Configuration de la prise en charge DLP et CASB pour Generative AI et ChatGPT

Table des matières

Introduction

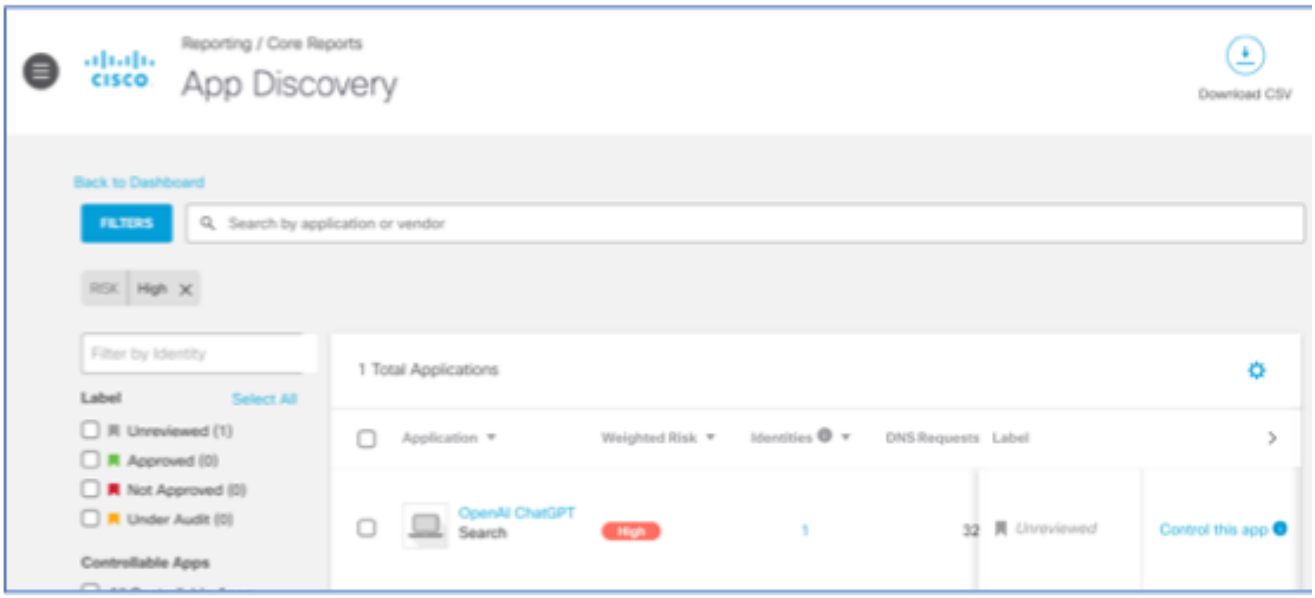
Ce document décrit la prise en charge du courtier de sécurité d'accès au cloud (CASB) et de la prévention de perte de données (DLP) pour l'IA générative et ChatGPT.

Aperçu

Nous avons publié de nouvelles améliorations CASB (Cloud Access Security Broker) et DLP (Data Loss Prevention) à notre suite de produits Umbrella, conçue pour aider les clients à gérer plus efficacement l'utilisation de ChatGPT au sein de leur entreprise.
Ces améliorations permettent à nos clients de s'assurer que leurs employés utilisent ChatGPT de manière responsable et sécurisée tout en protégeant les informations sensibles contre les risques potentiels.

Voici les principales caractéristiques :

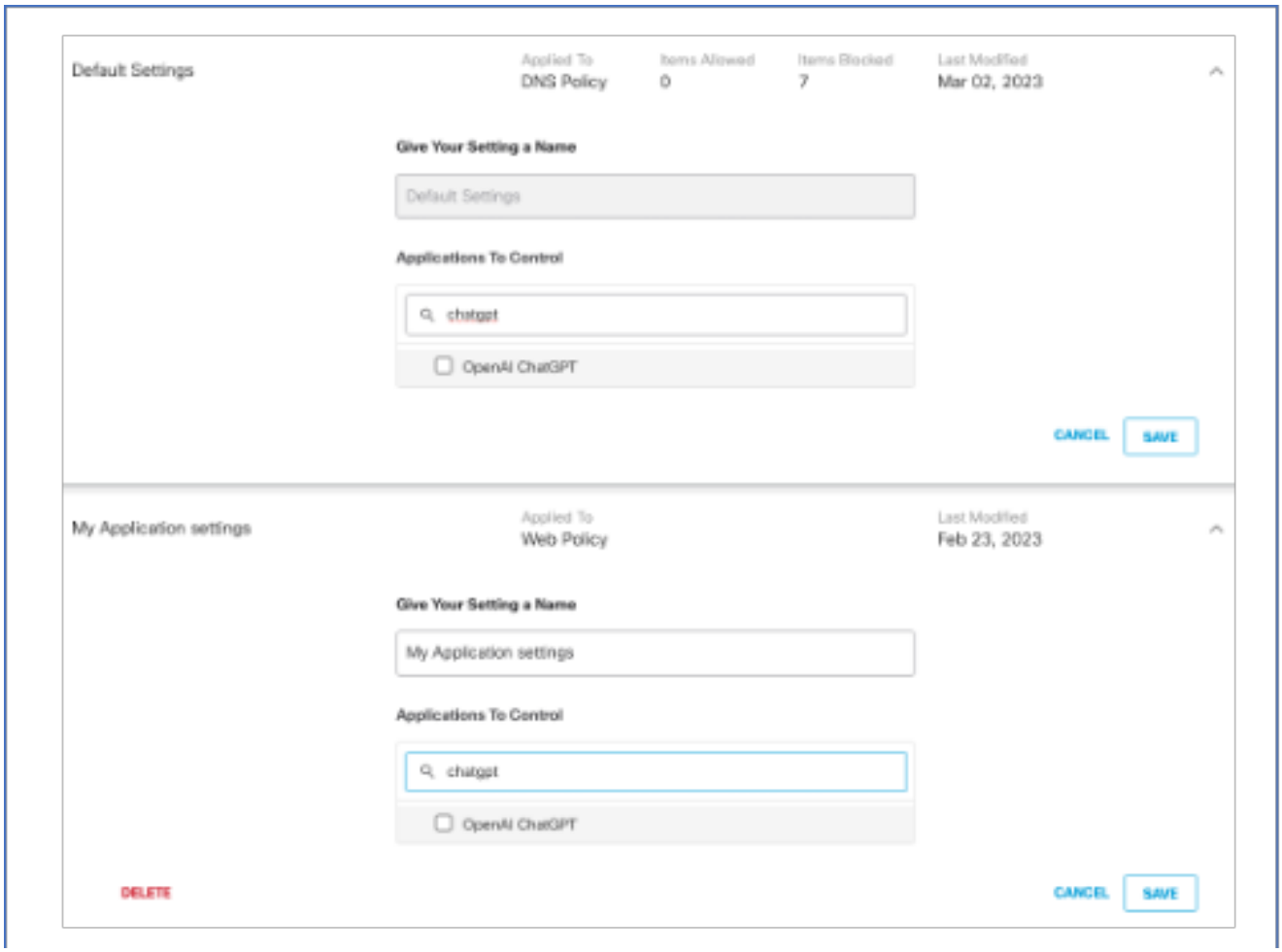
1. Découverte de l'utilisation de ChatGPT dans l'organisation :
   À l'aide du rapport App Discovery (Rapports -> Rapports principaux), les clients peuvent identifier et surveiller l'utilisation de ChatGPT dans leur organisation.
   Ils disposent ainsi d'informations précieuses sur la manière dont les employés utilisent l'outil, ce qui leur permet d'optimiser son utilisation et d'assurer la conformité avec leurs politiques internes.



16221272854164

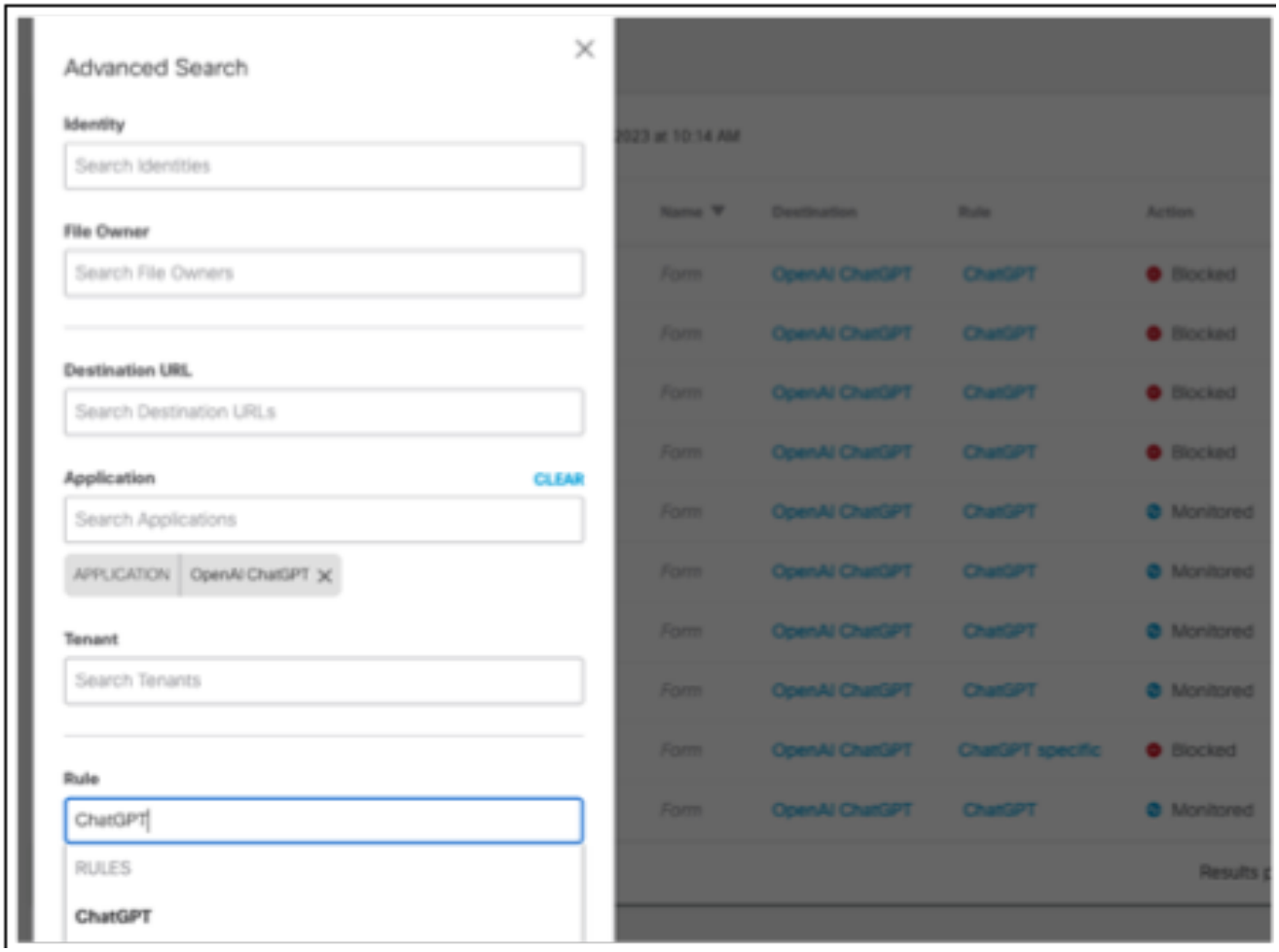
16221291406100

2. Contrôle granulaire de l'accès GPT de chat :
   Les clients peuvent désormais bloquer l'accès à ChatGPT pour tout le monde ou autoriser l'accès uniquement à des utilisateurs ou groupes d'utilisateurs spécifiques.
   Ce contrôle granulaire permet de gérer l'utilisation de ChatGPT conformément aux exigences de sécurité et de conformité. Le blocage est possible via les stratégies DNS et Web en sélectionnant openAI ChatGPT dans les paramètres d'application.



16221268217748

3. Évaluation des risques d'utilisation de ChatGPT avec DLP :
   La fonction DLP en temps réel permet désormais aux clients de surveiller le type d'informations sensibles envoyées et partagées avec ChatGPT. Cela permet d'évaluer le risque associé à l'utilisation de ChatGPT et de prendre les mesures appropriées pour limiter les fuites de données potentielles ou les violations.
   Pour activer la surveillance DLP pour ChatGPT, les clients peuvent utiliser des règles en temps réel avec la destination définie sur Toutes les destinations ou choisir openAI ChatGPT spécifiquement dans la liste des applications disponibles.



16221283948052

4. Utilisation sécurisée de ChatGPT avec DLP :
   Grâce à notre solution DLP, les clients peuvent désormais bloquer les invites de ChatGPT contenant des informations sensibles. Cela garantit que les employés peuvent continuer à utiliser ChatGPT en toute sécurité, sans exposer l'entreprise à des risques potentiels.
   Pour activer le blocage DLP pour ChatGPT, les clients peuvent utiliser des règles en temps réel avec la destination définie sur Toutes les destinations ou choisir openAI ChatGPT spécifiquement dans la liste des applications disponibles.

16221311959572

5. Prévention des fuites de code source vers ChatGPT avec DLP :
   Avec un nouvel identifiant de données de code source, les clients peuvent utiliser DLP pour garder un oeil sur et arrêter le partage de code source avec ChatGPT, protégeant ainsi leur propriété intellectuelle (IP).

6. Catégorie d'application IA nouvelle génération :
   Une nouvelle catégorie d'applications d'IA générative a été introduite pour aborder la découverte de l'utilisation et la prévention pour une gamme plus large d'outils.

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.