

# Dell Trusted Infrastructure

為您的組織打造現代化、安全、具韌性且智慧化的技術基礎，以助推動創新。

實體與軟體定義系統、AI、多雲環境、邊緣裝置和即服務交付，共同定義了現代化時代的基礎結構，這正在改變我們對網路安全性和網路韌性的所有認知。

在 Dell，我們認為 IT 安全性與復原能力應涵蓋三個核心實務領域：

- 減少攻擊面
- 偵測及因應網路威脅
- 從網路攻擊中復原

除此之外，同時還運用零信任原則來協助提升您的網路安全性和復原能力狀態。

# 現代化時代的基礎結構。

我們生活在一個資料導向的世界。IT 運作遍及業務所及之處，資料的產生和存取已不再侷限於過去集中式的大型資料中心。如今，「基礎結構」係指資料儲存和超融合系統、伺服器、網路和資料保護 (可能為實體分散式或以即服務形式交付)，但無論 IT 基礎結構如何使用，在 Dell，我們都認為它都必須贏得客戶和合作夥伴的信任。

受信任的基礎結構能在任何地方運作，同時發揮最大的彈性與商業靈活度，且無需犧牲安全性。它不僅現代化、具備復原能力且具備彈性，並且支援零信任方法，或是您所選擇之保護並保留組織最重要數位資產的方式。



## 現代化

為創新而設計的現代化基礎結構為高度分散式或以即服務形式交付，並包含邊緣裝置和多雲環境，以支援現代化組織運作。



## 具備彈性

為了實現復原能力，解決方案應在有安全生命週期的情況下進行開發。從元件到系統再到完整整合的解決方案，安全的供應鏈可確保您環境中的裝置都值得信賴。



## 智慧型

智慧型基礎結構包含 AI、機器學習和自動化等先進技術，使您能夠透過一致的控管和強制來擴展安全性狀態。



# Dell Trusted Infrastructure

無論是硬體或軟體，Dell Trusted Infrastructure 都是一系列安全且具復原能力的 IT 解決方案和服務，專為提供信心、控制力和擴展性而設計打造。



**保護**  
資料和系統



**增強**  
網路復原能力



**克服**  
安全性的複雜性



**DELL**Technologies

# 保護資料和系統

無論是在邊緣、到場或跨多個雲端提供商，您都能透過單一提供商來對抗組織關鍵系統、應用程式和資料的網路威脅。Dell Trusted Infrastructure 透過在遍及整個企業的儲存裝置、伺服器、超融合系統、網路和資料保護解決方案產品線中內嵌安全性功能，協助您實現零信任原則。

確保系統的存取安全無虞，並且確保偵測和消除威脅。我們的解決方案包含強化的裝置和程序，為資料和應用程式所在的每個環境提供內建的安全性優勢。

運用保護資料、網路和系統的智慧型軟體與 AI 及機器學習，藉此運用創新解決方案和最佳實務來保護邊緣到核心再到雲端。

透過實施全面的安全性，協助確保關鍵資料、應用程式和作業的完整性和可用性，藉此秉持著無論靜態、運作中或傳輸中的資料都安全無疑的信心，來執行您的 IT 基礎結構。

# 強化網路恢復能力

規劃、準備和演練復原程序，以減輕網路攻擊的影響，並能快速且有信心地恢復營運。Dell Trusted Infrastructure 提供自動化工作流程和軟體定義解決方案，可在您的環境變得更加分散時保護關鍵系統、應用程式和資料。

確保您的資料、系統和營運能夠抵禦網路攻擊，並透過完善的 IRR 計畫，在事件發生時獲得適當的協助，以便復原。

運用 MDR 功能讓業務程序遵循事件回應與復原，藉此在網路事件發生時維持營運連續性和資料可見性。

透過應用現代化技術來強化高度分散式遠端員工與多雲環境中的存取、驗證和授權，建立合規性並遵循零信任原則。



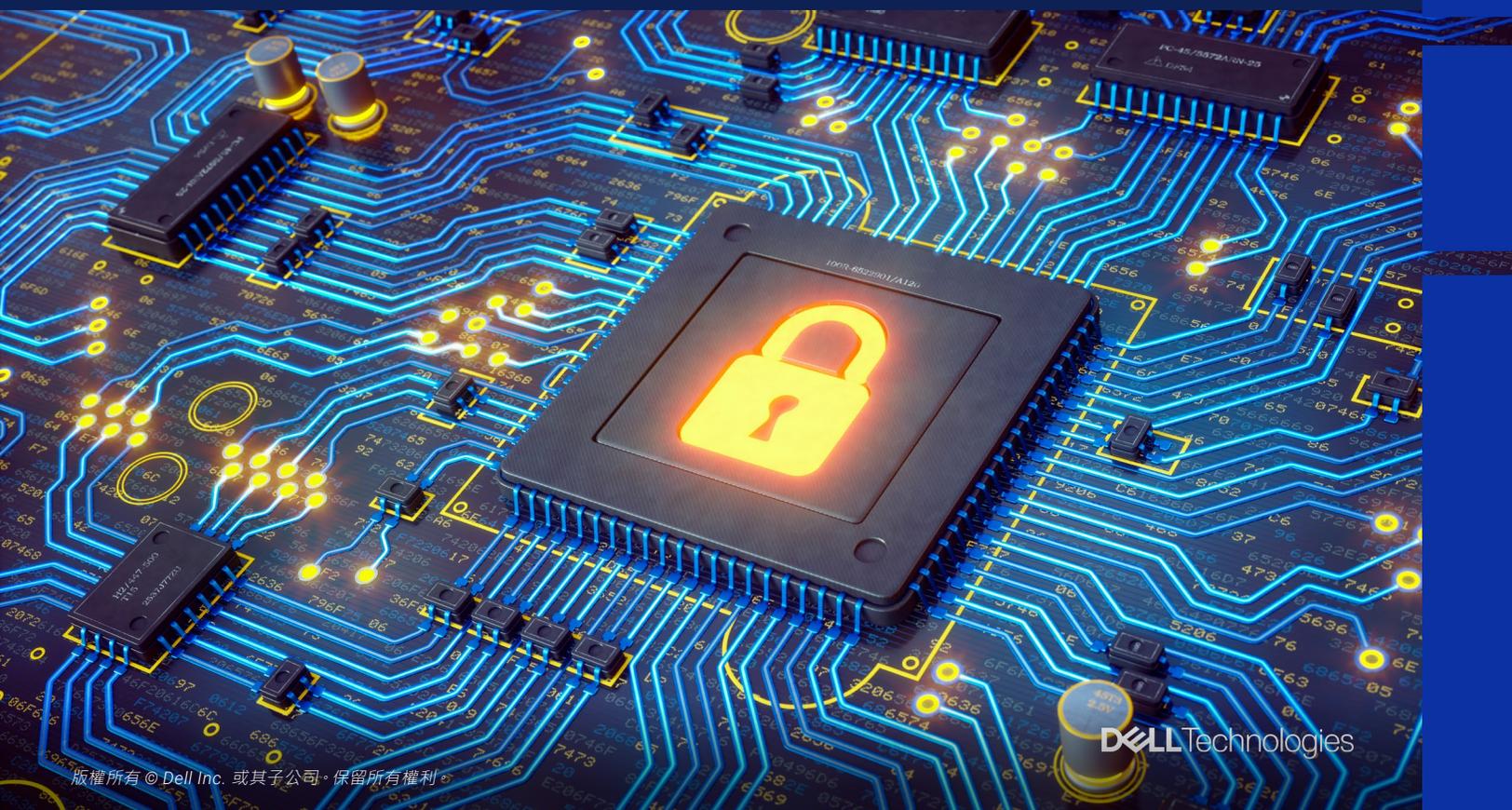
# 克服安全性複雜度

將資安營運現代化，儘管複雜性增加也能有信心地建立或擴充您的零信任架構。Dell Trusted Infrastructure 提供自動化協調流程和智慧創新，可加強我們的硬體安全性功能、韌體型安全性功能和軟體安全性功能。

透過減少安全性應用程式和供應商的數量來簡化您的基礎結構。作為整個企業的解決方案提供者，Dell Technologies 可協助您透過端對端解決方案整合環境中的安全性功能。現在，您可以與一個瞭解您挑戰的值得信賴的合作夥伴合作。

透過專業資源和服務擴展您的安全性工作人員。運用我們的網路安全性服務和即服務方案來與 Dell 安全性專家合作，藉此擴展您的人員資源並將支出營運化。

使用自動化和智慧化技術取代手動人工操作，增強現有的安全性系統並快速擴展您的安全性策略。



**DELL**Technologies

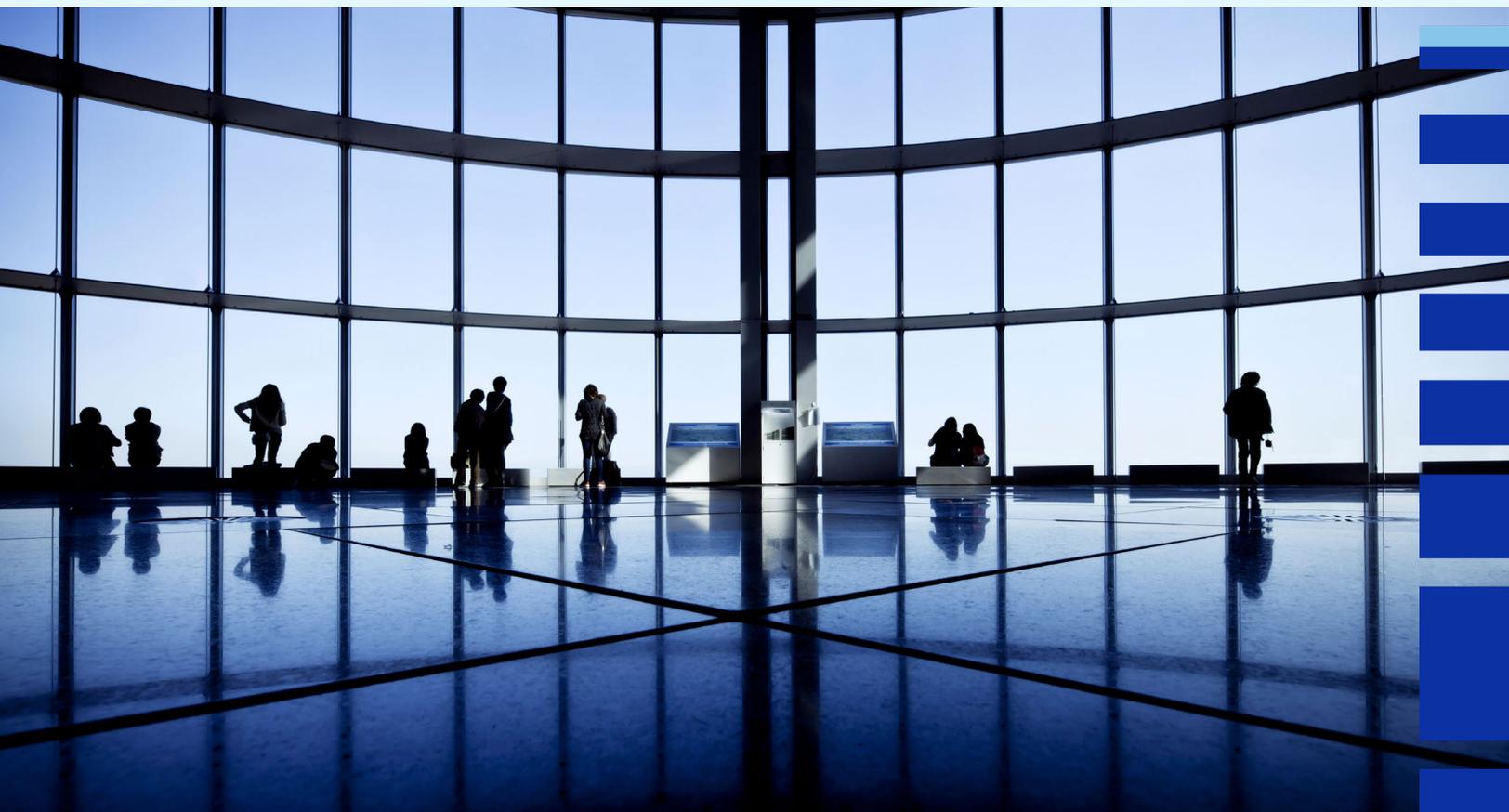
# 從單一提供者獲得適用於整個 IT 基礎結構之值得信賴且現代化的安全性解決方案。

<h2>Dell Storage</h2> <p>讓您安心確信您的資料是安全、受保護且可用的。</p>	是否可能同時擁有安全的儲存解決方案以及全面的威脅偵測和回應能力？是，這是有可能的。我們的解決方案透過彙總威脅情報並將其串聯至上游安全性平台，來克服安全性複雜度。
<h2>Dell 伺服器</h2> <p>以提供不斷演進之安全性控管措施、功能和解決方案的具網路韌性架構，來因應現今的威脅環境</p>	透過在每個產品生命週期階段內建的安全性功能提升網路韌性。Silicon Root of Trust 作為錨點，提供對簽署韌體、偏移偵測、BIOS 復原、系統管理整合和供應鏈保證的控制。
<h2>Dell Networking</h2> <p>透過在邊緣和在網路之硬體和軟體中運用多層防禦來強化安全性。</p>	全方位的調適型安全性策略是在現今動態商業環境中維持信心和控制的關鍵。透過結合先進架構、嚴格的安全性認證、強大的存取協定和流暢整合，這種方法可確保您的網路保持安全，同時以最高效能執行。
<h2>Dell 超融合基礎結構</h2> <p>在每一層的堆疊強化和修改應用程式 — 從供應鏈到硬體基礎結構，再到軟體開發和生命週期管理軟體。</p>	並非所有超融合基礎結構解決方案都是相同的。採用 Dell 技術後，您可以擁有具備完整堆疊完整性和全方位生命週期管理的靈活基礎結構，可提升營運效率並降低風險。這就是為什麼 Dell 在超融合基礎結構市場連續 20 個季度保持領先地位的原因 <sup>1</sup> 。現在，您的團隊可以專注於業務，而不是努力瞭解最新的威脅。
<h2>Dell Data Protection</h2> <p>透過最適合您基礎結構和 IT 需求的解決方案，在核心、邊緣和多雲環境中保護資料安全。</p>	運用經過產業驗證的現代化智慧資料保護，簡化並自動化大規模作業。透過完整的整合式產品組合和管理工具，您可以隔離重要資料、識別可疑活動並加速自動化資料復原。有了 Dell Data Protection，您可以迅速恢復正常營運。
<h2>Dell APEX AIOps</h2> <p>透過網路安全性評估和快速補救措施，確保基礎結構的安全性。</p>	透過就位在管理員用於管理基礎結構健全狀況、容量和效能之應用程式中的安全性通知，來提升回應效率。監控和預測分析結合人類與機器情報，提供可確保您 IT 基礎結構符合業務需求的深入解析。
<h2>Dell Professional Services</h2> <p>提供經過整合的最佳化自動體驗，讓安全性作業輕鬆簡單。</p>	深入瞭解貴組織如何採取更全面的網路安全性措施。保護資料與系統、提升網路韌性並克服安全性複雜度，藉此運用網路韌性 IT 解決方案來強化您的環境，並且運用 Dell Technologies 的現代化端對端解決方案，來獲得解決安全性挑戰所需的信心、控制和規模。

<sup>1</sup> 《IDC Worldwide Quarterly Converged Systems Tracker》(IDC 全球季度融合系統追蹤報告)，2022 年第 1 季

# 現代化、具韌性且智慧化的基礎結構解決方案和服務。

我們絕不接受任何妥協。



在 Dell Technologies，我們認為安全性技術在現今現代化時代中，比以往任何時候都更加重要。

我們瞭解您需要專注於業務，確保您全球 IT 環境中每個資料中心之每個機架的每部伺服器中，每個晶片都安全無虞。這就是我們在所有設計中都融入安全性的原因。

數十年來，從重新定義[安全供應鏈](#)到[安全開發生命週期](#)，我們已改進各方面業務。我們在設計、採購、建置、運送和管理產品的方式方面都極為謹慎，讓您能夠放心讓這些產品在您的環境中運作。

# Dell Trusted Infrastructure

網路威脅永不止息，但您能放心，IT 轉型的旅程安全無虞。

深入瞭解

