DELL Technologies

后量子密码学

立即开始

简介

量子计算正在推动技术领域的彻底革新，既带来了非凡机遇，也催生了全新挑战。量子计算的前景虽然令人振奋，却对我们保护数字世界的密码体系构成了重大威胁。

量子计算兴起的原因何在？

无论是笔记本电脑、智能手机还是服务器，这些经典计算设备都是以“比特”为信息处理单元，其状态只能是“0”或“1”。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。

什么是后量子密码学？

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。

组织在量子计算中面临哪些直接风险?

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”的威胁加剧了紧迫性：攻击者只需在当前截取加密数据，然后等待未来出现解密方法即可。等到具备加密数据破解能力的量子计算机问世，造成的损害将难以挽回。

“先窃取，再解密”也称为“先记录，后解密”，是指攻击方在当前收集并存储加密数据，意图等到未来量子计算机具备加密数据破解能力时，再对这些数据进行解密的行为。

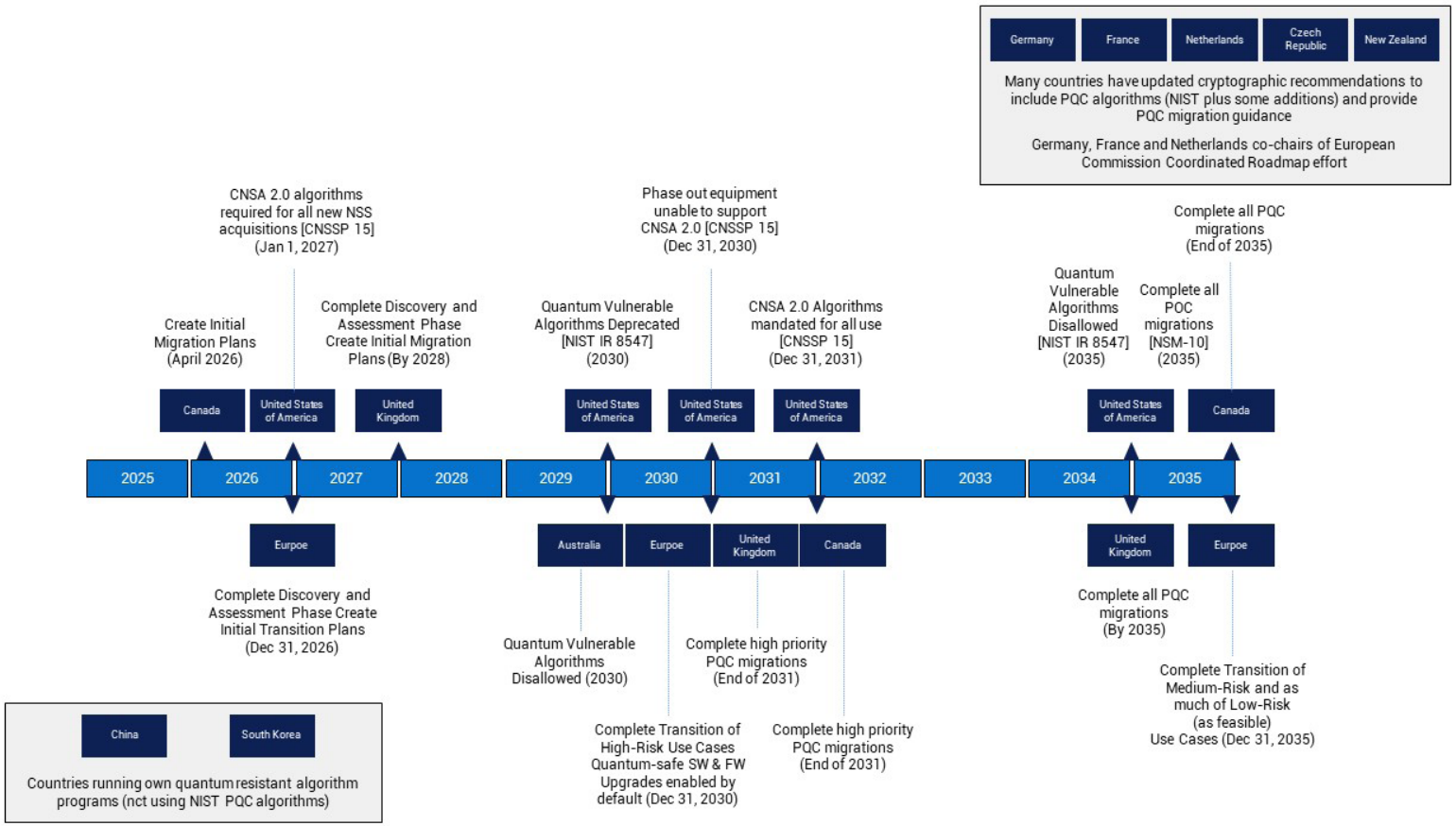
组织应如何为过渡到 PQC 做好准备?

通往量子安全未来的旅程是一场马拉松，而非短跑冲刺，更是一段持续演进的旅程。采用前瞻性、分层分阶段的策略，将助力您的组织管控风险、优化资源配置，并为构建具备长期弹性的安全态势奠定基础。戴尔为您提供技术和指导，支持您应对各个阶段的挑战。以下是指导您的组织制定 PQC 过渡计划的关键步骤。

PQC 过渡时间表

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。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布 PQC 相关要求。相关文件包括：《第 10 号国家安全备忘录》(NSM-10)、《美国商业国家安全算法套件 2.0》(CNSA 2.0)、《美国白宫管理与预算办公室备忘录 23-02》(OMB M-2302) 以及《美国国家标准与技术研究所跨机构报告 8547》(NIST IR 8547) 等。

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



清点与核查加密威胁

您的首要任务是了解当前的加密环境。此基础步骤将为整体迁移战略提供关键依据。

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。对于较新的系统而言，提升最低安全强度标准同样至关重要（比如对称加密采用 AES-256，摘要算法采用 SHA-384 或更高强度），这有利于应对格罗弗算法带来的安全余量降低威胁。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。

清点与核查加密资产

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、客户数据、归档数据等。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。对于长期保留的数据（如医疗记录或机密档案），应给予最高优先级，因为它们最容易受到“先窃取，再解密”攻击的威胁。

PQC 试用与实验

有了清晰的资源清册，您便可开始动手实施支持 PQC 的技术，以验证其性能与集成效果。

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。

采取具有互操作性的方法

PQC 标准成熟后，您便可着手规划生产环境部署。
通过采用混合模式，您可稳步过渡至完整的量子安全环境。

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

最终目标是打造全面集成且持续验证的量子安全型企业。

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。借助融合了经典计算机与量子计算机的混合架构，用户可以模拟攻击场景、验证加密机制完整性，并确保其系统在面对不断演变的威胁时仍能保持弹性。

协作与知识共享

面对这一挑战，任何组织都不应孤军奋战。

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。

总结

量子时代已经不再是遥不可及的未来，而是迫近的现实，需要我们即刻采取前瞻性的行动。为应对这一技术变革做好准备，是保护您宝贵数据资产的战略要务。正如我们所概述的，采取从清点与核查、再到完整迁移的分阶段推进方式，是通往量子安全未来的一条极为清晰的推进路径。

向 PQC 体系进行迁移，将成为未来数十年来最重大的基础架构变革之一。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的迁移计划，并已规划一系列行动方案，以帮助您制定 PQC 过渡战略并对这一过程进行方案规划、落地执行和持续监控。