# 為生成AI和ChatGPT配置DLP和CASB支援

## 目錄



## 簡介

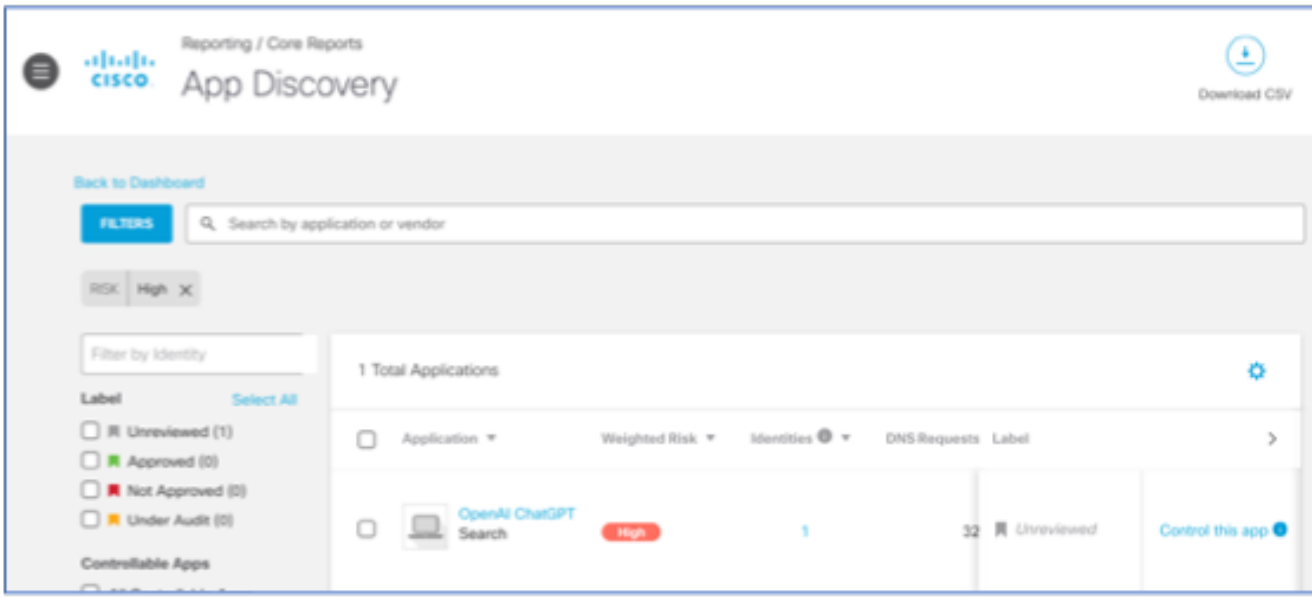
本檔案介紹雲存取安全代理(CASB)和資料丟失防範(DLP)對產生AI和ChatGPT的支援。

## 概觀

我們已對Umbrella產品套件發佈新的Cloud Access Security Broker(CASB)和Data Loss Prevention(DLP)增強功能，旨在幫助客戶更有效地管理其組織內的ChatGPT使用。
這些增強功能使我們的客戶能夠確保其員工負責並安全地使用ChatGPT，同時保護敏感資訊免受潛在風險的侵害。

以下是主要功能：

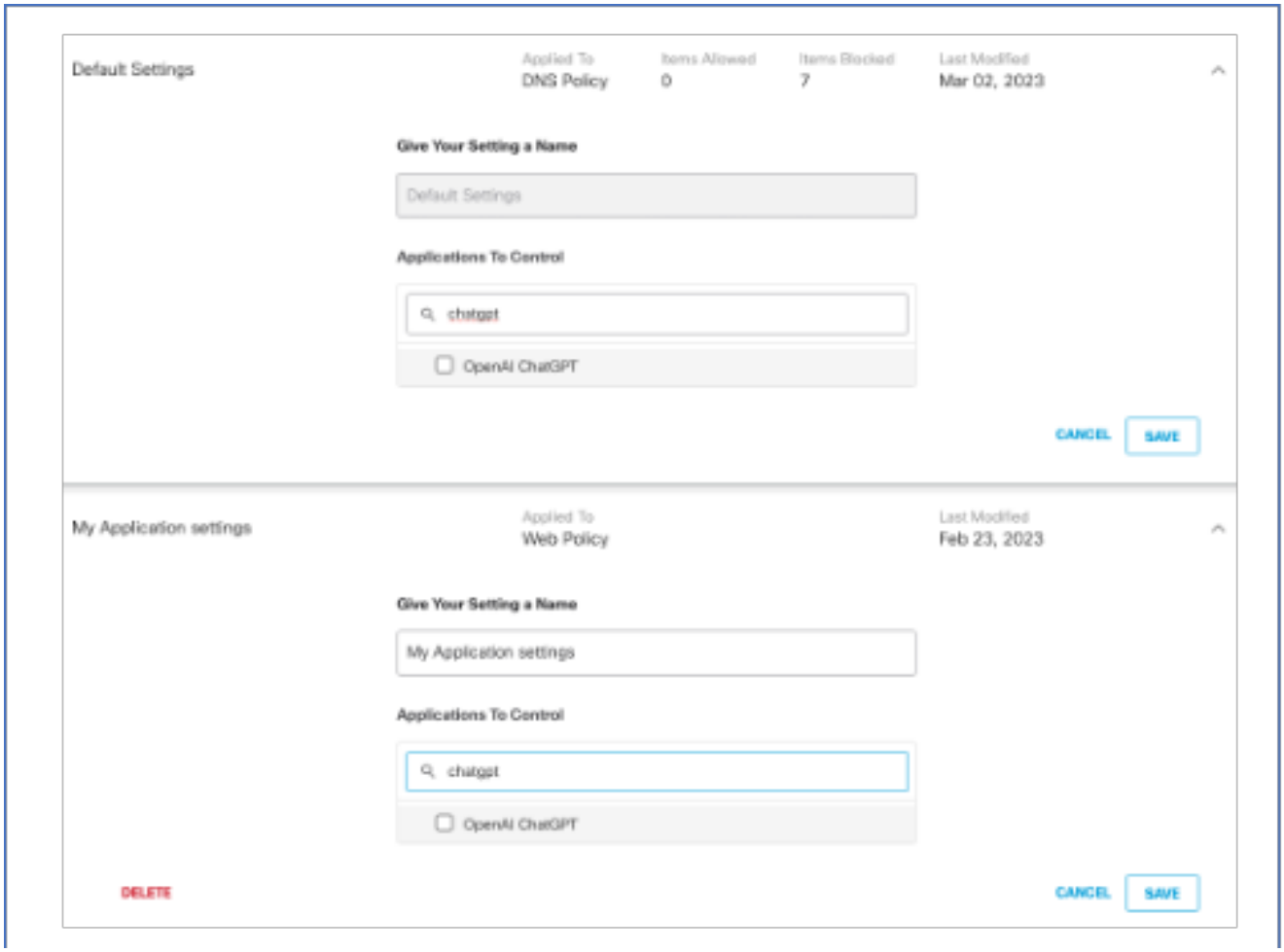
1. 在組織中發現ChatGPT使用情況：
   使用應用發現報告（報告 — >核心報告），客戶可以識別並監控整個組織中的ChatGPT使用情況。
   這讓他們能夠深入瞭解員工如何使用工具，使他們能夠最佳化工具的使用並確保符合其內部政策。




16221272854164

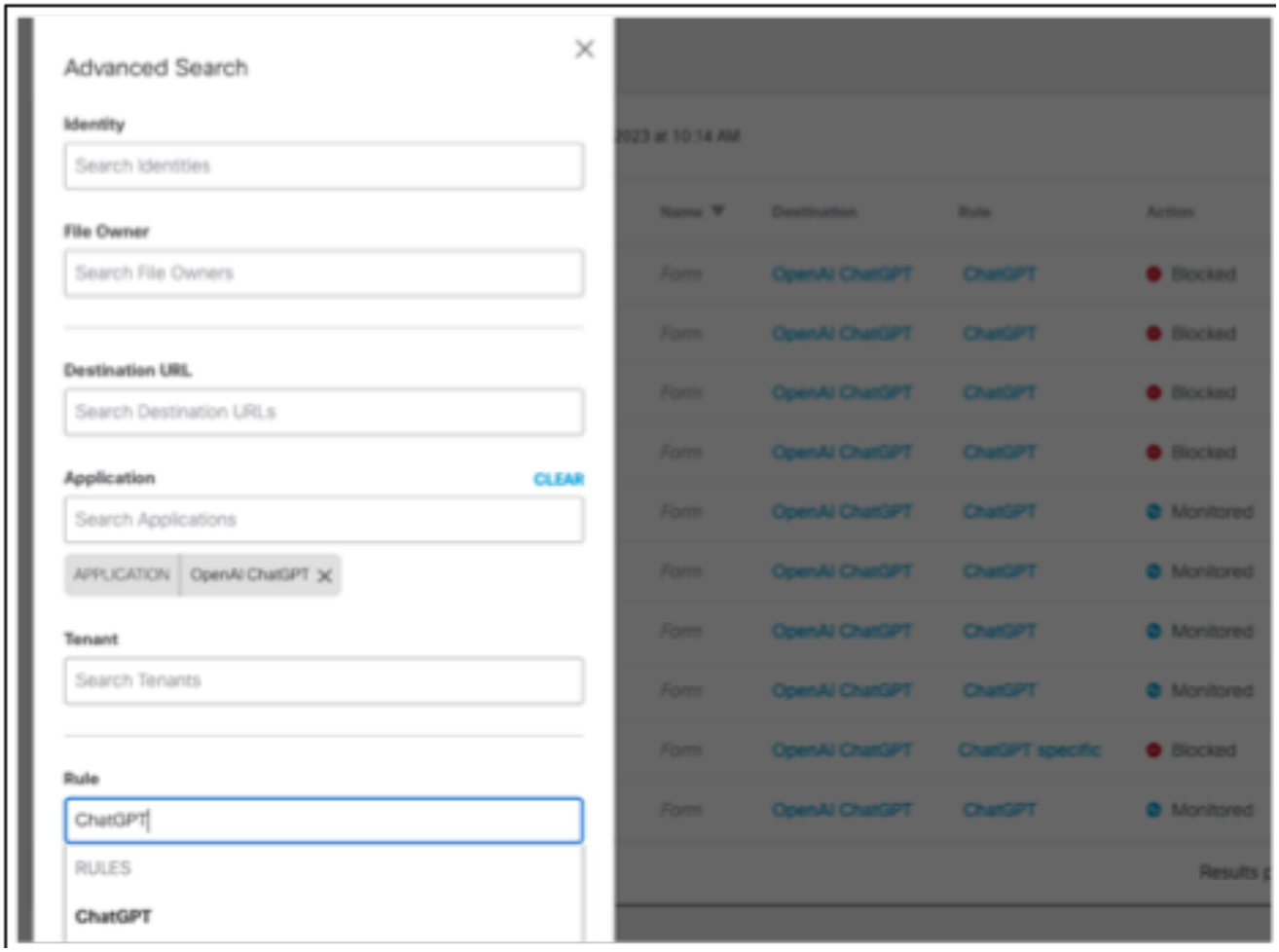

16221291406100

2. 對ChatGPT訪問的精細控制：
客戶現在可以阻止每個人訪問ChatGPT，或只允許特定使用者或使用者組訪問。
此精細控制有助於根據安全性和合規性要求管理ChatGPT的使用。 通過在Application Settings中選擇openAI ChatGPT，可以通過DNS和Web策略進行阻止。




16221268217748

3. 使用DLP評估ChatGPT使用風險：
現在，Real Time DLP使客戶能夠監控與ChatGPT傳送和共用的敏感資訊的型別。這有助於評估與ChatGPT的使用相關的風險，並採取適當措施減少潛在的資料洩漏或漏洞.
要啟用ChatGPT的DLP監控，客戶可以利用目標設定為All Destinations的Real Time規則，或者從可用應用程式清單中選擇openAI ChatGPT。




16221283948052

4. 允許通過DLP安全使用ChatGPT:
   通過使用我們的DLP解決方案，客戶現在可以阻止包含敏感資訊的ChatGPT提示。這可確保員工繼續安全安全地使用ChatGPT，而不會將組織暴露在潛在風險中。
   要為ChatGPT啟用DLP阻止，客戶可以利用目標設定為All Destinations的即時規則，或者從可用應用程式清單中專門選擇openAI ChatGPT。


16221311959572

5. 防止使用DLP向ChatGPT洩露原始碼：
   通過新的原始碼資料標識符，客戶可以使用DLP監視並停止與ChatGPT共用原始碼，從而保護他們的寶貴智慧財產權(IP)。

6. 新的創成AI應用類別：
   引入了一個新的創成式AI應用類別，以解決更廣泛工具的使用發現和預防。

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）。