Netskope One AI 閘道

資料表

保護 AI 應用程式

隨著組織建立 AI 應用程式，主要資料流風險從人類提示轉為自主、應用程式對 LLM 的 API 呼叫，這些呼叫往往會繞過傳統的安全邊界。Netskope One AI 閘道可保護此現代生態系統，驅動 AI 創新。

為何 Netskope 是最佳選擇？

Netskope One AI 閘道可保護私有 AI 應用程式和與其通訊的 LLM（無論是私有或公用）之間的關鍵 API 流量。AI 閘道以軟體層的形式部署在環境中，可集中進行驗證和流量管理，同時提供內容檢查，以保護驅動 AI 應用程式的自主資料流。

集中進行驗證、流量管理和內容檢查

- **放心建立 AI 應用程式**
  加快 AI 計畫，提供安全的應用程式至 LLM 流量檢查點，針對存取敏感資料和工具的 API 和代理程式控制驗證和管理。
- **安全的代理程式驗證和記錄**
  確保只有經過驗證的代理程式才可透過唯一閘道 token 與 LLM 通訊。保留可搜尋 API 紀錄，確保沒有任何互動繞過安全控制措施。
- **將可靠性和效能最佳化**
  以 API 要求為單位追蹤 AI 使用量，並對要求數量和頻率進行速率限制，以防止濫用並管理流量。
- **整合全面的內容檢查**
  統一內容檢查，透過 SkopeAI 整合 Netskope One AI Guardrails、DLP 和威脅防護以進行集中式原則偵測，在單一總覽中提供連貫的脈絡並加快調查速度。

主要效益和能力

主要效益和能力

透過單一閘道器集中控管部署於私有及公有基礎設施中的 OpenAI、Gemini 與 Claude AI 模型，藉此實施統一的身分驗證與一致的流量管理。

提升安全營運效率

將整合式內容檢測的偵測結果，對應至 MITRE ATLAS 框架以及 OWASP Top 10 for LLMs 風險清單。這種統一檢視可縮短調查時間，並讓團隊與最新 TTP 同步。

集中化流量管理與稽核可視性

透過流量限制維持應用程式穩定性，同時完整紀錄 API 調用之可搜尋稽核日誌，以滿足法規合規與使用監控需求。

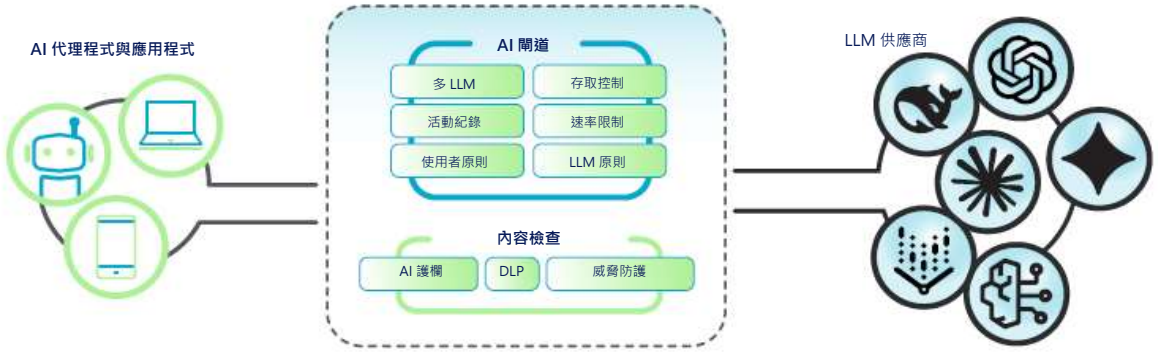
靈活的私有化部署

在您的私有託管環境（從 AWS 到 VMware ESXi）中直接部署輕量化、高效能的虛擬設備，藉此在任何地方執行一致的安全政策。

「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 One AI 閘道提供現代代理式 AI 工作負載所需的可見性和控制，讓組織能夠加速邁進。傳統代理伺服器是專為從使用者到應用程式的流量而設計，代理式互動則通常自主發生在內部系統與 LLM 之間，繞過標準安全機制。Netskope 以靈活的部署結構填補此缺口，將輕量型 VM 部署於模型所在位置。此架構優勢讓資安團隊能在私有環境中即時採取行動，為 AI 創新提供快速通道。

Netskope 將安全性直接嵌入於流量路徑中，讓您分層實施複雜的原則，包括精細存取控制、提示速率限制，並且可整合 Netskope One AI Guardrails、DLP 和威脅防護，提供統一的 AI 安全解決方案。這些工具確保自主代理程式可調用工具和存取資料，而不會導致敏感的智慧財產外洩或遭受提示注入攻擊。此外，閘道集中治理多家供應商（包括 OpenAI、Google Gemini、Anthropic Claude），將 AI 的商業價值最大化。此整合簡化驗證和流量管理，將可靠性最佳化。Netskope 確保隨著 AI 普及加速，您的生態系統能與企業資料和網路安全環境的其餘部分一樣保持安全、受治理和受管理。

效益	說明
靈活部署	Netskope One AI 閘道以輕量型虛擬機器的形式提供，可用於 AWS 公用雲端部署，或 VMware ESXi 私有雲端部署。
整合式軟體層	以軟體定義閘道的形式運作，攔截並治理內部應用程式、自主代理程式與私有 LLM 之間的 API 流量。
統一 API 控制	提供統一的 API 進入點，管理多個供應商（包括 OpenAI、Google Gemini、Anthropic Claude）以及遵循這些模型的 API 結構描述的自訂模型之間的互動。
代理程式驗證	每個要求都必須具備由 AI 閘道產生的有效 token，確保只有經過驗證的代理程式才能與 LLM 通訊。
監測和可搜尋紀錄	保留 API 呼叫和互動內容的可搜尋紀錄，以滿足法規要求和觀察內部使用規律。