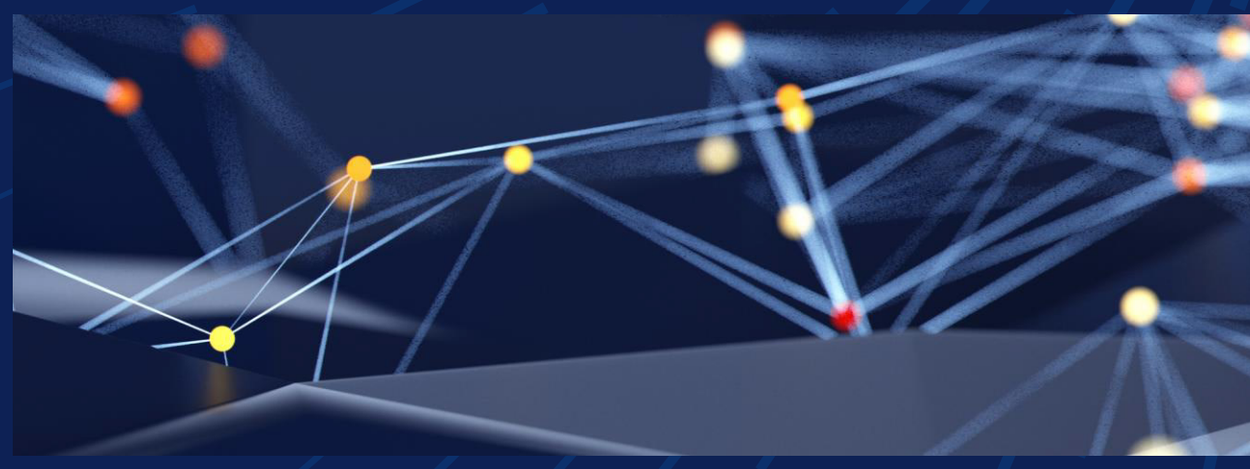
網路安全的未來：

適應新的數位時代



網路安全專業人員經常專注於防範攻擊和制定復原計畫，但與此同時，整體安全性環境也在持續演進。因此，為接下來的事情做好計畫非常重要。

展望未來，有三個領域相當顯眼——後量子密碼學、不斷變化的法規環境，以及新興威脅。組織應立即採取行動，當有可用的解決方案時，隨即規劃和實施。

後量子密碼學的曙光

量子運算有望改變產業，提供驚人的運算能力，能夠解決傳統電腦無法解決的問題。但是，同樣的功能也可能會讓目前的加密方法過時。RSA 和 ECC 這類演算法支撐著現今大部分安全通訊，卻有可能在幾秒鐘內被夠先進的量子電腦破解。這種迫在眉睫的威脅，加劇了後量子密碼學的急迫性。

後量子密碼學 (PQC) 涉及開發加密演算法，以在量子運算時代保持安全。美國國家標準暨技術研究院 (NIST) 已經意識到這項風險近在眼前，正帶頭標準化抗量子演算法。

對於企業來說，為這種轉變做準備是不容妥協的工作。儘早採用 PQC 解決方案，以便在攻擊者獲得量子運算功能時，確保資料安全。

Dell 網路安全副總裁暨業務部門安全長 Bobbie Stempfley 指出，組織在開始時應著重於兩個關鍵領域：

識別和清點目前使用的所有密碼編譯模型。

不僅僅是靜態資料，也要考慮流動中資料。考慮金鑰管理、程式碼簽署、裝置識別、安全存取和遙測。建立全方位庫存，然後建構藍圖。

瞭解供應商狀態。

鑒於現代企業可能擁有數千家供應商，請留意他們可能帶來的風險。努力確保他們也在規劃進行改變。

除了這些起點之外，還要進行風險評估以識別易受攻擊的系統，考慮實施混合加密模型以在過渡期間維持營運，並與已經在探索量子安全解決方案的廠商合作，但請記住，沒有單一廠商或技術是一站式解決方案。

全球化世界中的法規變化

塑造網路安全未來的另一個關鍵驅動因素，是不斷變化的法規環境。法規現在已遠遠超出法規遵循的範圍，在互連的資料導向世界中，成為灌輸責任、推動技術升級和保護公民的關鍵框架。然而，它們正在迅速發展，並且因地理位置而異，進而增加法規遵循的複雜性。

也就是說，這些法規不僅僅是對違規行為的處罰，更是改善網路安全實務的催化劑。積極使其政策與法規要求保持一致的企業，可以發揮更高層次的信任和營運效率。為此，組織應建立能夠彈性適應法律變化的治理框架，定期進行法規遵循稽核，並投資員工訓練，以便根據最新標準處理敏感資訊。

當安全主管為法規遵循做準備時，確保法規可理解和被理解非常重要。資安專業人員說話時經常使用安全術語，這可能不會與客戶、監管機構和其他利害關係人產生共鳴。資安專業人員有責任確保他們的話被理解，而不是由聽眾來解釋。

> 將轉移至後量子密碼學，想像成拿起並移動一棟傢俱齊全的房子。這就是那麼複雜，而挑戰在於過程中不要破壞任何東西。」
>
> ***Bobbie Stempfley***
> *Dell Technologies* 網路安全副總裁暨業務部門安全長

威脅 (和防禦) 態勢的演變

AI 正在革新業務、提高生產力，以及開創人類潛能的新商機。在網路安全方面，AI 對惡意人士和防禦者都有好處：

攻擊用途：利用 AI 可以進行更複雜的攻擊，例如高度令人信服的魚叉式網路釣魚和深度偽造。

防禦用途：AI 透過以下方式幫助防禦者：

- 快速處理大量安全性資料。
- 更有效地確定威脅的優先順序。
- 強化偵測與回應能力。

然而，安全性工具只會越來越進步，因為自然語言處理可讓安全性專業人員更直接地與其系統互動，並讓系統能夠主動採取修正性網路安全措施。

組織應努力同時利用這些功能，同時確保其訓練和其他防禦機制保持最新狀態。為防止員工淪為更複雜攻擊的受害者，訓練是最佳方法。

邁向無密碼

密碼不再是身分與存取管理的最安全方法。

傳統基於密碼的系統存在重大漏洞，針對現代網路安全需求，這類解決方案日益不足。密碼容易受到憑證填充、網路釣魚和暴力破解等攻擊，通常會使組織面臨不必要的風險。此外，不良的使用者行為 (例如重複使用密碼或建立弱式密碼) 會加劇這些漏洞。

無密碼驗證方法 (例如生物特徵辨識、憑證和硬體權杖) 透過消除整個與密碼相關類型的威脅，提供更強大、更安全的替代方案。遷移到無密碼系統代表身分與存取管理的關鍵演變，針對日益複雜的網路威脅，建立相應的安全措施。

採用無密碼技術還提供許多好處，包括減少攻擊面、透過更快、順暢的登入來改善使用者體驗，以及透過減少與密碼相關的事件來降低 IT 成本。進階方法的使用可確保更強大的安全狀態，並協助組織遵循法規標準。過渡到無密碼系統不僅是一種趨勢，更是為個人和組織建構更安全、更有效率的數位生態系統的必要步驟。

結論

在量子運算、不斷變化的法規和日益複雜的威脅的影響下，網路安全正進入一個變革性時代。為了保持領先地位，組織必須採用創新技術，例如後量子密碼學、AI 導向的防禦和無密碼驗證。透過優先考慮準備、協作和策略投資，企業可以建構更安全、更有彈性的數位環境。現在就是行動的時候

可提供協助的 Dell 產品和解決方案

精選 Dell 解決方案	說明
網路安全諮詢服務	專家指引可協助您針對不斷演變的威脅態勢 (包括目前和新興威脅)，進行規劃。
vCISO	虛擬資安長和網路安全專家可協助識別和管理風險，以及指引策略性決策。

造訪 **dell.com/cybersecuritymonth**，瞭解如何解決當今一些主要的網路安全挑戰