DELL Technologies

白皮书

# 后量子密码学: 为量子时代做好准备

**Dell Technologies 白皮书**

# 目录

# 执行概述

量子计算正以前所未有的速度从理论研究迈向实际应用。在硬件发展、算法演进和投资加大的推动下，曾被视为遥不可及的量子计算机将加速实现，它能够破解经典计算机无法解决的难题。这将对整个行业产生深远影响。从药物研发到气候建模再到全球物流，量子计算有望解锁以往无法企及的创新。

但这一突破也带来了颠覆性的挑战：量子计算机会破坏数字经济所依赖的密码基础。数十年来，RSA 和椭圆曲线密码 (ECC) 算法等公钥密码一直为数字通信、金融系统、医疗记录和国家安全提供保护。这些方法依赖于经典计算机难以破解的数学问题。但随着密码相关量子计算机 (CRQC) 的问世，这些难题能够被高效破解，导致当今的安全体系失效。

这种威胁并不是理论分析。一些组织已在使用一种名为“先窃取，再解密”(HNDL) 的手段，在当下收集加密数据，待量子计算机成熟后将数据解密。当前看似安全的敏感信息在几年后可能不堪一击。采取行动的时机不是 CRQC 问世之时，而是现在。

本白皮书介绍了量子威胁的紧迫性，探讨了后量子密码学 (PQC) 这一新兴领域，并就组织如何做好准备提供了指导。本文强调了 Dell Technologies 致力于打造量子安全的未来，遵循 NIST 的后量子密码 (PQC) 标准 (FIPS 203、FIPS 204 和 FIPS 205) 以及商业国家安全算法套件 2.0 (CNSA 2.0) 准则，将安全性嵌入我们的供应链、硬件、固件、软件和合作伙伴生态系统。戴尔的目标很明确：确保在不牺牲安全性或信任的情况下，向前推进创新。

# 术语

在本书中，您将遇到许多术语。我们尝试列出了其中一些术语以便于您理解本书。

后量子密码学 — 一种新的密码数学方法，采用新型算法，旨在防范量子计算机攻击。这些算法在经典计算机上运行，可抵御量子攻击和已知的经典密码攻击。

量子弹性 — 量子弹性是指即使面对密码相关量子计算机 (CRQC)，也能保持安全的系统、算法或基础架构。量子弹性系统使用后量子密码学 (PQC) 或其他可承受经典攻击和量子攻击的保护措施，确保数据在将来的机密性、完整性和真实性。量子弹性和量子安全等其他术语也可互换使用。

密码敏捷性 (有时也称为加密敏捷性) 是指组织的系统和应用程序能够快速、无缝地切换密码算法、协议或密钥长度，而无需进行重大重新设计或中断运营。

“先窃取，再解密”(HNDL) 也称为“先存储，再解密”，是攻击方当前收集并存储加密数据，意图在将来密码相关量子计算机 (CRQC) 问世后再解密数据的行为。

# 量子计算和对加密的威胁

## 量子计算的兴起

正如约一年前，首席技术官 John Roese 在我们的博客文章《后量子密码学：构建企业弹性的战略要务》中所述，无论是笔记本电脑、智能手机还是服务器，经典计算机均采用比特来处理信息，而比特始终处于非零即一的状态。这种二进制模型虽然推动了数十年的进步，但也限制了信息的表示和处理方式。量子计算机使用量子比特，量子比特通过叠加和纠缠等原理，可同时处于多个状态。因此，量子计算机可以并行探索大量可能的解决方案，从而为解决特定类别的问题提供计算优势。

量子计算的潜在应用非常广泛。通过以经典计算机无法达到的精度模拟分子相互作用，研究人员预计制药领域将取得突破。气候科学家有望获得更准确的全球系统模型，能源部门能够发现优化电网与储能的潜力。物流和制造也会受益于量子优化技术。这些优势切实存在且触手可及，但风险同样存在。

## 为什么加密面临风险

在数字时代，加密是信任的基础。当您输入信用卡号、登录安全网站或收到签名软件更新时，密码可确保机密性、真实性和完整性。这一保护主要依赖于公钥密码，如 RSA 和 ECC 等算法，这些算法基于经典计算机难以破解的数学难题。

量子计算将改变这一局面。使用**肖尔算法**，一台足够强大的量子计算机可以破解 RSA 和 ECC 所依赖的因数分解与离散对数难题。CRQC 问世后，保护软件更新的数字签名、建立 TLS 会话的密钥以及对设备进行身份验证的证书都可能会受到破坏。这一影响是系统性的，会对确保数字交易安全的机制造成威胁。

对称密码 (AES 等用于保护存储数据或安全通信的算法) 面临着一种虽不严重但不同寻常的挑战。**格罗弗算法**能够让量子计算机削弱对称密钥的有效强度，从而将其安全性有效减半。虽然采用 AES-256 等更大的密钥可以缓解这一问题，但这一调整正凸显了量子威胁无孔不入

## 紧迫性和后果

后果远远超出理论风险。未能做好准备的组织将面临敏感知识产权泄露、金融系统瘫痪、医疗数据泄露以及国家安全威胁等风险。“先窃取，再解密”的手段加剧了紧迫性：攻击者现在只需获取加密数据，等待解密方法。到 CRQC 问世时，损失已无法挽回。

# 后量子密码学和新兴标准

## 定义后量子密码学

后量子密码学 (PQC) 是旨在保护数字系统免受经典攻击和量子攻击的新一代算法。与需要专用硬件的量子密钥分发不同，PQC 专为在当今经典基础架构 (服务器、端点、网络) 上运行而设计，高度实用且可扩展，帮助组织为量子时代做好准备。

PQC 的基础是一系列数学难题，据目前所知，这些难题能够抵御肖尔算法与格罗弗算法等量子技术的攻击。基于网格的密码、基于哈希的签名、基于代码的方案和多元方程是极具前景的方法。这些方法正在经过严格测试和标准化，确保提供与 RSA 和 ECC 相同的可靠性与互操作性。

## 全球标准化工作 — 新兴行业标准

意识到威胁的紧迫性，各国政府和标准机构已将 PQC 列为全球优先事项。美国国家标准与技术研究院 (NIST) 于 2016 年启动了 PQC 项目，号召密码研究社区提出、分析并完善候选算法。经过多年测试，NIST 于 2024 年 8 月公布了第一组标准化算法：

- **用于公钥加密和密钥建立的 CRYSTALS-**Kyber
- **用于数字签名的 CRYSTALS-**Dilithium 和 SPHINCS+ 算法

其他算法仍在审核之中，以便为满足不同的实施需求提供多样性和灵活性，包括嵌入式固件等轻量级系统。这种不断演变的标准化流程可确保世界各地的组织都有明确的途径来采用抗量子解决方案。

## NIST 标准 — FIPS 203、204、205

2024 年 8 月，美国国家标准与技术研究院 (NIST) 最终确定了第一批 PQC 算法：

- FIPS 203 (ML-KEM) — 基于 CRYSTALS-Kyber 密钥封装机制。提供 IND-CCA2 安全性，这意味着即使在自适应选择密文攻击下，密文仍能保持不可区分性。
- FIPS 204 (ML-DSA) — 基于 Crystals-Dilithium 数字签名算法。提供强 EUF-CMA 安全性 (选择消息攻击下的存在不可伪造性)，这是数字签名的标准要求。
- FIPS 205 (SLH-DSA) — 基于 SPHINCS+，这是一种基于哈希的签名方案。它是不依赖于网格问题的保守型备用方案。

## 强制路线图

在意识到采用抗量子加密算法的重要性后，美国联邦政府已开始向各联邦机构发出 PQC 要求。这些要求包括第 10 号国家安全备忘录 (NSM-10)、商业国家安全算法套件 (CNSA 2.0)、美国国家标准与技术研究院 (NIST) 机构间报告 (IR) 8547、行政管理和预算局备忘录 23-02 (OMB M-2302) 等。

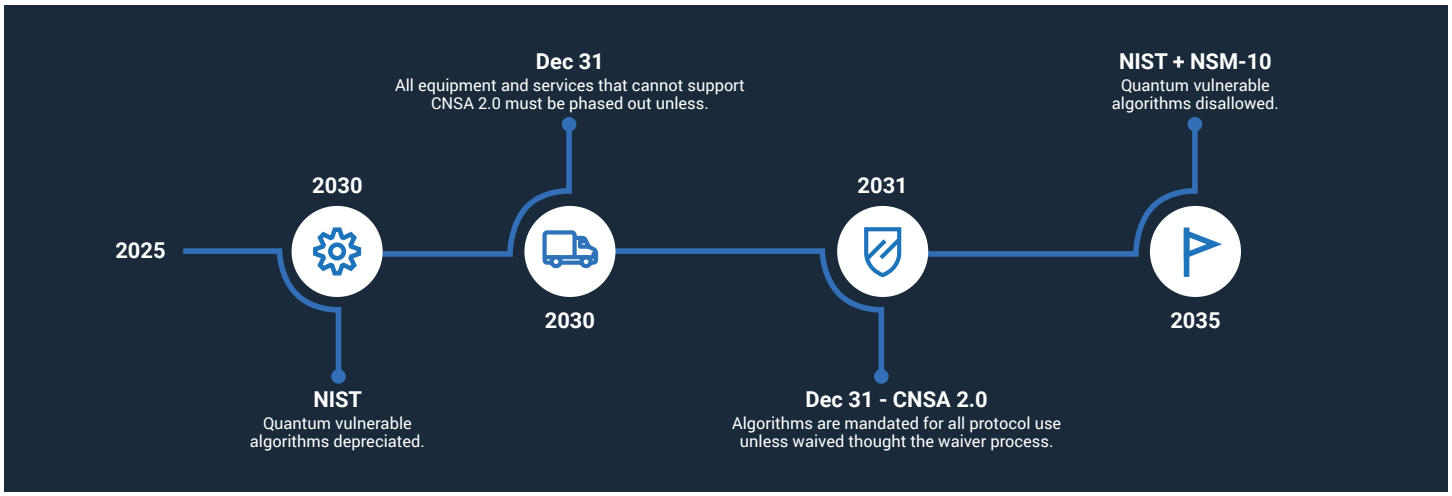
**National Security Memorandum 10 (NSM)**
Provides a roadmap to create crypto inventories, adopt crypto agility methodogies.

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

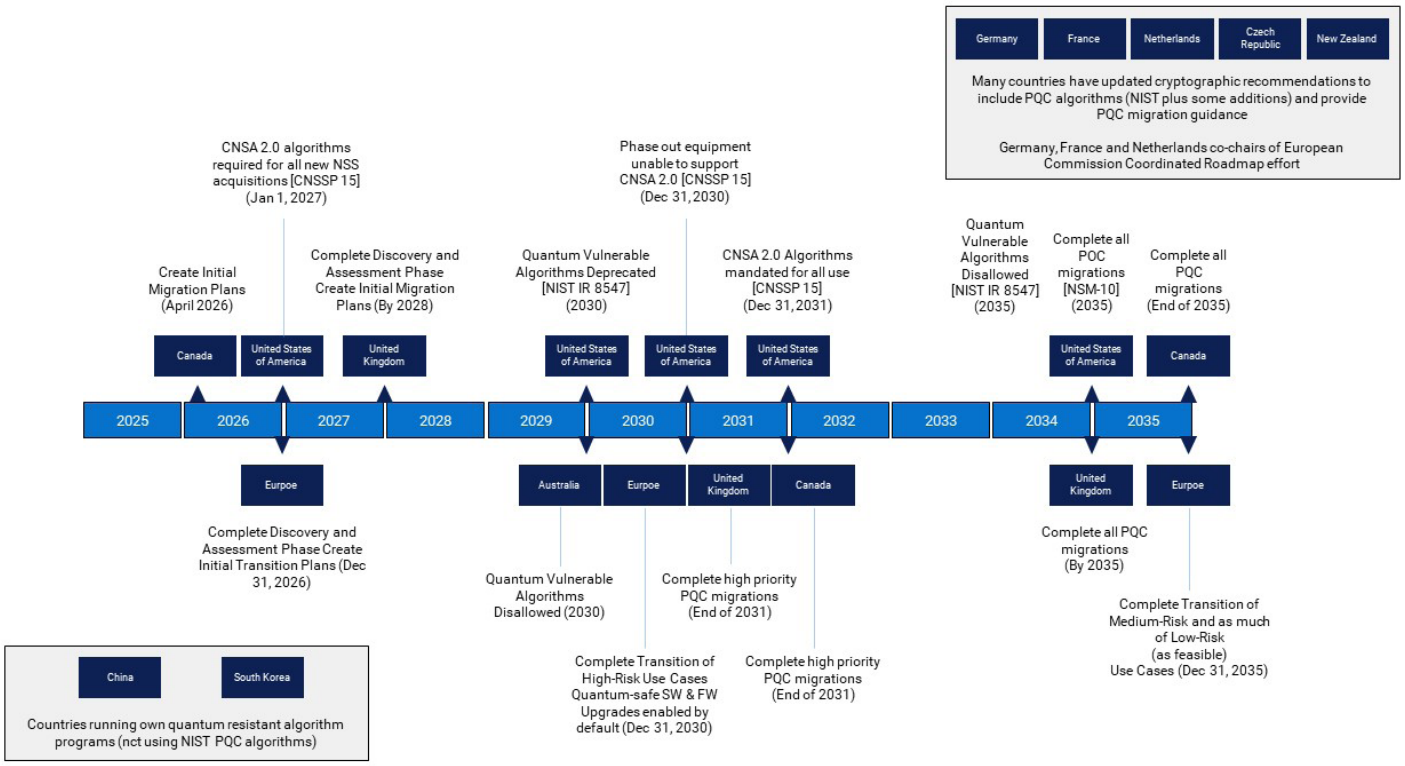
**NIST IR 8547**
Provides guidance on transition, outlining NIST'S expected approach to PQC digital signatures and key-establishment schemes

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

NSA 于 2022 年 9 月发布的 CNSA 2.0 引入了对于后量子密码算法的第一条建议。CNSA 2.0 为国家安全系统 (NSS) 采用抗量子算法设定了明确期限，同时也为准备自身过渡的企业提供有效指引：




全球其他组织也为 PQC 过渡制定了指导原则。 以下是一些不同国家/地区的要求。




这些日期不是随意选择的，它们反映了在复杂 IT 生态系统中重新设计、验证和部署密码所需的准备周期。企业不应将这些要求仅视为政府指令；它们是全球迈向量子弹性的实际指标。

## 行业合作

除 NIST 和 NSA 之外，戴尔还积极影响并参与那些推动互操作性与实际采用的行业联盟和标准组织。可信计算组织将 PQC 集成到可信平台模块 (TPM) 标准中。IETF 将 PQC 算法大量集成到行业协议，如 TLS、X.509 证书。OASIS 密钥管理互操作性协议 (KMIP) 委员会在密钥管理框架中启用 PQC。FIDO 联盟研究 PQC 对身份验证和设备接入标准的影响，而 SAFECode 等组织在努力向行业提供迁移准备方面的培训。

NIST 美国国家网络安全卓越中心 (NCCoE) 旨在通过聚焦特定领域的项目，促进 NIST 与工业界、学术界及政府机构间的协同合作。他们一直专注于多个方面，例如：

- 密码发现 — 确定需要迁移的加密算法以及迁移的优先顺序。
- 互操作性 — 确保常用密码功能和协议采用新的 PQC 算法，并确保来自不同供应商的实施可互操作。
- 加密敏捷性 — 专注于开发可快速适应新的密码原语和算法，而无需对系统基础架构进行重大更改的信息系统，这也称为密码敏捷性

这些项目有助于告知/推行他们制定的指导原则和标准，并确保针对他们提供的标准和指导原则具有示例行业解决方案。从 NCCoE 迁移到 PQC 项目开始之时，戴尔就参与其中。

现如今，PQC 不仅仅是一项研究主题，而是有着具体算法、期限和采用途径且不断发展的标准。立即着手准备的组织可以避免投入、中断和临阵仓促应对的风险。这一过渡不仅仅为了合规性，而是确保在量子计算重塑数字格局时，信任、机密性和完整性能够保持不变。

# 为什么应立即采取行动

## 威胁的迫近性

人们会想当然地认为量子计算是一种遥远的风险，在技术完全成熟之时即可解决这一问题。事实上，倒计时已经开始。敏感信息（金融交易、医疗记录、知识产权或政府通信）在当下可能安全加密，但一旦量子计算机能够破解 RSA 或 ECC，数据就会追溯性地泄露。因此，长期积存的历史通信与记录将瞬间暴露于风险之中。

## 长技术周期

现代 IT 生态系统的转型并非易事，更无法快速达成。从历史上看，单个算法的替换，例如从 SHA-1 过渡到 SHA-2 或从 DES/3DES 过渡到 AES，需要 10 年以上时间才能完成。这些算法深度嵌入到操作系统、应用程序、网络设备和硬件之中。要更换这些算法，需要跨各种环境，包括从数据中心到云平台再到边缘设备，进行重新设计、验证、测试和部署。对于许多组织而言，这需要耗费数年时间，远远超过了量子计算带来真正威胁的剩余窗口期。因此，监管机构、标准机构和安全领导者纷纷强调应立即着手准备。等到 CRQC 普及之时，就没有时间进行有序过渡。

## 不作为的风险

延迟迁移的后果不仅限于技术风险：

- 数据安全风险：一旦量子计算机成熟，病历、财务记录或国防信息等长期保留数据可能会发生追溯性地泄露。
- 软件真实性和完整性风险：如果使用当前签名方法签名，并且在量子计算机成熟后仍使用该方法，则恶意代码可能会危及软件真实性和完整性。
- 运营风险：公用事业、交通网络和紧急服务等关键基础设施系统被公认为难以升级。如果现在不进行规划，日后可能会发生运营中断。
- 监管与合规风险：**CNSA 2.0** 等框架已建立明确的合规时间表。未能做好准备的组织不仅面临风险，还可能无法满足政府或行业预期。
- 信誉和财务风险：由于未解决的密码漏洞而导致的泄露可能会对品牌信任造成持久损害，并导致重大财务损失。

## 主动行动的必要性

主动准备不仅仅是一种防御行动，而是加强长期弹性的机会。通过进行密码清点、升级对称密钥长度、试用 PQC 就绪解决方案以及与提供抗量子产品的供应商合作，组织可以确保持续可信。早期采用者能够更好地实现未来无忧的运营，保持合规性，并向客户、合作伙伴和监管机构展示领导力。

## 戴尔的后量子密码学方法

在戴尔，我们相信技术推动人类进步，而安全是这一进步的基础。作为一家公司，Dell Technologies 确保其产品组合、IT 基础设施和生命周期支持系统为过渡到抗量子算法做好准备。为过渡做好准备所采取的步骤包括：

- 确定在产品、服务、IT 基础架构和支持系统中采用密码的特定方面和用途，以制定全面的过渡计划。
- 提升对于后量子密码学 (PQC) 算法的内部了解，考虑与加密敏捷性相关的实施方面和设计原则，以便顺利过渡到 PQC 算法。
- 评估 PQC 算法在与 Dell Technologies 多样化产品组合相关的各种应用场景中的性能、适用性和适配性。

由于 PQC 过渡的复杂性，密码应用场景的升级可能会分阶段融入到 Dell Technologies 的产品中。例如，从数据角度来看，易受“先窃取，再解密”攻击的应用场景 (如传输中数据或静态加密) 会优先过渡。

在考虑技术平台时，密码应用场景的过渡可能涉及完整产品更新/更换或产品升级。 这取决于相关产品，以及在该产品和周围系统中实施密码的位置与方式。

推出抗量子产品将成为未来 5 年以上的工作重心，确保客户能够符合政府与行业协会制定的 2027-2035 年 PQC 过渡时间表。

客户应与其戴尔客户团队合作，获取产品特定详细信息 (如发布路线图和时间表) ，以将其纳入迁移计划。戴尔将在接下来的几个月内，提供 PQC 集成到各产品线和产品的具体时间表，敬请关注。

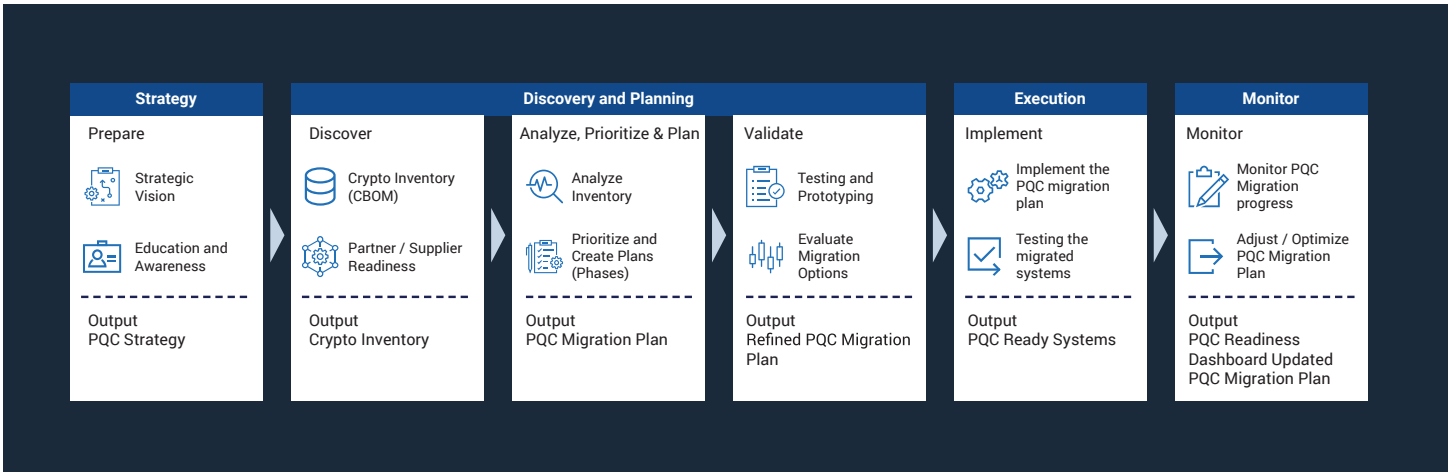
## 为量子弹性创新做好准备

戴尔的目标不仅是帮助客户遵守新兴标准，而是支持他们在量子时代安全创新。无论是部署 AI 工作负载、管理混合云环境还是实现边缘基础架构现代化，客户都可以放心实施，因为戴尔解决方案在设计时充分考虑了弹性。安全性并非事后打补丁，它已融入戴尔产品组合的每一层，确保组织能够充满信心地过渡到后量子密码学。

## 为过渡做好准备

过渡到后量子密码学将是几十年中最重要的基础设施变革之一。从服务器和存储到端点、云平台和网络协议，这一过渡几乎涉及 IT 的方方面面。要取得成功，需要远见、规划和严格执行。在 Dell Technologies，我们将前进道路视为分阶段的旅程：既确保当下的安全改进，又为 PQC 采用做好长期准备，从中取得平衡。

戴尔随时准备帮助您制定 PQC 实施战略。我们建议采用分阶段迁移计划，并列出了一系列活动来帮助您制定战略、规划、执行和监控 PQC 迁移。



# 应对当今安全态势

## *良好的安全卫生*

为量子未来做好准备的第一步是加强现有防御措施。机构应采用强健的安全卫生最佳实践，如执行最小权限访问、实施多因素身份验证以及保持严格的补丁管理。还有另外两项考虑因素。禁用较弱的密码非常重要，以便具有更高强度密码的新系统可以与传统系统互操作。对于新系统，将对称密码升级到更长的密钥长度 (AES-256 和 SHA-384 或更高) 也很重要，这可以应对格罗弗算法带来的安全余量减少。这些措施不仅能够降低当前风险，还可以充分减少密码债务积压，避免将来迁移的复杂化。

## *清点和审核密码资产*

可见性是一切迁移计划的基石。组织必须进行全面的密码清点，确定公钥密码在应用程序、设备和工作流中的使用位置及方式。这包括 TLS 证书、VPN、电子邮件系统、代码签名机制和归档数据。确定资产后，应根据业务关键性、敏感度和生命周期来确定资产优先级。长期保留数据 (如医疗记录或机密档案) 应被视为具有最高紧迫性，因为此类数据最易受到“先窃取，再解密”攻击的威胁。

## *PQC 试用和实验*

了解密码环境后，组织应开始在受控环境中测试 PQC 解决方案。通过在实验室中试用这些解决方案，IT 团队可以在大规模部署之前验证性能、互操作性和可管理性。建立这种加密敏捷性 (无需改造整个系统即可切换密码算法) 对于长期弹性和轻松迁移至关重要。

## *采用互操作性方法*

随着标准的成熟，混合模式将提供通往未来的桥梁。许多供应商已支持混合密码套件，将经典算法与抗量子算法结合到单一实施中。这种双重方法可提供持续保护，即使一种算法在日后受到破坏也能确保安全。企业应立即开始采用混合战略，同时根据基础架构供应商的产品路线图和里程碑调整内部时间表。这可确保在量子安全算法实现标准化时，组织可以在不中断的情况下扩展采用规模。

## *执行完整迁移和持续验证*

最终目标是在整个企业内完全过渡到 PQC。这不是一次性事件，而是一个持续的验证和适应过程。组织应执行详细的迁移计划，将 PQC 融入到 IT 堆栈的每一层，同时持续测试新标准和实施。使用混合量子经典实验室，客户可以模拟攻击场景、验证密码完整性，并确保其系统对于不断变化的威胁保持弹性。

## *协作和知识共享*

最后，没有一个组织应独自面对这一挑战。行业联盟、学术研究人员和政府机构正在汇集相关知识，以加快 PQC 过渡。参与标准小组、工作组和试点计划能够让企业始终遵循最佳实践和新兴要求。戴尔积极参与 NIST NCCoE PQC 项目等计划，确保客户能够直接从这些集体专业知识中获益。

为 PQC 做好准备是一场持久战，而不是突击。通过采取分阶段方法，包括强化当下防御措施、审核密码资产、试用 PQC、采用混合战略和执行全面迁移，组织可以自信地实现量子弹性。与戴尔合作，这一旅程不仅可以实现，更将成为加强信任、推动未来创新的重要契机。

# 实际应用和优势

过渡到后量子密码学不仅仅是合规性练习，而是直接关乎信任、弹性和长期竞争力的企业当务之急。对于电信提供商、金融机构、医疗保健组织和政府机构，采用抗量子算法可确保关键数字基础架构持续防范当前和未来的威胁。

## 电信

电信网络是全球数字化的支柱。从应急服务和物联网连接到安全的客户通信，电信网络提供方方面面的支持。电信领域的量子攻击可能会危及 SIM 卡配置、eSIM 激活，以及支持 4G 和 5G 网络的身份验证流程。通过立即部署混合和量子安全密码，运营商可以保持客户信任、保护数据隐私，并确保跨几代移动技术的无缝服务连续性。

### *金融服务*

金融行业是网络攻击者最主要的目标之一，交易完整性取决于密码。后量子就绪性可保护数字支付、网上银行和银行间转账，防范量子欺诈。早期采用还可让监管机构和客户安心无忧，表明机构致力于保护资产并维护系统稳定性。在该领域采用未来无忧的密码可以降低监管风险和声誉风险。

### *医疗*

患者记录、基因组数据和互联医疗设备都面临“先窃取，再解密”攻击的风险。医疗行业面临额外一项挑战：敏感医疗数据需要保留较长时间。通过即刻开始向 PQC 过渡，医院和医疗服务提供商可确保病历不仅在当下保持私密，在未来几十年都能安全无虞。这对于保持患者信任，同时符合不断演变的数据保护法规至关重要。

### *政府和关键基础设施*

从国防通信到能源分配系统，政府和基础设施运营商都依靠密码来确保持续运营和国家安全。后量子密码学不仅可防范近期攻击者，还可抵御对加密通信进行的战略性收集，防止通信数据在将来遭到利用。遵循 CNSA 2.0 等框架，可确保政府系统在量子时代保持互操作性、安全性和可信度。

## 更广泛的业务优势

尽管 PQC 的技术必要性显而易见，但业务理由同样重要：

- 信任和品牌声誉：在保护客户和合作伙伴数据方面表现出领导力。
- 监管合规：符合 NIST 标准和政府指令 (如 CNSA 2.0) 。
- 运营弹性：降低因密码被破解而导致的灾难性中断风险。
- 竞争优势：推动组织成为主动创新者，而不是被动追随者。

立即采取行动的优势远不止于提升技术弹性。早期采用 PQC 的组织不仅可以降低风险，还能增强自己在依赖信任的数字经济中进行创新、合规和竞争的能力。

## 后续行动

量子计算的到来既是一个代际机遇，也是前所未有的安全挑战。尽管有关密码相关量子计算机的确切时间表尚不确定，但毋庸置疑的是，相关准备工作需要付出巨大努力。过渡到后量子密码学需要耗费多年时间进行协调规划、投资和执行。等到量子计算机投入使用之时再采取行动不是可行之策。

对于任何组织而言，首先要做的是认知：了解在其环境中在何处以及如何使用密码。在此基础上，企业必须开始清点、确定优先级和试用量子安全解决方案这一流程。混合密码结合了经典算法和后量子算法，可在标准不断演变的情况下，提供即刻实现弹性的途径。根据全球框架（如 NIST 的 PQC 标准和 CNSA 2.0 时间表）制定内部路线图，组织可以信心十足地朝着合规性和互操作性迈进。

Dell Technologies 致力于帮助客户顺利完成这一过渡。通过我们的方法，我们可以建立供应链完整性、硬件嵌入式安全性和软件支持适应性的坚实基础。我们与领先安全提供商密切合作，并在行业标准机构中积极发挥作用，确保戴尔解决方案不仅符合全新要求，还能通过实际性能与互操作性的检验。

立即着手准备。从发现和风险分析开始，与值得信赖的供应商接洽，并试用量子安全技术。当下采取的每一步都能降低将来的中断风险。在数字信心至关重要的时代，及早行动的组织不仅能保护其数据和系统，还能赢得客户、监管机构和合作伙伴的信任。

## 关于我们

Dell Technologies 致力于为每个人提供可获得、可信赖、可赋能的先进技术。我们帮助人们和组织安全利用创新，引领人们走向更加安全、包容和互联的未来。

详细了解戴尔 [产品名称] 解决方案

联系 Dell Technologies 专家

查看更多资源

加入 #HashTag 对话



DELL Technologies