Microsoft Security

Indice de sécurité des données

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

Rapport 2024

Préface

Alors que nous entrons dans notre deuxième année de recherche sur l'évolution du paysage de la sécurité des données, les défis et les opportunités que nous rencontrons n'ont jamais été aussi poussés. L'année passée, la gravité des incidents liés à la sécurité des données a augmenté. Dans l'ère actuelle, centrée sur les données, les stratégies et les outils utilisés pour les protéger évoluent rapidement.

Cette année, nous nous concentrons sur une nouvelle barrière : le rôle et l'impact de l'IA générative (IA) sur les stratégies de sécurité des données.

L'IA fait couler de l'encre dans le monde entier, notamment grâce à ses capacités sans précédent permettant de booster l'innovation et l'efficacité. Cependant, face à cet énorme potentiel, les entreprises sont également préoccupées par d'éventuels risques liés à la sécurité des données et par la manière dont ils pourraient redéfinir les responsabilités des équipes chargées de la sécurité des données. Selon nous, l'IA permet aux entreprises de renforcer plus rapidement leurs pratiques fondamentales en termes de sécurité des données, ce qui les aide à limiter l'impact du partage excessif de données, et des fuites, et à créer des processus favorisant une adoption sécurisée de l'IA. D'autre part, l'IA peut également aider les entreprises à améliorer leurs pratiques liées à la sécurité des données en identifiant les risques cachés et les éventuelles lacunes dans leur protection, et en recommandant des stratégies de protection, mais aussi en accélérant l'analyse et la correction des incidents de sécurité.

L'objectif de notre recherche est de fournir aux responsables de la sécurité des données des informations et des conseils pertinents qui leur permettront d'aider leurs équipes à adapter leur stratégie de sécurité des données en toute confiance, afin de protéger efficacement l'utilisation de l'IA et de l'intégrer dans les stratégies concernées. Bien qu'impressionnante de par sa portée et son potentiel, l'IA ne représente que la dernière vague de transformation ayant touché les entreprises. Ces dernières années, ce sont le travail hybride, le cloud et la mobilité qui ont mis en évidence le besoin intemporel de visibilité dans leur utilisation pour atténuer les risques et optimiser l'impact de l'entreprise. Grâce à ces enseignements, assurer une protection appropriée des données utilisées avec l'IA, et utiliser l'IA pour améliorer les mesures liées à la sécurité des données, permettront d'améliorer la productivité, la résilience et l'agilité des équipes face aux défis futurs.

Nous vous invitons à consulter nos dernières conclusions, en espérant que ces informations vous aideront à renforcer votre niveau de sécurité des données, à adopter l'IA et à définir une stratégie de sécurité des données complète, boostant ainsi l'innovation et offrant un avenir plus sécurisé pour tous.

Rudra Mitra
vice-président
Sécurité et conformité des données Microsoft

Présentation

Chaque année, les entreprises constatent en moyenne 156 incidents liés à la sécurité des données. L'impact de ces incidents reste donc une préoccupation constante pour les décisionnaires en matière de sécurité des données. Et ce pour une bonne raison : un seul incident peut entraîner des dommages considérables, notamment en termes de finance et de réputation, en particulier dans un paysage des menaces en constante évolution dans lequel les attaquants exploitent toutes les vulnérabilités possibles. Ce risque est amplifié par l'adoption rapide de l'IA. En effet, en l'absence de protections et de mesures de sécurité appropriées, les utilisateurs peuvent, intentionnellement ou non, mettre en danger des données sensibles de l'entreprise (notamment des informations sur les collaborateurs et les clients, la propriété intellectuelle, les prévisions financières et les données opérationnelles). Alors que les entreprises cherchent de nouvelles façons de protéger ces multiples données sensibles, de nombreux décisionnaires se sont tournés vers l'essor spectaculaire de l'IA.

Le défi de l'IA est double. Deux tiers des entreprises admettent que leurs collaborateurs utilisent des outils d'IA non-autorisés, il est donc essentiel qu'elles vérifient que ces outils sont exploités de manière sécurisée. De plus, l'IA peut être un outil efficace dans le cadre d'une stratégie de sécurité des données sophistiquée.

Les solutions de sécurité des données optimisées par l'IA jouent déjà un rôle essentiel dans l'identification des menaces et leur réponse en temps réel, l'amélioration de la vitesse et de la précision globales des programmes de sécurité des données, et l'envoi d'informations permettant d'anticiper les incidents liés à la sécurité des données avant même qu'ils ne se produisent. En plus d'exploiter la puissance de l'IA, les entreprises doivent gérer les risques engendrés par cette dernière afin d'identifier à la vitesse de la machine les modèles pouvant s'avérer difficiles à traiter et à analyser pour l'humain, et pour contrer des cyberattaques de plus en plus sophistiquées.

En 2023, Microsoft a chargé une agence de recherche indépendante, Hypothesis, de mener une enquête internationale auprès de plus de 800 professionnels de la sécurité des données. Le but était de lancer une initiative visant à établir un indice de sécurité des données pour mieux répondre aux besoins de nos partenaires et clients, mais aussi pour aider les dirigeants à développer leurs propres stratégies de sécurité des données.

En 2024, ce rapport s'appuie sur de nouvelles recherches et fournit de nouvelles informations obtenues dans le cadre d'une enquête internationale élargie menée auprès de plus de 1 300 professionnels de la sécurité des données. Bien que les données révèlent certaines informations et tendances similaires sur les marchés étudiés, nous tirons également de nouveaux enseignements sur les dernières pratiques et tendances mondiales en matière de sécurité des données et d'IA.

hypothesis Microsoft Security

Principales conclusions

1

Le paysage de la sécurité des données reste fragmenté, ce qui accroît la nécessité d'établir des stratégies de sécurité des données cohérentes, malgré les risques (anciens et nouveaux) liés à l'utilisation de l'IA

Les entreprises déclarent avoir un niveau de confiance et de satisfaction élevé à l'égard de leurs mesures de sécurité des données. Toutefois, la gravité des incidents liés à la sécurité des données continue d'augmenter, en particulier à cause des différences constatées par les entreprises entre leurs politiques de sécurité des données actuelles, et l'utilisation et l'introduction accrues des applications basées sur l'IA. Face à ces enjeux et impératifs, de nombreuses entreprises s'appuient encore sur différents outils de sécurité des données, ce qui peut accroître leur vulnérabilité et leurs risques globaux.

2

À mesure que les utilisateurs finaux adoptent de plus en plus d'applications basées sur l'IA, l'intégrité des données les plus sensibles des entreprises est de plus en plus menacée, nécessitant ainsi une visibilité accrue et de nouveaux contrôles de protection

Les outils d'IA deviennent essentiels pour les tâches quotidiennes, les entreprises sont donc de plus en plus préoccupées par les risques en termes de sécurité des données. Elles reconnaissent qu'il est nécessaire de consolider leurs défenses et s'engagent à anticiper les incidents liés à la sécurité des données causés par l'IA, mais l'utilisation non-autorisée de ces outils met en évidence la nécessité d'une visibilité renforcée.

3

Les décisionnaires sont optimistes quant au potentiel de l'IA à renforcer leurs mesures liées à la sécurité des données

Les entreprises investissent activement dans des outils de sécurité des données intégrant l'IA pour améliorer leurs capacités de détection et de réponse. L'IA peut détecter les données non protégées, recommander des stratégies de protection, et aider à analyser et corriger plus rapidement les incidents liés à la sécurité des données, permettant ainsi aux équipes concernées de se concentrer davantage sur les tâches stratégiques. L'utilisation de l'IA renforce également la confiance et la satisfaction des entreprises quant à leur stratégie globale de sécurité des données, en particulier grâce à leur capacité à répondre rapidement et avec précision aux incidents.

1

Le paysage de la sécurité des données reste fragmenté, ce qui accroît la nécessité d'établir des stratégies de sécurité des données cohérentes, malgré les risques (anciens et nouveaux) liés à l'utilisation de l'IA

Il existe un décalage entre la confiance des décisionnaires à l'égard de leurs pratiques de sécurité des données et leur niveau réel de protection

Comme annoncé en 2023, la grande majorité des décisionnaires ont confiance en leurs stratégies de sécurité des données : 74 % se disent satisfaits de leurs solutions en 2024. Ils se sentent en sécurité dans leur capacité à suivre et à gérer les données sensibles : 88 % pensent savoir où résident la plupart de leurs informations sensibles, et 85 % affirment que leurs données sont correctement classées et étiquetées. La plupart d'entre eux font également confiance à leurs contrôles de défense : 79 % sont convaincus de pouvoir empêcher l'exfiltration de données et 76 % décrivent leur approche comme proactive plutôt que réactive.

Toutefois, leur confiance est mise à l'épreuve à mesure que la gravité des incidents augmente. **Le nombre moyen d'incidents annuels liés à la sécurité des données reste élevé, passant de 166 en 2023 à 156 en 2024, et la gravité de ces incidents est passée de 20 % d'incidents graves à 27 % en 2024.**

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 d'établissement de la plateforme logicielle, le lieu de stockage de ces données et les personnes autorisées à accéder à ces données ont compliqué la sécurité et la gestion des données de nos outils d'IA et de nos fournisseurs. Nous devons protéger et gouverner plus de 100 ans de données conformément aux exigences légales, et ce dans toutes les juridictions dans lesquelles nous opérons », déclare un responsable principal de la gouvernance des informations travaillant pour un fabricant d'équipements lourds.

L'augmentation de la gravité des incidents liés à la sécurité des données a, par conséquent, entraîné une augmentation du volume des alertes. **En moyenne, les entreprises sont confrontées à 66 alertes par jour, contre 52 en 2023.** Ce nombre varie considérablement selon la taille de l'organisation : les entreprises de taille moyenne (500-999 collaborateurs) et les grandes entreprises (1 000-4 999 collaborateurs) reçoivent en moyenne 56 alertes par jour, contre 80 pour les très grandes entreprises (plus de 5 000 collaborateurs).

Étant donné le volume considérable d'alertes liées à la sécurité des données, il n'est pas surprenant que la plupart des entreprises ne puissent tout simplement pas suivre le rythme. En moyenne, les équipes chargées de la sécurité des données examinent 63 % de leurs alertes quotidiennes. 35 % de ces alertes se révèlent être des faux positifs. Ce décalage entre le niveau de contrôle estimé par les entreprises et la réalité opérationnelle entraîne un surmenage des équipes chargées de la sécurité des données, qui tentent de vérifier si elles disposent des bonnes protections ou de les perfectionner, tout en craignant que des incidents potentiellement graves ne passent à travers les mailles du filet.

Pour lutter contre les risques (anciens et émergents) pensant sur les données liés à l'utilisation d'outils d'IA, les entreprises ont davantage besoin de stratégies de sécurité des données plus robustes et plus cohérentes

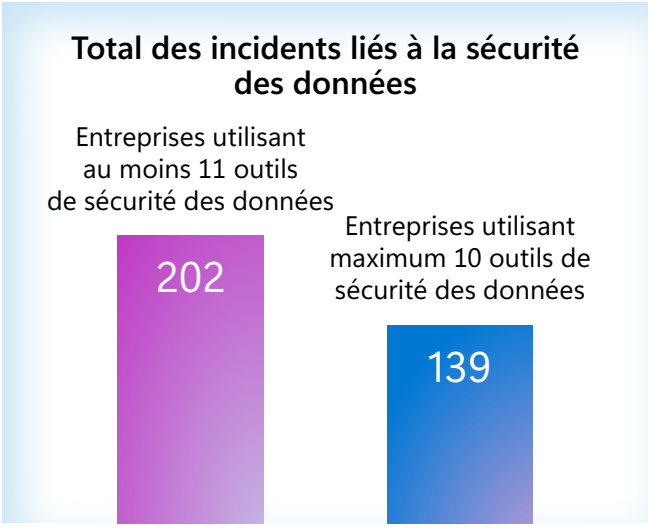
Malgré le nombre croissant d'outils à leur disposition, de nombreux décisionnaires continuent de reconnaître que plus ne signifie pas toujours mieux. En fait, 21 % d'entre eux déclarent que leur plus grand défi/risque réside dans le manque de visibilité renforcée et complète (et de compréhension partagée des risques) causé par des outils disparates.[1]

La plupart des décisionnaires (82 %) conviennent que disposer d'une plateforme complète et entièrement intégrée est plus efficace que de gérer plusieurs outils isolés. **En moyenne, ils jonglent avec 12 solutions de sécurité des données différentes, ce qui entraîne une complexité augmentant leur 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 montrent une forte corrélation entre le nombre d'outils de sécurité des données utilisés et la fréquence des incidents liés à la sécurité des données. Les moyennes et grandes entreprises signalent, en moyenne, 89 incidents par an, tandis que les très grandes entreprises sont confrontées à 248 incidents par an. Cette différence frappante met en évidence le risque élevé auquel les grandes entreprises sont confrontées, même si elles déclarent avoir une confiance élevée en leurs mesures de sécurité des données.

En 2024, les entreprises utilisant davantage d'outils de sécurité des données (11 ou plus) ont connu, en moyenne, 202 incidents de sécurité des données, contre 139 pour celles disposant de 10 outils ou moins.

1. Enquête de septembre 2024 sur les décisionnaires 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 solutions fragmentées rendent difficile la compréhension du niveau de sécurité des données d'une entreprise, car les données sont isolées et les flux de travail disparates peuvent empêcher une visibilité complète des risques potentiels. Si les équipes chargées de la sécurité des données utilisent des outils non-intégrés, elles doivent créer des processus permettant de corréler les données et d'obtenir une visibilité cohérente des risques, ce qui peut entraîner des angles morts, et complexifier la détection et l'atténuation efficaces des risques.

L'augmentation des incidents de sécurité des données liés à l'utilisation d'applications d'IA est une préoccupation croissante, puisque ces incidents ont presque doublé, passant de 27 % en 2023 à 40 % en 2024. Ce phénomène est alimenté par une recrudescence des attaques de logiciels malveillants et de ransomware, qui sont passées de 50 % en 2023 à 59 %. Les attaques causées par l'utilisation d'applications d'IA exposent non seulement les données sensibles, mais elles compromettent également les capacités des systèmes d'IA eux-mêmes, ce qui complexifie davantage un paysage de sécurité des données déjà fracturé. Pour résumer, il devient urgent d'adopter des stratégies de sécurité des données renforcées et plus cohérentes, capables de traiter tous les risques (anciens et émergents) liés à l'utilisation des outils d'IA.

La voie à suivre

L'augmentation de la gravité des incidents liés à la sécurité des données ouvre une porte à l'IA, qui pourrait s'avérer utile dans ce genre de situations. Les entreprises à la pointe de la technologie adoptent un système de sécurité des données reposant sur l'IA pour faciliter la hiérarchisation des incidents, automatiser la classification des données et identifier des façons de perfectionner les politiques de protection actuelles. L'IA peut synthétiser automatiquement la gravité potentielle des alertes d'incident, fournissant aux équipes chargées de la sécurité des données des informations pertinentes, pour une réponse rapide et une réduction du temps passé à traiter les faux positifs. Ce système rationalise les flux de travail et permet aux équipes chargées de la sécurité des données de se concentrer sur des améliorations de la sécurité des données plus stratégiques et sur des mesures proactives.

2

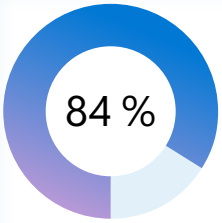
À mesure que les utilisateurs finaux adoptent de plus en plus d'applications basées sur l'IA, l'intégrité des données les plus sensibles des entreprises est de plus en plus menacée, nécessit-antainsi une visibilité accrue et denouveaux contrôles de protection

L'IA devient de plus en plus essentielle aux tâches quotidiennes, et les entreprises doivent s'adapter à cette nouvelle réalité de manière proactive

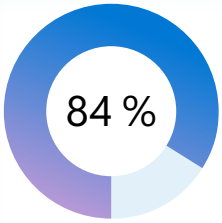
L'adoption rapide des outils d'IA par les collaborateurs a considérablement modifié l'approche des entreprises en termes de sécurité des données. Bien que l'IA transforme la productivité et les flux de travail, elle peut, comme toute technologie émergente, amplifier les risques actuels ou introduire de nouveaux risques qui nécessitent d'adopter une approche différente pour la protection des informations sensibles. Par conséquent, les entreprises continuent de chercher un certain équilibre dans ce paysage en constante évolution. Un responsable ingénierie et analyse de données dans le secteur des transports a déclaré : « Nous surveillons les données plus attentivement du côté de l'IA. Nous devons trouver un équilibre entre productivité et sécurité, et précision et confidentialité. »

La confiance en une utilisation sécurisée de l'IA par les collaborateurs reste mitigée. La majorité (84 %) aimerait être plus confiante quant à la gestion et la découverte de la saisie de données. Alors que 22 % des entreprises se sentent extrêmement confiantes quant à leurs capacités de sécurisation des données, la plupart (59 %) ne sont que « très confiantes », ce qui indique que des améliorations sont possibles. La plupart des entreprises (86 %) reconnaissent qu'elles aimeraient être plus optimistes quant à la gestion et la découverte des données générées par les outils d'IA.

À mesure que l'IA occupe une place de plus en plus essentielle en termes de productivité quotidienne, l'utilisation d'applications d'IA a également augmenté les préoccupations liées aux incidents de sécurité des données. **Près d'un tiers (31 %) des entreprises prévoient une augmentation des incidents liés à la sécurité des données dus à l'utilisation de l'IA par leurs collaborateurs, et 84 % admettent qu'elles doivent en faire davantage pour se protéger 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 confiantes 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 collaborateurs

L'utilisation non-autorisée de l'IA est très répandue

40 % des entreprises déclarent que leurs applications d'IA ont déjà été violées ou compromises lors d'un incident lié à la sécurité des données. 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 %).

L'utilisation non-autorisée de l'IA se produit souvent lorsque des collaborateurs se connectent à l'aide d'informations d'identification personnellesou utilisent des appareils personnels pour effectuer des tâches professionnelles. **En moyenne, 65 % des entreprises admettent que leurs collaborateurs utilisent des outils d'IA non-autorisés.** Voici différents cas dans lesquels les collaborateurs utilisent des outils d'IA non-autorisés :

- 53 % des cas concernent une connexion à l'aide d'informations d'identification personnelles à des fins professionnelles ;
- 48 % concernent l'utilisation d'un appareil personnel pour exploiter l'IA au travail ;
- 47 % concernent l'utilisation d'informations d'identification professionnelles pour exploiter l'IA à des fins personnelles.

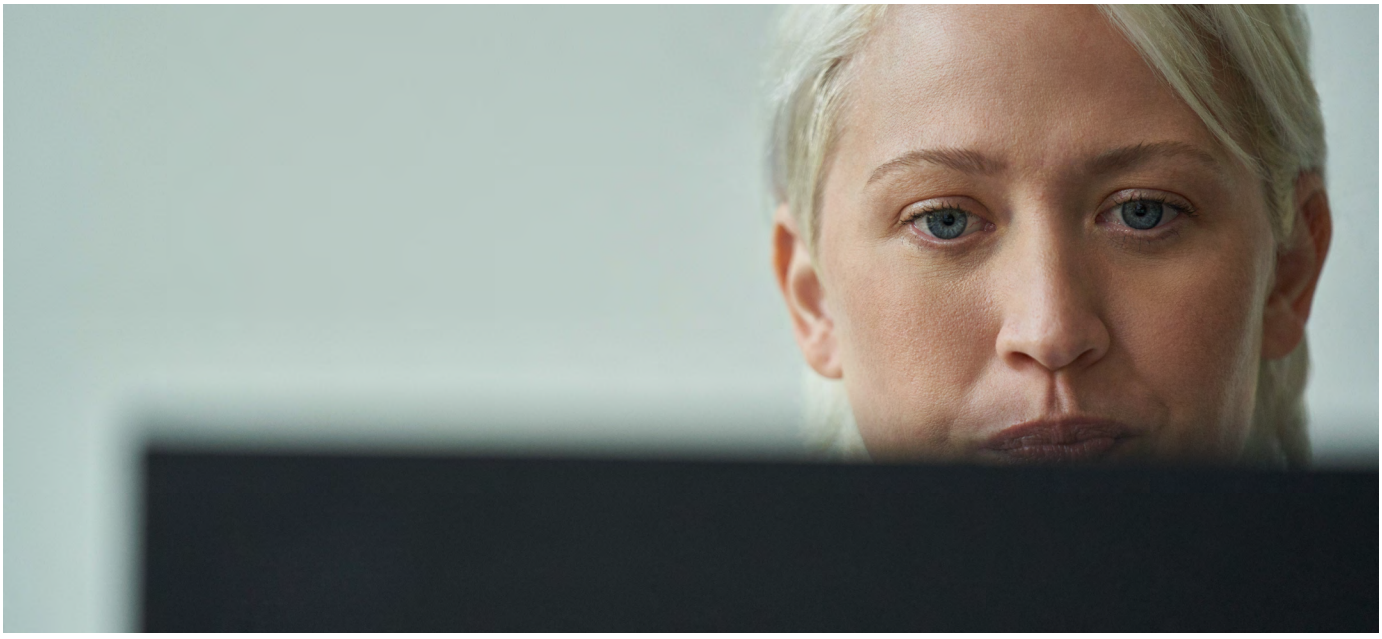
La moitié des entreprises se disent préoccupées par l'absence de contrôles visant à détecter et atténuer les risques lorsque les collaborateurs utilisent les applications d'IA de manière non sécurisée. Ce chiffre varie selon la taille de l'entreprise : 43 % des entreprises de taille moyenne, 50 % des grandes entreprises et 54 % des très grandes entreprises se disent préoccupées par leur capacité à gérer ces risques.

Compte tenu de l'utilisation accrue de l'IA, davantage de contrôles de sécurité des données sont nécessaires

Alors que l'IA s'intègre de plus en plus aux opérations quotidiennes, les entreprises reconnaissent la nécessité d'une protection renforcée. **96 % des entreprises sont préoccupées par l'utilisation de ces outils par leurs collaborateurs, mais presque autant sont prêtes à investir dans des solutions visant à répondre à ces inquiétudes.**

« Nous nous concentrerons surtout sur comment garder une longueur d'avance sur l'IA. La sécurité sera axée sur la réduction du volume des données, et sur une surveillance plus rigoureuse. Du côté de l'IA, vous avez besoin de plus de données pour rendre vos modèles plus représentatifs et identifier les biais. Alors, comment faire ? », se demande un responsable ingénierie, architecture et analyse de données dans le secteur des transports. La grande majorité des décisionnaires (87 %) sont prêts à consacrer du temps et de l'argent à former des collaborateurs aux pratiques sécurisées d'utilisation des outils d'IA. **C'est aussi parce que 85 % d'entre eux déclarent qu'il est essentiel que les collaborateurs utilisent ces outils pour rester compétitifs.**

Presque toutes les entreprises interrogées (93 %) en sont déjà au stade de la création ou de la mise en œuvre de contrôles relatifs à l'utilisation de l'IA, mais beaucoup en sont encore aux prémices. Seulement 39 % d'entre elles ont entièrement intégré des contrôles de sécurité des données relatifs à l'IA, et 24 % ont déjà créé des stratégies, mais elles ne les ont pas encore mises en œuvre. Un vice-président de la sécurité des données travaillant dans l'hôtellerie a déclaré : « Nous devons nous aligner sur les contrôles de l'IA, mais nous adoptons aussi l'utilisation de l'IA. Cela simplifie notre travail et nous aide à gagner en efficacité. »



Alors que les entreprises prennent des mesures pour protéger leurs données sensibles contre toute utilisation abusive dans les applications d'IA, elles doivent évidemment disposer de contrôles plus complets. Actuellement, 43 % des entreprises s'efforcent d'empêcher la saisie de données sensibles dans des applications d'IA, tandis que 42 % enregistrent l'ensemble des activités et contenus de ces applications en vue de potentielles enquêtes ou d'éventuelles réponses à un incident. De même, 42 % bloquent l'accès des utilisateurs aux outils non-autorisés, et un pourcentage égal investit pour former les collaborateurs à une utilisation sécurisée de l'IA.

Les entreprises dont les collaborateurs se livrent à une utilisation non-autorisée de l'IA ont davantage besoin de certains types de contrôles. **Parmi les entreprises présentant une utilisation non-autorisée de l'IA, 42 % doivent disposer de contrôles pour identifier les utilisateurs à risque en se basant sur les requêtes d'IA, contre 30 % pour celles dont les collaborateurs ne se livrent pas à une utilisation non-autorisée de l'IA. De plus, 40 % des entreprises confrontées à une utilisation non-autorisée de l'IA ont besoin de contrôles pour gérer le cycle de vie des données (tels que des protocoles de rétention et de suppression), contre 27 % pour les entreprises ne présentant pas ce problème.**

Les 5 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 collaborateurs à une utilisation sécurisée des outils d'IA	42 %
Identifier 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 ensemble complet de contrôles afin de découvrir, protéger et gouverner leurs données dans les applications d'IA. Voici trois stratégies clés que les équipes peuvent utiliser :

Augmenter la visibilité relative à l'utilisation de l'application d'IA et aux données circulant dans l'application : utilisez des outils de sécurité des données capables de détecter l'utilisation d'applications d'IA. Ces outils fournissent une liste d'informations complète comprenant les applications d'IA utilisées ainsi que leurs profils de risque, y compris des détails tels que les contrôles de sécurité des données pris en charge et la conformité aux réglementations. Utilisez des outils capables d'assurer une classification cohérente des données sensibles dans les interactions avec l'IA et d'afficher les tendances relatives à la façon dont les données circulent dans les applications d'IA.

Développer des stratégies et les renforcer : créez des stratégies basées sur les enseignements tirés de l'analyse de données. Ces stratégies peuvent inclure des instructions pour les applications d'IA autorisées et des procédures visant à bloquer ou restreindre l'utilisation d'applications non-autorisées par les collaborateurs. Même dans les applications d'IA autorisées, vous pouvez créer des stratégies granulaires pour permettre la circulation des données non-sensibles, tout en limitant l'utilisation des données sensibles et critiques de l'entreprise. Cela peut passer par le blocage de certaines actions, telles que le collage de données sensibles dans des outils d'IA basés sur un navigateur afin de garantir la sécurité des données.

Évaluer régulièrement les risques et perfectionner les stratégies : générez régulièrement des rapports montrant les niveaux de risque des applications d'IA utilisées, les tendances relatives à la façon dont les données sensibles circulent dans ces applications, ainsi que l'activité des utilisateurs dans ces applications. Cela permet d'évaluer le paysage global des risques et de prendre des décisions éclairées afin d'opter pour les stratégies de sécurité des données les plus appropriées.

3

Les décisionnaires sont optimistes quant au potentiel de l'IA à renforcer leurs mesures liées à la sécurité des données

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

La grande majorité (88 %) des entreprises investissent déjà dans l'IA pour améliorer leurs efforts de détection et de réponse : découverte des données sensibles, détection des activités anormales et protection automatique des données à risque. **77 % des entreprises pensent que l'IA accélérera ces processus, et 76 % pensent qu'elle améliorera la précision de leurs stratégies de détection et de réponse.**

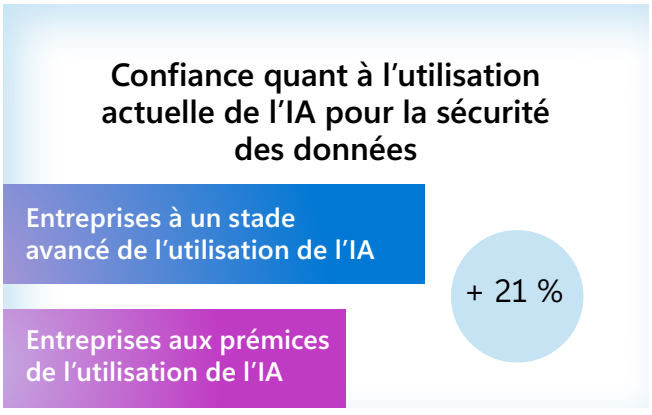
Alors que 73 % des décisionnaires sont préoccupés par le fait que l'IA soit de plus en plus utilisée pour renforcer la sécurité des données, 50 % affirment que cela ne les a pas empêchés d'utiliser l'IA pour renforcer la sécurité de leurs données. Seulement 23 % déclarent avoir été freinés par ces inquiétudes. En tout, une écrasante majorité de 93 % envisage au moins d'utiliser l'IA pour renforcer la sécurité des données, malgré les préoccupations actuelles.

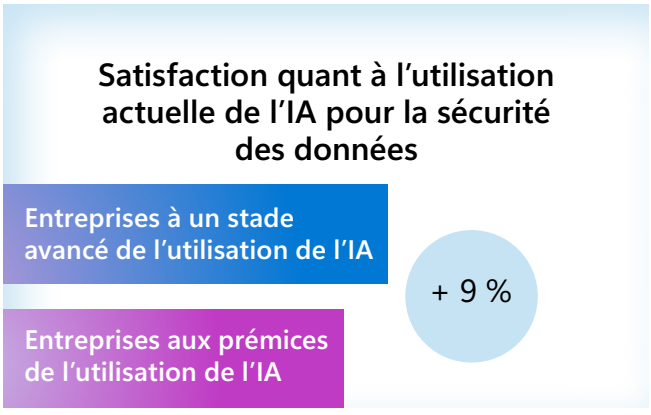
Utiliser l'IA pour renforcer la sécurité des données permet d'accroître la visibilité, la confiance et la satisfaction

L'un des principaux avantages de l'utilisation de l'IA pour renforcer la sécurité des données réside dans sa capacité à accroître la visibilité entre les systèmes, ce qui atténue l'une des préoccupations majeures des décisionnaires : savoir où les données sont stockées et comment elles sont classées (20 %).[1] 88 % des décisionnaires pensent qu'intégrer l'IA dans les solutions de sécurité des données offrira une visibilité accrue aux équipes, permettant ainsi aux entreprises de traiter et d'analyser beaucoup plus de données qu'avec d'autres solutions. Les entreprises de taille moyenne se concentrent principalement sur la réduction des risques à court terme, par exemple en limitant les erreurs humaines dans leurs processus de sécurité des données. En effet, 43 % des entreprises de taille moyenne priorisent la réduction des risques causés par l'erreur humaine, contre seulement 37 % chez les très grandes entreprises.

En revanche, les plus grandes entreprises adoptent une approche plus avancée mettant l'accent sur les risques à long terme et la nécessité de s'adapter. Ce niveau élevé de sophistication permet aux équipes chargées de la sécurité des données de mieux s'adapter aux risques en constante évolution, une priorité absolue pour 49 % des très grandes entreprises et 43 % des entreprises de taille moyenne.

Dans l'ensemble, les entreprises qui sont plus avancées dans l'utilisation de l'IA pour renforcer la sécurité des données déclarent des niveaux de confiance et de satisfaction beaucoup plus élevés à l'égard de leurs stratégies de sécurité des données. **Parmi celles qui en sont à un stade avancé de la mise en œuvre de l'IA, 90 % se sentent extrêmement ou très confiantes quant à leur utilisation de l'IA pour renforcer la sécurité des données, contre 69 % pour les entreprises moins avancées. De même, 76 % des entreprises présentant une utilisation avancée de l'IA se disent satisfaites de leurs solutions de sécurité des données, contre seulement 67 % pour celles qui ne sont pas encore à un stade avancé de leur adoption.**





1. Enquête de septembre 2024 sur les décisionnaires 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 entreprises limitent le nombre d'incidents liés à la sécurité des données et améliorent la gestion des alertes grâce à l'IA

Les entreprises qui utilisent l'IA pour renforcer leurs opérations de sécurité des données signalent beaucoup moins d'alertes. **En moyenne, celles qui ont intégré des outils de sécurité des données basés sur l'IA reçoivent 47 alertes par jour, contre 79 pour celles qui ne l'ont pas encore fait. En outre, celles qui utilisent l'IA sont en mesure d'examiner 66 % de leurs alertes quotidiennes, tandis que les entreprises n'utilisant pas l'IA ne parviennent à en examiner que 60 %.**

De plus, celles qui utilisent l'IA pour renforcer la sécurité des données sont plus susceptibles d'exploiter l'IA pour atténuer les risques (56 % contre 26 %). La réduction du volume des alertes, associée à la capacité d'atténuation accrue offerte par l'IA, semble avoir considérablement affecté le nombre total d'incidents liés à la sécurité des données. Les entreprises ayant utilisé l'IA pour renforcer la sécurité de leurs données signalent 65 % d'incidents liés à la sécurité des données de moins que celles qui n'utilisent pas l'IA pour ce type d'opérations.

Le principal impact de l'IA devrait être sur les capacités de réponse

En termes de détection, 33 % des décisionnaires s'attendent à ce que l'IA les aide à identifier les activités anormales, tandis que 23 % pensent qu'elle permettra d'enquêter sur les potentiels incidents liés à la sécurité des données. Aussi, 22 % considèrent que l'IA pourrait partager des recommandations visant à mieux sécuriser leurs environnements de données.

Cependant, selon les décisionnaires, le principal impact de l'IA devrait être sur les capacités de réponse. 34 % d'entre eux pensent que l'IA pourrait automatiquement bloquer le partage inapproprié des données sensibles, et 32 % déclarent qu'elle aidera à protéger les données à risque. En outre, 26 % estiment que l'IA contribue à atténuer les risques liés à la sécurité des données et à mettre en œuvre des contrôles appropriés, et le même pourcentage s'attend à ce que l'IA signale automatiquement les comportements à risque des utilisateurs.

La voie à suivre

Intégrer l'IA aux solutions de sécurité des données peut fournir aux équipes des conseils en temps réel, des capacités de synthèse et une prise en charge du langage naturel afin de mettre en lumière des domaines qui auraient pu être négligés. Cela peut également accélérer les enquêtes et renforcer les compétences des équipes chargées de la sécurité des données. Voici comment ces fonctionnalités peuvent avoir un impact :

Synthèse des alertes : les équipes chargées des enquêtes peuvent vite se décourager en raison de la quantité de sources à analyser et des nombreuses règles de stratégie. En intégrant l'IA dans la protection contre la perte de données (DLP) et la gestion des risques internes (IRM), ces équipes peuvent rapidement obtenir un résumé des alertes, y compris leur source, des règles de stratégie et des informations sur les utilisateurs à risque, afin d'identifier les données sensibles qui ont été compromises et le risque utilisateur associé.

Communications contextuelles : les entreprises doivent respecter les exigences réglementaires relatives aux communications commerciales, ce qui nécessite souvent un examen approfondi des violations. L'IA peut aider les équipes chargées de la sécurité des données à évaluer du contenu en le comparant aux réglementations et aux politiques de l'entreprise, afin de mettre en évidence les communications à haut risque susceptibles d'entraîner un incident lié à la sécurité des données.

Langage naturel vers une requête par mot-clé : les flux de travail liés à la recherche peuvent s'avérer complexes et chronophages pendant les enquêtes, car ils nécessitent généralement l'utilisation d'un langage de requête par mot-clé. L'IA permet aux équipes chargées de la sécurité des données de saisir des invites de recherche en langage naturel pour rationaliser le début de la recherche, et ainsi favoriser des enquêtes plus approfondies.

Recommandations finales

1 Protégez-vous contre les incidents liés à la sécurité des données en adoptant une plateforme intégrée

Adopter une plateforme de sécurité des données entièrement intégrée offre une stratégie plus sûre et rationalisée dans un environnement en constante évolution. Cela réduit la complexité et accroît la visibilité, tout en renforçant la protection. Une approche intégrée peut aider les entreprises à améliorer leur niveau de sécurité des données en centralisant les contrôles concernés et en offrant une visibilité unifiée des données, des utilisateurs et des activités, renforçant et rationalisant ainsi la détection et la protection relatives aux risques liés aux données. 82 % des entreprises s'accordent pour dire qu'une plateforme intégrée est plus efficace : favoriser la consolidation n'est donc pas seulement bénéfique, c'est devenu essentiel.

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 collaborateurs utilisent l'IA sans affecter la productivité

L'utilisation de l'IA au travail se généralise, mais elle peut amplifier les risques actuels et en introduire de nouveaux. Les entreprises reconnaissent qu'elles doivent en faire plus pour se protéger contre l'utilisation à risque de l'IA. Utiliser des contrôles intégrés et assurer une visibilité optimale des applications d'IA sont deux notions clés permettant de renforcer la sécurité des données sans pour autant compromettre la productivité. Former les collaborateurs à une utilisation sécurisée de l'IA peut aider les entreprises à limiter les comportements à risque, tout en veillant à ce que les équipes continuent d'exploiter au mieux ces puissants outils.

3 Améliorez votre stratégie de sécurité des données grâce à l'IA

L'IA permet aux équipes chargées de la sécurité des données de se concentrer sur des initiatives plus stratégiques au lieu de simplement réagir face à des menaces constantes et une quantité élevée d'alertes. Les entreprises se trouvant à un stade avancé de leur mise en œuvre de l'IA sont plus confiantes et plus satisfaites quant à leurs solutions de sécurité des données que celles qui en sont encore aux prémices. En déployant l'IA dans le cadre d'une stratégie globale de sécurité des données, les entreprises peuvent accroître leur visibilité, ce qui renforce leur capacité à détecter les risques ainsi qu'à y réagir, et, finalement, leur niveau de sécurité des données dans son ensemble.

Objectifs de la recherche

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 de 20 minutes, menée du 5 au 23 août 2024 auprès de 1 376 décisionnaires en matière de sécurité des données.

Les questions visaient à comparer le paysage de la sécurité des données et les incidents de sécurité des données par rapport à 2023. En outre, l'enquête de cette année comprenait des questions relatives à la sécurisation de l'utilisation de l'IA par les collaborateurs et l'utilisation de l'IA pour renforcer la sécurité des données.

Audience visée

Pour répondre aux critères de sélection, les décisionnaires de la sécurité des données devaient être :

- RSI et décisionnaires adjoints (C-2 et au-dessus) ayant compétence en matière de sécurité des données
- Des collaborateurs travaillant dans de grandes entreprises (plus de 500 collaborateurs ; 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 décisionnaires 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