DELL Technologies

白皮書

後量子密碼學：為量子時代做好準備

Dell Technologies 白皮書

目錄

執行概觀

量子運算正從理論研究快速邁向實際應用。業界曾經將其視為遙不可及的未來，如今在硬體、演算法和投資的進步推動下，能夠解決傳統電腦無法處理問題的機器正加速到來。這對產業的影響深遠。從藥物開發到氣候建模再到全球物流，量子運算有望釋放過去無法觸及的創新潛能。

但這項突破也帶來了顛覆性挑戰：量子電腦將破壞保護數位經濟的密碼學基礎。公開金鑰密碼學 (如 RSA 和橢圓曲線密碼學 (ECC) 等演算法) 數十年來一直保護著數位通訊、金融系統、醫療記錄和國家安全。這些方法依賴於對傳統電腦而言難以解決的數學問題。然而，隨著密碼學相關量子電腦 (CRQC) 的出現，已經可以高效解決這些相同的問題，使當今的安全防護變得過時。

這種威脅並非理論性質。部分組織已經在使用一種稱為「先竊取，後解密」(harvest now, decrypt later, HNDL) 的策略：今天先收集加密資料，期待在量子電腦成熟後破解。現在看似安全的敏感資訊可能在幾年內就會變得脆弱。採取行動的時機不是等到 CRQC 到來之時，而是今天。

本白皮書說明量子威脅的急迫性，探討新興的後量子密碼學 (PQC) 領域，並提供組織如何做好準備的指引。本文強調 Dell Technologies 致力於建構量子安全未來的承諾 (在我們的供應鏈、硬體、韌體、軟體和合作夥伴生態系統中嵌入安全性) 透過與 NIST 後量子密碼學 (PQC) 標準 (FIPS 203、FIPS 204 和 FIPS 205) 以及商業國家安全演算法套件 2.0 (CNSA 2.0) 指南保持一致。Dell 的目標很明確：確保創新能夠在不犧牲安全性或信任的前提下向前推進。

術語

在本文中您會遇到許多術語。我們試圖概述其中一些術語，以協助理解本文內容。

後量子密碼學：一種新的密碼學數學方法，採用新演算法，旨在抵禦量子電腦攻擊。這些演算法在傳統電腦上執行，並且能夠抵抗量子攻擊以及已知的傳統密碼學攻擊。

量子韌性：量子韌性指的是即使在密碼學相關量子電腦 (CRQC) 存在的情況下，仍能保持安全的系統、演算法或基礎結構。量子韌性系統使用後量子密碼學 (PQC) 或其他防護措施來抵禦傳統和量子攻擊，確保資料在未來的機密性、完整性和真實性。其他術語如量子抗性 (quantum-resistant) 和量子安全 (quantum-safe) 也可互換使用。

密碼敏捷性：(有時稱為加密敏捷性) 是指組織的系統和應用程式能夠快速且順暢地切換密碼演算法、協定或金鑰長度，而無需進行重大重新設計或造成營運中斷的能力。

「先竊取，後解密」(Harvest Now, Decrypt Later, HNDL)：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 (CRQC) 可用時進行解密的行為。

量子運算與加密威脅

量子運算的崛起

正如我們在近一年前由技術長 John Roese 撰寫的部落格文章《後量子密碼學：企業韌性的策略要務》中所述，傳統電腦無論是筆記型電腦、智慧型手機還是伺服器，都使用位元來處理資訊，位元存在於零或一的狀態。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。

量子運算的應用潛力非凡。研究人員預期在藥物研發方面取得突破，透過模擬傳統電腦無法達到的精確分子交互作用。氣候科學家設想更準確的全球系統模型，而能源產業則看到最佳化電網和儲能的潛力。即使是物流和製造業也能從量子最佳化技術中受益。這些好處是真實且觸手可及的，但風險也是如此。

為何加密面臨著風險

加密是數位時代信任的基石。當您輸入信用卡號碼、登入安全網站或接收經簽署的軟體更新時，密碼學確保了機密性、真實性和完整性。這些保護大多依賴公開金鑰密碼學，如 RSA 和 ECC 等演算法，這些演算法依據那些無法在傳統機器上運算的數學問題。

量子運算改變了這個等式。使用 **Shor 演算法**，一台足夠強大的量子電腦可以解決賦予 RSA 和 ECC 強度的因數分解和離散對數問題。若 CRQC 存在，保護軟體更新的數位簽章、建立 TLS 工作階段的金鑰，以及驗證裝置的憑證都可能遭破解。這種影響是系統性的，威脅到目前能使數位交易安全的根本機制。

對稱式密碼學 (如用於保護儲存資料或安全通訊的 AES 等演算法) 面臨不同但較不嚴重的挑戰。**Grover 演算法**允許量子電腦降低對稱金鑰的有效強度，從效果而言能將其安全性減半。雖然這可以透過移轉到更大的金鑰大小 (如 AES-256) 來緩解，但這種調整凸顯了量子威脅的普遍影響。

急迫性與後果

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」策略加劇了急迫性：對手只需在今天擷取加密資料，然後等待解密的方法。在 CRQC 到來時，損害將已無法挽回。

後量子密碼學與新興標準

定義後量子密碼學

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。

PQC 的基礎是一組數學問題，根據目前所知，這些問題能夠抵抗 Shor 和 Grover 演算法等量子技術。格基密碼學 (lattice-based cryptography)、雜湊簽章 (hash-based signatures)、編碼方案 (code-based schemes) 和多變量方程式 (multivariate equations) 代表最有前景的系列。這些方法正在經過嚴格測試和標準化，以確保它們提供與 RSA 和 ECC 曾經提供的相同可靠性和互通性。

全球標準化努力——新興產業標準

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。美國國家標準暨技術研究院 (NIST) 於 2016 年啟動其 PQC 專案，呼籲密碼學研究社群提出、分析和改進候選演算法。經過多年測試，NIST 於 2024 年 8 月宣布第一批標準化演算法：

- **CRYSTALS-Kyber：**用於公開金鑰加密和金鑰建立
- **CRYSTALS-**Dilithium 和 SPHINCS+：用於數位簽章

其他演算法仍在審查中，以為不同的實作需求提供多樣性和靈活性，包括嵌入式韌體等輕量級系統。這個不斷演進的標準化過程確保全球組織有明確的路徑來採用量子抗性解決方案。

NIST 標準：FIPS 203、204、205

2024 年 8 月，美國國家標準暨技術研究院 (NIST) 完成了第一批 PQC 演算法：

- FIPS 203 (ML-KEM)：以 CRYSTALS-Kyber 為基礎的金鑰封裝機制。提供 IND-CCA2 安全性，意味著密文即使在自動調整選擇密文攻擊下仍然無法區分。
- FIPS 204 (ML-DSA)：以 CRYSTALS-Dilithium 為基礎的數位簽章演算法。提供強大的 EUF-CMA 安全性 (在選擇訊息攻擊下的存在性不可偽造性)，這是數位簽章的標準要求。
- FIPS 205 (SLH-DSA)：以 SPHINCS+ 為基礎的雜湊簽章方案。經選為不依賴格問題的保守備案。

強制性路線圖

認識到採用量子抗性加密演算法的重要性，美國聯邦政府已開始向聯邦機構發布 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)、美國國家標準暨技術研究院 (NIST) 跨機構報告 (IR) 8547，以及管理與預算辦公室備忘錄 23-02 (OMB M-23-02) 等。

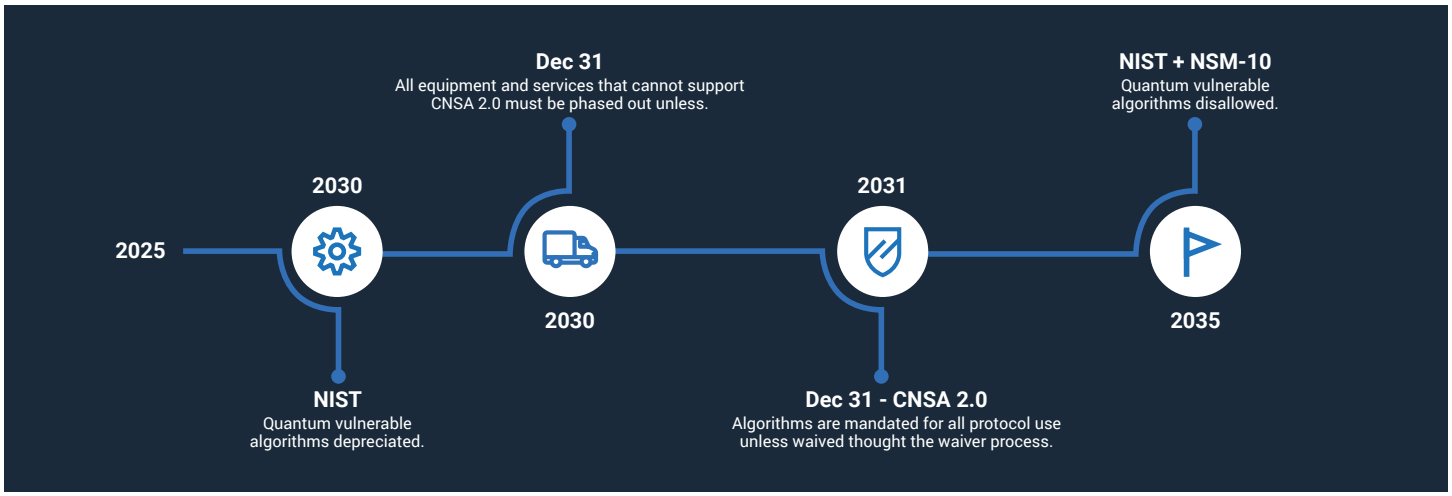
National Security Memorandum 10 (NSM)
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

Commercial National Security Algorithm Suite 2.0 (CNSA 2.0)
Introduces the first recommendations post-quantum cryptographic algorithms

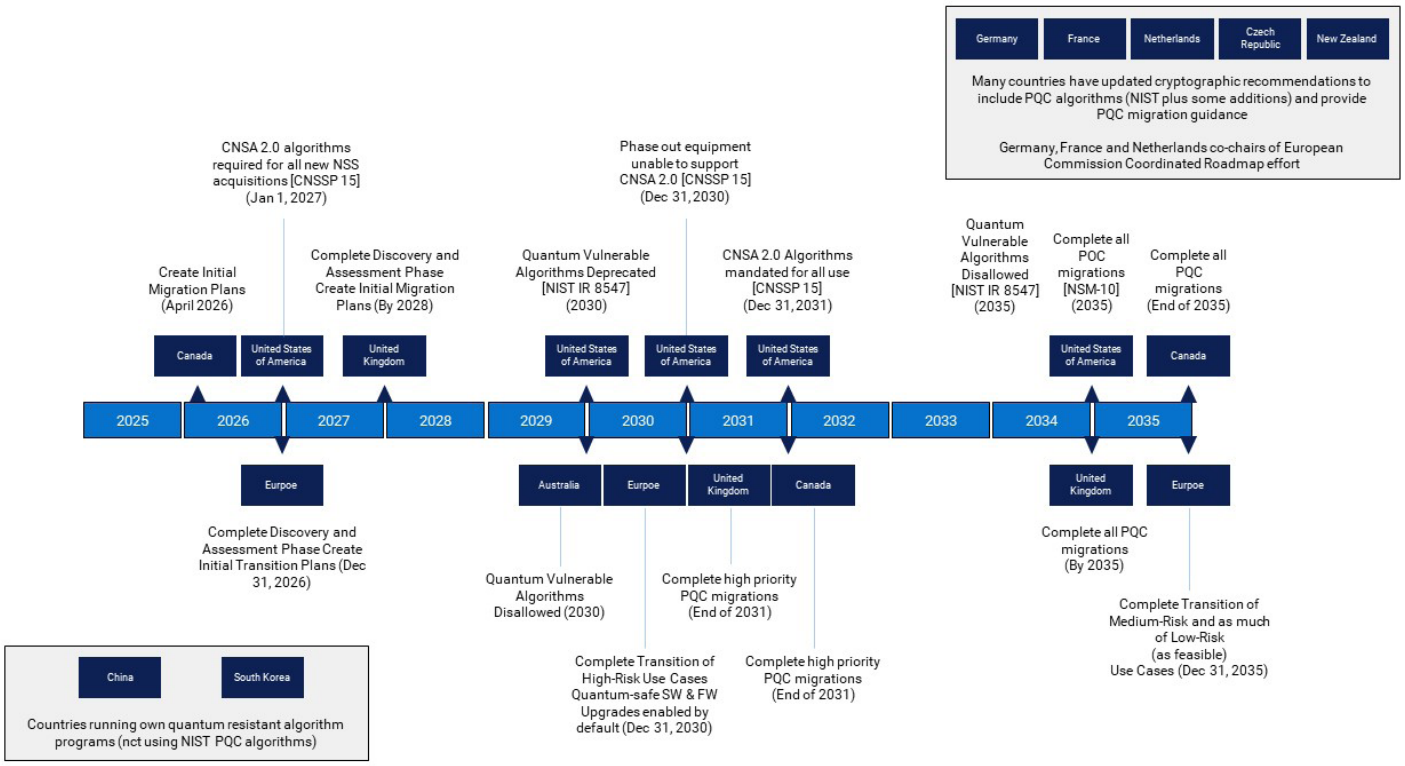
NIST IR 8547
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

OMB Memorandum 23-02 (OMB M-23-02)
Provides detailed guidelines for federal agencies to how to comply with NSM-10

CNSA 2.0 由 NSA 於 2022 年 9 月宣布，引入了首批後量子密碼演算法建議。CNSA 2.0 為國家安全系統 (NSS) 採用量子抗性演算法設定了明確的截止日期，並為準備自身轉換的企業提供了有力的指引：



全球其他組織也為 PQC 轉換制定了指南。 以下是一些不同國家的規範要求。



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。

產業協作

除了 NIST 和 NSA 之外，Dell 正積極影響並參與推動互通性和採用的產業聯盟和標準組織。可信賴運算群組正將 PQC 整合到可信賴平台模組 (TPM) 標準中。IETF 正推動將 PQC 演算法整合到產業協定中，例如 TLS、X.509 憑證等。OASIS 金鑰管理互通性通訊協定 (KMIP) 委員會正為金鑰管理框架啟用 PQC。FIDO 聯盟正在研究 PQC 對身分驗證和裝置上線標準的影響，而 SAFECode 等組織則致力於教育產業有關移轉準備的知識。

NIST 國家網路安全性卓越中心 (NCCoE) 是一個架構，允許 NIST 透過領域專注的專案與產業、學術界和政府機構合作。他們一直專注於許多事項，例如：

- 密碼學發現：識別需要移轉的密碼學以及如何優先處理首先移轉的項目。
- 互通性：確保流行的密碼學特性和協定納入新的 PQC 演算法，並且來自不同供應商的實作能夠互通。
- 密碼敏捷性：專注於開發鼓勵快速適應新密碼學原語和演算法的資訊系統，而無需對系統基礎結構進行重大變更，也稱為密碼敏捷性。

這些專案有助於告知/制定他們建立的指南和標準，並協助確保他們提供的標準和指南有產業解決方案範例。 Dell 自 NCCoE 移轉至 PQC 專案啟動以來一直參與其中。

如今，PQC 不僅僅是一個研究主題；它是一個正在發展的標準，具有具體的演算法、時間表和採用路徑。現在開始準備的組織可以避免最後一刻才匆忙行動的成本、中斷和風險。這種轉換不僅僅是為了合規，而是為了確保在量子運算重塑數位環境時，信任、機密性和完整性保持完整。

為什麼現在就是行動的時候

威脅的即時性

人們或許會傾向將量子運算視為遙遠的風險，認為只要這項技術完全實現後再處理即可。然而現實是，這個問題早已悄悄接近。敏感資訊 (金融交易、醫療記錄、智慧財產或政府通訊) 今天可能已安全加密，但一旦量子機器達到破解 RSA 或 ECC 的門檻，這些資料就可能被追溯曝光。結果是整個歷史通訊和記錄的積壓可能突然面臨風險。

漫長的技術週期

現代 IT 生態系統無法輕易或快速轉換。從歷史上看，單一演算法的替換，例如從 SHA-1 轉換到 SHA-2 或從 DES/3DES 轉換到 AES，需要 10 年以上才能完成。這些演算法深深嵌入作業系統、應用程式、網路裝置和硬體中。要汰換這些演算法，需要在整體環境各處，從資料中心到雲端平台再到邊緣裝置，進行重新設計、驗證、測試和部署。對許多組織而言，這將需要數年時間，遠超過量子運算構成現實世界威脅之前的剩餘時間窗口。這就是為什麼監管機構、標準組織和安全領導者強調立即準備的原因。等到 CRQC 廣泛可用將沒有時間進行有序轉換。

不作為的風險

延遲移轉的後果超出技術曝光範圍：

- 資料安全風險：當量子電腦技術成熟後，病歷、財務紀錄或國防情報等長期儲存的資料可能面臨事後遭破解的風險。
- 軟體真實性和完整性風險：如果使用目前的簽署方法簽署的軟體在量子電腦成熟後仍在使用，軟體真實性和完整性可能會因惡意程式碼而受到損害。
- 營運風險：關鍵基礎設施系統 (如公用事業、運輸網路和緊急服務) 眾所周知難以升級。現在不規劃，日後可能導致營運中斷。
- 監管和合規風險：**CNSA 2.0** 等框架已為合規建立了明確的時間表。不做準備的組織不僅面臨曝光風險，還面臨不符合政府或產業期望的風險。
- 聲譽和財務風險：因未處理的密碼學漏洞而導致的外洩，可能對品牌信任造成持久損害，並伴隨重大財務損失。

主動行動的理由

主動準備不僅僅是防禦性措施，更是加強長期韌性的機會。透過進行密碼學盤點、升級對稱金鑰長度、試行 PQC 就緒解決方案，以及與提供量子抗性產品的供應商合作，組織可以確保信任的持續。早期採用者將更有條件為營運做好未來準備、維持合規性，並向客戶、合作夥伴和監管機構展現領導力。

Dell 的後量子密碼學方法

在 Dell，我們相信技術推動人類進步，而安全是這種進步的基礎。做為一家公司，Dell Technologies 正在確保其產品組合、IT 基礎結構和生命週期支援系統為轉換至量子抗性演算法做好充分準備。為準備轉換而採取的步驟包括：

- 識別產品、服務、IT 基礎結構和支援系統中使用密碼學的特定領域和目的，以制定全面的轉換計畫。
- 增強對後量子密碼學 (PQC) 演算法的內部知識，考慮與密碼敏捷性相關的實作面向和設計原則，以促進順利轉換至 PQC 演算法。
- 評估 PQC 演算法在與 Dell Technologies 多樣化產品組合相關的各種使用案例中的效能、適用性和適合性。

鑑於 PQC 轉換的複雜性，密碼學使用案例的升級可能會分階段納入 Dell Technologies 的產品中。例如，從資料角度來看，轉換優先權會給予可能容易受到「現採後解」攻擊的使用案例，例如傳輸中或靜態資料加密。

在考慮您的技術平台時，密碼學使用案例的轉換可能涉及完整的產品更新/替換或產品升級。 這將取決於相關產品以及密碼學在該產品和周圍系統中的實作位置和方式。

量子抗性產品的發布將是未來 5 年以上的重點，以確保客戶能夠滿足政府和產業協會發布的 PQC 轉換時間表，這些時間表落在 2027 年至 2035 年之間。

客戶應與其 Dell 客戶團隊合作，以取得產品特定細節 (例如發布路線圖和時間表)，以納入其移轉計畫。請持續關注，Dell 將在未來幾個月就 PQC 整合至其產品線和產品，提供更具體的時間表。

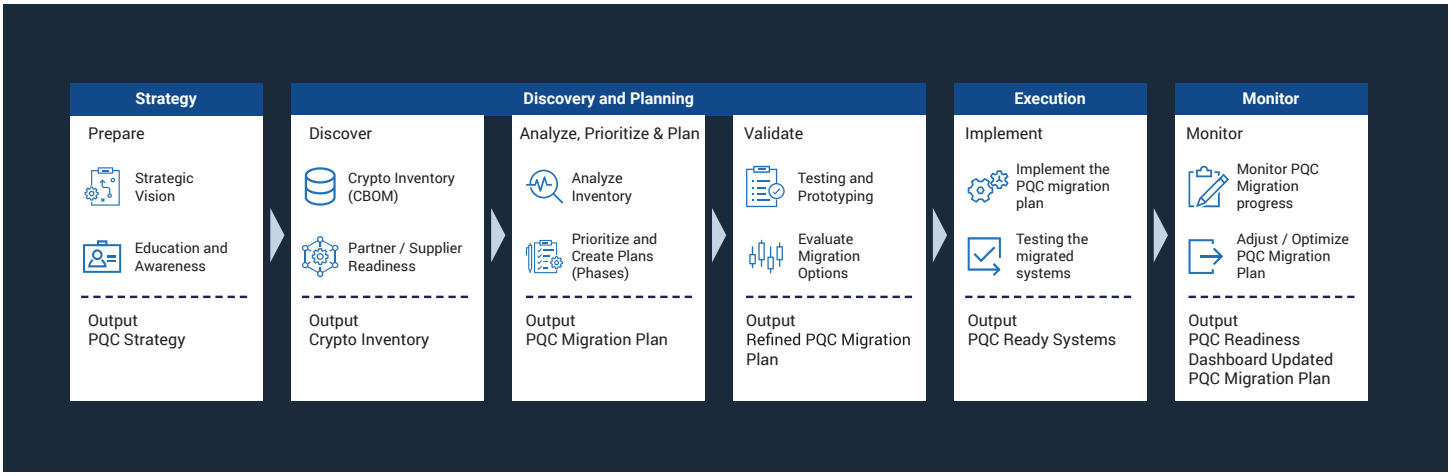
為量子韌性創新做好準備

Dell 的目標不僅是協助客戶符合新興標準，還要讓他們能夠在量子時代安全地創新。無論是部署 AI 工作負載、管理混合雲環境，還是現代化邊緣基礎結構，客戶都可以放心，Dell 解決方案的設計考慮到韌性。安全性不是事後才加上的——我們將其設計到 Dell 產品組合的每一層中，確保組織能夠自信地應對後量子密碼學的轉換。

為轉換做好準備

轉向後量子密碼學，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移轉計畫，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 移轉。



強化現今的安全性狀態

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。同樣重要的是，對於較新的系統，對稱式密碼學應升級至更長的金鑰長度 (AES-256 和 SHA-384 或更高)，以對抗 Grover 演算法帶來的安全邊際縮減。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、程式碼簽署機制和封存資料。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

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

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

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。使用混合量子-傳統實驗室，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

最後，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。

為 PQC 做準備是一場馬拉松，而非短跑。透過採取分階段方法，包括加強現今的防禦、稽核密碼學資產、試行 PQC、採用混合策略以及執行完整移轉，讓組織可以安心邁向量子韌性。有 Dell 作為合作夥伴，這段旅程不僅可以實現，而且是一個加強信任和促進創新的機會，並將持續到未來。

實際應用與效益

轉換採用後量子密碼學不僅僅是一項合規工作；它是一項直接影響信任、韌性和長期競爭力的業務要務。對於電信供應商、金融機構、醫療組織和政府機構而言，採用量子抗性演算法能確保關鍵數位基礎結構面對眼前和未來威脅，都能保持安全。

電信

電信網路是全球數位化的骨幹。這些網路支援從緊急服務和 IoT 連線到安全客戶通訊等全方位功能。該領域的量子破解可能會危及 SIM 卡佈建、eSIM 上線或支撐 4G 和 5G 的身分驗證流程。透過現在部署混合和量子安全密碼學，營運商可以維持客戶信任、保護資料隱私，並確保跨世代行動技術的順暢服務連續性。

金融服務

金融業是網路歹徒最常鎖定的目標之一，交易的完整性取決於密碼學的保護技術。後量子準備保護數位支付、網路銀行和銀行間轉帳免受量子驅動的詐欺。早期採用也向監管機構和客戶保證，機構致力於保護資產和維持系統穩定性。在這個領域為密碼學做好未來準備可降低監管曝光和聲譽風險。

醫療保健

患者記錄、基因組資料和連網醫療裝置都面臨「先竊取，後解密」攻擊的風險。醫療保健領域還面臨多一重挑戰：敏感醫療資料需要長期保留。透過今天開始轉換至 PQC，醫院和醫療機構能確保健康記錄不僅現在保持私密，而且在未來數十年內也保持私密。這對於維護患者信任並滿足不斷演變的資料保護法規至關重要。

政府和關鍵基礎設施

從國防通訊到能源分配系統，政府和基礎設施營運商依賴密碼學來維持營運連續性和國家安全。後量子密碼學不僅能防範近期的進犯，還能防範為未來利用而進行的加密通訊策略性收集。與 CNSA 2.0 等框架保持一致，確保政府系統在量子時代保持互通、安全和可信賴。

更廣泛的業務效益

雖然 PQC 在技術上的必要性很明確，而業務理由同樣有力：

- 信任和品牌聲譽：展現在保護客戶和合作夥伴資料方面的領先。
- 監管合規性：遵循與 NIST 標準和 CNSA 2.0 等政府規範。
- 營運韌性：降低因密碼學破解而導致災難性中斷的風險。
- 競爭差異化：將組織定位為主動創新者而非被動追隨者。

現在採取行動的好處遠超出技術韌性。早期採用 PQC 的組織不僅會降低風險，還會增強其在依賴信任的數位經濟中創新、合規和競爭的能力。

採取下一步行動

量子運算的到來，既是一個新世代的機會，也代表前所未有的安全挑戰。雖然密碼學相關量子電腦的確切時間表仍不確定，但可以確定的是準備工作所需的努力。轉換至後量子密碼學需要多年的協調規劃、投資和執行。等到量子電腦開始運作後再行動並非實際可行的選項。

任何組織的第一步都是意識：了解密碼學在其環境中的使用位置和方式。從那裡開始，企業必須開始進行盤點、優先排序和試行量子安全解決方案的過程。混合密碼學 (結合傳統和後量子演算法) 在標準持續演進的同時，為企業提供了通往韌性的即時路徑。透過將內部路線圖遵循 NIST PQC 標準和 CNSA 2.0 時間表等全球框架，組織可以自信地邁向合規性和互通性。

Dell Technologies 致力於協助客戶應對這項轉換。透過我們的方法，我們提供強大的基礎，具備供應鏈完整性、硬體嵌入式防護措施和軟體驅動的適應性。我們與領先安全供應商的合作關係以及我們在產業標準組織中的積極角色，確保 Dell 解決方案不僅遵循最新要求，而且經過實際效能和互通性測試。

今天就開始準備。從發現和風險分析開始，與值得信賴的供應商合作，並試行量子安全技術。現在採取的每一步都能降低未來中斷的風險。早一步採取行動的組織不僅能保護其資料和系統，還能在數位信心至關重要的時代贏得客戶、監管機構和合作夥伴的信任。

關於我們

Dell Technologies 致力於讓進階技術對每個人而言都是易於取得、值得信賴且具有賦能作用的。我們協助人們和組織安全地利用創新，引領邁向更安全、更包容和更連通的未來。

深入瞭解 Dell [產品名稱] 解決方案

聯絡 Dell Technologies 專家

檢視更多資源

加入與 #HashTag 的對話

DELL Technologies