



IronCAP Quantum-Safe AI

HARDENED AI. PROTECT YOUR DATA.

THE FUTURE OF AI SECURITY STARTS NOW

Artificial intelligence is rapidly becoming the backbone of modern enterprise—powering decision-making, automation, and competitive advantage across every industry. AI systems are trained on vast volumes of sensitive data such as financial records, patient information, and proprietary algorithms. Such data faces risk of exposure during inference (use).

Meanwhile, quantum computing threatens to break the cryptographic foundations that protect global communications, transactions, and infrastructure. This puts prompt privacy and confidentiality at risk.

The result: These risks are rapidly materializing and becoming real issues. These issues increase security vulnerability in organizations and need to be addressed with urgency.

01 Quantum addresses this challenge with **Quantum AI Wrapper (QAW)**. QAW is Quantum-Safe AI, a new paradigm that integrates post-quantum cryptography with vaulted AI technology using Fully Homomorphic Encryption (FHE).

The Challenge

AI adoption is accelerating, but the operational security has not kept in pace.

Enterprises today rely on traditional security models that protect data:

- At rest (stored in databases)
- In transit (moving across networks)

However, AI introduces a critical third state: data in use—where sensitive information is actively processed, analyzed, and transformed.

This is where the greatest vulnerability exists.

Key Risk Factors

Prompt Privacy During Processing

- Sensitive inputs must typically be decrypted for AI models to operate, creating a window of eavesdropping vulnerability.

Model Theft and Reverse Engineering

- Proprietary AI models represent significant intellectual property and are increasingly targeted for extraction.

Regulatory Pressure

- Governments and regulators are tightening requirements across industries, including GDPR, HIPAA, PCI-DSS, and emerging AI-specific regulations.

The Solution: Quantum AI Wrapper (QAW)

Quantum AI Wrapper (QAW) redefines how AI is secured.

QAW is a support-and-services bundle from 01 Quantum based on open-source software, enabling organizations to run AI on fully encrypted data—without ever decrypting it.

This breakthrough is made possible through the integration of:

- Open-source Post-Quantum Cryptography (PQC) – resistant to quantum attacks
- Open-source Fully Homomorphic Encryption (FHE) – enabling computation on encrypted data

HOW IT WORKS

Unlike traditional approaches that require cleartext prompts and models for processing, QAW ensures:

- Data remains encrypted at all times (at-rest / in-use / in transit)
- AI models operate directly on encrypted inputs/prompts
- Outputs are generated without exposing underlying data

This eliminates the most critical vulnerability in AI systems—data-in-use exposure.



QAW

Protect your data.
Protect your models.
Protect your future.

SECURE AI FOR HIGH-STAKES INDUSTRIES

QAW is designed for environments where security, compliance, and trust are non-negotiable.

Banking & Financial Services



Secure innovation without regulatory risk.

Financial institutions are under constant pressure to innovate with AI while maintaining strict compliance and safeguarding sensitive data.

Challenges:

- Exposure of proprietary trading and risk models, financial transactions and customer data
- Compliance with PCI-DSS, SOC2, GDPR, and other regulations

QAW use-cases:

- Encrypted fraud detection and real-time risk analytics
- Protection of high-value trading, credit, and scoring models
- Confidential processing of customer and transaction data

Healthcare & Life Sciences



AI innovation without compromising patient trust.

Healthcare organizations rely on AI for diagnostics, research, and operational efficiency—but must ensure strict protection of patient data.

Challenges:

- Protection of sensitive research data, intellectual property and Patient Health Information (PHI)
- Compliance with HIPAA, PHIPA, and global privacy regulations

QAW use-cases:

- AI processing on fully encrypted patient records
- Secure analytics for clinical trials and medical research
- Protection of diagnostic and predictive models

National Defense & Government



Mission-critical AI with zero exposure.

Government and defense organizations require high security for AI operating in contested environments, at the network edges.

Challenges:

- Securing AI trained with classified intelligence and operational data
- Processing platforms that are physically vulnerable to capture

QAW Delivers:

- Secure AI for classified datasets
- On-premise and sovereign deployment capabilities

Business Impact



QAW delivers measurable value across security, operations, and innovation:

Reduce Risk

- Eliminate the largest vulnerability in AI systems—data exposure during processing

Lower Costs

- Minimize the need for complex security controls and reduce compliance overhead

Accelerate AI Adoption and ROI

- Unlock high-value AI use cases that were previously too risky for AI deployment



01 Quantum Inc.
789 Don Mills Road
Toronto, ON, M3C 1T5, Canada
1-800-668-2185
01quantuminc.com

Sales/VARs: sales@01com.com
Technical Support: help@01com.com
Customer Service: customerservice@01com.com