EnQuanta®

A Quantum+AI Resilient Cryptography Company

Crafting a New Era of Quantum Cyber Resilience Solutions
for Today's and Tomorrow's Cyber Threats

EnQuanta is crafting the next-gen solutions to protect critical data from current and future Quantum+AI threats through a **Dynamic-Hybrid Crypto-Agile Framework** that incorporates and improves upon NIST Post-Quantum Cryptography (PQC) standards.

Our **QuantaCrypt™** software solutions **seamlessly integrate** with existing Enterprise, Cloud, Operational, and Edge environments, as well as Key Management systems—supporting future NIST cryptography updates without the need for code refactoring.

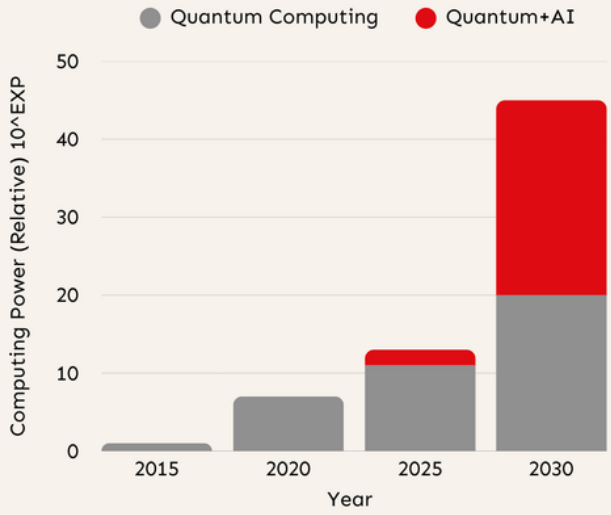
The clear choice for implementing PQC is our **QuantaCrypt** suite of products that deliver **PQC compliance** and **assumption-free cryptography** purpose-built to remain resilient against unbounded Quantum + AI threats while eliminating costly multi-year integration projects driven by future three-to-five-year PQC standard cycle changes.

EnQuanta's state-of-the-art **threat protection** technology is backed by a team of industry leading cryptographers providing assumption-free protection for your most sensitive data.

An Existential Risk to Data

The Power of Quantum Computing + Artificial Intelligence

End-of-life For Your Current Data Protection Policy and Standards



Quantum-Accelerated AI and AI-Enhanced Quantum Computing (**Quantum+AI**) presents an entirely new cyber threat landscape.

"The debate is over. Quantum computing is real and here now," Dr Rajeeb Hazra, CEO of Quantinuum.

Recent advancements, like Google's Willow chip achieving a 13,000x speed advantage with the Quantum Echoes algorithm, demonstrate the practical emergence of this "verifiable quantum advantage" for real-world applications like breaking classic cryptography

Quantum computers are already in use by nation-states, large tech companies, and research institutions. **The development of a Cryptographically Relevant Quantum Computer (CRQC) is likely to occur quickly and without warning, rendering today's data protection obsolete virtually overnight.** Timing is critical in addressing the near Quantum + AI cryptographic risk because quantum computers and AI will become exceptional at breaking legacy and even PQC cryptography.

In response, the U.S. Government has recognized the need to prepare for future unknown vulnerabilities posed by CRQC and AI. In January of 2025 the U.S. moved up the deadline for federal informations systems to be PQC compliant from 2035 to 2030. EU NIS2 legislated PQC standards adoption in 2024.

The New Cybersecurity Threat Landscape

Unprecedented Challenge for Enterprises, Critical Infrastructure and Government

Quantum Computing ✖ **AI** ✖ **Cryptographic Debt**

The capabilities of Quantum Computing combined with Artificial Intelligence in addition to existing cryptographic debt are amplifying existing threats such as Harvest Now, Decrypt Later.

sales@enquanta.com **(612) 423-9015** enquanta.com

The Solution to Quantum+AI Risk is QuantaCrypt

QuantaCrypt Dynamic-Hybrid Crypto-Agile Framework

Data Protection for the Post Quantum + AI Age

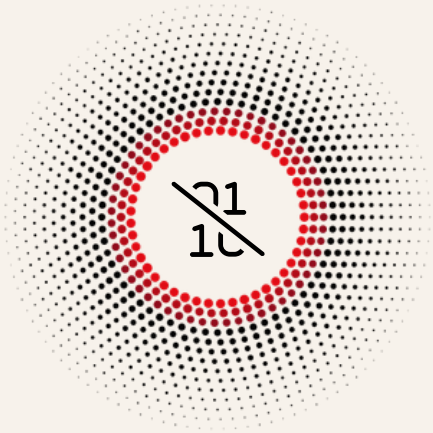
The QuantaCrypt suite of products is based on the auto-hybrid crypto-agile framework providing **assumption-free cryptography**, protecting data-at-rest and in-transit against unbounded Quantum+AI threats.

This framework utilizes a unique set of cryptographic techniques we call "**incryption**" - where dynamic stacks of NIST standard and patented ciphers change with each data package and are highly configurable based on network and software requirements.

This "incryption" method ensures both forward and backward compatibility by leveraging NIST standard ciphers with proprietary, unpublished algorithms that, when randomly combined, achieves a googol (10^{100}, or 1 followed by 100 zeros) times more protection than standard AES-256 encryption.

Multi-layered Protection

EnQuanta utilizes a multi-layered framework using stacks of standard and proprietary ciphers and keys that change with each package. **Even if one layer is compromised, the data remains secure behind others.**

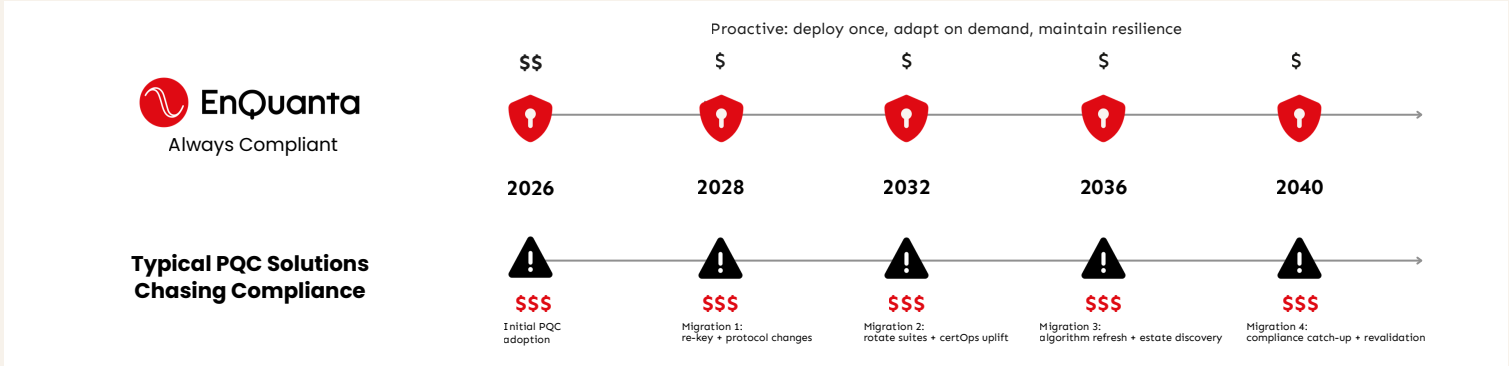


Our Crypto-Agility Stays Ahead of Current Standards

The QuantaCrypt suite of products are agile by design, built on EnQuanta's dynamic-hybrid crypto-agile software framework. Implementing the QuantaCrypt suite of products not only provides post Quantum+AI data protection, it transforms the enterprise security architecture into a dynamic, configurable data protection solution designed to be resilient against unbounded Quantum+AI threats.

QuantaCrypt vs Standard PQC Implementation Decision

EnQuanta's Configurable Software Cryptography Reduces Total Cost of Ownership



sales@enquanta.com (612) 423-9015 enquanta.com

EnQuanta

QuantaCrypt Solutions

Comprehensive Quantum+AI Resilient Data Protection

QuantaCrypt SDK

Easy-To-Use Development Tools
Simple to use APIs, services, communication libraries, and documentation to enable quantum resilient data protection.

QuantaCrypt Storage

Quantum Resilient Data Storage
RAID-10 Network storage solution delivering fault tolerant , and anti-ransomware security to mission critical data.

QuantaCrypt Vault

Firmware/Software Protection
Quantum harden digital assets that contain intellectual property, and data sets from tampering and reverse engineering.

Achieve assumption-free Post Quantum + AI data protection with no hardware replacement.

QuantaCrypt SDK

Powerful Developer Solutions for Ideal Quantum Hardening of Applications

Integrate **state-of-the-art assumption-free cryptography** into custom and commercial applications utilizing simple to use APIs, services, and communication libraries providing Post Quantum+AI protection for large data sets, real time communication, and safe data transfer over unsecure channels.

QuantaCrypt Storage

Data Storage Solution for Ransomware and HNDL Protection

Defend mission critical data with RAID-10 Network storage solution delivering fault tolerant, and anti-ransomware protection. Compatible with heterogeneous network environments such as bare metal, virtualized, edge, and cloud infrastructure. Supports simple APIs to Distribute, Retrieve, and Purge data.

QuantaCrypt Vault

Anti-Tamper Solution for Firmware and Non-Volatile Memory (NVM) Applications

Seamlessly **quantum harden intellectual property and sensitive data** from tampering and reverse engineering. Designed for SW/HS engineers deploying firmware and data sets to field deployed assets such as weapon and radar systems, sensors, and edge devices.

sales@enquanta.com **(612) 423-9015** enquanta.com