CASE STUDY

Integrating QuSecure with AWS for Cloud and Edge Computing

QuSecure

AWS and Qusecure partnered on a secure cloud military use case. The key objective was to enable post-quantum encrypted communications that could process radar data at the edge, provide tracking and data fusion, normalize the results, and distribute this data for cloud-based processing.

The Challenge & Opportunity

> *"But there's one threat on the horizon that dwarfs them all. That's the threat of a future quantum computer attack on our financial sector."*
>
> **Forbes** May 2023

AWS and QuSecure joined forces to deploy a cybersecurity solution tp address a number of concerns including hardening of security posture. The project had multiple requirements:

- Establishing quantum-resilient tunnels for secure connections between edge and cloud devices
- Conducting performance tests for both TCP and UDP
- Transferring data securely from Amazon Simple Storage Service (Amazon S3)
- Ensuring that the performance of other mission system elements wasn't adversely impacted

Our Approach

In response, QuSecure deployed QuProtect, a point-to-point Post-Quantum Cryptographic technology. The solution was deployed with out-of-the-box functionality and configured on a single day of onsite work and performance testing. Here's how QuProtect fortified the client's infrastructure:

Thorough Testing: Extensive tests, from S3 data transfers to TCP load testing at varying data rates, were conducted. This was crucial to simulate a real-world field configuration.

Quantum-Resiliency at the Edge: QuProtect was integrated with AWS Snowball - AWS's ruggedized data transport and edge computing device - ensuring quantum-safe encryption from data's origin point.

Robust Encryption: A quantum-resilient key exchange using the NIST-recommended Kyber algorithm.

Built on Zero Trust: With the tenet of zero trust, the QuProtect platform safeguarded digital infrastructure against contemporary and looming threats.

Seamless Integration: QuProtect provided secure, high-performance connections between different AWS regions including edge connections.

Ready for today. And tomorrow.

We demonstrated that quantum-resilient cybersecurity can effectively coexist with cloud technologies, enabling our customers to achieve their goals while ensuring the highest level of data protection. In our increasingly connected world, secure cloud solutions are no longer just an option, but an absolute necessity. For any organization leveraging cloud technologies, the key is to ensure not only functionality but the highest levels of security, especially in mission-critical environments.

A 2023 report from Air University at the United States Air Force warns that a sufficiently powerful quantum computer could decrypt even the most secure military communications in seconds. The study highlights the existential risk this poses to national security including the compromise of vital military data.

QuProtect™ Key Solution Benefits

- ✓ Quantum safe connections to protect critical data with unchanged end user experience
- ✓ Gain control over your data with cryptographic agility
- ✓ Zero Trust Foundations
- ✓ Standards based & compliant
- ✓ Rapid, ready compatible deployment built to scale

PARTNER SPOTLIGHT

aws

John DeRosa, PhD
Principal Program
Manager, AWS

Dr. John DeRosa is a distinguished security professional with a robust portfolio spanning various fields, primarily emphasizing national security and strategic development. Serving as a Principal Program Manager at Amazon Web Services (AWS), Dr. DeRosa possesses key expertise in digital and technological domains bringing technical expertise to QuSecure.

> *Over the last year, AWS has partnered with QuSecure to deliver cutting-edge technology to our defense customers. As a partner, QuSecure has truly delivered. They were selected for AWS accelerated development program and blazed the trail from start to finish completing the program in record time with zero remediation.*
>
> June 2023

INTRODUCING QUPROTECT

Quantum-grade security.
For Cloud Native Environments

READY FOR TODAY AND TOMORROW

The Post-Quantum Challenge in Mission-Critical Operations is Imminent, but Solvable.

With the growth of quantum computing, the need for post-quantum cryptographic solutions has never been more urgent:

Conventional Encryption Risks: Existing technologies may soon become obsolete, exposing sensitive information to threats.

Security Concerns: The potential misuse of radar data at the edge, with malicious actors intercepting, decrypting, and exploiting real-time tracking and data fusion.

Affected Sectors: Both government and private sectors face immense risks, including the disruption of critical infrastructures, undermining of security, and exposure of valuable intellectual property.

In response, QuSecure has implemented QuProtect, a cutting-edge solution:

Seamless Integration: Designed to work effortlessly with any system including AWS-based infrastructures.

Quantum-Resilient Tunnels: Offers secure connections for both TCP and UDP.

Secure Data Transfer: Ensures safe data transfer from Amazon Simple Storage Service (Amazon S3).

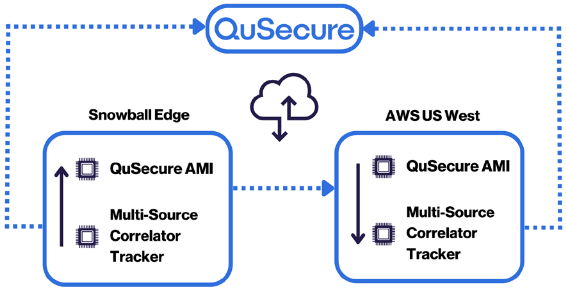
Advanced Government-Approved Algorithms: Equipped with NIST-recommended Kyber algorithm.

QuProtect is a comprehensive solution for any organization looking to future-proof its mission-critical environments against the emerging quantum threat. Today's readiness ensures tomorrow's resilience.

QuProtect™ Key Features

Quantum Safe Connections To Protect Critical Data With Unchanged End User Experience

- Web applications to web and mobile end devices
- Server to server and application-to-application


QuSecure
Snowball Edge
QuSecure AMI
Multi-Source Correlator Tracker
AWS US West
QuSecure AMI
Multi-Source Correlator Tracker

Cryptographic Agility

Full admin 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.

A Scalable Solution – Start Today

Step 1. Initial Pilot Deployment In Hours

Quantum protect your most vulnerable network segment

QuProtect's single day initial deployment does not require discovery nor a rip and replace overhaul to your mission critical systems. Select 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 the future.
Today.

Schedule A Demo Today