

配置私有ChatGPT並限制對其他生成AI應用的訪問

目錄

[簡介](#)

[概觀](#)

[步驟 1:建立允許私有ChatGPT的Web規則](#)

[步驟 2:阻止所有其他生成AI應用](#)

[DNS策略](#)

[Web策略](#)

簡介

本文描述如何配置私有ChatGPT並限制對其他生成AI應用的訪問。

概觀

人工智慧領域正在迅速發展，其中最突出的進展就是生成型人工智慧(Generated AI)的發展。其中，ChatGPT產生了重大影響。

隨著組織試圖將這些功能強大的工具整合到工作流程中，控制對創成AI應用的訪問的需求變得越來越明顯。對於已開發自己的私有ChatGPT例項的企業來說，確保這是其團隊唯一可訪問的AI工具，同時限制其他Generated AI應用，是一項關鍵的安全措施。

幸運的是，有一種簡單的方法可以使用Umbrella控制面板來實現這一點。本文會引導您完成必要的步驟，以使您的組織從您的私有ChatGPT中獲益，同時保持對其他AI應用程式使用的嚴格控制。

步驟 1:建立允許私有ChatGPT的Web規則

首先，您需要登入到您的Umbrella控制面板。在此之後，您可以建立DNS規則或Web規則。此規則必須包含帶有您的專用ChatGPT的特定URL的操作「Allow」和「Destination List」。此步驟可確保組織中的使用者能夠不受任何限制地訪問您的私有ChatGPT。

步驟 2:阻止所有其他生成AI應用

建立「Allow」規則後，必須立即建立第二個規則。此規則必須具有「阻止」操作，並且必須包括包含生成AI類別的「應用程式清單」。這樣，您就可以阻止訪問各種流行的創成AI應用程式，包括ChatGPT的公共版本。

DNS策略

確保使用DNS策略而不是Web策略時有效地執行這些規則。

啟用智慧代理和SSL解密以實現無縫體驗至關重要。此外，安裝Cisco Umbrella根證書對於SSL解密的正常運行是必需的。

有關設定DNS策略的全面指導，請參閱此處的正式[文檔](#)。

此外，要最佳化DNS策略的有效性，請在此處檢視最佳[實踐](#)。

Web策略

有關管理Web策略並根據組織的要求定製這些策略的更多詳細資訊，請訪[問此處](#)。

實施這些措施可讓您的組織充分利用您的私有ChatGPT，同時降低使用其他創成式AI應用可能帶來的資料洩露或干擾的風險。在安全性和可訪問性之間取得適當的平衡，對於利用創成AI的潛力，同時確保組織的資料和資源得到良好保護至關重要。

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）。