Microsoft 365

Libérez le potentiel de l’IA grâce à des bases sécurisées

Sommaire

INTRODUCTION

L'opportunité de l'IA et l'impératif de sécurité

Un écart grandissant en matière de capacité et de productivité se creuse au sein de la main-d'œuvre actuelle. Selon le récent rapport de l'Indice des tendances du travail, **plus de 80 %** des travailleurs du savoir interrogés dans 31 pays (qu'ils soient employés ou dirigeants) déclarent manquer de temps ou d'énergie pour accomplir leur travail[1]. Par ailleurs,, **plus de 50 %** des dirigeants d'entreprise interrogés ont indiqué que la productivité doit augmenter pour atteindre les objectifs[1]. Cette situation représente une opportunité d'évaluer les modes de travail et les solutions potentielles pour réduire cet écart. L'IA (y compris les agents d'IA) apparaît comme une réponse prometteuse. **Plus de 80 %** des dirigeants interrogés sont convaincus que leurs organisations adopteront des agents d'IA pour renforcer la capacité de leur main-d'œuvre d'ici 12 à 18 mois[1].

Cette ruée vers l'IA s'accompagne d'une mise en garde : l'innovation doit s'accompagner de mesures de sécurité et de protection des données robustes afin de réduire les risques potentiels. Dans une récente **étude d'iSMG**, plus de 70 % des dirigeants interrogés ont indiqué que garantir la confidentialité et la sécurité des données représente le principal obstacle à l'intégration de l'IA générative dans l'infrastructure informatique existante[2]. Les dirigeants sont donc confrontés à un double impératif : accélérer l'adoption de l'IA pour stimuler la productivité et protéger les données dans cette nouvelle ère.

Cet Ebook vous présentera des scénarios d'IA susceptibles de comporter des risques, des conseils pour les atténuer avec Microsoft 365 E3, ainsi qu'une liste de contrôle pour aider les organisations à démarrer ou à poursuivre leur préparation à l'adoption de l'IA à grande échelle. Préparez-vous à adopter l'IA en toute confiance : donnez à votre organisation les moyens d'innover grâce à l'IA, sans compromettre vos normes de sécurité ni de conformité.

De bonnes intentions, mais des risques potentiels : Exemples de scénarios d'IA

Les principaux risques liés à l'utilisation et à l'adoption de l'IA proviennent souvent d'employés bien intentionnés qui cherchent à faire leur travail et à maximiser leur impact. Dans la course à l'augmentation de la productivité, les employés peuvent, sans le vouloir, divulguer des informations sensibles à des outils d'IA ou utiliser des applications qui ne sont pas encore validées par le service informatique. Cela pourrait engendrer des risques et exposer l'organisation à de nouvelles menaces.

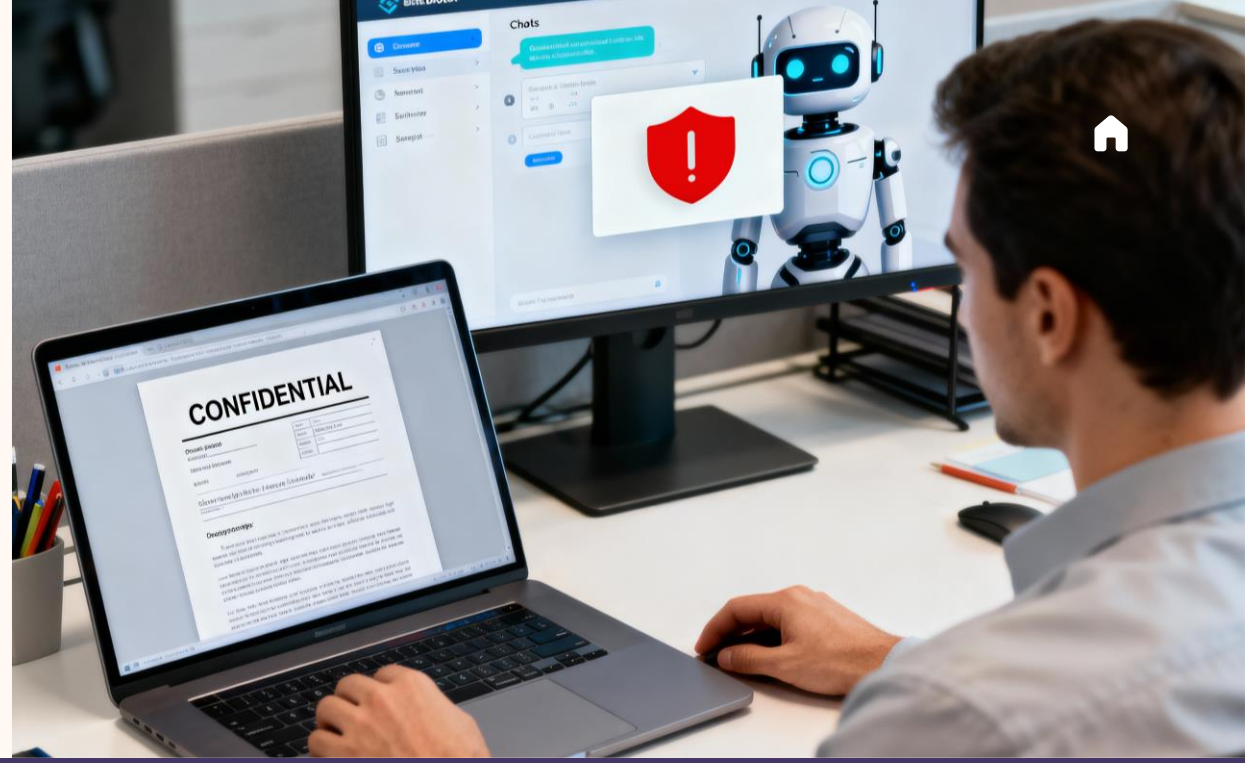
Examinons deux scénarios types pour illustrer ce point : l'un mettant en scène un directeur du marketing et l'autre un responsable de magasin.

Dans ces exemples fictifs, vous verrez : 1) comment une utilisation bien intentionnée de l'IA pourrait entraîner des failles de sécurité si elle n'est pas correctement gouvernée ; et 2) comment ces risques potentiels pourraient être atténués grâce à une base de sécurité robuste.

Scénario d'exemple 1[4]

Un directeur du marketing produit utilise un outil d'intelligence artificielle pour rédiger un communiqué de presse

Un directeur du marketing produit dans une entreprise de fabrication doit, dans un délai très serré, rédiger un communiqué de presse annonçant le lancement d'un nouveau produit prévu dans les prochains mois. Pour réfléchir à des idées et accélérer le processus de rédaction, il copie et colle des extraits d'une feuille de route produit confidentielle et d'une projection financière interne dans un assistant de rédaction en ligne gratuit alimenté par l'IA. L'outil d'IA génère rapidement quelques paragraphes bien rédigés, que le directeur utilise ensuite dans son brouillon du communiqué de presse. Cependant, cet outil n'a pas encore été vérifié ni approuvé par son organisation.



Risque potentiel :

En utilisant ce service d'IA externe, le directeur a téléchargé des données sensibles de l'entreprise (plans de produits et informations financières) vers un système tiers sur lequel l'équipe informatique n'a ni visibilité ni contrôle. Une fois que les données sont partagées avec l'outil d'IA, l'entreprise perd le contrôle car elles se trouvent au-delà des limites autorisées. L'entreprise n'est désormais plus en mesure de savoir pendant combien de temps les données sont stockées, qui y a accès, ou comment elles sont utilisées par ce tiers. Ce qui avait commencé comme un gain rapide en productivité s'est transformé en incident de fuite de données. Ce scénario reflète un risque interne potentiel lorsqu'un collaborateur bien intentionné partage des données sensibles avec un outil d'IA non autorisé, créant ainsi une vulnérabilité pour l'organisation.

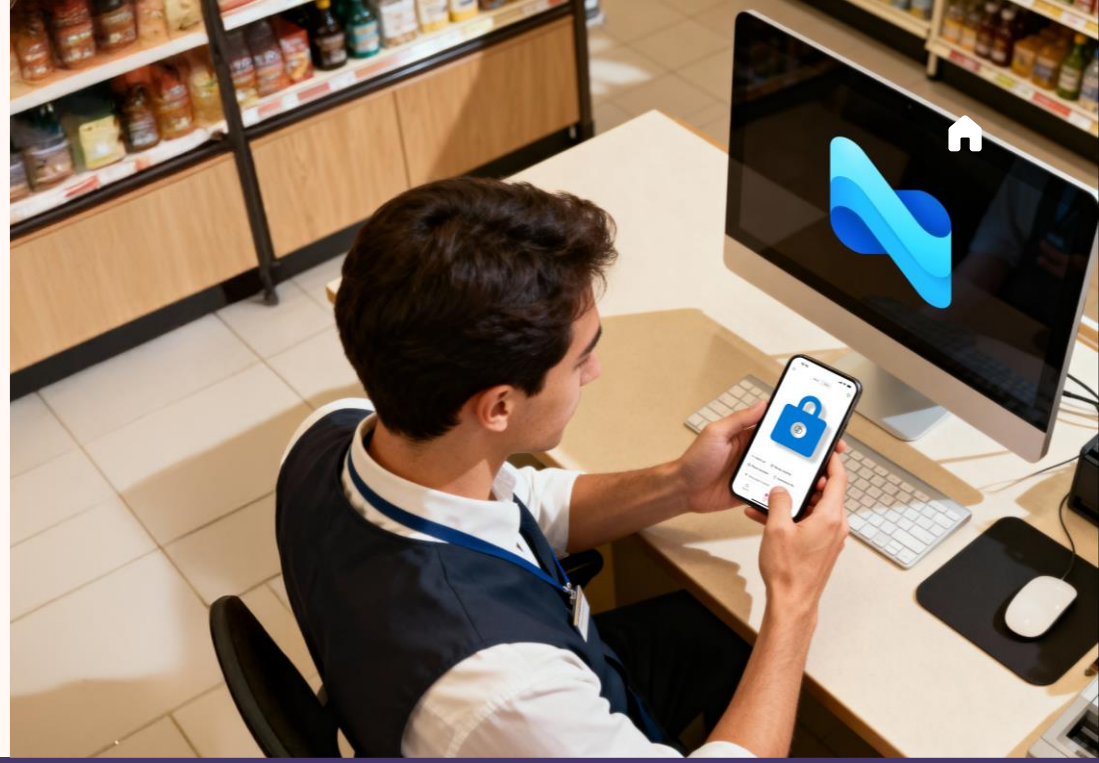
Atténuation des risques avec Microsoft 365 E3 :

Microsoft 365 E3 inclut plusieurs fonctionnalités et capacités qui pourraient permettre d'éviter cette situation. **Protection des données Microsoft Purview (Plan 1)** vous permet d'appliquer des étiquettes de confidentialité et un chiffrement à des documents tels que la feuille de route du produit et les documents de projet financier. Si ces documents avaient été classifiés et chiffrés avec des étiquettes de confidentialité telles que *Confidentiel* et du chiffrement, l'accès aux documents aurait pu être restreint uniquement aux utilisateurs autorisés. En outre, **Cloud App Discovery** peut aider à identifier les applications cloud d'IA générative utilisées (parmi les nombreuses applications répertoriées dans le catalogue), par quels utilisateurs, et à quelle fréquence. Le service informatique aurait pu découvrir que des collaborateurs utilisaient cet outil d'IA particulier et prendre des mesures pour limiter son utilisation avec **Microsoft Defender for Endpoint P1** ou proposer une alternative approuvée. Microsoft 365 E3 fournit les outils et les fonctionnalités nécessaires pour aider les organisations à améliorer leur visibilité et à atténuer les risques.

Exemple de scénario 2[4]

Un responsable de magasin utilise l'IA pour préparer les plannings et les notes de performance des employés

Un responsable de magasin dans une grande enseigne de distribution, débordé par les tâches administratives, découvre une application de productivité basée sur l'IA, gratuite, qui promet de l'aider dans la planification et la gestion de sa documentation. Pour gagner du temps, il télécharge dans l'outil d'IA une feuille de calcul contenant les noms des employés, leurs numéros de téléphone, leur salaire, leurs préférences de disponibilité et leurs dernières notes de performance. Il demande ensuite à l'application de créer un planning de travail optimisé et de l'aider à rédiger des synthèses pour les prochains entretiens individuels.



Risque potentiel :

En téléchargeant ces données sur une application d'IA non contrôlée, ce responsable a exposé les informations personnelles sensibles de ses employés à un système tiers échappant au contrôle et à la surveillance de l'entreprise. Cela pourrait créer des violations potentielles de la vie privée et des problèmes de conformité avec le droit du travail. Les départements RH et IT de l'entreprise n'ont aucune visibilité sur l'emplacement actuel des données des employés, leur durée de stockage, ni sur les personnes pouvant y accéder. Ce qui, au départ, semblait être un moyen de gagner en efficacité s'est transformé en sérieux problèmes juridiques, de confidentialité et de confiance des employés.

Atténuation des risques avec Microsoft 365 E3 :

Les fonctionnalités de gestion des appareils et des applications de Microsoft 365 E3 pourraient aider à atténuer les risques liés à ce type de scénario. Avec **Microsoft Intune P1**, l'équipe informatique du responsable de magasin pourrait appliquer des stratégies de protection des applications pour aider à imposer des règles aux applications qui accèdent aux données professionnelles, telles que la restriction du copier/coller et du transfert de données vers des applications non gérées. Si le responsable crée des stratégies d'accès conditionnel via **Microsoft Entra ID P1**, cela peut permettre de bloquer les tentatives de connexion à des comptes d'entreprise à partir d'applications ou d'appareils non gérés. Dans ce scénario, si le numéro de téléphone du responsable n'est pas conforme ou si l'application n'est pas gérée, ces stratégies pourraient empêcher l'accès aux fichiers sensibles de l'entreprise et leur téléchargement vers une application d'IA non approuvée.

POINT CLÉ : Dans les deux scénarios, l'objectif des collaborateurs était positif : améliorer l'efficacité au travail grâce à l'IA. Cependant, le résultat peut devenir négatif si les garde-fous et les stratégies appropriées ne sont pas en place. Ces exemples soulignent pourquoi l'adoption de l'IA sans filet de sécurité peut exposer les organisations à de nouveaux risques supplémentaires. L'objectif n'est pas de décourager l'utilisation de l'IA, mais de permettre son utilisation de manière responsable. La section suivante examine les principaux points à prendre en compte lors de l'évaluation de solutions susceptibles d'accroître la productivité, ainsi que les fonctionnalités de Microsoft 365 E3 qui aident les organisations à mettre en place des garde-fous pour garantir que les données sensibles restent dans des canaux sécurisés et approuvés.

Créer une base sécurisée et propice à l'IA avec Microsoft 365 E3

Votre organisation est-elle prête à déployer l'IA à grande échelle ? Examinez la liste de contrôle ci-dessous et découvrez comment Microsoft 365 E3 peut vous aider.

À mesure que l'adoption de l'IA s'accélère, il est crucial d'évaluer la posture de sécurité de votre organisation et de détecter les failles potentielles avant un déploiement à grande échelle. Microsoft 365 E3 est conçu pour être une base de productivité et de sécurité prête pour l'IA, combinant un large éventail d'outils d'identité, de sécurité, de conformité et de gestion qui fonctionnent ensemble pour vous permettre d'étendre l'adoption de l'IA en toute confiance.

Utilisez la liste de contrôle suivante comme point de départ pour comprendre la position actuelle de votre organisation. Si certains éléments ne sont pas encore entièrement mis en œuvre, votre organisation pourrait être exposée à des risques inutiles.

Appliquez des stratégies strictes de gestion des identités et des accès, telles que l'authentification multifacteur (MFA) et l'accès conditionnel.

Microsoft 365 E3 inclut **Microsoft Entra ID P1** qui permet l'application d'une gestion des identités et des accès robuste, aussi bien dans les environnements cloud que sur site. Des solutions telles que l'authentification multifacteur (MFA) et les stratégies d'accès conditionnel vérifient chaque connexion et restreignent ou autorisent l'accès en fonction de critères tels que le rôle d'utilisateur, l'intégrité de l'appareil et l'emplacement, ce qui contribue à limiter l'accès non autorisé et le partage excessif de données. Par exemple, vous pourriez restreindre l'accès aux applications d'IA à certains groupes d'employés et exiger l'authentification multifacteur pour la connexion. Vous pourriez ainsi réduire le risque de compromission de compte. Les stratégies d'accès conditionnel peuvent renforcer la protection des données sensibles en empêchant les collaborateurs d'accéder à des applications non autorisées avec des identifiants professionnels, tandis que les appareils partagés peuvent imposer des règles de déconnexion pour éviter l'utilisation non autorisée des sessions.

Favorisez une collaboration sécurisée sur l'ensemble des points de terminaison et appareils gérés.

Microsoft 365 E3 offre une sécurité intelligente des points de terminaison grâce à des solutions telles que **Intune P1, Defender for Endpoint P1 et Windows E3**. Ces outils aident à gérer et à renforcer la sécurité des PC, des appareils mobiles et des applications. Les organisations peuvent appliquer le filtrage web pour bloquer les sites à risque (y compris les outils d'IA non autorisés) et maintenir leurs appareils à jour avec des correctifs de sécurité via **Windows Autopatch et Autopilot**. Ces contrôles contribuent à maintenir les appareils sains, bien gérés et à jour grâce aux correctifs de sécurité, réduisant ainsi la surface d'attaque. La gestion unifiée des points de terminaison et la gestion des appareils permettent aux organisations de sécuriser les appareils professionnels et de garantir la conformité des applications, que les collaborateurs utilisent leurs propres appareils ou ceux fournis par l'entreprise.

Protégez les données à l'aide de fonctionnalités telles que l'étiquetage de confidentialité et les stratégies de protection contre la perte de données.

Microsoft 365 E3 offre les fonctionnalités principales de **Purview** : étiquetage de confidentialité, chiffrement et protection contre la perte de données (DLP), afin de protéger les informations sensibles dans les documents et les e-mails. Une fois les stratégies d'étiquettes publiées, les employés peuvent classer les fichiers contenant des données financières, des informations personnelles ou de la propriété intellectuelle (p. ex., avec une étiquette de confidentialité « Confidentiel »), en appliquant le chiffrement et un contrôle d'accès. Les stratégies DLP peuvent détecter et restreindre le partage non autorisé dans **Exchange Online et SharePoint Online/OneDrive Entreprise**. Même avec **Microsoft 365 Copilot**, ces mécanismes de protection demeurent actifs : Copilot respecte l'étiquette de confidentialité la plus élevée et empêche les utilisateurs non autorisés d'accéder ou d'analyser le contenu protégé.

Obtenez de la visibilité sur l'utilisation d'outils IA non autorisés et prenez des mesures éclairées.

Microsoft 365 E3 inclut **Cloud App Discovery**, qui vous aide à comprendre quelles applications d'IA sont utilisées (parmi celles incluses dans le catalogue d'applications cloud), par qui et avec quels scores de risque associés, afin que vous puissiez déterminer les actions appropriées à entreprendre. Si une application est jugée trop risquée, l'équipe informatique peut utiliser **Defender for Endpoint P1** pour limiter l'accès des utilisateurs à cette URL sur des appareils Windows 11 gérés. Par exemple, si vous découvrez que 100 utilisateurs recourent à un outil de génération d'images basé sur l'IA qui n'a pas été examiné ni approuvé par l'équipe informatique, celle-ci peut l'évaluer selon les normes de sécurité et de conformité de l'organisation. Si l'outil est jugé risqué, l'équipe informatique peut proposer une alternative approuvée. Ces fonctionnalités vous permettent d'atténuer les risques liés à l'IA fantôme et de prendre des décisions éclairées et adaptées à votre organisation concernant l'utilisation de l'IA.

Fournissez des applications d'IA approuvées, comme Microsoft 365 Copilot.

La fourniture d'applications d'IA approuvées offre une valeur ajoutée significative en donnant aux employés accès à des outils puissants et approuvés qui répondent aux normes de sécurité et de conformité de votre organisation. Par exemple, plutôt que de voir les employés se tourner vers des générateurs d'images ou des chatbots d'IA non vérifiés, l'équipe informatique peut proposer des alternatives approuvées (telles que **Microsoft 365 Copilot**) qui sont surveillées, prises en charge et intégrées aux stratégies existantes de l'entreprise. **Microsoft 365 Copilot** offre une solution d'IA sécurisée de classe entreprise, profondément intégrée à la suite de productivité Microsoft 365. **Copilot** permet aux employés de travailler plus intelligemment, d'automatiser les tâches routinières et de générer des informations, tout en respectant les stratégies d'identité et de protection des données. Cette approche réduit l'informatique fantôme, aide à limiter les fuites de données et donne aux entreprises de la visibilité et du contrôle sur la façon dont l'IA est utilisée.

Ces capacités ne fonctionnent pas de manière isolée : elles se renforcent mutuellement pour former une défense intégrée et multicouche. Les stratégies de protection des identités, des appareils et de la protection des données fonctionnent ensemble pour vous aider à atténuer les menaces. Lorsque les équipes de sécurité savent que de tels contrôles sont en place, la sécurité peut devenir un levier d'innovation plutôt qu'un frein.

Microsoft 365 E3 vous donne la possibilité d'établir les bons garde-fous afin que votre organisation puisse innover avec l'IA sans compromettre la sécurité.

Poursuivre l'adoption de l'IA

Toutes les organisations cherchent aujourd'hui à déterminer comment l'IA peut servir au mieux leurs objectifs. La promesse est séduisante, mais l'adoption de l'IA doit aller de pair avec une protection robuste. Avec Microsoft 365 E3, vous n'avez pas à choisir entre les deux. Vous bénéficiez d'une suite puissante qui élève votre posture de sécurité et de conformité, ce qui vous permet d'adopter l'IA en toute confiance.

Évaluez votre niveau de préparation en matière de sécurité pour l'IA.

Microsoft propose une **Évaluation de la sécurité pour l'IA**[3]. Cette évaluation en ligne (disponible sur security-for-ai-assessment.microsoft.com) fournit des recommandations pour améliorer la sécurité de votre IA en fonction des informations que vous fournissez. Elle vous aide à évaluer la sécurité actuelle de votre IA à travers quatre piliers clés : **Préparer**, **Découvrir**, **Protéger**, et **Gouverner**, ainsi que des recommandations exploitables.

En savoir plus et interagir avec Microsoft.

Explorez plus en détail les fonctionnalités de Microsoft 365 E3 et comment elles peuvent vous aider à adopter l'IA en toute confiance. www.microsoft.com/en-us/microsoft-365/enterprise/e3?activetab=pivot:overviewtab. Vous pouvez également contacter votre équipe de compte Microsoft ou votre partenaire.

1. Rapport annuel de l'Indice des tendances du travail, 2025 : L'année de naissance de l'entreprise pionnière Microsoft, Inc., avril 2025. Microsoft a analysé les données d'une enquête menée auprès de 31 000 travailleurs du savoir employés à temps plein ou indépendants dans 31 pays, entre le 6 février 2025 et le 24 mars 2025, ainsi que les tendances du marché du travail LinkedIn et des billions de signaux de productivité issus de Microsoft 365.
2. Second Annual Generative AI Study: Business Rewards vs. Security Risks, iSMG, Inc., février 2025 – d'après une enquête réalisée auprès de plus de 360 professionnels des affaires et de la cybersécurité, menée au troisième trimestre 2024.
3. Évaluation de la sécurité pour l'IA : security-for-ai-assessment.microsoft.com/ L'exactitude des résultats dépend de l'exactitude de vos données. Ce rapport est fourni à titre informatif uniquement et ne garantit ni les performances ni les résultats Il ne doit pas être interprété comme un engagement de la part de Microsoft. Les résultats réels peuvent varier en fonction de facteurs tels que l'emplacement, la méthode d'achat et l'utilisation. Microsoft n'offre aucune garantie expresse ou garantie implicite concernant le contenu de ce rapport ou site web.
4. Les scénarios présentés sont fictifs et proposés uniquement à titre illustratif.