autorisés.** Les cas de recours à des outils d'IA non autorisés se répartissent ainsi :

- Dans 53 % des cas, les employés se connectent avec des identifiants personnels pour des besoins professionnels;
- 48 % des cas impliquent l'utilisation d'un appareil personnel dans un cadre professionnel;
- 47 % des cas concernent l'exploitation d'informations d'identification professionnelles dans un contexte personnel

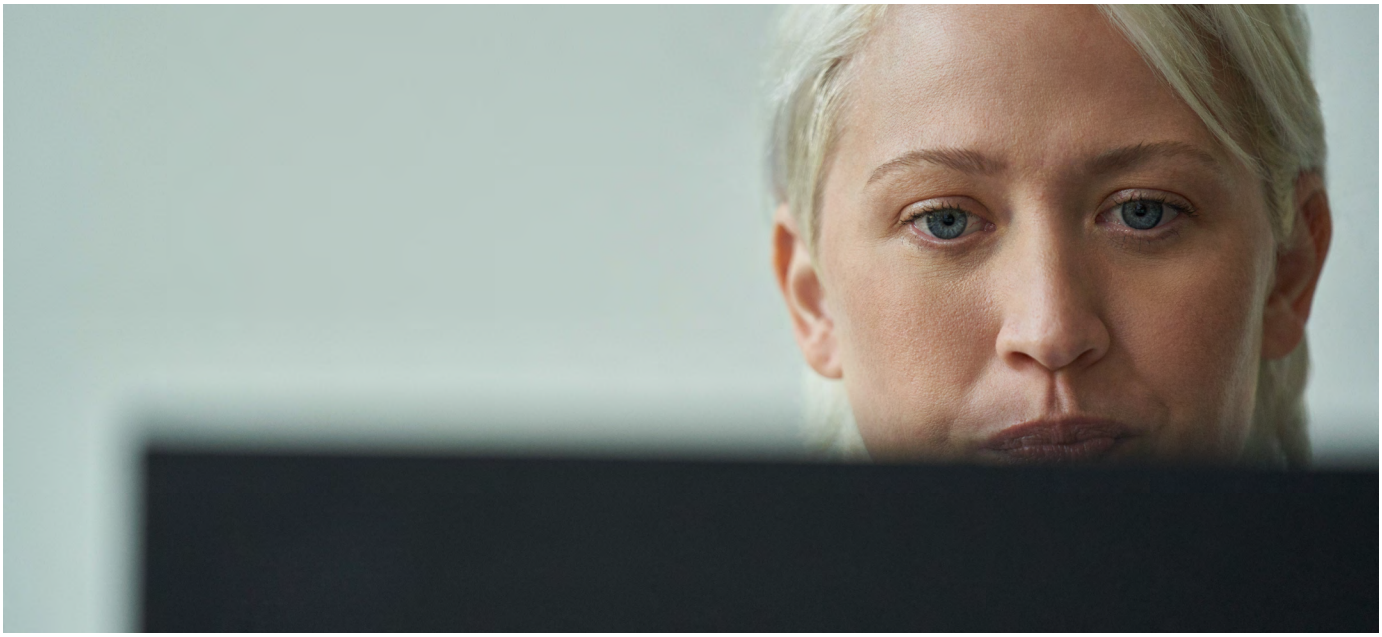
La moitié des entreprises expriment une préoccupation quant au manque de contrôles pour détecter et limiter les risques associés à l'usage non sécurisé des applications d'IA par leurs employés. Cette inquiétude varie selon la taille des entreprises : 43 % des entreprises de taille moyenne, 50 % des grandes entreprises et 54 % des très grandes structures se disent préoccupées par leur capacité à gérer ces risques.

Face à la montée en puissance de l'IA, des mesures de sécurité des données plus strictes sont nécessaires

Alors que l'IA s'impose davantage dans les opérations quotidiennes, les entreprises prennent conscience de l'importance de renforcer leur protection. **Près de 96 % des entreprises s'inquiètent de l'usage de ces outils par leurs employés, mais sont presque aussi nombreuses à envisager des investissements pour apaiser ces craintes.**

« Notre priorité sera de garder une longueur d'avance sur l'IA La sécurité s'articulera autour de la réduction du volume des données et d'une surveillance plus pointue. Du côté de l'IA, il faut davantage de données pour rendre les modèles plus représentatifs et repérer les biais. Alors, comment y parvenir? », s'interroge un responsable en ingénierie, architecture et analyse de données dans le secteur des transports. Une majorité de décideurs (87 %) se disent prêts à consacrer temps et ressources à la formation des employés pour une utilisation sécurisée des outils d'IA. **C'est également parce que 85 % d'entre eux estiment indispensable que les employés s'approprient ces outils pour préserver leur compétitivité.**

Presque toutes les entreprises sondées (93 %) ont déjà entamé la phase de création ou de mise en place de dispositifs de contrôle liés à l'usage de l'IA, bien que nombre d'entre elles n'en soient encore qu'aux premières étapes. À peine 39 % d'entre elles ont pleinement instauré des contrôles de sécurité des données adaptés à l'IA, tandis que 24 % ont déjà formulé des stratégies en ce sens, sans pour autant les avoir encore appliquées. Un vice-président en sécurité des données, œuvrant dans le secteur hôtelier, a confié : « Nous devons nous conformer aux contrôles de l'IA, tout en acceptant et en adoptant son potentiel. Elle simplifie notre travail et nous aide à accroître notre efficacité. »



Tandis que les entreprises avancent pour protéger leurs données sensibles de toute exploitation abusive au sein des applications d'IA, elles se doivent, sans conteste, de déployer des dispositifs de contrôle plus exhaustifs. Actuellement, 43 % des entreprises œuvrent à prévenir l'insertion de données sensibles dans des applications d'IA, tandis que 42 % surveillent l'ensemble des actions et contenus dans ces applications, en vue de potentielles enquêtes ou d'une réponse rapide en cas d'incident. Par ailleurs, 42 % des entreprises bloquent l'accès aux outils non autorisés, tandis qu'un pourcentage similaire investit dans la formation de leurs employés pour un usage sécurisé de l'IA.

Les entreprises confrontées à un usage non autorisé de l'IA par leurs employés requièrent plus de contrôles spécifiques. **Parmi celles-ci, 42 % estiment essentiel de pouvoir identifier les utilisateurs à risque en se fondant sur les requêtes d'IA, contre 30 % pour celles où les employés respectent les autorisations d'usage. De surcroît, 40 % des entreprises faisant face à une utilisation non autorisée de l'IA ont besoin de dispositifs pour gérer le cycle de vie des données (notamment des protocoles de conservation et de suppression), contre 27 % pour les entreprises non concernées par ce problème.**

Les cinq principaux contrôles d'IA nécessaires

Empêcher le transfert de données sensibles vers l'IA	43 %
Enregistrer l'ensemble des activités et contenus des outils d'IA pour d'éventuelles enquêtes ou réponses aux incidents	42 %
Bloquer l'accès des utilisateurs à des outils d'IA non autorisés	42 %
Former les employés à une utilisation sécurisée des outils d'IA	42 %
Détecter les utilisateurs à risque en se basant sur les requêtes d'IA	41 %

La voie à suivre

Pour renforcer leur niveau de sécurité des données, les équipes ont besoin d'un cadre de contrôles complet pour découvrir, protéger et administrer leurs données dans le cadre des applications d'IA. Voici trois stratégies majeures à adopter par les équipes :

Renforcer la visibilité autour de l'usage des applications d'IA et du flux de données dans ces applications : faites usage d'outils de sécurité des données capables de détecter l'usage des applications d'IA. Ces outils fournissent une vue d'ensemble détaillée qui incluent les applications d'IA employées, leurs profils de risque, et des informations comme les contrôles de sécurité des données en place et la conformité réglementaire. Exploitez des outils capables de classifier de manière cohérente les données sensibles lors des interactions avec l'IA et d'observer les tendances relatives à la circulation des données dans les applications d'IA.

Élaborer et renforcer les stratégies : concevez des stratégies fondées sur les enseignements tirés de l'analyse des données. Ces stratégies peuvent comporter des instructions pour les applications d'IA autorisées et des mesures pour bloquer ou restreindre l'utilisation d'applications non autorisées par les employés. Même au sein des applications d'IA autorisées, des stratégies fines peuvent être élaborées pour permettre la circulation des données non sensibles, tout en restreignant l'usage des données sensibles et critiques pour l'entreprise. Cela pourrait inclure, par exemple, le blocage d'actions spécifiques, comme l'insertion de données sensibles dans des outils d'IA sur navigateur, afin de garantir la sécurité des informations.

Évaluer régulièrement les risques et ajuster les stratégies : générez régulièrement des rapports indiquant les niveaux de risque des applications d'IA utilisées, les tendances sur la manière dont les données sensibles transitent par ces applications, ainsi que l'activité des utilisateurs autour de ces applications. Il est ainsi possible d'évaluer l'ensemble des risques et de prendre des décisions éclairées sur les politiques les plus pertinentes en matière de sécurité des données.

3

Les décideurs conservent une vision optimiste du potentiel de l'IA pour renforcer leurs dispositifs de sécurité

Les enquêtes liées à la sécurité des données reposent fortement sur l'IA

La grande majorité des entreprises, soit 88 %, investissent déjà dans l'intelligence artificielle pour affiner leurs efforts de détection et de réponse : détecter les données sensibles, déceler les activités anormales et protéger automatiquement les informations à risque. **Elles sont 77 % à estimer que l'IA accélérera ces processus, et 76 % pensent qu'elle augmentera la précision de leurs stratégies de détection et de réponse.**

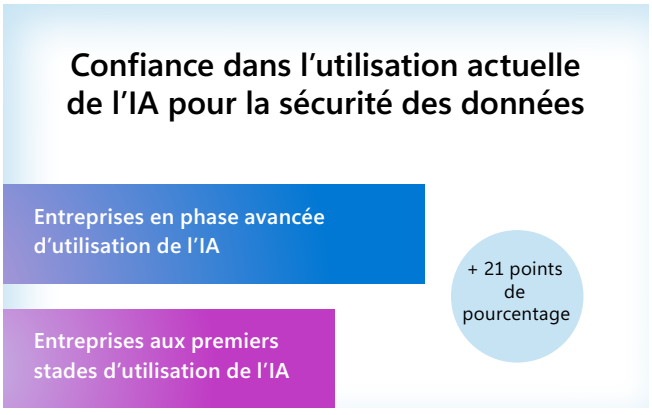
Toutefois, 73 % des décideurs demeurent inquiets quant à l'utilisation croissante de l'IA pour renforcer la sécurité des données. Malgré ces craintes, 50 % assurent que cela ne les a pas empêchés de recourir à l'IA pour protéger leurs informations. Seuls 23 % confessent que leurs appréhensions ont freiné cette adoption. Dans l'ensemble, une majorité écrasante de 93 % des entreprises envisage au moins d'utiliser l'IA pour sécuriser davantage leurs données, en dépit des inquiétudes persistantes.

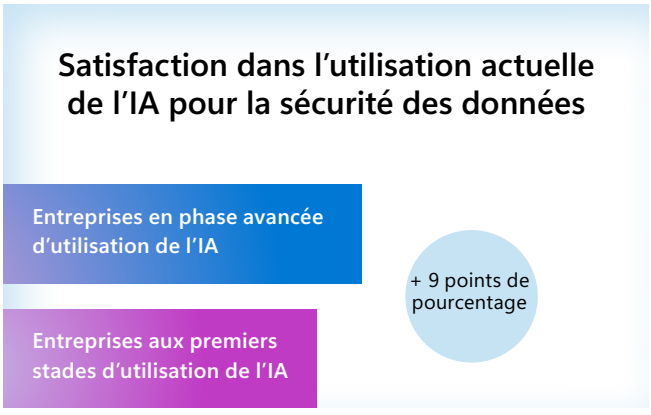
Utiliser l'IA pour la sécurité des données procure une visibilité, une confiance et une satisfaction accrues

L'un des atouts majeurs de l'IA réside dans sa capacité à offrir une visibilité accrue entre les systèmes, répondant ainsi à l'une des préoccupations centrales des décideurs : localiser et classifier efficacement les données (20 %)[1]. Ainsi, 88 % des décideurs pensent que l'intégration de l'IA dans les solutions de sécurité des données offrira aux équipes une visibilité élargie, permettant aux entreprises de traiter et d'analyser bien plus de données qu'avec d'autres solutions. Pour les entreprises de taille moyenne, l'accent est mis principalement sur la réduction des risques à court terme, notamment en limitant les erreurs humaines dans les processus de sécurité. En effet, 43 % d'entre elles placent la réduction des risques liés aux erreurs humaines en tête de leurs priorités, contre seulement 37 % chez les très grandes entreprises.

En revanche, ces dernières privilégient une approche plus avancée, orientée vers les risques à long terme et la nécessité d'adaptation continue. Cette sophistication accrue permet aux équipes de sécurité des données de mieux s'adapter aux menaces en constante évolution, une priorité pour 49 % des très grandes entreprises et pour 43 % des entreprises de taille moyenne.

Dans l'ensemble, les entreprises les plus avancées dans l'utilisation de l'IA pour sécuriser leurs données affichent des niveaux de confiance et de satisfaction bien supérieurs quant à leurs stratégies de sécurité. **Parmi celles ayant atteint un stade avancé d'intégration de l'IA, 90 % se disent extrêmement ou très confiantes dans l'efficacité de cette technologie pour renforcer la sécurité des données, contre 69 % pour celles qui en sont à un stade moins avancé. De même, 76 % des entreprises avec une utilisation avancée de l'IA se déclarent satisfaites de leurs solutions de sécurité, contre seulement 67 % parmi celles encore au début de leur adoption.**





1. Enquête de septembre 2024 sur les décideurs chargés de la sécurité, de la gouvernance, de la conformité et de la confidentialité des données, commandée par Microsoft à l'agence MDC Research

Les organisations réduisent le nombre d'incidents de sécurité des données et améliorent la gestion des alertes grâce à l'IA

Les entreprises qui exploitent l'IA pour sécuriser leurs données constatent une réduction des incidents et une meilleure gestion des alertes. **En moyenne, les entreprises ayant intégré des outils de sécurité basés sur l'IA reçoivent 47 alertes quotidiennes, contre 79 pour celles n'ayant pas encore adopté ces solutions. Les entreprises ayant recours à l'intelligence artificielle réussissent à examiner 66 % de leurs alertes quotidiennes, alors que celles n'employant pas l'IA ne parviennent qu'à en analyser 60 %.**

Par ailleurs, celles qui s'appuient sur l'IA pour renforcer la sécurité de leurs données se montrent plus enclines à utiliser cette technologie pour atténuer les risques (56 % contre 26 %). La diminution du volume des alertes, combinée à la capacité accrue d'atténuation fournie par l'IA, semble avoir un effet notable sur le nombre total d'incidents liés à la sécurité des données. Les entreprises ayant adopté l'IA pour sécuriser leurs données constatent une réduction de 65 % des incidents de sécurité par rapport à celles qui n'intègrent pas l'IA dans leurs processus de protection.

L'effet majeur de l'IA devrait se refléter dans les capacités de réponse

En matière de détection, 33 % des décideurs prévoient que l'IA les aidera à détecter les comportements anormaux, tandis que 23 % anticipent qu'elle facilitera l'investigation des incidents potentiels de sécurité. De plus, 22 % considèrent que l'IA pourrait proposer des recommandations pour renforcer la protection de leurs environnements de données.

Cependant, pour les décideurs, l'apport principal de l'IA semble devoir résider dans les capacités de réponse. En effet, 34 % d'entre eux estiment que l'IA pourrait automatiquement empêcher le partage inapproprié de données sensibles, tandis que 32 % comptent sur elle pour protéger les informations à risque. De plus, 26 % jugent que l'IA contribue à atténuer les risques de sécurité des données et à instaurer des contrôles adéquats, et un pourcentage identique prévoit que l'IA pourrait signaler d'elle-même les comportements à risque des utilisateurs.

La voie à suivre

L'intégration de l'IA aux solutions de sécurité des données permettrait de fournir aux équipes des conseils en temps réel, des capacités de synthèse et une prise en charge du langage naturel, soulignant ainsi des zones potentiellement négligées. Elle pourrait également accélérer les investigations et renforcer l'expertise des équipes de sécurité. Voici comment ces fonctionnalités pourraient avoir un effet tangible :

Synthèse des alertes : Les équipes en charge des investigations peuvent vite être découragées par la profusion de sources à analyser et la complexité des règles stratégiques. L'IA, intégrée à la protection contre la perte de données (DLP) et à la gestion des risques internes (IRM), permet à ces équipes d'obtenir rapidement un résumé des alertes, notamment leur origine, les règles de stratégie concernées et des informations sur les utilisateurs à risque, facilitant ainsi l'identification des données sensibles compromises et des utilisateurs associés.

Communications contextuelles : Pour se conformer aux réglementations relatives aux communications d'affaires, les entreprises doivent souvent analyser minutieusement les violations. L'IA peut aider les équipes de sécurité des données en comparant les contenus avec les politiques et les réglementations de l'entreprise, mettant en évidence les communications à haut risque susceptibles de provoquer un incident de sécurité.

Langage naturel vers requête par mot-clé : Les processus de recherche peuvent se révéler complexes et chronophages durant les enquêtes, nécessitant souvent un langage de requête par mot-clé. L'IA permet aux équipes de sécurité des données d'utiliser des recherches en langage naturel, simplifiant ainsi les premières étapes et facilitant des investigations plus poussées.

Recommandations finales

1 Préservez-vous des incidents de sécurité en adoptant une plateforme intégrée

Adopter une plateforme de sécurité des données pleinement intégrée confère une stratégie plus sûre et mieux harmonisée, adaptée à un environnement en perpétuelle mutation. Ce choix réduit la complexité, améliore la visibilité et, par là même, renforce la protection. Une approche intégrée permet aux entreprises de renforcer leur sécurité des données en centralisant les contrôles pertinents et en offrant une vision unifiée des données, des utilisateurs et des activités, ce qui perfectionne et simplifie à la fois la détection et la gestion des risques liés aux informations sensibles. Pour 82 % des entreprises, une plateforme intégrée se révèle plus efficace : encourager le regroupement devient non seulement avantageux, mais, désormais, indispensable.

2 Augmentez la visibilité relative à l'utilisation interne de l'IA afin d'évaluer les contrôles devant être mis en place pour que les employés utilisent l'IA sans affecter la productivité

L'usage de l'intelligence artificielle au travail se démocratise, mais il peut aussi exacerber les risques existants tout en en introduisant de nouveaux. Les entreprises sont conscientes qu'elles doivent intensifier leurs efforts pour se prémunir contre les risques liés à l'utilisation de l'IA. Recourir à des contrôles intégrés et garantir une visibilité accrue des applications d'IA sont deux principes clés pour renforcer la sécurité des données sans entraver la productivité. Sensibiliser les employés à une utilisation sûre de l'IA peut aider les entreprises à limiter les comportements à risque, tout en assurant que les équipes tirent pleinement parti de ces outils puissants.

3 Optimisez votre stratégie de sécurité des données avec l'IA

L'IA permet aux équipes responsables de la sécurité des données de se consacrer à des initiatives plus stratégiques, au lieu de se contenter de répondre à des menaces récurrentes et à un flot constant d'alertes. Les entreprises avancées dans l'intégration de l'IA se montrent plus confiantes et satisfaites de leurs solutions de sécurité des données, comparativement à celles encore aux premiers stades. En intégrant l'IA dans une stratégie globale de sécurité, les entreprises renforcent leur visibilité, améliorant ainsi leur capacité à détecter et à réagir face aux risques, et, en définitive, élèvent leur niveau global de sécurité des données.

Objectifs de l'étude

Les objectifs de cette étude étaient les suivants :

1. Comprendre le paysage de la sécurité des données, notamment les priorités et les mentalités, les défis ainsi que la cause et les répercussions des incidents liés à la sécurité des données.
2. Découvrir le futur de la sécurité des données, notamment les stratégies et innovations émergentes, et la façon dont les entreprises comptent investir à l'avenir.
3. Analyser le rôle que joue l'IA dans l'amélioration de la sécurité des données et la protection des données.

Méthodologie

Une enquête internationale en ligne, d'une durée de vingt minutes, a été conduite du 5 au 23 août 2024 auprès de 1 376 décideurs en matière de sécurité des données.

Les questions visaient à comparer le paysage actuel de la sécurité des données et les incidents liés par rapport à 2023. Cette année, l'enquête a également exploré la sécurisation de l'utilisation de l'IA par les employés ainsi que l'implémentation de l'IA pour renforcer la sécurité des données.

Public cible

Pour répondre aux critères de sélection, les décideurs en sécurité des données devaient :

- RSI et décideurs adjoints (C-2 et au-dessus) ayant compétence en matière de sécurité des données
- Des employés travaillant dans de grandes entreprises (plus de 500 employés; plage de taille)
- Un mélange de secteurs réglementés et non réglementés (sans les secteurs de l'enseignement, de l'administration ou du non lucratif)

Sur les 1 376 décideurs en matière de sécurité des données interrogés dans le cadre de l'étude, le décompte par pays est le suivant :

- É-U : 302
- R-U : 305
- Inde : 301
- Brésil : 158
- France : 156
- Australie : 154

hypothesis Microsoft Security