DELL Technologies

提升您的網路安全性與零信任成熟度

弭平資源和知識落差，以強化網路攻擊的防禦機制。

現今快速演變的威脅帶來了非預期的新挑戰，隨著生成式 AI 興起更是如此，即使是最富經驗的網路安全性專家也無可避免。瞭解與經驗豐富的安全性專業人員合作如何協助您避免網路攻擊，同時維護健全的安全性實務。

網路威脅如同野餐時出現的螞蟻

您處理了其中一隻。接著，另一隻便隨之在後。

在日益互連的世界中，組織重度仰賴數位基礎結構，而且資料已成為影響深遠的商品，最好假設手法高明的攻擊者已經入侵您的 IT 環境。

好消息是，有些經驗豐富的合作夥伴同時是技術和網路安全性方面的專家。

Dell Technologies 帶來組織內部可能未提供的創新解決方案和寶貴專業知識，可協助您掌握不斷演變的威脅態勢。

- 硬體與軟體安全性
- 對新興風險的深入解析
- 對進階攻擊技術的瞭解
- 可因應快速演變之威脅的 AIOps
- 新的安全性策略和最佳實務

建立多層防禦機制，以持續推動安全性實務並採用零信任方法。

Dell Technologies 是網路安全性合作夥伴，提供全方位專業服務、硬體與軟體解決方案，以及強大的合作夥伴生態系統，可限制攻擊機會、找出並有效減少漏洞，同時協助您快速恢復業務營運。

減少攻擊面 →

偵測及因應網路威脅 →

快速地從攻擊中復原 →

邊緣 **核心** **多雲端**

專業服務

業務/技術合作夥伴生態系統 **安全的供應鏈**

DELL Technologies

減少攻擊面

減少網路罪犯偏好利用的途徑，藉此提高您的防禦能力，使自己成為較小的目標。

為了強化安全性狀態，您必須找出可能入侵各種網域 (包括邊緣、核心及雲端) 中之應用程式、系統或網路的漏洞和進入點，並將這些漏洞和進入點減至最少。

找出漏洞點

- 軟體漏洞
- 錯誤組態
- 驗證機制較弱
- 系統未修補
- 使用者權限過多
- 開放式網路連接埠
- 實體安全性不佳

實作預防性措施

- 與安全可靠的供應商合作
- 套用全方位網路分段
- 隔離關鍵資料
- 強制執行嚴格的存取控制
- 更新和修補系統與應用程式
- 透過 AI、定期評估及測試找出並解決漏洞

採用零信任方法

零信任架構意味著貴組織不會自動信任其周邊內部或外部的任何內容。相反地，在授予存取權限之前，所有嘗試連線至系統的內容均會進行驗證。這是美國國防部建立和規定的模式，當中納入了相互關聯的 7 大支柱，可有系統地建立成熟度。

1. 使用者信任
2. 裝置信任
3. 資料信任
4. 應用程式和工作負載
5. 網路與環境
6. 可見度和分析能力
7. 自動化和協調流程

DELL Technologies

減少攻擊面

在問題來臨前找出影響系統的弱點。

網路安全性並非一次性工作，而是一個持續不斷的過程。在經驗豐富的安全性服務合作夥伴提供協助下，定期稽核、滲透測試及漏洞評估將有助於找出並填補缺口，從而降低風險。

安全的供應鏈實務	安全性比想像中更早開始。使用以安全的供應鏈、安全的開發生命週期及嚴謹的威脅建模所設計、製造和交付的裝置與基礎結構，建立值得信賴的基礎。
內建安全性	使用具備內建硬體型安全性的裝置與基礎結構，讓您搶先找出攻擊並加以消除，以免其造成損害。
定期修補和更新	透過最新的安全性修補程式，讓應用程式、韌體及作業系統隨時保持最新狀態，從而解決已知漏洞並將遭盜用的風險降到最低。
最低權限	將使用者和系統帳戶限制為僅擁有執行其工作所需的最低存取權限。此方法可限制取得未經授權之存取權限的攻擊者帶來的潛在影響。
網路分段	針對關鍵的資料和業務群組與應用程式，使用現代化網路分段，藉此隔離關鍵資產以限制網路存取。這可藉由防止橫向移動來遏止攻擊。
應用程式安全性	實作安全編碼實務、定期進行安全性測試和程式碼審查，以及使用 Web 應用程式防火牆 (WAF) 來協助防範常見的應用程式層級攻擊，同時減少 Web 應用程式的攻擊面。
專業服務與合作關係	與網路安全性服務供應商合作，並與業務和技術合作夥伴建立合作關係，引進組織內部可能未提供的專業知識和解決方案。
使用者教育和認知	訓練員工和使用者辨識和報告潛在安全性威脅、網路釣魚嘗試及社交工程手法，以將利用人為漏洞的風險降到最低。

DELL Technologies

偵測及因應網路威脅

在現今資源需求量最大的環境中，舊有的學校安全性實務如同撥接網際網路，速度太慢且效果不彰。

為了對抗複雜的網路威脅，您必須具備更有效的安全性技巧，例如內建於應用程式和方法的 AI 和 ML，以識別及因應已知和未知的內容。

實作強大的入侵偵測和預防系統

運用 AI 和 ML 進行異常偵測

建立網路流量和使用者行為的即時監控機制

與經驗豐富的專業服務部門合作，以獲得特殊的專業知識，進而提升復原能力。

身為經驗豐富的技術合作夥伴，Dell Technologies 可協助您建立主動式事件應變與復原通訊協定，這些通訊協定會概述角色和責任，並確保成員之間的溝通與協調順暢無礙。

使用以下進階功能，強化您主動偵測及因應網路威脅的能力：

- 威脅情報
- 事件回應
- 安全性資訊和事件管理
- 端點保護
- 行為分析

透過以下方式促進高效率的快速復原，並有效減少資料遺失：

- 完善的事件應變計畫與協作
- 關鍵資料和系統的定期備份
- 安全的異地儲存解決方案和資料加密

DELL Technologies

偵測及因應網路威脅

保持警覺並迅速採取行動。

偵測及因應網路威脅意味著保持警覺並為最壞情況做好規劃。建立持續更新且定期實踐的應變與復原計畫，讓您的整個組織瞭解如何減輕攻擊的影響。這是一個持續且反覆的過程，需要結合技術、專業技術人員、完善的程序及團隊協作。

持續監控	安全性工具 (例如入侵偵測系統 [IDS]、入侵預防系統 [IPS]、記錄分析及威脅情報) 可協助識別未經授權存取、入侵、惡意軟體感染及資料外洩的跡象。
威脅偵測	善用 AI 和 ML 來分析資料，找出可能指向威脅的模式、異常狀況及入侵指標 (IoC)。這包括辨識已知的攻擊特徵和識別偏差行為。
警示與通知	提供早期警告，以提示執行調查並做出回應。適時浮現警示和通知，以便透過整合式安全性快速採取行動。提供作業系統上層的裝置層級遙測，以協助加快威脅偵測速度，並在偵測到潛在威脅或事件時，發揮資安人員或安全性作業中心 (SOC) 的能力。
事件應變	啟動應變計畫，以調查並緩解已確認的資安事件。這包括遏止影響、找出根本原因及採取必要的行動，以還原系統並防止進一步的損害。
鑑識分析	對事件進行詳細分析，以瞭解攻擊方法、判斷資料外洩程度、識別受影響的系統或資料及收集證據，從而找出並解決安全漏洞。
補救和復原	採取步驟來補救漏洞、修補系統、移除惡意軟體並實作強化的安全措施，以防範類似的事件。將受影響的系統和資料還原至正常狀態，以完成復原程序。

DELL Technologies

從網路攻擊中復原

全速展開行動，讓您的業務回到快速發展的狀態。

網路韌性在現今的資料導向環境中為必要條件，也是客戶和合作夥伴期望擁有的能力。為獲致成功，您需要多層保護機制來確保關鍵資料受到保護和隔離，以便在遭受攻擊後能安心地快速還原資料。評估您的網路恢復能力 ›

採取行動以減輕網路攻擊造成的損害

重新建置遭入侵或中斷的服務和裝置

分析事件以防範日後的攻擊

滿足業務 SLA 並讓作業恢復正常

制定全方位的網路安全性策略，讓您的組織能以兼具效果和效率的方式復原。

若要從網路攻擊中復原，將需要進行涉及 IT 團隊、網路安全專業人員、管理部門 (有時也包括外部專家) 的協調工作。復原的關鍵在於讓系統和作業快速恢復正常，同時從事件中學習，以減少中斷情形和停機時間、還原服務和資料完整性、將財務和商譽影響降到最低，並強化網路安全性，藉此防範日後類似的攻擊。

- 評估攻擊對業務營運的影響
- 優先處理關鍵服務
- 部署資料保護系統
- 討論任何事件和復原進度
- 制定計畫並不斷實踐以確保持續性

DELL Technologies

從網路攻擊中復原

在事件發生後還原系統、網路及資料，藉此恢復營運狀態。

實現網路恢復能力策略可將人員、程序及技術整合至能夠保護您整個組織的全方位架構中。

事件控制	第一步是隔離並遏止網路攻擊的影響。這包括中斷受影響系統的網路連線、停用遭入侵的帳戶，以及實作相關措施來防範進一步的擴散或損害。
系統或裝置還原	事件受到控制後，受影響的系統和網路便會還原至乾淨且安全的狀態。這可能包括重新建置遭入侵的系統、重新安裝軟體，以及套用安全性修補程式和更新。自動化和自我修復在恢復營運方面扮演著重要角色。
資料復原	必須復原在遭受攻擊期間可能遭到破壞、加密或刪除的資料。這可能包括從備份還原資料，或使用專業的資料復原技術，以重新取得遺失或加密的檔案。
鑑識分析	遭受攻擊後，請務必瞭解發生資料外洩的原因、遭到利用的漏洞，以及可防範類似攻擊的相關步驟。安全性資訊和事件管理 (SIEM) 等系統和離機 BIOS 比較等功能可提供實用的深入解析。
事件應變評估	復原後，請務必評估事件應變程序，並找出需要改善的區域。從攻擊中學到的經驗可用於強化安全性實務、更新事件應變計畫，以及提供更有效的保護機制來防範日後的事件。
專業服務與合作關係	網路安全性服務供應商和技術合作夥伴可提供寶貴的專業知識與資源，協助貴組織復原。他們可協助執行鑑識分析等工作，識別入侵事件的發生頻率，以及提出可防範日後事件的相關措施。

DELL Technologies

將網路安全性延伸至邊緣和雲端環境

隨著網路從核心擴展到邊緣再到雲端，環境已成為關鍵的漏洞點。

在推動網路安全性策略時，貴組織應將零信任原則延伸至邊緣和雲端，以確保嚴謹的存取控制、持續驗證，以及完整的網路流量能見度和控制能力。隨著威脅態勢不斷演變，將 AI 功能部署為第一道防線是明智的選擇。此外，只有在核心網路和雲端環境具備安全措施 (例如網路分段、加密及持續監控) 時，策略才算完整。

網路安全性專業服務可協助您採取全方位措施。

連接各種安全性解決方案可能是一大挑戰。與專精於邊緣、核心及雲端安全性的專業服務團隊合作，您將能獲得相關的專業知識，藉此制定可從各個角度保護貴組織的有效措施。

邊緣

在邊緣、網路及硬體和軟體內建立多層安全性。

核心

使用 AI、ML 及自動化技術，讓您的基礎結構與零信任方法保持一致。

多雲端

保護任何環境中的任何工作負載，包括公有雲、容器及雲端原生工作負載。

DELL Technologies

生成式 AI：網路安全性的雙面刃

新一代 AI 讓我們不僅加速面臨新風險，同時也獲得提升的安全性。

作為 AI 發展的下一個階段，生成式 AI 涵蓋可在一系列的工作中瞭解、學習、調整及實作知識的系統。

一方面，生成式 AI 預期將能改善威脅偵測與應變、預測功能及營運效率。另一方面，這項技術也帶來了新的挑戰，您必須具備與時俱進的網路安全性策略，以透過強大的安全措施、持續監控、定期更新和修補，以及不斷演進的資料隱私權與道德方法來解決風險。

透過生成式 AI 保護組織

生成式 AI 已成為網路安全性的關鍵助力，並開啟保護組織的新途徑。

- 提升威脅偵測與應變機制的效能。
- 預測未來威脅或找出潛在漏洞。
- 自動化威脅偵測並提供效率。
- 鑑識分析可快速找出模式、異常狀況及入侵指標。
- 個人化安全意識訓練。
- 藉由更快地存取更豐富的深入解析擴大安全性作業規模。

保護生成式 AI 系統

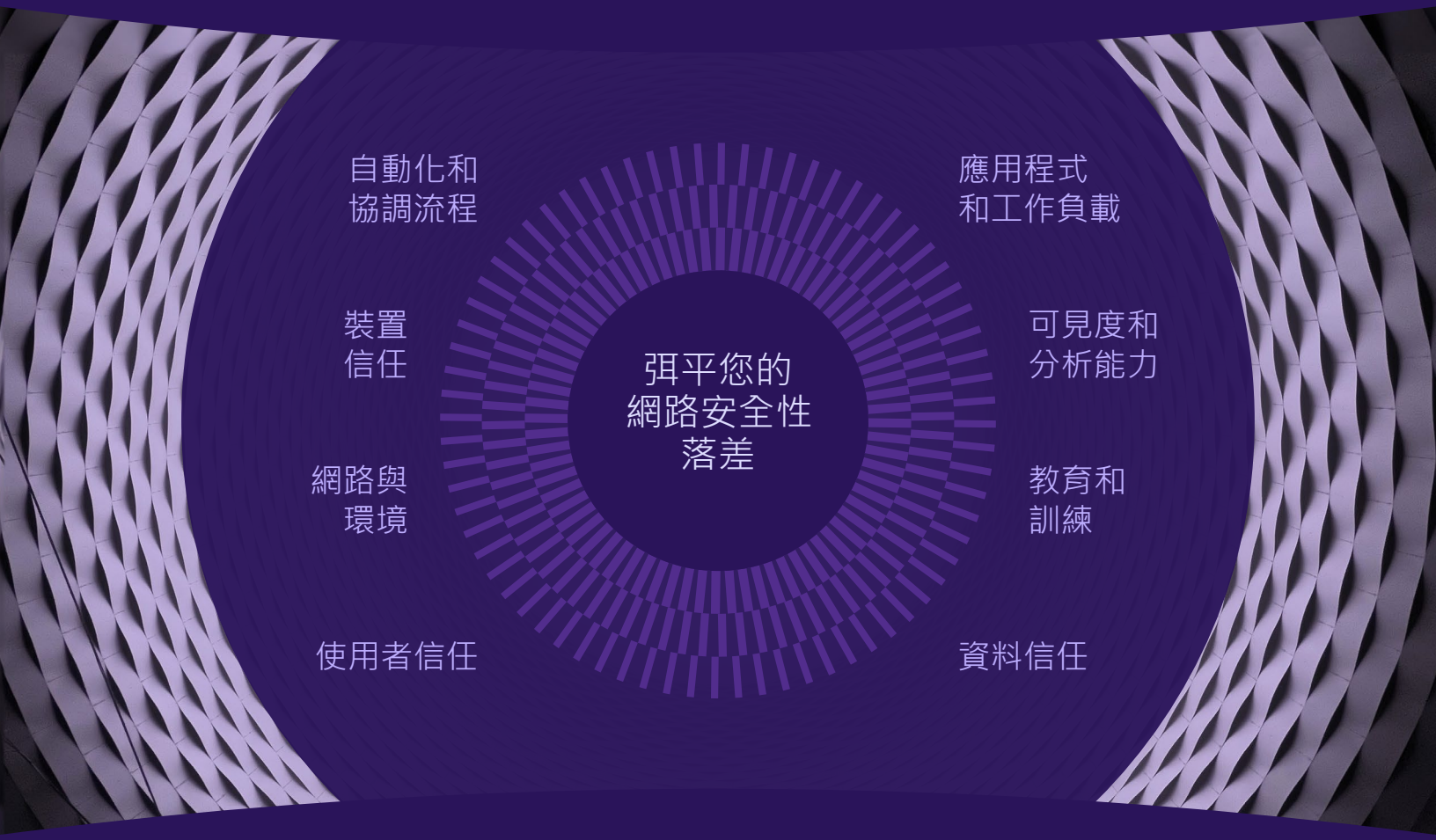
雖然生成式 AI 可帶來實質的安全性優勢，但如果未妥善保護，其功能可能會遭他人惡意使用。

- 確保資料隱私權和完整性。
- 緩解旨在欺騙 AI 系統並導致系統故障的惡意攻擊。
- 偵測及因應來自惡意 AI 的系統誤用。
- 稽核並減緩道德問題和偏見。
- 為 AI 系統實作強大的存取控制。
- 安全地保護並還原大型語言模型 (LLM)。

DELL Technologies

現代化網路安全性應具備智慧、可擴充且自動化的特性

Dell Technologies 可協助您建立全方位安全性，以防範不斷演變的網路威脅。隨著技術進步，我們的網路安全性方法也不斷保持領先優勢，運用 AI 和 ML 的強大力量來保護您的數位基礎結構，並維持對數位領域的信任。無論您在網路安全性旅程的哪個階段，我們都會與您合作，除了透過可讓您保持靈活度和彈性的步驟來保護貴組織外，亦可協助您達成更多目標。



DELL Technologies

Dell.com/SecuritySolutions

要求回電

與資安顧問交談

請致電 1-800-433-2393