Microsoft 365

De la surveillance à l’analyse approfondie : Gestion des risques liés à l’IA fantôme

Sommaire

Présentation 03

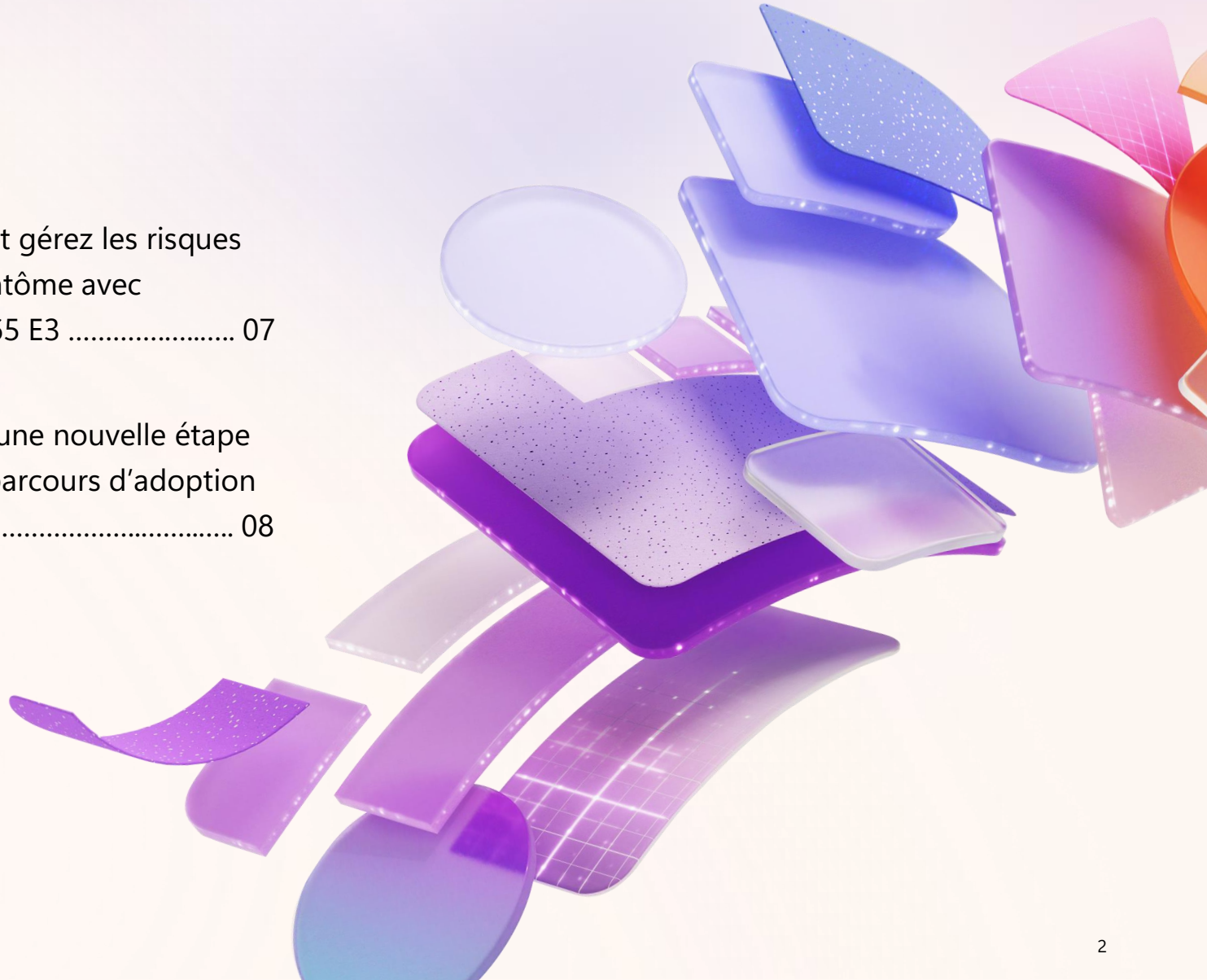
Qu'est-ce que l'IA fantôme ?
Et pourquoi la visibilité est-elle
importante 04

L'IA fantôme en entreprise :
Exemples de scénarios et
de risques potentiels 05

Cinq façons de gérer les risques
liés à l'IA fantôme 06

Découvrez et gérez les risques
liés à l'IA fantôme avec
Microsoft 365 E3 07

Franchissez une nouvelle étape
dans votre parcours d'adoption
de l'IA 08



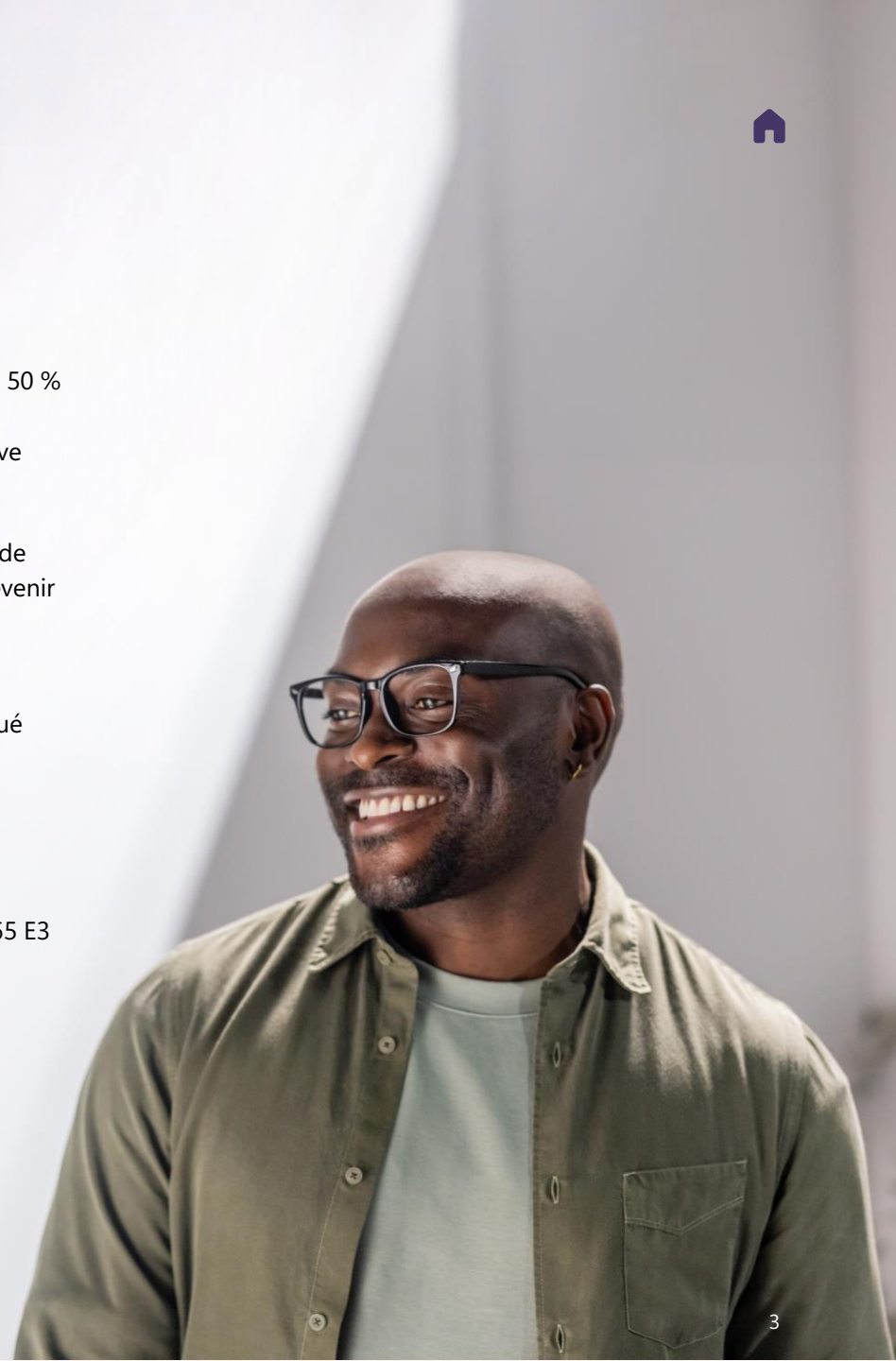
Présentation

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. Par ailleurs, plus de 50 % des dirigeants d'entreprise interrogés estiment que la productivité doit augmenter pour atteindre leurs objectifs[1]. Selon le rapport 2024 de l'Indice des tendances du travail de Microsoft, de nombreux employés se tournent vers des outils d'IA générative pour combler cet écart et n'attendent pas l'approbation officielle du service informatique pour commencer à les utiliser.

Lorsque des outils échappent à la vigilance du service informatique, ils peuvent exposer l'organisation à des risques en matière de sécurité et de conformité. Et l'IA fantôme (l'utilisation d'outils d'IA sans l'approbation du service informatique) est en train de devenir la dernière forme d'informatique fantôme dans les environnements de travail actuels.

À mesure que l'adoption de l'IA s'accélère, les chefs d'entreprise s'efforcent de garder une longueur d'avance et d'atténuer les risques potentiels que ces outils peuvent poser. Dans une récente étude 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]. De plus, plus de 90 % des DSI et CTO interrogés ont indiqué que l'IA générative a déjà conduit ou entraînera des investissements plus importants dans la cybersécurité au sein de leur organisation[3].

Dans cet Ebook, vous allez découvrir comment l'IA fantôme s'introduit dans les environnements de travail, identifier les risques qu'elle peut représenter pour votre organisation, apprendre cinq stratégies clés pour les maîtriser et voir comment Microsoft 365 E3 peut vous accompagner.



[1] **Rapport annuel de l'Indice des tendances du travail Microsoft 2025,** 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 Microsoft 365.

[2] **iSMG Second Annual Generative AI Study: Business Rewards vs. Security Risks,** étude basée sur les réponses à une enquête menée au troisième trimestre auprès de plus de 360 professionnels du business et de la cybersécurité dans 6 régions (Amérique du Nord, Europe, Asie, Amérique du Sud, Australie et Afrique).

[3] **The AI Security Balancing Act: From Risk to Innovation," NTT DATA, juin 2025,** étude basée sur les données d'une enquête NTT DATA auprès de plus de 2 300 décideurs seniors en GenAI, dont 1 500 membres de la direction dans 34 pays.

Qu'est-ce que l'IA fantôme ? Et pourquoi la visibilité est-elle importante ?

L'IA fantôme fait référence à l'utilisation d'outils et d'applications d'intelligence artificielle par des collaborateurs sans l'approbation explicite ou la supervision des services informatiques, souvent en dehors des cadres officiels de sécurité et de conformité. Alors que les collaborateurs cherchent à améliorer leur productivité et à répondre aux exigences croissantes de leur charge de travail, ils peuvent se tourner vers ces solutions non approuvées pour rationaliser les tâches, collaborer ou générer de nouveaux contenus, souvent sans se rendre compte des risques potentiels encourus. L'IA fantôme échappe à la visibilité des services informatiques, ce qui rend difficile pour les organisations d'identifier les applications utilisées et celles qui présentent les risques les plus élevés.

L'importance de la visibilité de l'IA fantôme

Lorsqu'un service informatique ignore l'existence d'une application ou d'un service, il ne peut ni le sécuriser ni le prendre en charge. Ce *manque de visibilité* rend difficile l'identification, la gestion ou l'atténuation précise des menaces potentielles liées à l'exposition de données sensibles, à la non-conformité réglementaire et à la perte de contrôle sur les informations propriétaires. Les responsables informatiques et les dirigeants d'entreprise doivent gagner en visibilité sur l'utilisation de l'IA fantôme au sein de leur organisation, aborder les risques émergents associés à l'utilisation de l'IA et décider quels outils doivent être autorisés avec les bons garde-fous. Les organisations ont l'opportunité de faire de l'IA fantôme non pas un risque, mais un moteur d'innovation dans la façon de travailler, tout en garantissant la sécurité. Pour y parvenir, il est nécessaire de trouver un meilleur équilibre : permettre aux employés de tirer parti d'outils d'IA utiles au sein d'un cadre gouverné et sécurisé, afin de limiter les risques potentiels.

PERSPECTIVE

On ne peut pas sécuriser ce que l'on ne voit pas. Lorsque le service informatique n'a pas connaissance de l'utilisation d'une application ou d'un service, il ne peut pas en assurer la sécurité. C'est là tout le problème de l'IA fantôme et cela met en évidence la nécessité d'une nouvelle approche. Interdire purement et simplement tous les outils externes n'est pas réaliste si les employés estiment que ces outils d'IA sont essentiels pour atteindre leurs objectifs. Les organisations doivent plutôt mettre en lumière l'IA fantôme : comprendre quels outils sont utilisés, instaurer les contrôles appropriés et proposer des alternatives sécurisées et approuvées qui répondent aux besoins de l'entreprise. En résumé, le défi consiste à donner aux équipes les moyens d'utiliser l'IA *sans* compromettre la sécurité.

L'IA fantôme en entreprise : Exemples de scénarios et de risques potentiels

L'IA fantôme résulte de l'initiative d'employés qui souhaitent accroître leur productivité et leur impact ou essayer une nouvelle technologie. Vous trouverez ci-dessous plusieurs exemples fictifs illustrant comment des outils d'IA non approuvés peuvent être utilisés et les risques potentiels associés.

Domaine	Exemple de scénario	Risques potentiels liés aux outils non approuvés
Marketing	Utilisation d'un outil d'IA générative pour créer du contenu marketing ou des designs à partir de données de la marque.	Fuite d'informations sensibles sur la marque ou les produits, perte de contrôle sur la façon dont un service d'IA externe pourrait stocker ou utiliser les ressources créatives de l'entreprise.
Finance	Téléchargement des données financières d'une entreprise dans un service d'analyse pilotée par l'IA ou de visualisation pour obtenir rapidement des informations.	Divulgation de données financières confidentielles (budgets, prévisions) à un tiers, violations potentielles de la conformité (p. ex., RGPD) si des données de clients ou d'employés sont incluses sans mesures de protection appropriées.
Support client	Partage des données client ou des transcriptions de conversations du support dans un outil d'IA afin de rédiger des réponses ou de résumer des dossiers.	Violation des règles de confidentialité et de gestion des données : des informations client sensibles pourraient être stockées en dehors des systèmes de l'entreprise, aucune garantie quant à la rétention ou à la suppression correcte des données par le fournisseur d'IA.
Personnel de première ligne – Distribution	Des responsables de magasin utilisent des applications d'IA de planification sur leur téléphone pour optimiser les plannings des équipes.	Données du personnel de l'entreprise (noms des employés, plannings) transférées vers une application non autorisée, ce qui risque de poser des problèmes de confidentialité. Des conflits d'horaires ou des violations de politiques internes peuvent également survenir si les suggestions de l'IA ne respectent pas la réglementation du travail.
Personnel de première ligne – Santé	Des infirmiers ou des médecins utilisent un chatbot d'IA pour aider à rédiger des notes sur le suivi des patients ou répondre à des questions médicales.	Les informations de santé des patients pourraient être exposées à un service externe sans aucune protection, en violation des exigences de conformité et de confidentialité. Les conseils médicaux fournis par l'IA ne sont pas forcément vérifiés, ce qui présente des risques pour la sécurité.

Dans chacun des cas ci-dessus, l'employé avait de bonnes intentions et cherchait simplement à gagner en productivité, mais c'est l'organisation qui peut se retrouver exposée à des risques.

Les informations de l'entreprise peuvent se retrouver dispersées sur des plateformes non approuvées, créant *de véritables casse-têtes en matière de gouvernance des données*. Des applications non vérifiées peuvent introduire des malwares ou des vulnérabilités de sécurité, élargissant la surface d'attaque en dehors du champ de contrôle des services informatiques. Il peut également y avoir des implications en matière de conformité. Du point de vue du support IT, si un problème survient avec un outil d'IA fantôme, le service d'assistance risque de ne pas pouvoir aider les utilisateurs, faute de visibilité ou de contrôle sur cet outil.

Cinq façons de gérer les risques liés à l'IA fantôme

Avec la bonne stratégie et les bons outils, vous pouvez faire passer l'IA fantôme d'une menace potentielle à une opportunité de favoriser une culture d'innovation sécurisée. Offrez à vos équipes des outils d'IA de productivité *tout en* maintenant la supervision nécessaire pour protéger votre entreprise. Il s'agit de passer de « non, jamais » à « oui, mais avec les bons garde-fous ». Les cinq conseils suivants sont conçus pour vous aider à gérer et reprendre le contrôle de l'IA fantôme au sein de votre organisation :

01 Identifier votre empreinte d'IA fantôme pour évaluer et hiérarchiser les risques

Vous ne pouvez pas protéger ce que vous ne voyez pas. Gagnez en visibilité sur les applications utilisées au sein de votre organisation grâce à vos journaux d'activité. Une fois que vous avez recensé les applications utilisées, vous pouvez déterminer quels outils sont adaptés à la gestion des données sensibles, tout en identifiant ceux qui ne sont pas conformes à vos stratégies de sécurité et de conformité. Grâce à ces informations, vous pouvez prendre une décision plus éclairée sur les applications que vous souhaitez autoriser, surveiller ou limiter afin de réduire les risques potentiels.

02 Mettre en œuvre des solutions rapides grâce aux stratégies de sécurité et de conformité

Activez ou appliquez des correctifs de stratégie afin de mieux atténuer les risques potentiels liés à l'usage de l'IA fantôme. Vous pouvez utiliser des stratégies d'accès conditionnel pour restreindre l'utilisation des applications à haut risque, appliquer une protection contre la perte de données pour les informations sensibles afin de réduire la divulgation excessive et les fuites de données, et imposer une authentification multifacteur de base ainsi que la conformité des appareils pour tous les utilisateurs. Ces actions permettent de réduire rapidement les risques les plus évidents, même si vous n'avez pas encore une visibilité complète sur les applications d'IA utilisées.

03 Sensibiliser les employés aux risques potentiels de l'IA fantôme

Souvent, les employés ne sont pas conscients des risques que l'utilisation d'outils d'IA non approuvés peut faire peser sur l'organisation. Communiquez régulièrement les risques liés à l'IA fantôme au moyen d'avertissements bien ciblés sur la protection contre la perte de données, de rappels des politiques de l'entreprise et de courtes formations. L'objectif est d'orienter les utilisateurs vers des pratiques plus sûres, sans recourir à des mesures trop contraignantes.

04 Fournir des outils d'IA approuvés pour atténuer davantage les risques

Dans la mesure du possible, proposez aux employés des outils d'IA approuvés comme alternatives aux outils non autorisés. Une excellente façon de réduire l'IA fantôme consiste à couvrir les cas d'utilisation les plus courants dans votre organisation avec une solution approuvée. Cela permet au service informatique de conserver une visibilité et un contrôle, tout en offrant un support aux utilisateurs en cas de problème.

05 Établir une gouvernance continue

Intégrez des contrôles dans votre routine de gouvernance informatique : examinez régulièrement les journaux d'activité et les rapports, mettez à jour les politiques à mesure que de nouveaux services d'IA apparaissent, et tenez la direction informée des progrès réalisés (comme la baisse de l'usage d'applications non approuvées ou les incidents évités). Cela vous aidera à atténuer les risques potentiels dès maintenant et à l'avenir, à mesure que le paysage évolue.

En suivant les étapes ci-dessus, vous favorisez à la fois l'innovation et la sécurité.

Les employés peuvent utiliser des solutions d'IA approuvées au travail, et le service informatique conserve le contrôle et la conformité de ces outils.

Découvrez et gérez les risques liés à l'IA fantôme avec Microsoft 365 E3

Microsoft 365 E3 offre aux organisations la capacité de détecter l'IA fantôme, d'évaluer les risques potentiels et de mettre en œuvre des stratégies de sécurité et de conformité *sans* freiner l'innovation. Cette suite de fonctionnalités intégrées de productivité, de sécurité et de gestion peut vous permettre de relever directement les défis de l'IA fantôme.

Solution Microsoft 365 E3	Comment cette solution vous aide à gérer les risques potentiels liés à l'IA fantôme
Cloud App Discovery	**Identifiez et prenez les mesures nécessaires concernant les applications non autorisées.** Cloud App Discovery vous permet de télécharger des journaux d'activité et de créer des rapports instantanés pour obtenir une visibilité sur plus de 31 000 applications cloud (dont plus de 400 applications d'IA générative). Il vous permet de voir ce qui est utilisé dans votre organisation, par qui et à quelle fréquence. Ces informations vous permettent de prendre des décisions éclairées sur les applications à autoriser ou à limiter au sein de votre organisation.
Protection contre la perte de données Microsoft Purview (DLP)	**Réduisez les fuites de données sensibles.** Microsoft Purview DLP vous permet de définir et d'appliquer des stratégies qui détectent les informations sensibles et en bloquent ou en restreignent le partage dans les services Microsoft 365, que ce soit pour les e-mails ou les fichiers. Par exemple, vous pouvez créer une règle pour surveiller, auditer ou empêcher les utilisateurs de partager des informations sensibles par e-mail ou via le partage de fichiers, tout en les avertissant.
Microsoft Entra ID P1	**Gérez l'accès aux applications cloud.** Microsoft Entra ID P1 permet de mettre en place des stratégies d'accès conditionnel afin de contrôler qui peut accéder à quelles applications, et dans quelles conditions. Par exemple, vous pouvez exiger une authentification multifacteur ou même limiter les connexions avec des identifiants professionnels pour les applications que vous avez identifiées comme présentant un risque plus élevé. Microsoft Entra ID P1 permet l'accès aux ressources cloud aux bonnes personnes, sur des appareils conformes, dans des conditions approuvées (tout en limitant l'accès aux applications non approuvées).
Microsoft Intune P1	**Appliquez des stratégies d'utilisation des appareils et des applications.** Microsoft Intune P1 vous donne la possibilité d'autoriser l'utilisation d'appareils gérés et conformes à des fins professionnelles, et vous fournit des outils pour gérer ces appareils. Par exemple, Intune peut interdire l'installation de logiciels non approuvés sur les PC de l'entreprise, ou déployer des configurations qui limitent l'accès à certains sites web ou services.
Microsoft Defender for Endpoint P1	**Limitez le trafic vers les URL non approuvées.** Microsoft Defender for Endpoint P1 vous aide à réduire les risques liés aux sites que vous jugez dangereux en bloquant le trafic vers une URL non approuvée depuis des appareils gérés. Par exemple, un employé tentant d'accéder à un site d'IA connu comme risqué depuis un ordinateur portable de l'entreprise en serait empêché.

Franchissez une nouvelle étape dans votre parcours d'adoption de l'IA

Tout commence par la sensibilisation, les bons outils et une approche proactive. Microsoft 365 E3 fournit les outils permettant à votre organisation d'établir une base de sécurité robuste et un cadre de gouvernance pour les solutions d'IA. Vous pourrez gagner en visibilité sur les outils non autorisés, mettre en place des stratégies pour protéger les données sensibles, et maintenir le contrôle sur l'accès des utilisateurs ainsi que sur la sécurité des appareils. Préparez-vous à passer d'une posture réactive (repérer et bloquer l'IA fantôme après son apparition) à une approche plus proactive consistant à orienter l'utilisation de l'IA vers des canaux gérés et sécurisés. Passez l'Évaluation de la sécurité pour l'IA et découvrez comment renforcer votre posture de sécurité pour l'IA. Découvrez également les fonctionnalités incluses dans Microsoft 365 pour les grandes entreprises.