CASE STUDY

Integrating QuSecure with Otio
Post-quantum security in healthcare

QuSecure

QuSecure partnered with Otio, a digital experiences SaaS company, to enhance their security with a first-to-market post-quantum cryptography (PQC) solution. Otio's healthcare clients face evolving cyber threats while maintaining strict compliance standards. QuProtect enabled Otio to securely transfer data from operating rooms to servers, develop insights, and improve patient outcomes. With QuProtect, Otio ensures quantum-resilient data exchange and gains a competitive edge.

The Challenge And Opportunity

> *"Today, approximately 30% of the world's data volume is being generated by the healthcare industry. By 2025, the compound annual growth rate of data for healthcare will reach 36%... 6% faster than manufacturing, 10% faster than financial services, and 11% faster than media & entertainment.*
>
> **RBC**
> Cost of a Data Breach Report 2023

Understanding the importance and enduring consequences of this data, Otio eagerly seized the opportunity to proactively tackle this challenge. They partnered with QuSecure to evaluate a post-quantum cryptography solution, guaranteeing their preparedness for upcoming regulatory mandates. When considering a solution, Otio had several key considerations:

Critical Healthcare Data Otio's cutting-edge technological solutions require secure transmission of sensitive HIPAA patient and treatment data, which have a significant lifespan.

Data In Transit The collection of sensitive data occurs in the field through their treatment web app, utilized by mobile workforces at care facilities. This data is continuously transmitted across data stores in the AWS cloud.

Easy Integration They sought a solution that seamlessly integrates with their treatment suite application without requiring any code modifications.

Compatible Security Moreover, they aimed to engage in a solution offering that leverages TLS, widely regarded as the current industry standard for data security.

Otio had the foresight to see the future of cybersecurity given the rapid advances in AI and quantum computing and the associated threats they pose. They were seeking a competitive advantage in how their client's healthcare data was protected. Understanding that implementing PQC presented a compelling opportunity for Otio to fortify their data security, foster trust among patients, partners, and stakeholders with a first mover advantage, they engaged QuSecure to pilot their PQC solution, QuProtect.

By safeguarding their patients' sensitive medical records and personal information from potential quantum computing threats, Otio knew they could enhance their reputation for reliability and privacy protection. This proactive approach not only aided in ensuring compliance with stringent data protection regulations but also distinguished Otio as a leader in the industry, allowing them to attract discerning customers who prioritize a new generation in cybersecurity. Embracing post-quantum cryptography not only future-proofed their systems but also established a competitive edge, bolstering Otio's position in the marketplace as a trusted custodian of confidential healthcare data.

Our Approach

Otio engaged QuSecure to pilot the implementation of QuProtect, a software solution that enables quantum-resilient security for data in transit. Acknowledging the significance of a seamless solution that wouldn't necessitate altering application code or disturbing the end user experience, QuProtect Web App Security's proxy-based architecture facilitated effortless integration without any modifications to Otio's current infrastructure.

QuSecure collaborated with iVALT, a next generation identity solution that enhances Otio's cybersecurity by verifying multiple dynamic identity user attributes with a single click. The implementation of these complementary solutions in parallel ensured top-notch security, encompassing encryption and advanced identity.

EARLY ADOPTER SPOTLIGHT

otio

Otio
Driving Value Together

At Otio, we create delightful digital experiences that harmonize form and function while staying grounded in security, privacy, and accessibility best practices.

"The Otio Platform uniquely enables regulatory compliance by providing uninterrupted end user experiences utilizing QuSecure's post-quantum cryptography. Our first to market solution differentiates us from our competition and accelerates adoption and go to market strategies."

Aaron Wentzel
Chief Executive Officer, Otio

Ready For Today. And Tomorrow.

QuProtect enabled Otio to seamlessly implement quantum-resilient protection for their web app communications. This innovative solution ensures secure data transmission between end user browser sessions and throughout the AWS cloud, without any disruption to existing systems.

QuProtect provided the Otio team with realtime visibility and control over cryptography in use to protect their critical data, offering built-in guidance that instilled confidence in their security choices.

By testing the interoperability of the solution with existing architectures on a small scale, it became clear that adding additional proxies in the future and adjusting protection as Otio's solution offering expands would be effortless.

Otio's partnership with QuSecure represents a proactive defense model, marking a quantum-secure era for healthcare data security. Their adoption of QuProtect showcases their commitment to excellence and safeguarding clients' sensitive information.

CASE STUDY

READY FOR TODAY, AND TOMORROW

Quantum-grade security.
For healthcare organizations.

Securing Healthcare Data From Quantum Computing, Today.

In the healthcare sector, where patient privacy and the security of sensitive medical data are paramount, the urgent need for quantum-resilient encryption cannot be overstated.

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

Security Concerns The improper acquisition and misuse of sensitive healthcare data, including electronic health records and connected medical devices, can lead to devastating outcomes.

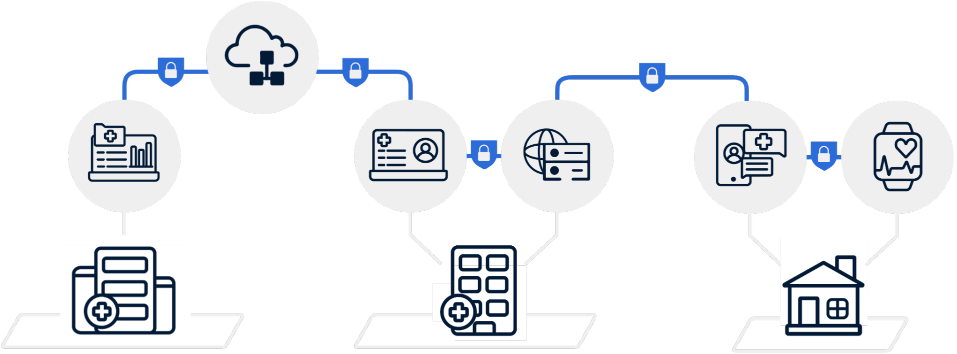
A Targeted Industry The healthcare industry, which carries the weight of safeguarding patient confidentiality and managing critical real-time data systems, is particularly vulnerable to quantum computing attacks.

> *"Since 2020, healthcare data breach costs have increased 53.3%... For the 13th year in a row, the healthcare industry reported the most expensive data breaches, at an average cost of USD 10.93 million."*
>
> **IBM Security**
> Cost of a Data Breach Report 2023

Now is the time to secure the future of medical records and patient confidentiality with QuProtect's advanced, quantum-safe solutions designed to meet the specific needs of healthcare information security. Act now to safeguard your patients' most sensitive information from the quantum threat on the horizon.

QuProtect™ Key Features

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



Cryptographic Agility

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

Zero Trust Foundations

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

Standards Based And Compliant

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

Easily Integrating With Legacy Systems

Designed to be simple to deploy, operate, and manage.

A Scalable Solution – Start Today

Step 1. Plan Your Protection

Strategy to quantum protect your most vulnerable network segment

Our skilled team specializes in helping you identify priority use cases to protect the data and systems that matter most to you.

Step 2. Test

Explore & Experience Protection Concurrently

Easily implement QuProtect within hours and experience real-time post-quantum security without changing existing systems with a cost-effective initial test deployment to explore protection like never before.

Step 3. Protection At Scale

Seamlessly Transition to Managed Cryptography

QuProtect's cloud-native architecture effortlessly scales horizontally, providing comprehensive protection for all your data in transit. Break the encryption upgrade cycle and take control of managing your cryptography with cryptographic agility and on-demand cryptographic inventory.

Secure the future.
Today.

Schedule A QuProtect Demo

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