Guide exécutif pour sécuriser les données dans le cadre de l'IA générative

Protéger la transformation de l'IA et la productivité de la main-d'œuvre avec la sécurité des données en tout lieu.

Introduction

Comme cette tasse de café du matin, les invites de chat GenAI sont devenues essentielles à notre journée de travail. Du marketing et de la finance à l'ingénierie et à l'informatique, l'IA révolutionne la façon dont les services de votre entreprise ou de votre agence gouvernementale fonctionnent. C'est comme les changements numériques que nous avons vus dans le passé – seulement sous stéroïdes. L'intégration des outils d'IA générative dans les flux de travail quotidiens stimule la productivité et la croissance. Cependant, cette efficacité retrouvée ouvre également la porte à l'exposition potentielle des données sensibles en ligne.

Lorsque les utilisateurs téléchargent ou collent des informations privées dans les chats GenAI, les modèles de langue stockent souvent ces données et en tirent des leçons. Quelle que soit la façon dont on le présente, c'est un risque important de perte de données. L'appétit insatiable de l'IA pour les données, combiné à des menaces comme les ransomwares, fait de la protection de la vie privée et du respect de la conformité réglementaire, un défi complexe.

Pour exploiter le potentiel de l'IA sans risquer votre entreprise, vous avez besoin de la liberté d'expérimenter en toute sécurité. C'est là qu'une approche de sécurité axée sur les données peut être un avantage concurrentiel. En unifiant la visibilité et le contrôle, vous pouvez innover en toute sécurité.

Ce guide vous aidera à réussir votre transformation en matière d'IA en toute sérénité, en offrant des recommandations et des informations sur les capacités de sécurité essentielles et les bonnes pratiques. De plus, nous explorerons comment la plateforme alimentée par l'IA de Forcepoint peut réduire de manière significative les risques et prévenir la perte de données dans les applications, faisant de Zero Trust pour l'IA une réalité tout en simplifiant la conformité.

Des entreprises utilisent ou prévoient d'utiliser l'IA dans les 12 prochains mois

Source : Enquête IDC sur la valeur de l'IA dans les entreprises, septembre 2023

Des entreprises adoptent l'IA générative à un rythme très rapide

Source : Deloitte : État de l'IA générative dans le rapport d'entreprise du 2e trimestre, avril 2024

plus de ROI pour chaque dollar investi dans l'IA

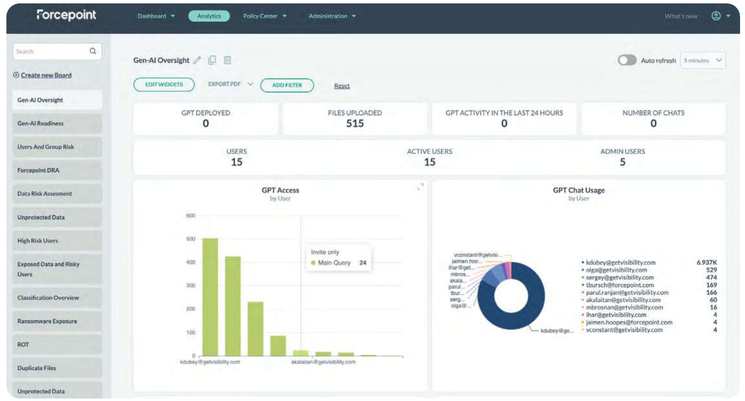
Source : Enquête IDC sur la valeur de l'IA dans les entreprises, septembre 2023

Obtenir une visibilité des données sensibles

Imaginez vous frayer un chemin à travers une forêt dense sans carte. Vous n'avez aucune idée de l'endroit où les dangers se cachent ou de l'endroit où les précieuses ressources sont cachées. Obtenir une visibilité dans votre environnement d'IA s'apparente à la création d'une carte en direct et détaillée. Vous identifiez l'endroit où les données sensibles sont stockées et vous comprenez qui y a accès. Certaines solutions de sécurité de l'IA utilisent également la criminalistique numérique et le suivi des modèles d'utilisation pour identifier les vulnérabilités comme les failles de conformité. Avec cette clarté, vous pouvez identifier et atténuer les risques avant qu'ils ne s'aggravent. La découverte des données, la classification et la surveillance permanente servent de compas et de guide, pour que vous ayez toujours une longueur d'avance sur les menaces potentielles.

Avantages Forcepoint :

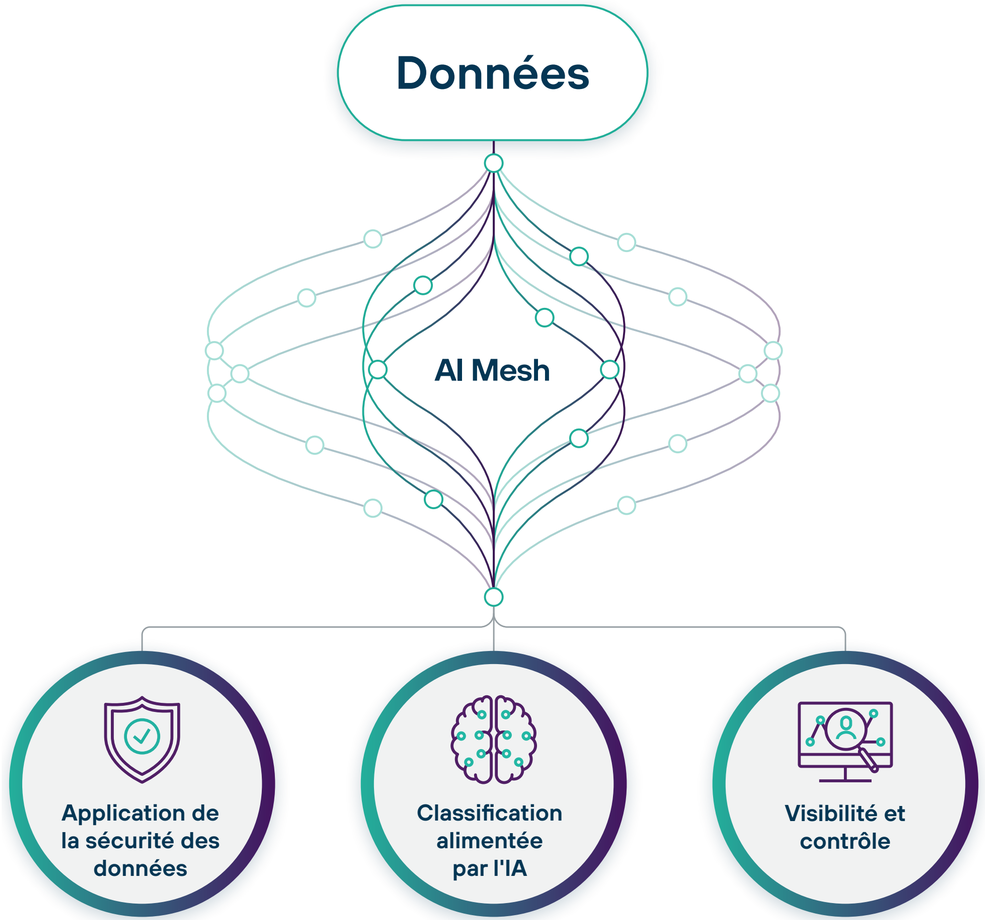
- **Data Security Posture Management (DSPM) :** optimisée par l'IA Mesh, la DSPM permet une gestion proactive des risques liés aux données en découvrant les vulnérabilités sur les réseaux, les appareils et le cloud. Elle analyse un million de fichiers par heure et utilise l'IA Mesh pour classifier les données sensibles avec précision en un temps quasi instantané, aidant les administrateurs à réduire les informations obsolètes, à définir les autorisations appropriées et à déplacer les données vers des sites sécurisés. Pour ChatGPT Enterprise, DSPM résume l'utilisation des données sensibles dans les chats d'IA et signale les violations de sécurité et de confidentialité.
- **DLP avec Risk-Adaptive Protection :** cette solution surveille en permanence le flux de données et le comportement de l'utilisateur, en ajustant automatiquement les niveaux de protection en fonction des évaluations des risques en temps réel. Les utilisateurs peuvent sans le savoir commettre des erreurs qui pourraient entraîner des fuites ou une perte de données ; Forcepoint fournit un coaching automatique pour guider l'utilisation sécurisée de l'IA, ainsi que des rapports criminalistiques sur les tentatives de perte de données et les réponses des utilisateurs, ce qui aide les administrateurs à affiner les programmes de coaching et de formation.
- **Intégration de l'API OpenAI :** Forcepoint est l'une des huit entreprises choisies par OpenAI comme outils de conformité et d'administration pour ChatGPT Enterprise. Forcepoint DSPM tire parti des API OpenAI pour fournir des tableaux de bord clairs qui montrent qui utilise ChatGPT Enterprise, quels fichiers sont téléchargés et les risques commerciaux potentiels. Cette visibilité complète sur l'utilisation des données sensibles vous permet de créer plus facilement des politiques de sécurité des données robustes, que les solutions Forcepoint ONE SSE et DLP appliquent pour prévenir les téléchargements de données inappropriés.



Forcepoint fournit des rapports d'évaluation des risques qui vous aident à visualiser les risques pour toute plateforme GenAI, y compris l'affichage du comportement de l'utilisateur et la remédiation complète dans ChatGPT Enterprise.

Classifier les données à l'aide de l'IA Mesh

L'IA Mesh de Forcepoint combine des modèles de langage, des réseaux de neurones profonds, des éléments de données et l'apprentissage machine pour classifier rapidement et avec précision les données en moins de 200 millisecondes. Elle est hautement personnalisable, pour qu'elle puisse être ajustée à leurs exigences sectorielles, réglementaires ou clients pour une classification des données incroyablement précise et nécessitant peu d'entretien qui réduit de manière significative le risque d'exposition aux données sensibles.



Obtenir le contrôle des données sur GenAI Chat

Vous savez où se trouvent les ressources critiques (données sensibles), mais vous devez maintenant gérer qui détient les clés et comment elles sont utilisées. La prochaine étape est de contrôler l'accès, l'utilisation et le partage de contenu dans les applications, les sites web et les outils d'IA. Pour cela, vous avez besoin d'un système de sécurité intelligent qui non seulement accorde l'accès, mais surveille chaque entrée, ajuste les autorisations à la volée et traite immédiatement les tentatives de violation comme le collage ou le téléchargement de données sensibles dans les chats d'IA. C'est ce qu'offrent des autorisations précises et des contrôles fondés sur les risques. En unifiant le cadre politique pour diverses capacités de sécurité comme la DLP, CASB, SWG et ZTNA, vous rationalisez la gestion, en veillant à ce que vos données propriétaires et réglementées soient sécurisées.

Avantages Forcepoint :s:

- **Forcepoint DLP :** protège les données en limitant ou en bloquant l'accès aux outils GenAI sanctionnés. Forcepoint applique des actions de sécurité des données pour prévenir la perte de données grâce à GenAI. Les capacités de Risk-Adaptive Protection aident les équipes à mettre en œuvre rapidement et avec précision la remédiation automatisée et les contrôles d'accèsfondés sur les risques pour appliquer les politiques de manière dynamique. Nous utilisons également l'IA pour identifier les données avec une classification très précise afin que les politiques de sécurité soient plus efficaces.
- **Forcepoint ONE SSE (trafic Web, SaaS applications, applications privées) :** garantit l'accès Zero Trust aux applications d'IA, sites web et contenu en analysant les risques et la réputation des sites, en désignant des catégories de sites autorisés, en restreignant les utilisateurs et en bloquant ou limitant les activités impliquant des informations sensibles. Notre plateforme gérée dans le cloud isole le contenu web pour prévenir les programmes malveillants et désinfecte les fichiers pour supprimer les menaces, protégeant les utilisateurs et les données de l'IA sans perturber les flux de travail.
- **Politique unifiée basée dans le cloud : r**ationalise l'application des politiques pour Forcepoint ONE Data Security et Forcepoint ONE SSE dans plusieurs domaines de sécuritéy compris les points de terminaison, le courriel, les réseaux, les sites web, les applications cloud et les applications privées. Avec une application cohérente et unifiée, les équipes de sécurité peuvent gérer une politique de sécurité unique dans le cloud ou sur site pour tous les canaux.

Augmenter la productivité et le ROI

Désormais, avec des itinéraires clairs et des checkpoints sécurisés vous aidant à trouver tous les chemins de données cachés, les dangers et les trésors, il est temps de tirer le meilleur parti de votre parcours de transformation de l'IA. Une fondationbasée sur une gestion unifiée protège non seulement vos données dans les interactions avec l'IA, mais améliore également la productivité et réduit les coûts en regroupant les outils et les relations avec les fournisseurs. Votre entreprise peut désormais permettre aux employés d'explorer en toute sécurité le potentiel innovant de l'IA et au-delà, que ce soit dans les applications cloud, les sites web, les appareils ou les courriels. La simplification de votre infrastructure de sécurité avec moinsd'outils et un seul fournisseur facilite la mise en œuvre et le maintien d'une sécurité complète. En sécurisant toutes vos données à partir d'un seul ensemble de politiques et d'emplacement, vous pouvez réduire les coûts opérationnels grâce à l'automatisation et à l'élimination des processus redondants.

Croissance de la productivité pour les travailleurs qui accèdent à l'IA

Source : Le Bureau national de la recherche économique

Réduction des coûts opérationnels en rationalisant la gestion des politiques DLP

source: IDC

Envisager l'unification de la sécurité des données de plusieurs produits DLP dans une seule interface

Source: IDC

Conclusion

Dans un monde où l'IA remodèle les industries, comment garantir la sécurité de vos données ? La stratégie d'intégration de l'écosystème d'IA de Forcepoint et les capacités de « sécurité des données en tout lieu » vous permettent d'utiliser les systèmes et les outils d'IA en toute sérénité. Notre approche multicouche de la sécurité de l'IA protège les données, quel que soit le type ou la compétence de l'utilisateur de l'IA. Commençons le voyage ensemble pour prendre le contrôle de vos systèmes et de vos flux de travail d'IA générative.

Prochaines étapes :

- → **Évaluez votre posture de sécurité actuelle de l'IA :** comprenez vos forces et vos faiblesses.
- → **Identifiez les domaines clés à améliorer :** repérez les vulnérabilités et les opportunités.
- → **Mettez en œuvre une stratégie de sécurité axée sur les données :** obtenez une visibilité et un contrôle unifiés dans vos initiatives d'IA.

Prêt à sécuriser votre transformation de l'IA ?

Parlez à un expert dès aujourd'hui pour en savoir plus sur la façon d'innover en toute sécurité.

Parler à un expert

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint simplifie la sécurité pour les entreprises et les gouvernements dans le monde. La plateforme tout-en-un de Forcepoint, véritablement native dans le cloud, facilite l'adoption de Zero Trust et empêche le vol ou la perte de données sensibles et de propriété intellectuelle, quel que soit le lieu de travail. Basée à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables pour les clients et leurs employés dans plus de 150 pays. Engagez-vous avec Forcepoint sur www.forcepoint.com, Twitter et LinkedIn.

[FP-Exec Guide to Securing Data within GenAI ebook-FR] 05Aug2024