QuSecure

QuProtect™ capability highlight.
Secure application-to-application communication.

QuSecure offers the world's first post quantum cryptographic (PQC) security solution that enables organizations to address their post quantum cryptography business and technology challenges and opportunities.

Our solution for quantum-resilient cryptographic orchestration, QuProtect enables organizations to integrate, deploy, and evaluate post quantum cryptographic solutions that suit their unique infrastructure environments.

With QuProtect organizations can realize the rare opportunity for first-mover market advantage and become quantum cyber security leaders. With the capability to be deployed in a matter of hours and provide layered and configurable classical and quantum-safe encryption, QuProtect provides valuable protection and differentiation across industries.

Securing Inner Network Communications

Organizations rely on critical data within their networks for daily operations of their employees and customers – and this data in transit is vulnerable.

QuProtect with QuNetwork capabilities provides protection, insights and control over those connections in a way never experienced before.

QuProtect With QuNetwork Capabilities Key Solution Benefits

Quantum Safe Connections With Unchanged End User Experience
Server to server and application-to-application

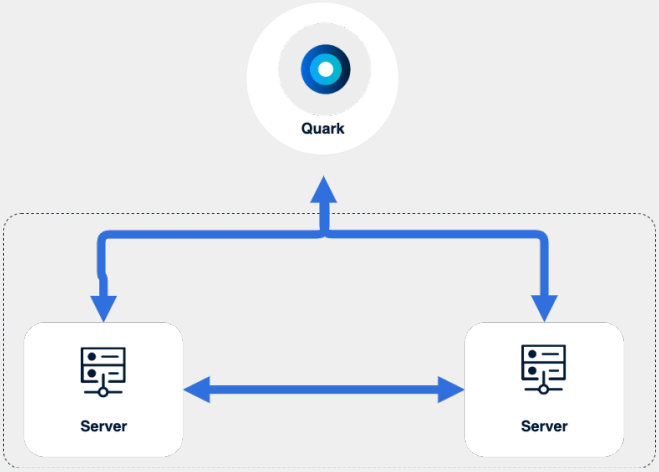
Cryptographic Agility
Full administrative control over multiple post-quantum cryptographic algorithms, key lengths, and rotation frequencies that enable high entropy keys for post-quantum resilient connections.

Zero Trust Foundations
Enabling Zero Trust network architecture as defined by NIST SP 800-207

Standards Based & Compliant
Including NIST and compliance with the new Quantum Computing Cyber Security Preparedness Act for trusted delivery of quantum resilience.

QuNetwork Overview

QuNetwork provides post-quantum, agile encryption channels for communication between servers over unsecured networks.



- **Quantum-Resilient Protection Between Applications**
  Post-quantum secure connections for application to application and server to server communications.
- **Cryptographic Controls**
  QuProtect's revolutionary control plane provides administrators with real time insights to monitor and manage secure connections. Admins can select which NIST recommended post-quantum algorithms are utilized and with cryptographic agility to "hot-swap" one quantum safe algorithm for another or change key strength on a per-client basis, all without disruption to service.
- **Post-Quantum Protection Works In Tandem With TLS**
  QuNetwork delivers quantum-resilient communications in tandem with pre-quantum TLS.
- **High Performance, Low Latency**
  Secure communication channels are created with negligible impact to current speeds and performance.

QuNetwork
Use Case Overview

QuNetwork Recommended Use Cases

Protecting Data In Amazon S3 Storage

Many enterprises and public sector ogranizations utilize Amazon AWS Cloud Simple Storage Service (Amazon S3) to store and transfer sensitive data such as national secrets, financial records, and contractual agreements.

QuProtecting S3 Storage

QuProtect with QuNetwork capabilities establishes a quantum resistant encrypted connection to ensure all data transferred between services remains confidential and protected from interception. The solution integrates seamlessly with Amazon S3 and the end user is able to transfer the sensitive date that is now secured against classical threats and store now, decrypt later.

Results & Benefits

- Robust framework for protected exchange of data between servers
- Leverages the scalability and reliability of the AWS cloud infrastructure

Protecting REST APIs

REST APIs have become a cornerstone of modern application development, enabling seamless communication and data exchange between different systems. However, the security of these APIs is crucial to prevent unauthorized access, data breaches, and other malicious activities.

QuProtecting REST APIs

To protect the sensitive data transmitted over REST API requests, QuProtect with QuNetwork capabilities enables end-to-end encryption. Utilizing QSL to establish secure connections and encrypt data in transit, the solution encrypts data transmissions with classical and quantum resilient protections.

Results & Benefits

- Proactively mitigates security risks so corporations can confidently provide secure and reliable API's to their customers
- Protects brand reputation and minimizes the likelihood of data breaches

A Scalable Solution – Start Today

STEP 1 – GET STARTED

Post-quantum protect your most vulnerable network segment within hours

Deploying QuProtect does not require discovery nor a rip and replace overhaul to your mission critical systems. Start by selecting a small section of your network with critical data to protect with a low, fixed cost initial deployment on-prem or in the cloud.

STEP 2 – PRIORITIZE & PLAN

Expert guidance to plan your protection

QuSecure's certified Solution Architects will work with you to design a prioritized plan to scale and protect the data and systems that matter most to you.

STEP 3 – PROTECTION AT SCALE

Horizontally scale your quantum protection with ease

QuProtect's cloud native architecture is built to scale with minimal effort to support larger enterprise PQC infrastructure needs.

Secure tomorrow.
Today.

Request A Demo

+1 (650) 356-8001
www.qusecure.com
info@qusecure.com