Netskope One Agentic Broker

資料表

保護代理式 AI 企業

隨著組織改用支援模型脈絡協定 (MCP) 的應用程式（包括 AI 程式碼編輯器、聊天介面和開發人員工具），LLM 現在可直接與資料互動。

Netskope One Agentic Broker 可保護這些自主的非人類互動，提供統一的 AI 可見性和控制。

為何 Netskope 是最佳選擇？

Netskope Agentic Broker 可獨立使用，也可作為 Netskope One 次世代安全網頁閘道的連接功能，讓您能夠保護整個 AI 生態系統，包括從使用者到 LLM 以及 MCP。Agentic Broker 統一可見性、清單和整合式原則，以保護 MCP 環境。我們將安全洞見嵌入工作流程中，防止資料外洩並在 AI 環境中確保統一、即時的保護。

解決自主 AI 的安全性使用案例

- **對代理式 AI 和 MCP 通訊的可見性**

  接收工作階段資訊（包括 MCP 伺服器名稱、用戶端和工具、資源和提示要求）以及事件（包括初始化和工具要求），以監督非人類互動。

- **對公用和私有 MCP 伺服器清單進行風險評估**

  使用 Netskope Cloud Confidence Index (CCI) 在部署前評估公用 MCP 伺服器，確定高風險屬性、驗證類型和協定版本。

- **存取控制和整合式 DLP**

  實施原則以禁止未經授權與遠端 MCP 伺服器通訊，並透過與 Netskope One DLP 的整合來防止涉及 MCP 伺服器的資料外洩。

- **稽核代理式工具互動**

  建立全面的 MCP 事件紀錄，包括初始化、工具要求和回應，提供妥善的 AI 治理和回溯性調查所需的可稽核性。

主要效益和能力

MCP 流量可見性

持續探索在組織內部使用的遠端 MCP 伺服器、用戶端、工具、資源和提示要求。

降低供應鏈風險

評估第三方 MCP 伺服器和程式碼儲存庫並提供全面性風險評分，找出構成安全性與合規性風險的整合。

防止敏感資料外洩

對 MCP 互動套用 Netskope DLP 控制，保護智慧財產和密碼。

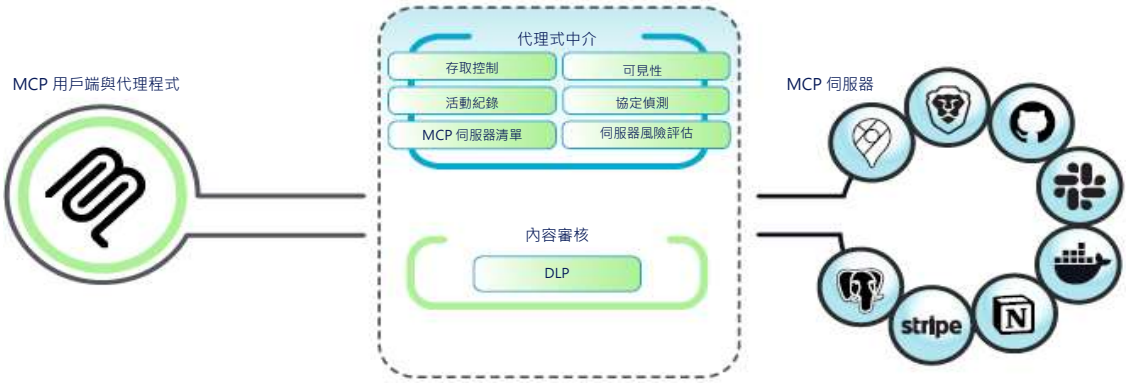
將原則控制延伸至代理式 AI

實施精細原則控制以封鎖已編目公用 MCP 伺服器和 MCP 伺服器事件，並提供所有公用 MCP 伺服器使用的預設封鎖選項。

「到 2028 年，25% 的企業資料外洩將起源於 AI 代理程式濫用，來自外部和內部惡意行為者。」

–Gartner，Top Strategic Predictions for 2025 and Beyond，2025 年

Netskope One Agentic Broker



netskope

Netskope 的獨特之處

Netskope 提供統一平台，保護 MCP 和代理式 AI 以及人類身分，應對 LLM、工具與資料之間日益複雜的通訊問題。Netskope One Agentic Broker 可作為 Netskope One 次世代安全網頁閘道的連接功能，為使用者至 LLM 控制增加公用 MCP 安全性，也可搭配 Netskope One AI Gateway，讓團隊能夠保護公用和私有 AI 部署的代理式 AI 流量，進而保護整個 AI 生態系統。

我們從全面的可見性開始，對 MCP 流量進行解碼，以找出繞過傳統安全層的工作階段、工具要求和回應。我們將經驗證的 Cloud Confidence Index (CCI) 延伸至 MCP 伺服器領域，為資安團隊提供公用 MCP 伺服器清單，並分析每個伺服器的協定版本、加密類型和驗證風險。這些情報直接傳送至即時原則引擎，實現精細控制，例如封鎖特定工具呼叫或防止敏感資料到達不受信任的遠端伺服器。Netskope 將 Nestkope One DLP 和威脅防護整合至代理式工作流程的核心，確保 AI 代理程式可根據企業資料進行推理和採取行動，而不影響安全態勢。此整合式方法將安全性轉化為賦能工具，讓現代企業放心且大規模利用代理式 AI 進行創新，同時維持全面控制。

效益	說明
MCP 流量解碼	Netskope One Agentic Broker 分析所有通過代理伺服器的 MCP 流量，以識別作用中代理程式和遠端伺服器。
Netskope CCI 風險評分	根據風險概況、驗證類型和協定版本評估公用 MCP 伺服器，以確保安全採用。
即時存取控制	實施精細原則，針對特定 MCP 通訊事件和未經授權的工具要求進行封鎖或發出警報。
DLP 整合	在 AI 互動過程中識別並防止敏感資料外洩，例如密碼和智慧財產。
非人類流量監測	追蹤 MCP 伺服器、用戶端與工具之間的自主通訊。包括資源和提示要求，以及初始化、工具要求等事件。
整合式事件記錄	記錄詳細的工作階段資訊、初始化和工具回應，建立全面的稽核軌跡並支援鑑識分析。
MCP 伺服器清單	在 Netskope One 主控台應用程式目錄中提供專用類別，以協助評估及核准公用遠端 MCP 伺服器。
GenAI 用戶端支援	使用 MCP 確保熱門的生成式 AI 用戶端（包括 ChatGPT、Cursor、VS Code）之間的通訊安全性。