10 項網路安全建議

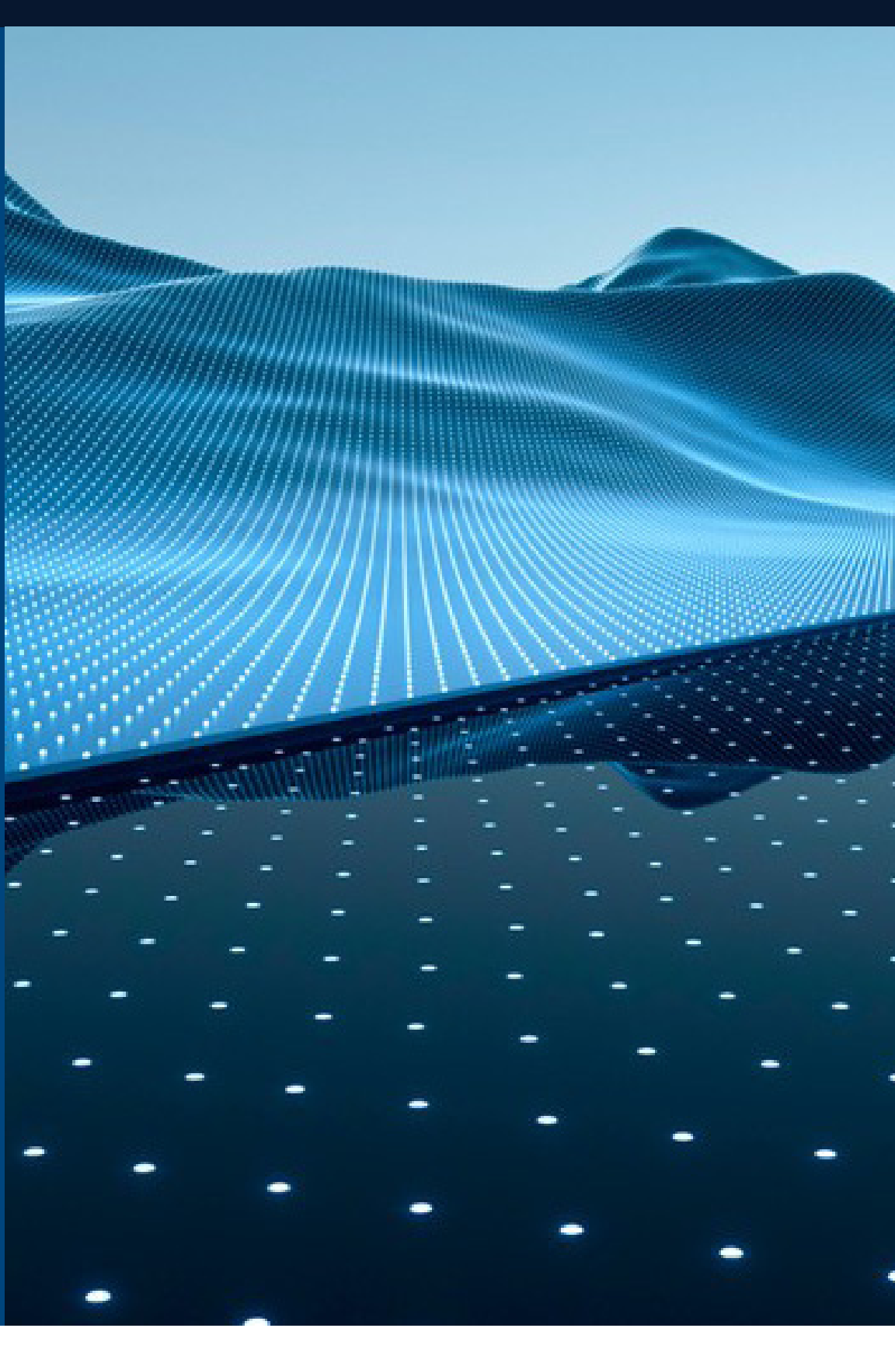
技術正在以如此快的速度發展，當我們採用新的工具和系統來強化我們的運算基礎設施時，我們也同時為想要利用漏洞的網路威脅創造了新的機會。在此情況下，必須實施防範這些新興威脅的健全網路安全措施，並確保創新能夠在安全的環境中蓬勃發展。隨著組織要不斷因應新的風險，Dell Technologies 的網路安全專家提出 10 項基本行動建議，以提升您的網路安全成熟度。

1

瞭解您的威脅風險態勢。

經驗豐富的網路安全合作夥伴可以提供寶貴的專業知識和資源，協助因應快速演變的威脅態勢。

- 進行徹底的漏洞評估和滲透測試，以識別需要解決的潛在弱點，並找出策略中可能存在的任何差距。
- 受益於內部可能沒有的專業技能和知識，例如對新興風險、先進攻擊技術，以及最新安全策略和最佳實務的深入見解。
- 定義存取權和基本原理，可讓您建立適當的安全框架，實施業務控制和管控。



2

制定全方位的網路安全策略。

若要確保網路韌性，將需要進行涉及 IT 團隊、網路安全專業人員、管理部門的協調工作，有時也需要外部專家的參與。

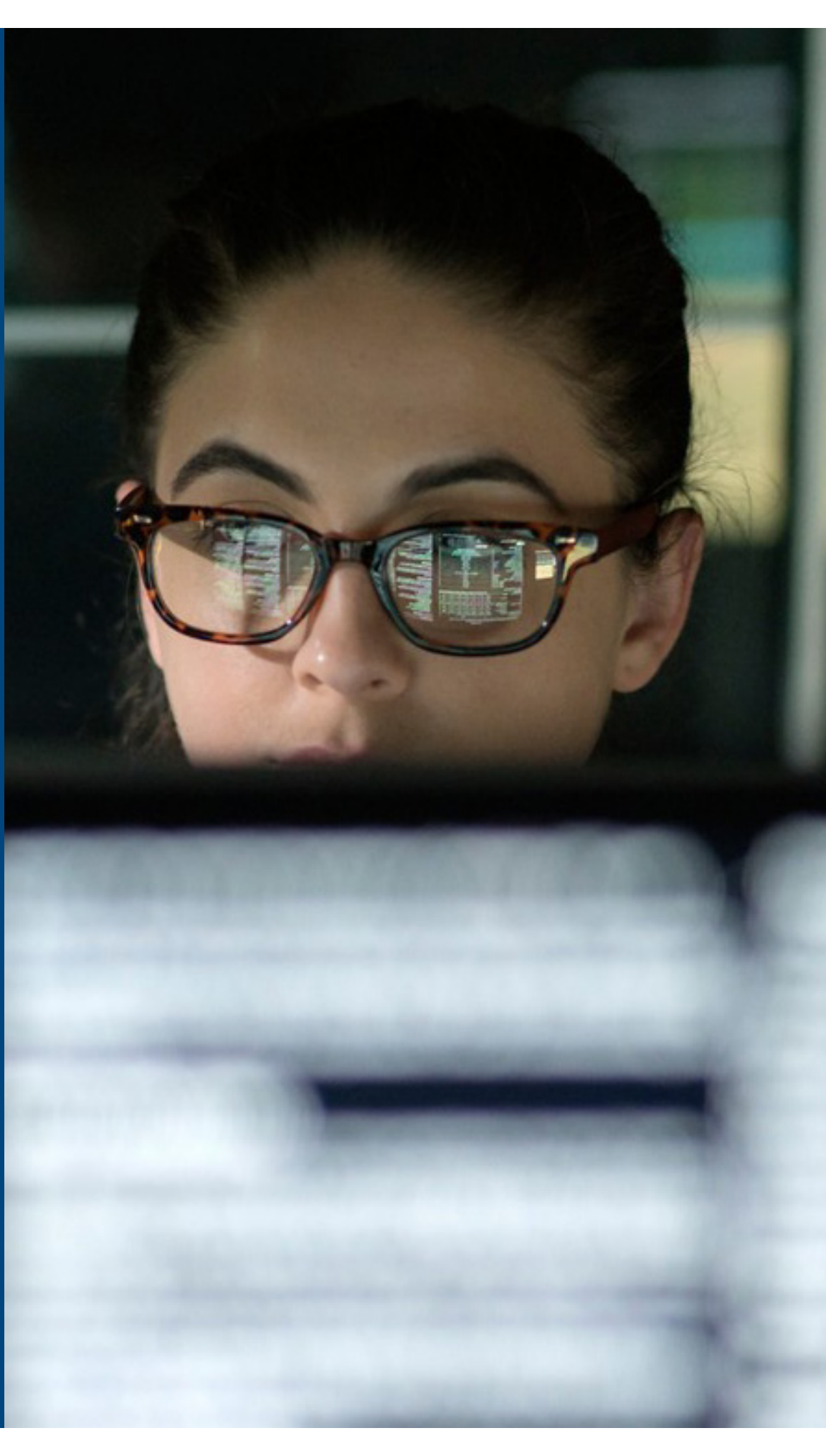
- 推動整個公司的積極參與 – 安全性是每個人的責任。
- 盡可能利用自動化。
- 確保您有一個經過精心演練的 IRR 計畫，以便在發生網路攻擊時，向所有相關人員示警。

3

與擁有安全供應鏈的供應商合作。

安全性比想像中更早開始。與在設計、製造及交付裝置和基礎結構時優先考慮安全性的供應商合作，確保值得信賴的基礎。提供安全供應鏈、安全開發生命週期和嚴格威脅建模的供應商，有助於掌握先機，防範威脅源起方。

- 提供說明橫跨 IT 供應鏈的機密性、完整性和資訊可用性資訊，以及參與 IT 供應鏈的廠商相關資訊。
- 確保供應鏈中的 IT 產品或服務是正版原廠狀態、未經變更，並且符合採購商的規格，沒有任何其他不必要的功能。
- 減少可能限制元件預期功能、導致元件故障或提供入侵機會的漏洞。



4

採用零信任原則。

零信任是一種安全概念，其核心概念是組織不應自動信任其邊界內外的任何內容，而是必須在授予存取權之前，驗證嘗試連線至其系統的一切。

- 摒棄邊界型安全模式，並採用零信任原則。
- 實現最低權限原則，該原則限制使用者和系統帳戶僅具有其工作所需的最低存取權。此方法可減少攻擊面和攻擊者未經授權存取的潛在影響。
- 整合微切分、身分識別與存取管理 (IAM)、多因素驗證 (MFA) 和安全性分析等解決方案。

5

減少攻擊面。

攻擊面代表惡意行為者可利用的潛在漏洞和進入點。為了強化安全狀態，組織必須盡可能減少攻擊面、降低風險，並針對全新和新興威脅，強化整體網路防禦能力。

- 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，將利用人為漏洞攻擊成功的風險降到最低。
- 實施預防措施，例如全面網路切分、關鍵資料隔離、實施嚴格的存取控制，以及定期更新和修補系統和應用程式。
- 確保系統、網路和裝置已使用安全性最佳實務正確配置，例如停用不必要的服務、使用強式密碼以及實施存取控制。

6

偵測及因應網路威脅。

面對複雜的威脅，傳統的安全性措施已不足夠。組織應利用進階威脅偵測技術和方法來有效地識別和因應已知和未知威脅。

- 監控和分析網路流量、系統記錄和其他區域，以及安全資料，以主動識別未經授權的存取、入侵、惡意軟體感染、資料違規或其他網路威脅的跡象。
- 啟動應變計畫，以迅速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。
- 利用 AI/ML，透過即時分析異常資料模式或行為，快速偵測網路威脅。這些技術還透過評估威脅嚴重性、預測影響、自動化某些防禦措施和擴展最佳實務來加速快速應變，進而將潛在損害降到最低。

7

從網路攻擊中復原。

即使已採取關鍵的主動措施，組織仍應隨時假設本身遭到入侵，並且必須具有適當的韌性運算基礎設施。而這些運算基礎設施要經常進行測試，以確保可從成功的網路攻擊中有效復原。

- 立即採取行動，隔離並控制影響，以緩解網路攻擊造成的損害。
- 可採取的行動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，防範進一步的擴散或損害。
- 使用 AI/ML 後，可快速找出受影響的系統和資料，並自動執行備份還原程序，藉此加快復原速度。

8

善用經驗豐富的合作夥伴。

沒有任何單一廠商具備提供端對端安全性所需的所有必要能力，包括人員、程序或技術，而是需要合作。因此，與經驗豐富的合作夥伴網路協同合作至關重要。

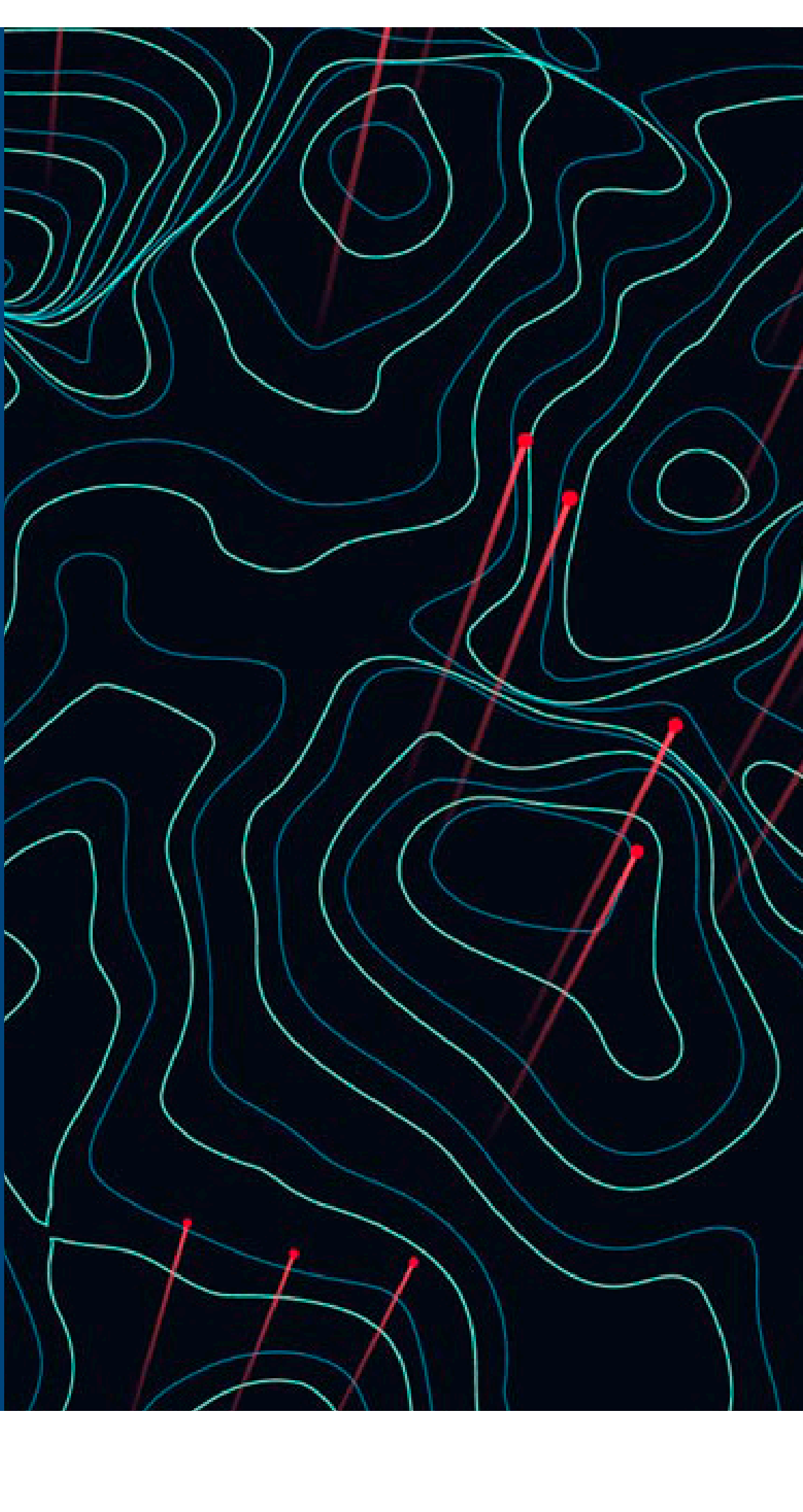
- 與經驗豐富的網路安全合作夥伴合作，他們可提供寶貴的專業知識和資源，協助因應快速演變的威脅態勢。
- 受益於內部可能沒有的專業技能和知識，包括對新興風險、先進攻擊技術，以及最新安全策略和最佳實務的深入見解。
- 利用經驗豐富的專業服務提供的專業知識，並與值得信賴的業務合作夥伴建立協同合作關係，以建立全方位的安全狀態，有效防範不斷演變的網路威脅。

9

將網路安全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，這些環境已成為關鍵的漏洞點。無論應用程式如何部署，都需要相同層級的安全性，並與業務政策保持一致，以確保應用程式使用者和管理的一致性。

- 確保延伸零信任原則以涵蓋邊緣和雲端環境，並提供健全的存取控制、持續認證，以及對網路流量的全方位可見度與控制。
- 在核心網路和雲端環境中實施安全性措施，例如網路切分、加密和持續監控，以防範潛在威脅。
- 與專精於邊緣、核心及雲端安全性之經驗豐富的專業服務團隊合作，運用其在實作可從各個角度保護貴組織之有效措施方面的專業知識。



10

主動管理並提高端對端復原能力。

管理威脅情報、事件與因應以及安全性作業，可強化組織偵測和因應網路威脅的能力。

- 建立清楚概述角色和責任的主動事件因應和復原通訊協定，確保團隊成員之間順暢溝通與協調。
- 強化環境的可見度，使組織能夠主動監控和因應其網路內的威脅，同時在必要時提供復原警示。
- 運用進階威脅情報、安全性資訊和事件管理 (SIEM)、端點保護解決方案和行為分析，強化您主動偵測及因應網路威脅的能力。

別讓安全風險阻礙創新。
請前往 dell.com/SecuritySolutions，瞭解如何提升網路安全
與零信任成熟度

DELL Technologies