Entender a descoberta de aplicativos de terceiros do CASB

Contents

Introdução

Este documento descreve como descobrir e avaliar aplicativos de terceiros conectados a usuários do Microsoft 365 via OAuth.

Overview

O Third-Party Apps Discovery fornece informações abrangentes sobre aplicativos, extensões e plug-ins de terceiros que concedem acesso a um locatário Microsoft 365 (M365) por meio do OAuth. Este recurso permite a identificação de aplicativos conectados e a compreensão de escopos de acesso autorizados, incluindo uma pontuação de risco para destacar permissões potencialmente arriscadas.

Importância

Esse recurso aprimora a capacidade de gerenciar e proteger ambientes M365, fornecendo visibilidade em conexões de aplicativos de terceiros e destacando escopos de acesso arriscados. Ele possibilita a tomada de decisões conscientes e a mitigação proativa de possíveis ameaças à segurança.

Riscos de integrações baseadas em OAuth

As integrações baseadas em OAuth melhoram a produtividade e simplificam os fluxos de trabalho, mas podem apresentar riscos de segurança significativos. Aplicativos de terceiros frequentemente solicitam várias permissões ou escopos de acesso, variando de acesso básico somente leitura a permissões confidenciais permitindo modificação de dados ou controle administrativo. O gerenciamento inadequado dessas permissões pode expor a empresa a violações de dados, acesso não autorizado e outras vulnerabilidades.

Cálculo da Pontuação de Risco

O sistema classifica todos os escopos de autorização como de baixo, médio ou alto risco com base no impacto potencial. Por exemplo:

- Os escopos que concedem acesso aos detalhes básicos do usuário são de baixo risco.
- Os escopos que permitem a gravação de dados, edição ou alterações de configuração são de alto risco.

O nível de risco mais alto entre todos os escopos de acesso concedidos a um aplicativo é exibido. Essa abordagem garante o reconhecimento dos riscos mais significativos associados a cada aplicativo de terceiros.

Acessando a descoberta de aplicativos de terceiros

Para acessar esse recurso no painel Umbrella, navegue para Relatórios > Relatórios adicionais > Aplicativos de terceiros.

Informações adicionais

Consulte a documentação do Umbrella para obter orientação sobre o uso do relatório de Aplicativos de Terceiros:

Relatório de aplicativos de terceiros

Habilitar Agente de Segurança de Acesso à Nuvem para Locatários do Microsoft 365

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.