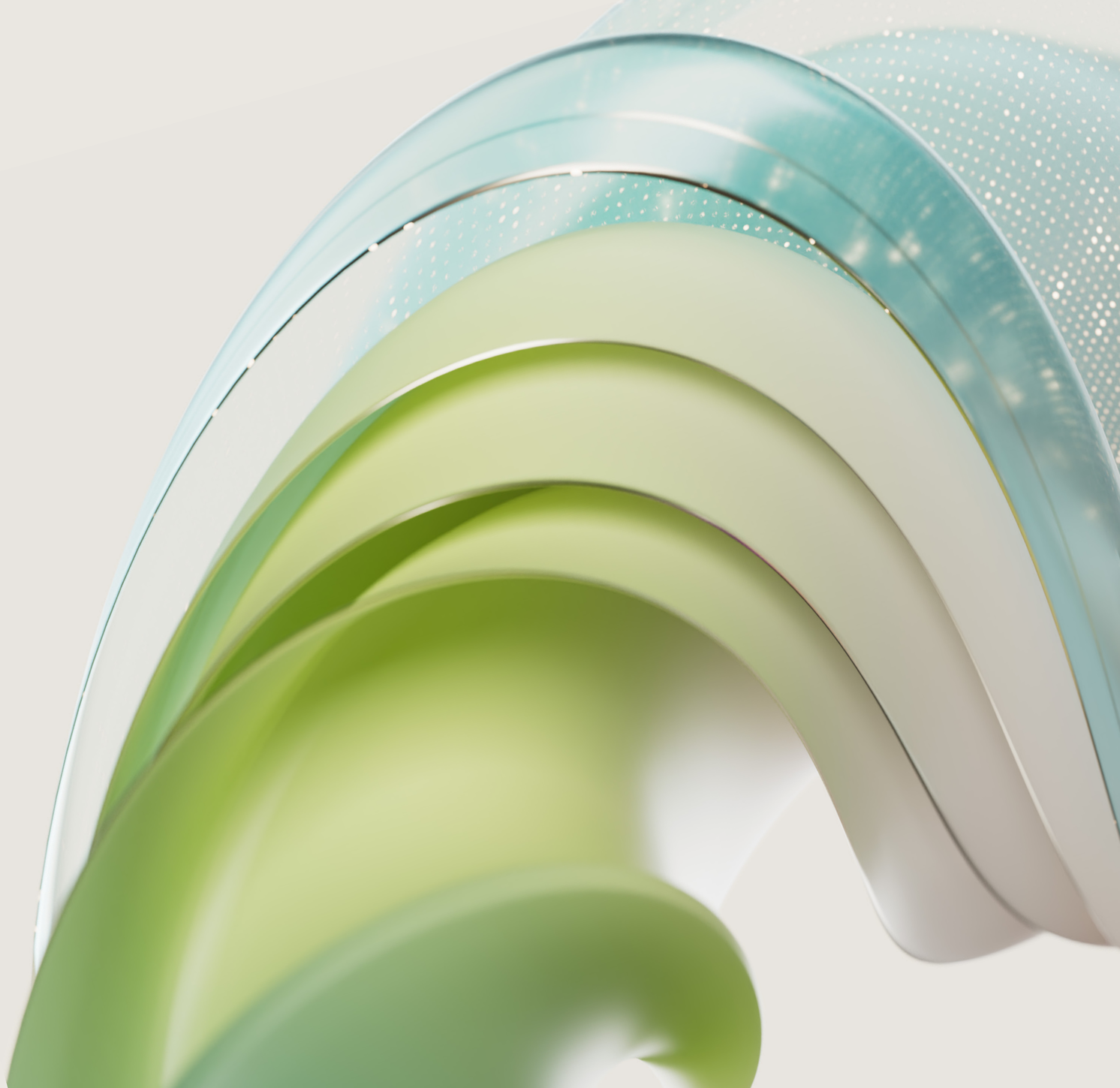
Microsoft

Développez votre entreprise avec une IA fiable

Éléments à prendre en compte par les chefs d'entreprise pour planifier en toute confiance leur transformation par l'IA



Sommaire

Introduction

Les solutions d'IA offrent aux organisations de toute taille et de tout secteur d'activité la possibilité d'augmenter leur chiffre d'affaires, de réduire leurs coûts, d'améliorer le bien-être de leurs collaborateurs et d'être plus efficaces. Les chefs d'entreprise sont donc sans surprise pressés d'adopter des solutions d'IA le plus rapidement possible et d'éviter de prendre du retard.

Malgré tout le battage médiatique autour de l'IA, les répercussions négatives de cette technologie suscitent également des inquiétudes. Dans le présent document, nous décrivons plusieurs aspects que les chefs d'entreprise peuvent prendre en compte pour exploiter les promesses de cette nouvelle technologie et éviter les conséquences imprévues.

L'établissement de pratiques responsables et sécurisées en matière d'IA pour votre entreprise vous aide à mettre en œuvre des outils d'IA en toute sécurité. Et comme la réglementation mondiale en matière d'IA s'intensifie, investir dans une IA responsable vous permet désormais de mieux vous équiper pour répondre aux nouvelles exigences réglementaires à mesure qu'elles se présentent. Par ailleurs, l'adoption d'une approche réfléchie de la mise en œuvre d'une IA responsable et sécurisée dans votre entreprise peut aider les dirigeants à adopter l'IA et l'innovation.

des chefs d'entreprise se sont déclarés « **à la fois inquiets et enthousiastes** » à l'égard de l'IA générative [1].

Nous nous engageons à mettre en place une IA fiable et à créer une technologie de soutien à la pointe de l'industrie. Avec des fonctionnalités qui améliorent la sécurité, la sûreté et la confidentialité, nous continuons à permettre aux clients d'utiliser et de construire des solutions d'IA fiable.

En savoir plus

Appliquer des pratiques d'IA responsable

Envisager des principes d'IA responsable

Les politiques publiques et les meilleures pratiques du secteur tentent encore de s'adapter aux dernières évolutions de la technologie de l'IA. Les chefs d'entreprise sont donc à la recherche de conseils fiables sur la façon de mettre en œuvre des systèmes d'IA ayant un impact positif sur les entreprises, les individus et la société.

Prendre le temps de réfléchir à une approche d'IA responsable pour votre organisation peut vous aider, vous et vos équipes, à aller de l'avant en toute confiance et à vous protéger contre les risques involontaires. Nous avons défini six principes d'IA responsable à prendre en compte lors de la planification et de l'élaboration de votre propre approche. Ces principes sont les suivants :

- **Confidentialité et sécurité**
- **Responsabilisation**
- **Transparence**
- **Fiabilité et sûreté**
- **Inclusion**
- **Équité**

Confidentialité et sécurité

Les systèmes d'IA doivent respecter les mêmes normes de confidentialité et de sécurité que celles appliquées par les entreprises à leurs données les plus sensibles.

Donnez la priorité à la sécurité de votre infrastructure et à la confidentialité de vos données.

Déterminez où se trouvent les données, comment elles sont utilisées et confirmez qu'elles sont sécurisées au repos et en transit. Vérifiez que les outils d'IA respectent les valeurs de votre entreprise en matière de confidentialité et de sécurité.

Lorsque vous mettez en œuvre des autorisations strictes pour les données et attribuez des autorisations aux utilisateurs en fonction de leur rôle et de leur appartenance à un groupe, seules les personnes autorisées auront accès aux informations sensibles, ce qui réduira le risque de violation interne.

Par ailleurs, vous pouvez garantir la sécurité et répondre aux critères de conformité grâce à une solution de gouvernance, qui comprend la conservation et l'enregistrement des interactions avec les applications d'IA, l'aide à la détection de toute violation de la réglementation ou de la politique organisationnelle lors de l'utilisation de ces applications, et l'enquête sur les incidents lorsqu'ils surviennent.

Le déploiement de l'IA doit également se conformer à toutes les lois et réglementations locales relatives à l'utilisation des données et à la confidentialité. En matière de sécurité des données, il vaut mieux ne pas être trop prudent et travailler avec des fournisseurs d'outils de sécurité qui ont fait leurs preuves.

Un exemple de confidentialité et de sécurité en pratique :

L'utilisation d'un outil d'IA pour analyser les communications des clients afin de résoudre un ticket de support pourrait impliquer l'accès à des données client sensibles ou identifiables. Ainsi, la compréhension des lois et réglementations locales, l'adhésion aux normes élevées de votre organisation en matière de sécurité et l'application de contrôles adéquats peuvent contribuer à préserver la confidentialité de ces données sensibles.

Conformité avec les réglementations en matière d'IA

Microsoft s'engage à développer des produits et des solutions conformes aux réglementations telles que la loi européenne sur l'IA pour aider ses clients à utiliser l'IA de manière conforme.

En savoir plus

Fiabilité et sécurité

La fiabilité et la sécurité impliquent que les systèmes d'IA fonctionnent comme prévu, sans erreurs ni interruptions. Les développeurs d'outils d'IA ont la responsabilité de s'assurer que leur produit fournit des résultats précis grâce à des tests et à la documentation, mais un système de surveillance permet de vérifier si l'outil répond à l'utilisation prévue. Les systèmes doivent également faire l'objet d'un pilotage régulier, d'une maintenance, d'un retour d'information et de processus d'évaluation afin d'identifier de nouvelles utilisations, de dépanner rapidement les problèmes et d'améliorer le système d'IA au fil du temps.

Effectuer régulièrement des tests de contrainte.

Les tests de contrainte préparent un système d'IA à gérer les types d'utilisation et le volume d'utilisation que ce système doit gérer sans produire d'erreurs ou de vulnérabilités aux risques.

Le Red Teaming est un type de test de contrainte qui consiste à simuler des attaques réelles et à utiliser les techniques fréquemment utilisées par les pirates pour accéder à des systèmes sécurisés. En 2018, Microsoft a créé notre Red Team spécifique à l'IA, et nous avons élargi la mission de l'équipe pour cartographier les risques en dehors des risques de sécurité traditionnels, y compris les risques provenant d'utilisateurs non contradictoires qui compromettent les normes d'IA fiable. Par exemple, le Red Teaming d'un outil d'IA générative permet de tester si un utilisateur peut générer un contenu qui stéréotype un groupe marginalisé à l'aide de l'outil. Un modèle d'IA peut également être soumis au Red Teaming afin d'identifier les abus potentiels, d'évaluer ses capacités et de comprendre ses limites. Ces informations peuvent ensuite être appliquées aux futures versions du modèle pour s'assurer qu'il fonctionnera avec fiabilité et sécurité.[2]

Faire preuve de diligence raisonnable quant à la fiabilité et aux mesures de sécurité d'un système d'IA au moment de l'achat et effectuer régulièrement des tests de contrainte pour identifier les risques par la suite.

Un examen attentif de la documentation aide les organisations à comprendre les mesures prises par le fournisseur du système d'IA pour faciliter l'utilisation fiable et sûre de son système et les aide à se conformer à toutes les exigences relatives à l'exploitation du système en toute sécurité.

Un exemple de fiabilité et de sécurité dans la pratique :

Un outil d'IA est utilisé pour modéliser les résultats financiers et rendre compte de la performance. Des tests sont effectués régulièrement pour s'assurer que l'outil d'IA produit des résultats précis et fiables, évitant ainsi tout impact négatif sur la santé financière de l'organisation.

Responsabilisation

Dans de nombreux cas, l'IA responsable est centrée sur l'humain. La mise en place d'un système de supervision clair aide votre personnel à contrôler les outils d'IA que vous mettez en œuvre et à rester responsable des résultats produits par ces outils.

Mettre en place un système de supervision qui définit clairement les rôles et les responsabilités à chaque étape du parcours vers l'IA.

La mise en œuvre d'un système de supervision qui effectue des tests d'impact et réagit aux résultats de l'impact permet de garder l'humain au centre du processus. Cela permet également une protection contre d'éventuelles conséquences négatives et la garantie que des contrôles adéquats sont mis en œuvre à chaque étape.

S'assurer que les outils d'IA sont adaptés à l'objectif visé.

Vérifiez régulièrement que les outils d'IA apportent les solutions adaptées aux problèmes qu'ils doivent résoudre et déterminez la réaction de votre organisation si un outil n'atteint pas l'objectif visé.

Un exemple de responsabilité dans la pratique :

L'utilisation d'un outil d'IA pour réviser des contrats juridiques implique la supervision d'une personne disposant d'un contexte et d'une expertise adéquats pour vérifier la conformité avec les lois et réglementations applicables, et pour approuver le résultat final de la révision assistée par l'IA.

Inclusion

L'inclusivité exige que les outils d'IA soient accessibles à toutes les personnes, quelles que soient leurs capacités. Cela signifie que les outils créés ou achetés par les chefs d'entreprise doivent respecter des principes de conception accessible et la norme européenne sur l'accessibilité EN 301 549, ainsi que la section 508 du U.S. Rehabilitation Act et les directives Web Content Accessibility Guidelines (WCAG).

Identifier les possibilités de développer l'inclusivité au sein de votre organisation grâce à l'IA.

Par exemple, les bénéficiaires de subventions de Microsoft créent une plateforme d'embauche pour les candidats neurodivers, mettent au point des affichages en braille plus performants et plus abordables pour les étudiants malvoyants et créent une application web pour aider les personnes souffrant de troubles de la parole à communiquer.

Transparence

La transparence est l'un des fondements de la confiance. Pour atteindre la transparence et la garder, il faut toujours expliquer clairement comment et quand l'IA est utilisée, ainsi que ses capacités et ses limites.

Faire preuve de transparence sur la manière dont l'IA est déployée et utilisée dans votre organisation.

Les parties prenantes et les collaborateurs peuvent se sentir plus confiants dans l'utilisation des outils d'IA s'ils comprennent comment ces derniers parviennent à des conclusions, mais aussi s'ils en connaissent clairement les limites. Cette transparence les aide à renforcer leur capacité à utiliser les outils d'IA et à savoir quand compléter leurs résultats par des informations ne relevant pas du champ d'application de l'outil.

Les clients veulent savoir quand ils interagissent avec un outil d'IA, quand l'IA est utilisée dans la prise de décision ou quand un élément audio ou visuel a été généré ou manipulé par l'IA. Les chefs d'entreprise doivent réfléchir à la manière dont ces informations seront divulguées aux clients.

Un exemple de transparence dans la pratique :

L'IA générative est utilisée pour créer du contenu pour une campagne de marketing, et l'organisation identifie les éléments créés par l'IA. Un spécialiste examine le contenu créé par l'IA pour en vérifier l'exactitude, de sorte qu'il n'induise pas les clients en erreur sur les caractéristiques ou les capacités du produit annoncé.

Équité

Un déploiement équitable de l'IA permet de répartir équitablement les opportunités, les ressources et les informations entre les personnes qui utilisent l'IA et qui en subissent les conséquences.

Garantir que vos systèmes d'IA offrent une qualité de service et une prestation de ressources et d'opportunités similaires à toutes les personnes qui les utilisent ou qui sont concernées, tous groupes démographiques confondus.

Lorsque vous utilisez des outils d'IA qui décrivent, illustrent ou représentent des personnes d'une autre manière, minimisez le risque de stéréotype ou de dévalorisation des personnes, en particulier celles qui appartiennent à des groupes marginalisés, afin de promouvoir l'équité.

Intégrez des membres d'horizons, d'expériences, de niveaux d'éducation et de perspectives différents dans l'équipe qui gère le déploiement de l'IA, et identifiez les biais statistiques dans les ensembles de données pour contribuer à l'équité d'un système d'IA. L'examen humain par des experts en la matière des décisions qui font appel à l'IA peut également contribuer à protéger contre les résultats biaisés.

Un exemple d'équité dans la pratique :

Un outil d'IA est utilisé pour examiner les candidatures et identifier les candidats prioritaires dans le processus d'embauche, sous la supervision d'un représentant des ressources humaines. Cette personne confirme que l'outil évalue les informations avec précision, sans biais statistique, et a le dernier mot dans la prise de décision.

Prendre des décisions éclairées sur l'IA et la sécurité

Le déploiement de l'IA minimise les risques de manière responsable tout en permettant à votre entreprise de bénéficier du potentiel de ses différents usages. Utilisez les questions suivantes pour entamer la conversation avec votre équipe lorsque vous commencez à réfléchir à votre mise en œuvre de l'IA.

Confidentialité et sécurité

- [ ] Les données auxquelles accèdent les systèmes d'IA sont-elles sécurisées conformément aux politiques de votre organisation en matière de traitement des données sensibles ?
- [ ] Avez-vous le contrôle de vos données, notamment de leur lieu de stockage et de leur mode d'utilisation ?
- [ ] Vos données sont-elles sécurisées à tout moment, y compris lorsqu'elles transitent d'un système à un autre ?
- [ ] Disposez-vous d'outils de sécurité de qualité pour vous protéger contre l'accès de tiers ou les cyberattaques ?
- [ ] Disposez-vous d'outils d'identification des menaces et de réaction en cas de cyberattaque ?

Inclusion

- [ ] Avez-vous confirmé que les outils que vous avez l'intention d'utiliser respectent les principes d'accessibilité ?
- [ ] Les outils sont-ils conformes à la norme européenne d'accessibilité EN 301 549 ?
- [ ] Les outils sont-ils conformes à la section 508 du U.S. Rehabilitation Act ?
- [ ] Les outils sont-ils conformes aux directives Web Content Accessibility Guidelines (WCAG) ?

Fiabilité et sûreté

- [ ] Les outils que vous avez l'intention d'utiliser ont-ils été testés de manière adéquate afin de minimiser les erreurs ?
- [ ] Avez-vous mis en place un plan pour remédier aux éventuelles défaillances ?
- [ ] Les outils feront-ils l'objet d'une surveillance régulière afin de détecter toute problématique de fiabilité ?
- [ ] Êtes-vous prêt à respecter toutes les exigences relatives à l'utilisation en toute sécurité des outils ?

Transparence

- [ ] Avez-vous informé les parties prenantes du fonctionnement de ce déploiement, y compris de ses capacités et de ses limites, ou avez-vous prévu de le faire avant qu'elles ne commencent à utiliser les outils d'IA ?
- [ ] Avez-vous prévu de communiquer avec les collaborateurs sur la manière dont votre organisation va utiliser l'IA et sur la manière dont ses résultats doivent être interprétés ?
- [ ] Avez-vous déterminé comment et quand vous informerez les clients qu'ils interagissent avec une IA ou qu'ils consultent du contenu généré par une IA ?

Responsabilisation

- [ ] Avez-vous évalué l'impact de ce déploiement sur vos collaborateurs, votre organisation et vos clients ?
- [ ] Avez-vous mis en place un système de surveillance et de réaction en cas de conséquences négatives potentielles ?
- [ ] Avez-vous mis en œuvre les meilleures pratiques en matière de gouvernance et de gestion des données ?
- [ ] Avez-vous déterminé qui supervisera les outils d'IA et veillé à ce que ces personnes bénéficient d'une formation et d'un contrôle adéquats ?
- [ ] Avez-vous vérifié que cette solution est adaptée à l'usage auquel elle est destinée ?

Équité

- [ ] Avez-vous vérifié que ce déploiement offrira la même qualité de service à toutes les personnes concernées ?
- [ ] Avez-vous testé les résultats du système pour vous assurer qu'il répartira équitablement les ressources et les opportunités entre les différents groupes démographiques ?
- [ ] Les résultats du système sont-ils exempts de stéréotypes et de représentations négatives des groupes marginalisés ?

Protéger vos données et vos systèmes d'IA

Sécuriser vos outils d'IA aujourd'hui et à l'avenir

Déployée de manière incorrecte, toute technologie ayant accès à des données sensibles peut présenter un risque pour la sécurité des entreprises. Puisque les systèmes d'IA nécessitent une grande quantité de données propriétaires, il est essentiel de prioriser la sécurité dès le départ lorsque le déploiement de l'IA ou l'acquisition de solutions d'IA sont envisagés.

Chez Microsoft, nous avons lancé notre Secure Future Initiative, rassemblant nos apprentissages pour faire face et se préparer à l'ampleur croissante et aux risques accrus de cyberattaques à l'ère de l'IA. La Secure Future Initiative identifie trois principes défendus par Microsoft pour aider à sécuriser l'ensemble de l'écosystème numérique :

1. **Sécurité dès la conception**
   La sécurité est une priorité lors de la conception d'un produit ou d'un service.

2. **Sécurité par défaut**
   Les dispositifs de sécurité sont activés et appliqués par défaut, ne nécessitent aucun effort supplémentaire et ne sont pas facultatifs.

3. **Sécurité des opérations**
   Les contrôles et la surveillance de la sécurité seront constamment améliorés pour répondre aux menaces actuelles et futures.

La sécurité est le fondement essentiel de tout déploiement de l'IA. Lorsque vous assurez des pratiques d'hygiène de sécurité de base, vous protégez vos données, votre personnel et vos appareils contre plus de 98 % des cyberattaques.[3]

Les pratiques d'hygiène efficaces en matière de sécurité sont les suivantes :

- Activer l'authentification multifacteur (MFA) pour se protéger contre la compromission des mots de passe des utilisateurs et contribuer à renforcer la résilience des identités.
- Appliquer les principes Zero Trust, qui impliquent une vérification explicite, l'utilisation d'un accès basé sur les privilèges minimum et l'hypothèse d'une violation, afin de limiter l'impact d'une attaque.
- Utiliser des logiciels malveillants de détection et de réponse étendues pour bloquer automatiquement les attaques et fournir des informations aux logiciels de gestion de la sécurité pour des temps de réponse plus courts.
- Veiller à ce que tous les systèmes soient maintenus à jour avec les dernières versions des microprogrammes, des systèmes d'exploitation et des applications.
- Mettre en œuvre les protections adaptées pour les données critiques, ce qui nécessite de savoir quelles sont les données les plus importantes et où elles se trouvent.

Gérer vos systèmes d’IA avec gouvernance

Un modèle de gouvernance solide permet de jeter des bases solides pour un déploiement responsable de l'IA. C'est le rôle des gouvernements et des organismes de réglementation de maintenir des exigences de base pour réduire au minimum les effets négatifs de l'utilisation de l'IA sur la société. Les organisations commerciales ont également la responsabilité éthique de créer une structure de gouvernance pour gérer leur propre développement ou leur utilisation de systèmes d'IA conformément à leurs valeurs organisationnelles, aux lois et réglementations locales et à l'intérêt général.

Établir votre propre gouvernance

Lorsque vous créez le système de gouvernance de votre organisation, n'oubliez pas que l'objectif de la gouvernance est de faire adhérer les solutions d'IA à la politique de l'entreprise et aux principes de l'IA responsable par le biais d'une série de politiques et de procédures. Il s'agit notamment d'appliquer des politiques d'évaluation et de mise en œuvre de solutions d'IA tierces, de coordonner l'implication et l'éducation des parties prenantes et de produire de la documentation pour informer les collaborateurs, les clients et les autres utilisateurs sur les outils d'IA.

Risques

Mapper

Le mappage des risques est la première étape de la gouvernance de l'IA et doit éclairer les décisions relatives à la sécurité, à la fiabilité et à l'adéquation à l'objectif d'un outil. Il implique la réalisation d'évaluations de l'impact de l'IA et d'examens de la protection de la confidentialité et de la sécurité, y compris la mise en place d'une équipe d'experts et de tests de contrainte.

Évaluer

La mesure des risques consiste à élaborer des paramètres permettant d'évaluer les risques identifiés et à tester les méthodes d'atténuation prévues afin de déterminer leur efficacité.

Gérer

La gestion des risques implique que les organisations surveillent constamment leurs performances. À ce stade, il convient d'identifier les opportunités pour les agences d'utilisateurs et de former les parties prenantes à une utilisation responsable. Le processus de gestion doit prévoir un examen et une surveillance par un humain, ainsi que des meilleures pratiques en matière de transparence, conformément aux principes de l'IA responsable.

Exploiter le potentiel de l'IA

Évolution des entreprises axée sur la sécurité

Utilisée de manière responsable et sécurisée, l'IA peut améliorer les opérations commerciales, aider votre organisation à relever les défis les plus urgents et instaurer la confiance avec vos clients. Inspirez-vous d'exemples concrets et de l'impact pour comprendre comment.

Créer un conseil dédié à l'IA

Wipro, qui compte 240 000 collaborateurs répartis dans 65 pays, est une entreprise particulièrement bien placée pour évaluer le potentiel des outils d'IA à transformer les méthodes de travail. Les collaborateurs de Wipro ont été formés aux principes de la GenAI et l'organisation reste déterminée à utiliser la technologie pour fournir de la valeur plus rapidement aux clients et améliorer les résultats dans l'ensemble de l'entreprise.

Pour mettre la puissance de l'IA au service de la main-d'œuvre, les dirigeants de Wipro ont d'abord créé un conseil dédié à l'IA afin d'établir la meilleure approche pour lancer un programme d'IA en interne. Lors de sessions bihebdomadaires, les dirigeants de Wipro ont élaboré un modèle responsable, axé sur les personas, pour la mise en œuvre de Microsoft 365 Copilot dans l'ensemble de l'entreprise. En établissant des personas distincts, y compris les commerciaux, les développeurs et les membres de l'organisation CTO, Wipro a découvert que les différents modules de Microsoft 365 Copilot complétaient des rôles distincts.

En savoir plus

Protéger la recherche vitale et les données sensibles

L'Oregon State University (OSU), une université axée sur la recherche R1, accorde une grande importance à la protection de ses recherches afin de maintenir sa réputation. Elle doit favoriser un environnement ouvert propice à la collaboration avec d'autres institutions et chercheurs, tout en veillant à ce que toutes leurs recherches restent sécurisées et conformes aux normes en vigueur.

En réponse à un incident, l'OSU a créé son Centre des opérations de sécurité. L'OSU a intégré la licence Microsoft 365 A5 et s'est engagé dans une approche Zero Trust en matière de cybersécurité en déployant largement Microsoft Sentinel et Microsoft Defender. L'OSU estime avoir atteint cinq ans de maturité en deux ans environ grâce au déploiement de la technologie de sécurité, ainsi qu'à l'assistance et aux conseils fournis par Microsoft qui ont permis de maximiser l'utilisation de cet outil.

En savoir plus

IFAD
Investing in rural people

Extraire les bonnes données au bon moment

Avec pour mission globale d'éradiquer la pauvreté et la faim dans certaines des communautés rurales les plus fragiles des pays en développement, le FIDA (Fonds international de développement agricole) travaille main dans la main avec les gouvernements pour financer des projets et des pratiques innovantes qui permettent aux petits producteurs de développer des pratiques agricoles durables, de transformer les systèmes alimentaires et de renforcer la résilience face à certains des principaux défis mondiaux. Le FIDA avait besoin d'un meilleur outil pour permettre à ses équipes mondiales et ses partenaires d'accéder à des informations critiques et de les partager depuis et vers les lieux éloignés où ils travaillent.

En utilisant Microsoft Azure OpenAI Service, Azure AI Search et Power BI, l'organisation a créé Omnidata, une plateforme d'analyse de données centralisée qui connecte les données, les tableaux de bord, les visualisations et les analyses optimisées par le machine learning et l'IA. La solution offre à tous les membres du personnel un accès rapide et direct aux données essentielles dans chaque région desservie par le FIDA, ainsi qu'une formation à l'analyse et à le machine learning afin qu'ils puissent activement créer des outils pour relever des défis quotidiens spécifiques.

En savoir plus

avanade

Réduire la complexité et renforcer la sécurité

Avanade, une coentreprise entre Accenture et Microsoft, est un cabinet de conseil qui aide à stimuler la transformation numérique dans les organisations du monde entier. Avanade dispose d'un ensemble de données vaste et complexe. L'entreprise utilise les données et l'analyse pour une variété d'activités à travers l'organisation, de la prise de décision à la garantie des meilleurs résultats pour leurs clients.

Auparavant, elle utilisait plusieurs ressources, notamment Microsoft Azure Synapse Analytics, Azure SQL Database et Power BI, pour gérer les données et les analyses. L'équipe informatique devait donc dupliquer les données chaque fois qu'un utilisateur avait besoin d'extraire des informations d'un outil vers un autre. Aujourd'hui, Avanade passe à Microsoft Fabric, qui intègre tous ses outils préférés. Il n'est donc plus nécessaire de dupliquer les données, ce qui permet de réduire la complexité, de gagner du temps et d'améliorer l'expérience des collaborateurs.

En savoir plus

Faire progresser le développement durable de l'IA

Tout comme la sécurité est un fondement essentiel de l'IA responsable, la durabilité est cruciale pour une utilisation consciencieuse de l'IA. L'IA était un outil puissant pour comprendre et réduire l'impact sur l'environnement, elle peut aider les entreprises à progresser dans leurs objectifs de durabilité et aider les entreprises privées et les institutions publiques à mieux comprendre et à s'engager dans la préservation de l'environnement, la gestion des ressources et l'atténuation du changement climatique.

Grâce aux outils de gestion des données et aux rapports de l'IA, les organisations peuvent donner de la visibilité à leurs activités de développement durable afin d'enregistrer, de rapporter et de réduire leur impact sur l'environnement. L'IA peut fournir les informations nécessaires pour prendre des décisions plus éclairées et rester sur la bonne voie pour atteindre vos objectifs en matière de développement durable.

En parallèle, nous reconnaissons l'intensité des ressources de ces applications et la nécessité d'aborder l'impact environnemental sous tous les angles.

Les chefs d'entreprise peuvent rendre leurs propres datacenters plus durables ou travailler avec des fournisseurs qui prennent déjà ces mesures, afin de réduire l'impact environnemental des datacenters qui alimentent leurs solutions d'IA.

Chez Microsoft, nous sommes très investis et nous nous concentrons davantage sur trois domaines principaux, conformément à nos engagements en matière de développement durable : l'optimisation de l'efficacité énergétique des datacenters et de l'eau, la progression des matériaux à faible teneur en carbone et l'amélioration de l'efficacité énergétique des services d'IA et de Cloud, tout cela dans le but de fournir à nos clients et à nos partenaires les outils nécessaires pour progresser de manière collective.

Commencez votre transformation par l'IA

En analysant attentivement les pratiques responsables en matière d'IA et en donnant la priorité à la sécurité dans l'ensemble de votre organisation, vous pouvez explorer le potentiel de l'IA pour contribuer à la croissance de votre entreprise.

Nos engagements et nos capacités vous permettent d'accélérer votre transformation par l'IA en toute confiance. Vous pouvez faire confiance à Microsoft pour donner la priorité à la sécurité, à la confidentialité et à la sûreté de votre IA.

En savoir plus sur l'IA Microsoft pour commencer votre transition.

Découvrez comment Microsoft s'engage à développer et à faire progresser l'IA de manière responsable.

Découvrez comment Microsoft vous aide à protéger l'IA grâce à des solutions complètes de sécurité et de gouvernance.

Sources

[1] « What Business Leaders Really Think About Generative AI », INSEAD, 11 avril 2024, https://knowledge.insead.edu/leadership-organisations/what-business-leaders-really-think-about-generative-ai.

[2] « 2024 Microsoft Responsible AI Transparency Report », Microsoft, consulté le 10 juillet 2024, https://www.microsoft.com/corporate-responsibility/responsible-ai-transparency-report.

[3] Quy Nguyen, « Basic cyber hygiene prevents 98% of attacks », Microsoft Tech Community, 18 septembre 2023, https://techcommunity.microsoft.com/t5/security-compliance-and-identity/basic-cyber-hygiene-prevents-98-of-attacks/ba-p/3926856.