DELL Technologies

# 後量子密碼學

開始使用

# 簡介

量子運算正在推動技術的根本性重新設計，同時創造出驚人的商機和全新的挑戰。雖然這樣的未來令人興奮，卻對保護數位世界的密碼系統帶來了重大威脅。

## 為什麼量子運算正在興起？

不論是筆記型電腦、智慧型手機還是伺服器形式的傳統電腦，都使用以零或一之狀態存在的位元來處理資訊。這種二進位模型推動了數十年的進步，但它限制了資訊的表示和操作方式。量子電腦使用量子位元，透過疊加和糾纏等原理，可以同時存在於多種狀態。這使量子機器能夠平行探索大量可能的解決方案，為特定類別的問題提供運算優勢。

## 什麼是後量子密碼學？

後量子密碼學 (PQC) 是指新一代演算法，旨在保護數位系統免受傳統和量子攻擊。與需要專用硬體的量子金鑰分發不同，PQC 設計為在現今的傳統基礎結構上執行 (伺服器、端點、網路)，可成為針對量子時代做準備時最實用且可擴展的方式。

# 組織面臨量子運算所帶來的哪些直接風險？

後果遠超出理論風險。未能做好準備的組織將面臨敏感智慧財產的曝光、金融系統的中斷、醫療資料的外洩以及國家安全的威脅。

「先竊取，後解密」威脅加劇了急迫性：對手只需在今天擷取加密資料，然後等待解密的方法。在密碼學相關量子電腦到來時，損害將已無法挽回。

**「先竊取，後解密」**(Harvest Now, Decrypt Later)：也稱為「先記錄，後解密」(Record Now, Decrypt Later)，是指對手今天收集並儲存加密資料，意圖在未來密碼學相關量子電腦可用時進行解密的行為。

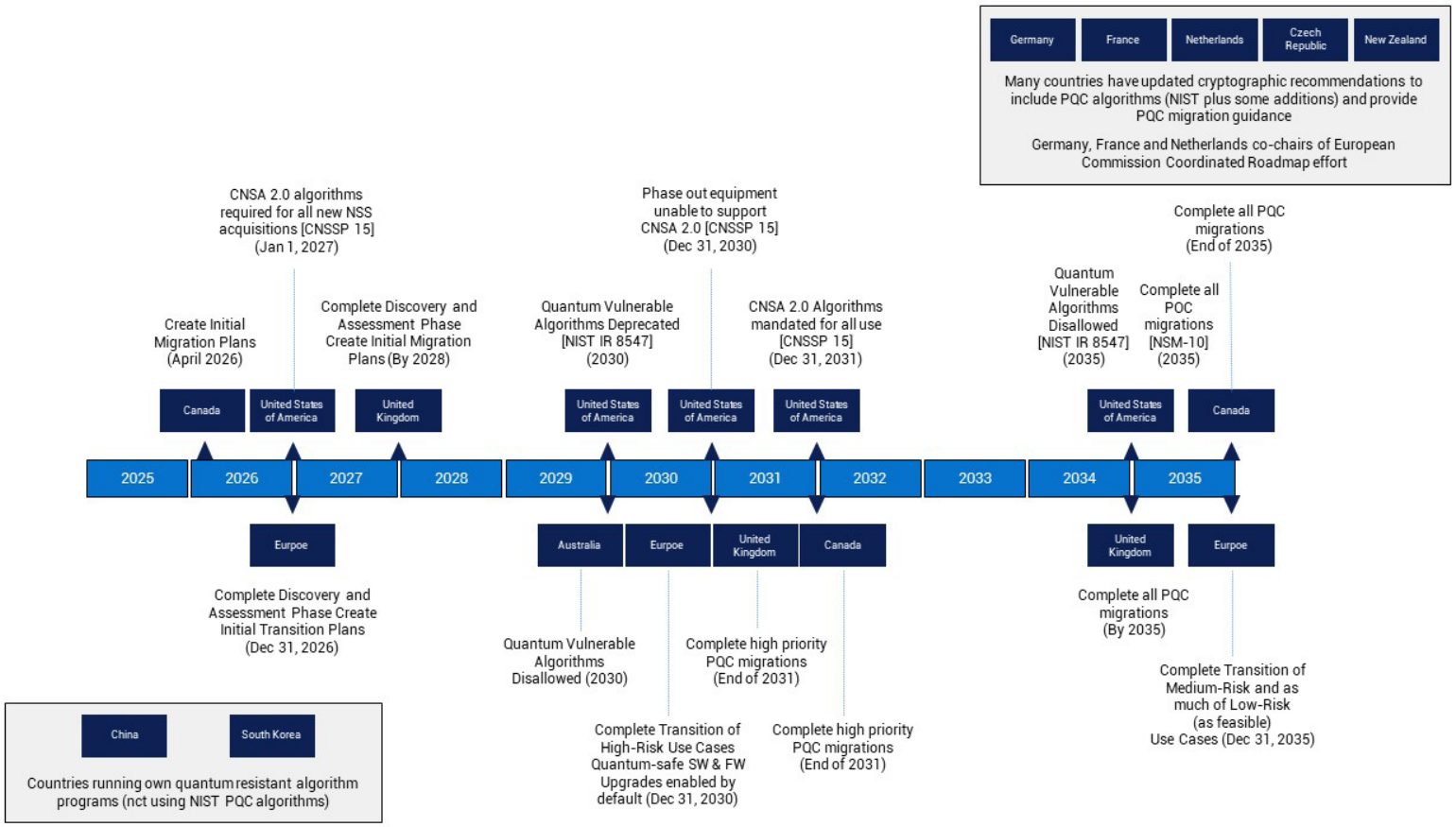
# 組織該如何為轉換到 PQC 作好準備？

通往量子安全未來的旅程是一條漫漫長路，並非一蹴可幾，必須經歷不斷的演變。一套主動式、分層且分階段的方法將有助於貴組織管理風險、安排資源並打造具復原能力的長期安全性狀態。Dell 會提供在每個階段支援您的技術和指引。以下是引導貴組織建立 PQC 轉換計畫的重要步驟。

# PQC 轉換時間表

認識到威脅的急迫性，各國政府和標準組織已將 PQC 列為全球優先事項。認識到採用量子抗性密碼學演算法的重要性，美國聯邦政府已開始向聯邦機構發佈 PQC 要求。這些要求包括國家安全備忘錄 10 (NSM-10)、商業國家安全演算法套件 (CNSA 2.0)、管理與預算辦公室備忘錄 23-02 (OMB M-23-02)，以及美國國家標準暨技術研究院 (NIST) 跨機構報告 (IR) 8547 等。

全球其他組織也為 PQC 轉換制定了指南。這些日期並非任意設定，它們反映了在複雜 IT 生態系統中重新設計、驗證和部署密碼學所需的前置時間。企業應將它們視為不僅僅是政府規範；它們是全球轉向量子韌性的實際指標。以下是一些不同國家的規範要求。



# 盤點和稽核密碼學威脅

第一優先要務是瞭解您目前的密碼學環境。這項基本步驟可為您的整個遷移策略提供情報。

## 良好的安全衛生習慣

為量子未來做準備的第一步是加強現有的防禦措施。組織應採用強大的安全衛生最佳實務，例如強制執行最小權限存取、實作多因素驗證，以及維持嚴格的修補程式管理。還有兩個其他考量因素。可能需要停用較弱的密碼學，以便具有更高密碼學強度的新系統能夠與舊有系統互通。對於較新的系統來說，提高最低安全性強度也十分重要 (AES-256 用於對稱密碼學，SHA-384 或更高版本用於摘要)，這樣才能彌補 Grover 演算法所導致的利潤減少。這些措施不僅能降低現今風險，還能最大限度減少密碼學債務的積壓，否則會使未來的移轉變得複雜。

## 盤點和稽核密碼學資產

任何移轉的基石都是可見性。組織必須進行全面的密碼學盤點，識別公開金鑰密碼學在應用程式、裝置和工作流程中的使用位置和方式。這包括 TLS 憑證、VPN、電子郵件系統、程式碼簽署機制、客戶資料、封存資料和其他項目。識別出來後，應根據業務關鍵性、敏感性和生命週期對資產進行優先排序。長期資料 (如病歷或機密檔案) 應以最高急迫性處理，因為它們最容易受到「先竊取，後解密」威脅的影響。

# 試行和實驗 PQC

確切盤點後，您就可以開始對支援 PQC 的技術進行實務實驗，以驗證效能和整合。

了解密碼學環境後，組織應開始在受控環境中測試 PQC 解決方案。透過在實驗室中試行這些解決方案，IT 團隊可以在大規模部署之前驗證效能、互通性和可管理性。建立這種密碼敏捷性 (在不徹底改造整個系統的情況下切換密碼演算法的能力) 對於長期韌性和移轉便利性至關重要。

# 採用互通性方法

PQC 標準成熟後，您就可以開始為生產推出進行規劃。混合式方法為完全量子安全的環境提供銜接。

隨著標準的成熟，混合模式提供了通往未來的橋樑。許多供應商已經支援混合密碼套件，在單一實作中結合傳統和量子抗性演算法。這種雙重方法，即使在其中一個演算法後來被破解的情況下，也能提供持續保護。企業現在應開始採用混合策略，同時將其內部時間表與基礎結構供應商的產品路線圖和里程碑保持一致。這確保當量子安全演算法達到標準化時，組織可以在不中斷的情況下擴大採用規模。

# 執行完整移轉和持續驗證

終極目標是完全整合且持續驗證的量子安全企業。

## 執行完整移轉和持續驗證

最終目標是在整個企業中完全轉換至 PQC。這不會是一次性事件，而是一個持續的驗證和適應過程。組織應執行詳細的移轉計畫，將 PQC 納入其 IT 堆疊的每一層，同時持續測試新標準和實作。使用由傳統電腦和量子電腦構成的混合式方法，客戶可以模擬攻擊場景、驗證密碼學完整性，並確保其系統對不斷演變的威脅保持韌性。

# 協作和知識共享

## 沒有組織應該單獨面對這項挑戰。

產業聯盟、學術研究人員和政府機構正在匯集知識以加速 PQC 轉換。參與標準組織、工作組和試行計畫，使企業能夠與最佳實務和新興要求保持一致。Dell 積極參與 NIST NCCoE PQC 專案等倡議，確保我們的客戶直接受益於這種集體專業知識。

# 結論

量子時代不再是遙不可及的可能性；這是即將發生的現實，企業必須立即採取具前瞻性的行動。對於保護您最寶貴的資產 (您的資料) 來說，為這項技術性改變作好準備是策略性必要事項。正如我們所概述的，從盤點與稽核到完全遷移的分階段方法，是通往量子安全未來的最清楚路徑。

移轉到 PQC 將是數十年來最重大的基礎結構變革之一。這種轉換幾乎觸及 IT 的每個面向，從伺服器和儲存到端點、雲端平台和網路協定。成功需要遠見、規劃和嚴格執行。在 Dell Technologies，我們將前進的道路視為分階段的旅程：在即時安全改進與 PQC 採用的長期準備之間取得平衡。

Dell 已經做好準備，協助您制定實作 PQC 的策略。我們建議採用分階段遷移計畫，並概述了一系列活動來協助您制定策略、規劃、執行和監控您的 PQC 轉換。