BANKING AND FINANCE

Protecting your organization's future. Today.

QuSecure

READY FOR TODAY AND TOMORROW

CASE STUDY

Helping a large financial institution secure their sensitive customer data

QuSecure

A large financial services organization is in the process of building a secure document management and transactional platform to provide a single, enterprise-wide, quantum-resilient file and data transfer platform serving information from internal systems to both employee and external customers and partners.

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

A customer engaged QuSecure to deploy a cyber security solution which addresses a number of concerns and harden the organization's security posture, including:

- Deployment of certified, industry-accepted, and validated NIST Post-Quantum Cryptographic finalist algorithms with cryptographic agility for risk-mitigation
- Simple integration with existing platforms with no disruptions to business operations
  - Identity and access management (IAM)
  - Key management (KMS)
  - Policy
  - Security Information and Event Management (SIEM)
- Provide controls to manage cryptographic upgrades – future-proofing against upcoming attacks on cryptography
- Enable monitoring and auditing of cryptography in use

The customer needed seamless deployment without service interruption so that users can continue to access data throughout the upgrade and the overall customer experience is not negatively impacted.

Our Approach

To fully address the customer's needs, QuSecure's certified solution architects worked to design a prioritized plan to scale and protect the data and systems that were a priority to the financial institution.

- Supported staged integration – working with the customer to implement targeted upgrades through test, approval, and staged rollout
- Deployed the QuProtect robust, all-in-one software based solution that facilitates simple integrations and compliance, and enables scaled deployment to meet future demand
- Paid close attention to existing systems, network, and platform types and capacity requirements ensuring minimal, if any, impact to network performance
- Engaged with the customer's compliance and certification teams, to ensure the protection regulatory programs are supported and strengthened from the start
- Tight administrative and operational integration so the system is easy on the IT security team

Ready for today. And tomorrow.

Seamlessly integrating into their existing platforms, QuProtect ensured no disruption to their business operations. It significantly enahanced the overall user experience by providing robust, reliable, quantum-resilient protection without compromising performance.

A 2022 study conducted by Arthur Herman at the Hudson Institute revealed that an attack from a quantum computer that disrupts any of the five largest financial institutions' access to the Fedwire Funds Service could cost up to nearly $2 Trillion.

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

SME SPOTLIGHT
Lisa Hammitt
Board Member, QuSecure

Lisa Hammitt is a visionary leader and senior executive with demonstrated success transforming early technology into viable operations that drive strategic growth. As Chairwoman of the Board of Directors at Intelsat and former Global Vice President of Data and Artificial Intelligence at Visa, Lisa brings more than 30 years of experience to QuSecure's board of directors.

> *The quantum threat is expected to have a large and disruptive impact on the current digitally dependent economy... It is a business imperative that organizations start to think about what a secure quantum transition could look like and understand their cryptographic and data exposure to avoid disruption of business operations.*
>
> **World Economic Forum** Sep 2022

INTRODUCING QUPROTECT

Quantum-grade security.
For today's financial organizations.

READY FOR TODAY AND TOMORROW

The quantum threat to today's banking and financial organizations is real, but preventable. Find out why you need to act today.

With the ability to simulate highly complex systems and interactions, the game-changing capabilities of quantum computers will provide an easy avenue for criminals and other adversaries to steal your data and exploit your organization.

Store Now, Decrypt Later (SNDL) is a common cyber attack where a bad actor will harvest an encrypted data source with the expectation of being able to decrypt it in the future. Once decrypted, it will be distributed or sold on the dark web, compromising the confidentiality and integrity of an organization's digital assets and information. For today's banking and finance organizations, the security and compliance risks are high. As we accelerate towards a cashless society, banking and financial organizations face an increasing number of cyber attacks due to interconnected attack surfaces, ransomware, emerging technologies such as deepfakes and 5G, and malware attacks that spur multiparty and cross-sector targeting.

In response, QuSecure has developed QuProtect™ – a robust all-in-one software-based quantum security solution that's quick to implement and effortless to manage. Highly compatible with today's technologies, and easily integrated across various devices, QuProtect offers a powerful and seamless solution, so that banks and financial organizations are ready for today. And tomorrow.

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

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

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