了解CASB第三方应用发现

目录

简介

本文档介绍如何发现和评估通过OAuth连接到Microsoft 365租户的第三方应用程序。

概述

第三方应用发现提供对通过OAuth授权访问Microsoft 365(M365)租户的第三方应用、扩展和插件的全面见解。此功能可识别连接的应用并了解授权访问范围，包括风险评分以突出显示可能具有风险的权限。

重要性

此功能通过提供对第三方应用连接的可视性和突出显示有风险的访问范围，增强了管理和保护M365环境的能力。它能够做出明智的决策，并主动缓解潜在的安全威胁。

基于OAuth的集成的风险

基于OAuth的集成可提高工作效率并简化工作流程，但会带来严重的安全风险。第三方应用通常请求各种权限或访问范围，从基本的只读访问到允许数据修改或管理控制的敏感权限。对这些权限管理不当，可能会使组织面临数据泄露、未授权访问和其他漏洞。

风险评分计算

系统根据潜在影响将所有授权范围评定为低、中或高风险。例如：

- 授予对基本用户详细信息访问权限的范围风险较低。
- 允许数据写入、编辑或配置更改的范围风险很高。

系统将显示授予应用的所有访问范围中的最高风险级别。此方法可确保了解与每个第三方应用程序相关的最重大风险。

访问第三方应用发现

要在Umbrella控制面板中访问此功能，请导航到报告>其他报告>第三方应用。

Additional Information

请参阅Umbrella文档，了解有关使用第三方应用报告的指南：

第三方应用报告

为Microsoft 365租户启用云访问安全代理

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。