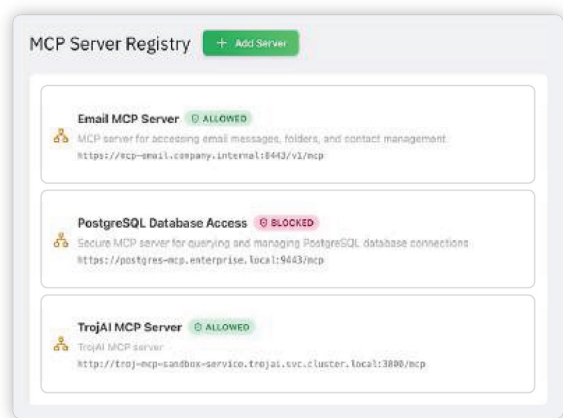


TrojAI Defend for MCP by A10 Networks

掌控您的代理程式。適合企業的 MCP 安全性。



適合企業的 MCP 執行階段安全性

Model Context Protocol (MCP) 是一種開放式協定，可讓 AI 代理程式以標準方式連結外部資料、工具及服務。MCP 讓 AI 代理程式有能力自主行動，但同時也造成了全新類別的風險。每個 MCP 伺服器、工具及連線都會導入另一個持續移動的部分，無法由傳統的安全性工具加以監控或管理，讓新的攻擊向量有機會趁虛而入。

TrojAI Defend for MCP 提供完整的可視性及控制功能，協助掌控 MCP 工作流程。其中可為 MCP 伺服器及工具提供登錄檔，揭露可能含有提示注入或其他攻擊的惡意工具描述，並長期追蹤工具完整性。TrojAI Defend for MCP 可協助企業安全運用代理式 AI 從事創新。

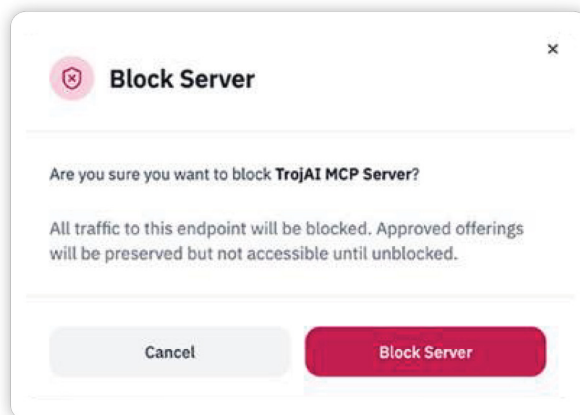
探索及保護每個 MCP 伺服器

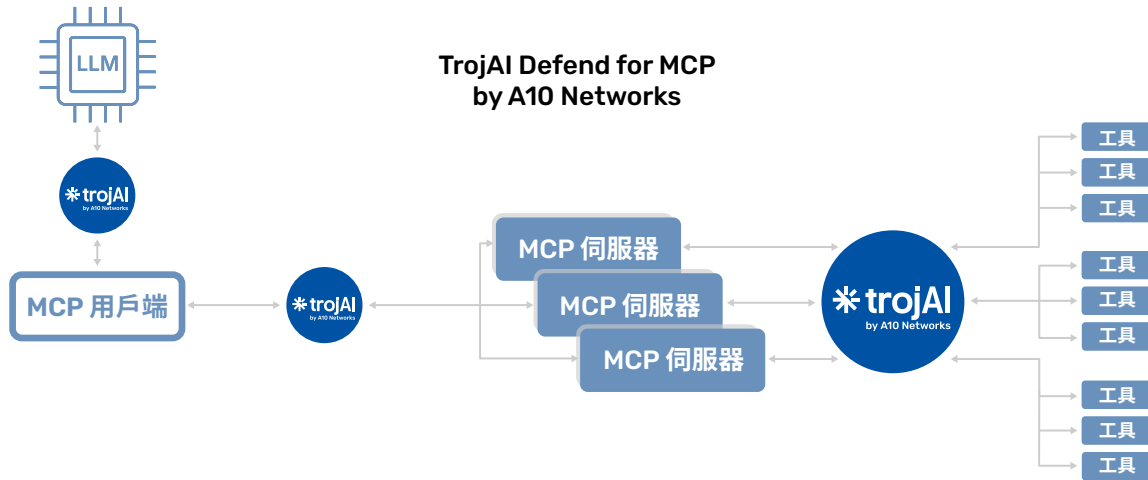
由於組織迅速採用 MCP 以驅動代理式 AI 工作流程，掌握伺服器是否作用及安全便成為重大挑戰。而各個 MCP 伺服器可能呼叫多項未經審查的工具，更讓這類風險雪上加霜。

TrojAI Defend for MCP 能夠探索及登錄所有 MCP 伺服器，阻止惡意行動者的未授權存取，並可消除影子 MCP。之後 MCP 伺服器及其相關工具就可在登錄檔中獲得核准，防止失控或未授權使用高風險工具。

阻止失控 MCP 伺服器及防止操控攻擊

惡意或未經驗證的伺服器，可能會暴露工具執行未授權行動或洩漏敏感資料。攻擊者可能會在看似無害的名稱、說明或參數等工具中繼資料隱藏提示注入，但實際上會改變 AI 行為。





TrojAI Defend for MCP 能夠識別與個別伺服器之間往返的所有 MCP 流量，以封鎖未登錄或失控的伺服器。可消除隱藏的通訊路徑，以抵禦提示注入、資料外洩等常見的 AI 攻擊。

保所有活動遵循企業資料處理規則，並維持詳細的稽核軌跡，提供法規遵循及事件回應所需的證明。

立即偵測竄改

即使是核准的 MCP 伺服器及工具，也可能遭到竄改，導致在可信賴的工作流程內部建立隱藏風險。TrojAI Defend for MCP 可持續驗證每個伺服器及工具定義，即時偵測任何偏移或變更。如果出現未授權變更，TrojAI Defend for MCP 就會隔離及封鎖工具、阻止竄改、中毒或所謂的拉地毯 (rug-pull) 攻擊擴散。

專為保護 MCP 工作流程而建構的 AI 原則

MCP 逐漸成為代理式 AI 的骨幹，因此企業需要原則以瞭解代理程式的實際行為。如果沒有 MCP 專屬的防護措施，則提示注入、資料外洩及未授權工具使用就可能趁虛而入。

TrojAI Defend for MCP 執行全方位可自訂原則，可檢測、稽核及保護每項代理程式互動。這類原則可強化治理，確

關於 A10 Networks

A10 Networks (NYSE: ATEN) 提供各種安全的應用程式及網路解決方案，協助保護、最佳化及擴充關鍵業務系統，範圍涵蓋內部部署、混合雲及邊緣環境。我們的產品組合可協助全球各地的大型企業、服務供應商及雲端平台，提供效能、可靠性及保護措施抵禦網路威脅，同時讓網路準備好因應 AI 及新一代應用程式的需求。A10 Networks 於 2004 年成立，總部位於加州聖荷西 (San Jose)，為全球 7,000 多家客戶提供服務。

如需詳細資訊，請造訪 [A10Networks.com](https://www.a10networks.com) 並在 @A10Networks 關注我們。

深入瞭解

關於 A10 Networks

聯絡我們

apac@a10networks.com

©2026 A10 Networks, Inc. 保留所有權利。A10 Networks、A10 標誌、A10 Control、A10 Defend、A10 Harmony、Harmony、A10 Thunder、Thunder、ACOS、A10 SSL Insight、SSL Insight、SSLi、vThunder、ThreatX 和 ThreatX Protect 是 A10 Networks, Inc. 或其關係企業在美國和其他國家/地區的商標或註冊商標。所有其他商標均為其各自所有者的財產。A10 Networks 對本文文件中的任何不精確處不承擔任何責任。A10 Networks 保留變更、修改、轉讓或以其他方式修訂本出版品的權利，恕不另行通知。有關商標的完整清單，請造訪：[A10Networks.com/a10trademarks](https://www.a10networks.com/a10trademarks)。

Part Number: A10-SB-19217-TW-01 July 2026

A10 中文資源網

