瞭解CASB第三方應用發現

目錄

簡介

本文檔介紹如何發現和評估通過OAuth連線到Microsoft 365租戶的第三方應用程式。

概觀

第三方應用發現提供對通過OAuth授予對Microsoft 365(M365)租戶訪問許可權的第三方應用、擴展和外掛的全面深入分析。此功能可識別連線的應用並瞭解授權訪問範圍，包括風險評分以突出顯示可能具有風險的許可權。

重要性

此功能通過提供對第三方應用連線的可視性，以及突出顯示有風險的訪問範圍，增強了管理和保護M365環境的能力。它能夠做出明智的決策，並主動緩解潛在的安全威脅。

基於OAuth的整合的風險

基於OAuth的整合可提高工作效率並簡化工作流程，但會帶來嚴重的安全風險。第三方應用經常請求各種許可權或訪問範圍，從基本的只讀訪問到允許資料修改或管理控制的敏感許可權。對這些許可權的不當管理可能使組織暴露在資料洩露和未經授權的訪問等漏洞之下。

風險評分計算

系統會根據潛在影響將所有授權範圍評定為低、中或高風險。舉例來說：

- 授予對基本使用者詳細資訊訪問許可權的範圍風險較低。
- 允許資料寫入、編輯或配置更改的範圍風險很高。

將顯示授予應用的所有訪問範圍中的最高風險級別。此方法確保瞭解與每個第三方應用程式相關的最重大風險。

訪問第三方應用發現

要在Umbrella控制面板中訪問此功能，請導航到Reporting > Additional Reports > Third-Party Apps。

其他資訊

請參閱Umbrella文檔，瞭解有關使用第三方應用報告的指導：

第三方應用報告

為Microsoft 365租戶啟用雲訪問安全代理

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。