DELL Technologies

AI 安全性與復原能力服務

信任您的 AI 使用

解決採用 AI 的挑戰

人工智慧 (AI) 為企業帶來巨大變革，可實現突破性創新並加快決策。然而，可觀的潛力也伴隨重大挑戰。AI 採用在安全性、信任和法規遵循方面帶來了獨特的問題，讓組織面臨新的壓力。在 Dell Technologies，我們重新構思 AI 安全性應如何運作。我們的方法以獨特的方式整合資料管理、基礎結構安全性和 AI 模型保護，提供量身打造的全方位解決方案。無論是剛接觸 AI 或要擴充現有解決方案，我們的端到端服務都能讓您更快、更安全、更可靠地採用 AI。

安全性不僅是 IT 人員的工作

現代的 AI 相關安全性需要跨團隊協作。AI 安全性就像團隊運動，需要整個組織的投入和決策。傳統孤立的 IT 作業模式，無法在這不斷演進的局勢中發揮作用。我們獨特的方法將資料、基礎結構、應用程式和模型整合到一個統一的策略中，能適應您的特定業務需求，提供可助您保持領先的全方位解決方案。

解決 AI 的獨特安全性挑戰

採用 AI 會帶來複雜的安全性和法規遵循靠考量，可能會危及其潛在優點，例如：

- 資料保護不足或未經授權的存取，導致資料違規和智慧財產權 (IP) 損失。
- 採用 AI 技術的威脅，例如惡意攻擊、模型操縱或訓練資料中毒。
- 現今關鍵 AI 工具 (如支援專員) 持續運行的可用性挑戰。
- 互連系統的第三方供應鏈漏洞。
- AI 應用程式在混合雲和多雲環境中擴充，攻擊面隨之擴張。
- 雖然幻覺不完全是安全問題，但可能會誤導使用者

主要優點

增強信任和透明度：保護資料、智慧財產權和 AI 完整性，以維持利害關係人的信心。

運作復原能力：讓關鍵任務 AI 系統保持運作並抵禦威脅。

法規遵循：助您符合業界及政府法規要求，避免高額罰款和聲譽受損。

可擴充的解決方案：部署可調適的 AI 安全性措施，隨組織與技術堆疊一起成長。

專家支援和指導：與經認證的安全性專家合作，量身打造專屬解決方案，並提供可衡量的成果。

端對端服務，提供量身打造的安全性架構

Dell 開發的安全性架構專為滿足您的獨特需求而設計，提供彈性且可靠的基礎。此架構與 Dell AI Factory 順暢整合、啟動零信任原則，並加入經專業整合的合作夥伴技術，以推動安全且具前瞻性的創新。

AI 模型和應用程式

資料

基礎結構

	功能
建議 讓 AI 安全性符合組織需求和法規遵循要求	• **AI 諮詢服務的安全性和復原能力**：包括業務和技術研討會，擬定全方位的安全性和可用性策略 • **AI CISO 顧問**：提供虛擬 CISO，作為您的 AI 專家，啟動 AI 安全性策略 • **AI 資料安全性**：有助於減少資料安全性威脅和資料風險
實作 設計和實作安全性軟體以提升 AI 堆疊的可視性	• **安全軟體設計和設定**：整合保護存取管理、應用程式和網路的工具
管理 實現跨堆疊深度可視性以快速偵測和回應威脅	• **Managed Detection and Response (MDR)**：可在各種資料、基礎結構、應用程式及模型，提供全年無休的威脅偵測 • **管理型 AI 防火牆**：採用一組隔離的 AI 型護欄，並檢查提示和輸出的原則合規性 • **AI 滲透測試**：模擬惡意攻擊並發現弱點 • **事件應變與復原服務**：協助快速復原，並在最少中斷的情況下恢復業務

安心打造安全的 AI 未來

Dell 的 AI 安全性與復原能力服務，旨在解決將 AI 整合至組織時產生的相關新風險。我們的服務專為與您的團隊合作而設計，讓您盡快啟用 AI，為您提供專業知識來指導策略規劃、解決方案實施和管理型安全服務，以減輕營運負擔，方便您運用 AI 安全創新。

探索 Dell 安全性與復原能力服務

聯絡 Dell Technologies 專家

使用 #DellTechnologies 加入對話