Solution Brief

后量子时代准备始于加密敏捷性

cpl.thalesgroup.com

THALES
Building a future we can all trust

为量子做好准备

量子计算机即将破解传统加密技术，因此您需要立即采取措施保护数据。现在收集，以后解密 (HNDL) 攻击已经发生，网络攻击者收集并存储加密数据，目的是将来使用量子计算机解密。

为后量子密码学 (PQC) 做好准备，为您的企业创建一个可信的环境，以测试 PQC 加密技术，并确定量子计算可能对您的基础设施安全产生的潜在影响，并制定快速调整计划。

2024年，NIST已经发布并标准化了后量子密码 (PQC) 算法，供组织机构采用，以防范量子计算攻击。随后，世界各地的管理机构将根据 NIST PQC 标准化流程发布合规要求。这些要求将触发合规指令的发布，组织机构将争先恐后地实施。

使用内置加密敏捷架构的 PQC 网络加密解决方案来保护传输中的数据

为什么现在要采用 PQC?

将当前的加密方法转换为 PQC 需要花费大量时间，最佳策略是现在就做好准备。通过抢占先机，您可以最大限度地减少对组织和客户的干扰，降低成本和风险，并确保转型期间的业务连续性。这还将使您的组织能够在 NIST 和其他行业 PQC 法规发布后立即完全遵守这些法规。如今，HNDL 已经引发了量子攻击，明智的做法是现在就开始使用临时解决方案，例如使用更长的对称密钥长度或带外密钥。这不仅可以保护您的组织免受 HNDL 的侵害，而且在后量子加密可用时，您可以更好地准备实施后量子加密。

使用 PQC 入门套件迈出第一步

带有 Thales High Speed Encryptors (HSE) 的 PQC 入门套件是一种低成本解决方案，可帮助组织创建测试环境，以加速在安全环境中测试量子弹性措施的过程。在此 PQC 实验室中，您可以使用后量子密码学和熵模拟运行应用程序、传输数据等，帮助您验证架构。通过今天的准备，您将制定行动计划，以确保当算法在固件中最终确定时，操作将继续顺利运行。

使用以下工具轻松设置您的量子安全测试环境：

✓ **预先实现 NIST 后量子算法**

✓ **带外密钥管理，采用 NIST 批准的密钥派生函数（KDF）方法**

✓ **可选的量子密钥分发，通过 ETSI eQKD v14.01 实现**

✓ **可选的量子随机数生成器（QRNG）或外部熵源（BYOE——自带加密）**

HSE PQC 入门套件包含的内容

入门套件由功能齐全的 HSE 组成，可以投入生产环境，为现有网络提供额外的安全性和改进的性能。

- **从 Thales HSE 产品组合中选择的 3 台 HSE 网络加密设备**
  - **CN4010/CN4020：** 高达 1 Gbps 的网络加密器，经过认证，性能高，外形小巧，非常适合 CNI、SCADA、语音/视频等远程位置
  - **CN6010:** 1Gbps 和 10 Gbps 网络加密器，机架式，完全冗余的坚固设计，非常适合私有网络和数据中心
  - **CN6140:** 高达 4x10 Gbps 网络加密器，4 个独立加密通道，支持高可扩展性和多链路网络
- **CM7 网络管理器 – 加密管理平台（可从客户服务门户下载）**
- **建议添加**
  - 电源线（CN6000 系列型号）
  - 转发器（专用于 CN6000 和 CN4020 单元）
  - 维护和支持
  - 远程安装和配置

扫描二维码申请 HSE PQC 入门套件