Configurer GPT de conversation privée et limiter l'accès à d'autres applications d'IA génératives

Table des matières

Introduction

Ce document décrit comment configurer un ChatGPT privé et restreindre l'accès à d'autres applications d'IA génératives.

Aperçu

Le paysage de l'intelligence artificielle évolue rapidement, et l'une des avancées majeures a été le développement de l'IA générative. Parmi ceux-ci, ChatGPT a eu un impact significatif.
Alors que les entreprises cherchent à intégrer ces outils puissants dans leurs workflows, la nécessité de contrôler l'accès aux applications d'IA générative est devenue de plus en plus évidente. Pour les entreprises qui ont développé leurs propres instances privées ChatGPT, s'assurer qu'il s'agit du seul outil d'IA accessible à leur équipe tout en limitant d'autres applications d'IA générative, est une mesure de sécurité essentielle.

Heureusement, il existe un moyen simple d'y parvenir à l'aide du tableau de bord Umbrella. Cet article vous guide à travers les étapes à suivre pour permettre à votre organisation de bénéficier de votre ChatGPT privé tout en maintenant des contrôles stricts sur l'utilisation d'autres applications d'IA.

Étape 1 : Créer une règle Web pour autoriser votre discussion privéeGPT

Tout d'abord, vous devez vous connecter à votre tableau de bord Umbrella. Une fois sur place, vous pouvez créer une règle DNS ou une règle Web.
Cette règle doit avoir l'action « Autoriser » et une « Liste de destinations » avec l'URL spécifique de votre GPT de discussion privée.
Cette étape garantit que les utilisateurs au sein de votre organisation peuvent accéder à votre GPT de discussion privé sans aucune restriction.

Étape 2 : Bloquer toutes les autres applications d'IA génératives

Immédiatement après la création de la règle « Autoriser », vous devez créer une deuxième règle. Cette règle doit avoir l'action « Bloquer » et doit inclure une « Liste d'applications » qui englobe la catégorie IA générative.
Ce faisant, vous êtes en mesure d'empêcher l'accès à un large éventail d'applications populaires d'IA générative, y compris la version publique de ChatGPT.

Stratégie DNS

Garantir que ces règles sont effectivement appliquées lors de l'utilisation de la stratégie DNS et non de la stratégie Web.
Il est essentiel d'activer le proxy intelligent et le décryptage SSL pour une expérience transparente. En outre, l'installation du certificat racine Cisco Umbrella est nécessaire pour le bon fonctionnement du déchiffrement SSL.

Pour obtenir des conseils complets sur la configuration de la stratégie DNS, reportez-vous à la documentation officielle ici.
En outre, pour optimiser l'efficacité de vos politiques DNS, consultez les meilleures pratiques ici.

Stratégie Web

Pour plus d'informations sur la gestion des stratégies Web et leur adaptation aux besoins de votre entreprise, rendez-vous ici.

La mise en oeuvre de ces mesures permet à votre entreprise de tirer pleinement parti de votre ChatGPT privé tout en limitant le risque de fuite de données ou de distractions pouvant découler de l'utilisation d'autres applications d'IA générative. Le juste équilibre entre sécurité et accessibilité est essentiel pour exploiter le potentiel de l'IA générative tout en assurant une protection adéquate des données et des ressources de votre entreprise.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.