Comprendre la détection des applications tierces CASB

Table des matières

Introduction

Ce document décrit comment découvrir et évaluer des applications tierces connectées aux locataires Microsoft 365 via OAuth.

Aperçu

Third-Party Apps Discovery fournit des informations complètes sur les applications, extensions et plug-ins tiers ayant accès à un locataire Microsoft 365 (M365) via OAuth. Cette fonctionnalité permet d'identifier les applications connectées et de comprendre les étendues d'accès autorisées, y compris un score de risque pour mettre en évidence les autorisations potentiellement risquées.

Importance

Cette fonctionnalité améliore la capacité à gérer et à sécuriser les environnements M365 en offrant une visibilité sur les connexions d'applications tierces et en mettant en évidence les zones d'accès à risque. Elle permet de prendre des décisions éclairées et de réduire de manière proactive les menaces potentielles.

Risques des intégrations basées sur OAuth

Les intégrations basées sur OAuth améliorent la productivité et rationalisent les flux de travail, mais peuvent poser des risques de sécurité importants. Les applications tierces demandent souvent diverses autorisations ou étendues d'accès, allant d'un accès de base en lecture seule à des autorisations sensibles permettant la modification des données ou le contrôle administratif. Une mauvaise gestion de ces autorisations peut exposer l'entreprise à des violations de données, des accès non autorisés et d'autres vulnérabilités.

Calcul du score de risque

Le système évalue tous les domaines d'autorisation comme présentant un risque faible, moyen ou élevé en fonction de l'impact potentiel. Exemple :

- Les étendues octroyant l'accès aux détails utilisateur de base présentent un risque faible.
- Les étendues permettant l'écriture, la modification ou les modifications de configuration des données présentent un risque élevé.

Le niveau de risque le plus élevé parmi toutes les étendues d'accès accordées à une application s'affiche. Cette approche permet de connaître les risques les plus importants associés à chaque application tierce.

Accès à la détection des applications tierces

Pour accéder à cette fonctionnalité dans le tableau de bord Umbrella, accédez à Reporting > Additional Reports > Third-Party Apps.

Additional Information

Reportez-vous à la documentation Umbrella pour obtenir des instructions sur l'utilisation du rapport Third-Party Apps :

Rapport sur les applications tierces

Activer le courtier de sécurité d'accès au cloud pour les locataires Microsoft 365

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.