INTEGRATED QUANTUM TECHNOLOGIES

Quantum-Resilient Infrastructure for AI & Machine Learning

Investor Presentation (Q2-2026)

DISCLAIMER

General

The information provided in this presentation pertaining to Integrate Cyber, Inc ("Integrated Cyber" or the "Company"), its business assets, strategy, and operations is for general informational purposes only and is not a formal offer to sell or a solicitation of an offer to buy any securities, options, futures, or other derivatives related to securities in any jurisdiction and its content is not prescribed by securities laws. Information contained in this presentation should not be relied upon as advice to buy or sell or hold such securities or as an offer to sell such securities. This presentation does not take into account, nor does it provide any tax, legal or investment advice or opinion regarding the specific investment objectives or financial situation of any person. While the information in this presentation is believed to be accurate and reliable, Integrated Cyber and its agents, advisors, directors, officers, employees, and shareholders make no representation or warranties, expressed or implied, as to the accuracy of such information and Integrated Cyber expressly disclaims any and all liability that may be based on such information or errors or omissions thereof. Integrated Cyber reserves the right to amend or replace the information contained herein, in part or entirely, at any time, and undertakes no obligation to provide the recipient with access to the amended information or to notify the recipient thereof.

The information contained in this presentation is intended only for the persons to whom it is transmitted for the purposes of evaluating the Company. The information contained in this presentation supersedes any prior presentation or conversation concerning the Company. Any information, representations, or statements not contained herein shall not be relied upon for any purpose.

Neither we nor any of our representatives shall have any liability whatsoever, under contract, tort, trust, or otherwise, to you or any person resulting from the use of the information in this presentation by you or any of your representatives or for omissions from the information in this presentation. Additionally, the Company undertakes no obligation to comment on the expectations of, or statements made by, third parties in respect of the matters discussed in this presentation.

Confidentiality

This presentation is confidential and is intended, among other things, to present a general outline of the Company. The contents are not to be reproduced or distributed to the public or press. Each person who has received a copy of this presentation (whether or not such person purchases any securities) is deemed to have agreed: (i) not to reproduce or distribute this presentation, in whole or in part, without the prior written consent of the Company, other than to legal, tax, financial and other advisors on a need to know basis, (ii) if such person has not purchased securities, to return this presentation to the Company upon its request, (iii) without the prior written consent of the Company, not to disclose any information contained in this presentation except to the extent that such information was (a) previously known by such person through a source (other than the Company) not bound by any obligation to keep such information confidential, (b) in the public domain through no fault of such person, or (c) lawfully obtained at a later date by such person from sources (other than the Company) not bound by any obligation to keep such information confidential, and (iv) to be responsible for any disclosure of this presentation, or the information contained herein, by such person or any of its employees, agents or representatives.

Forward-Looking Statements and Financial Projections

Certain information in this presentation and oral statements made in any meeting are forward-looking and relate to Integrated Cyber and its anticipated financial position, business strategy, events, and courses of action. Words or phrases such as "anticipate," "objective," "may," "will," "might," "should," "could," "can," "intend," "expect," "believe," "estimate," "predict," "potential," "plan," "is designed to" or similar expressions suggest future outcomes. Forward-looking statements and financial projections include, among other things, statements about: our expectations regarding our expenses, sales, and operations; our future customer concentration; our anticipated cash needs, our estimates regarding our capital requirements, our need for additional financing; our ability to anticipate the future needs of our customers; our plans for future products and enhancements of existing products; our future growth strategy and growth rate; our future intellectual property; and our anticipated trends and challenges in the markets in which we operate. Forward-looking statements and financial projections are based on the opinions and estimates of management at the date the statements are made and are subject to a variety of risks and uncertainties, and other factors that could cause actual events or results to differ materially from those anticipated in the forward-looking statements and financial projections. Although we believe that the expectations reflected in the forward-looking statements and financial projections are reasonable, there can be no assurance that such expectations will prove to be correct. We cannot guarantee future results, level of activity, performance, or achievements, and there is no representation that the actual results achieved will be the same, in whole or in part, as those set out in the forward-looking statements and financial projections.

By their nature, forward-looking statements and financial projections involve numerous assumptions, known and unknown risks and uncertainties, both general and specific, that contribute to the possibility that the predictions, forecasts, projections and other forward-looking information will not occur, which may cause the Company's actual performance and financial results in future periods to differ materially from any estimates or projections of future performance or results expressed or implied by such forward-looking statements and financial projections. Important factors that could cause actual results to differ materially from expectations include, but are not limited to: business, economic and capital market conditions; the heavily regulated industry in which the Company carries on business; current or future laws or regulations and new interpretations of existing laws or regulations; legal and regulatory requirements; market conditions and the demand and pricing for our products; our relationships with our customers, developers and business partners; our ability to successfully define, design and release new products in a timely manner that meet our customers' needs; our ability to attract, retain and motivate qualified personnel; competition in our industry; competition; technology failures; failure of counterparties to perform their contractual obligations; systems, networks, telecommunications or service disruptions or failures or cyber-attack; ability to obtain additional financing on reasonable terms or at all; our ability to manage risks inherent in foreign operations; litigation costs and outcomes; our ability to successfully maintain and enforce our intellectual property rights and defend third party claims of infringement of their intellectual property rights; our ability to manage foreign exchange risk and working capital; and our ability to manage our growth. Readers are cautioned that this list of factors should not be construed as exhaustive.

The forward-looking statements and financial projections contained in this presentation are expressly qualified by this cautionary statement. Except as required by law, we undertake no obligation to update or revise publicly any forward-looking statements, whether as a result of new information, future events, or otherwise, after the date on which the statements are made or to reflect the occurrence of unanticipated events. Readers are cautioned not to place undue reliance on forward-looking statements or financial projections.

Prospective investors should not construe the contents of this presentation as legal, tax, investment, or other advice. All prospective investors should make their own inquiries and consult their own advisors as to legal, tax, investment, and related matters concerning an investment in the securities of the Company.

United States Disclaimer

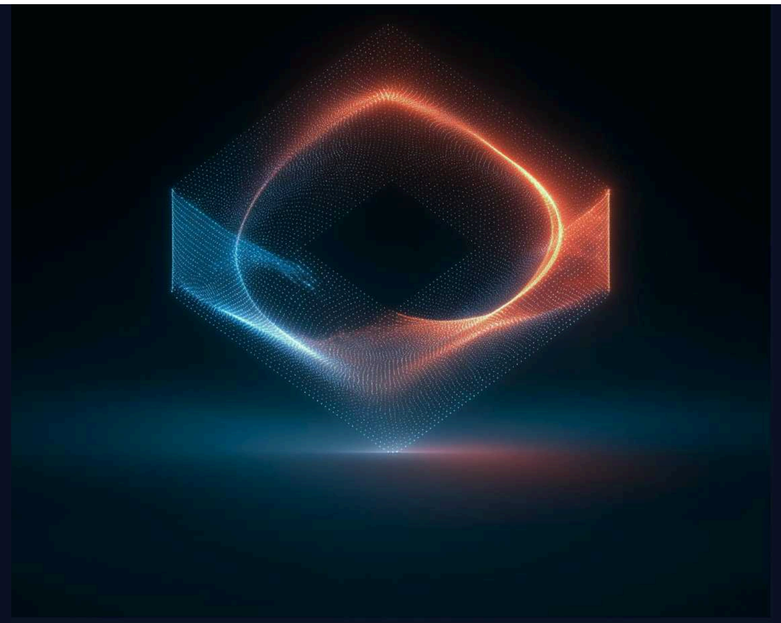
This document does not constitute an offer to sell or a solicitation of an offer to buy securities in the United States. The securities offered hereby have not been, and will not be, registered under the United States Securities Act of 1933, as amended (the “U.S. Securities Act”), or under any of the securities laws of any state of the “United States” (as defined in Regulation S under the U.S. Securities Act). Accordingly, the securities offered hereby may not be offered or sold, directly or indirectly, to, or for the account or benefit of, a person in the United States or a “U.S. person” (as defined in Regulation S under the U.S. Securities Act) unless exempt or excluded from the registration requirements of the U.S. Securities Act, and the securities laws of all applicable states of the United States or pursuant to registration under the U.S. Securities Act and under the securities laws of all applicable states of the United States. None of the United States Securities and Exchange Commission or any other securities commission or regulatory authority in the United States has approved or disapproved of the securities of the Company or determined if this document is truthful or complete. Any representation to the contrary is a criminal offense.
Also, please reach out to your U.S. counsel to confirm the extent you can use this slide deck to offer special warrants in the US, especially since 1332996 BC Ltd isn’t registered with the SEC. As we are not licensed in the US, we cannot advise on this subject. If your current counsel doesn’t have expertise in securities laws, please let us know and we can recommend a U.S. law firm.

OUR STORY

A Research and Innovation Company for Next-Generation AI Infrastructure

Grounded in research and innovation, Integrated Quantum Technologies is shaping the next frontier of intelligent AI infrastructure. We develop quantum resilient technologies that allow AI to operate securely, adapt dynamically, and unlock new possibilities in a connected post quantum world.

Integrated Quantum Technologies is the foundation of a new era in AI, built to secure, accelerate, and scale intelligence. AIQu VEIL is the first of many solutions, delivering quantum-resilient, privacy-preserving AI pipelines today and beyond.



TECHNOLOGY AT THE CORE

Our Mission

Build a future where AI can be trusted at every level, from the data that powers it to the models and systems that run it. Integrated Quantum Technologies empowers organizations with quantum-resilient data protection, privacy-preserving model practices, and advanced compression, enabling AI that is faster, more reliable, and infinitely scalable.

INTRODUCING AIQU VEIL

AIQu VEIL : The Quantum-Resilient Engine for High-Performance AI

Emerging from Integrated Quantum Technologies' Innovation Center, AIQu VEIL enables organizations to harness AI while keeping sensitive data fully protected. By ensuring data is never exposed in raw form, AIQu VEIL allows models to operate with full fidelity, unlocking insights and innovation without compromising privacy.

The Challenge

AI and machine-learning pipelines are exposed to vulnerabilities at every stage, from data leaks to tampered models. Current solutions provide only partial protection, leaving pipelines fragile today and increasingly at risk in a post-quantum world.

The Solution

AIQu VEIL uses proprietary technology to integrate quantum-resilient security directly into data and model layers, safeguarding sensitive information while maintaining high performance, setting a new standard for AI and machine learning pipelines.

The Impact

With AIQu VEIL, organizations can confidently run AI and ML pipelines with secure data, simplified governance, and streamlined operations, making their ML operations ready for the challenges of today and the post-quantum environment of tomorrow.

9 out of 10 executives see AI as the future of revenue growth, yet most are held back by concerns over data security and compliance risks.

Source:
Gartner: Gartner. (2024). Gartner 2024 CEO and Senior Business Executive Survey. Author.
IBM: IBM. (2024). IBM Global AI Adoption Index 2024. Author.

INTEGRATED QUANTUM TECHNOLOGIES

THE PROBLEM

Why Today's AI Systems Fall Short on Security, Compliance, and Scalability?

Regulatory hurdles:

Local deployment rules prevent economies of scale, driving up costs and slowing efficient expansion.

Privacy constraints:

GDPR, HIPAA, APRA, and other laws require data to stay in specific regions, making compliance harder to navigate.

Security vulnerabilities:

Centralized, monolithic data storage creates single points of failure, exposing ML models and sensitive data.

Compliance bottlenecks:

Strict rules often block global scaling of AI and ML deployments, limiting reach and operational efficiency.

Future-readiness gaps:

Enterprises need robust solutions that protect AI systems and sensitive data against emerging quantum era threats.

OUR SOLUTION

Why Enterprises Need AIQu VEIL Now?

Our solution closes a critical market gap that currently limits AI adoption while equipping companies for a quantum-ready future.

Enterprises can’t afford to wait. AIQu VEIL eliminates these barriers, enabling secure, compliant, and scalable AI deployments immediately.

50%

Fewer than 50% of AI projects are expected to progress from proof of concept to production by 2027 (Gartner AI Hype Cycle, 2023–2024).

73%

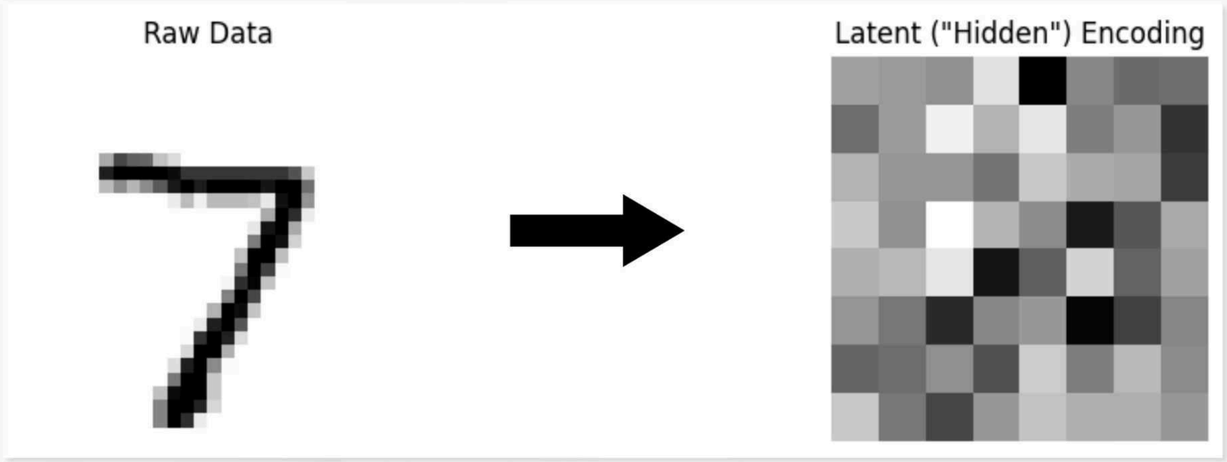
73% of CEOs report being unable to scale AI initiatives due to compliance, governance, or ethical concerns (KPMG CEO Outlook, 2023–2024).

65%

65% of global enterprises cite compliance with evolving data privacy regulations as the top barrier to scaling AI (PwC AI Predictions 2024).

PRIVACY PROTECTION

How AIQu VEIL Secures AI Ecosystems?



* NIST integer data set used as an example, from test environment

If attacked or intercepted, ML data remains impossible to reconstruct. Attackers gain nothing but unusable fragments with zero context or value.

Even a successful breach becomes a dead end by design, turning data security from risk mitigation into a true competitive advantage.

UNMATCHED PERFORMANCE

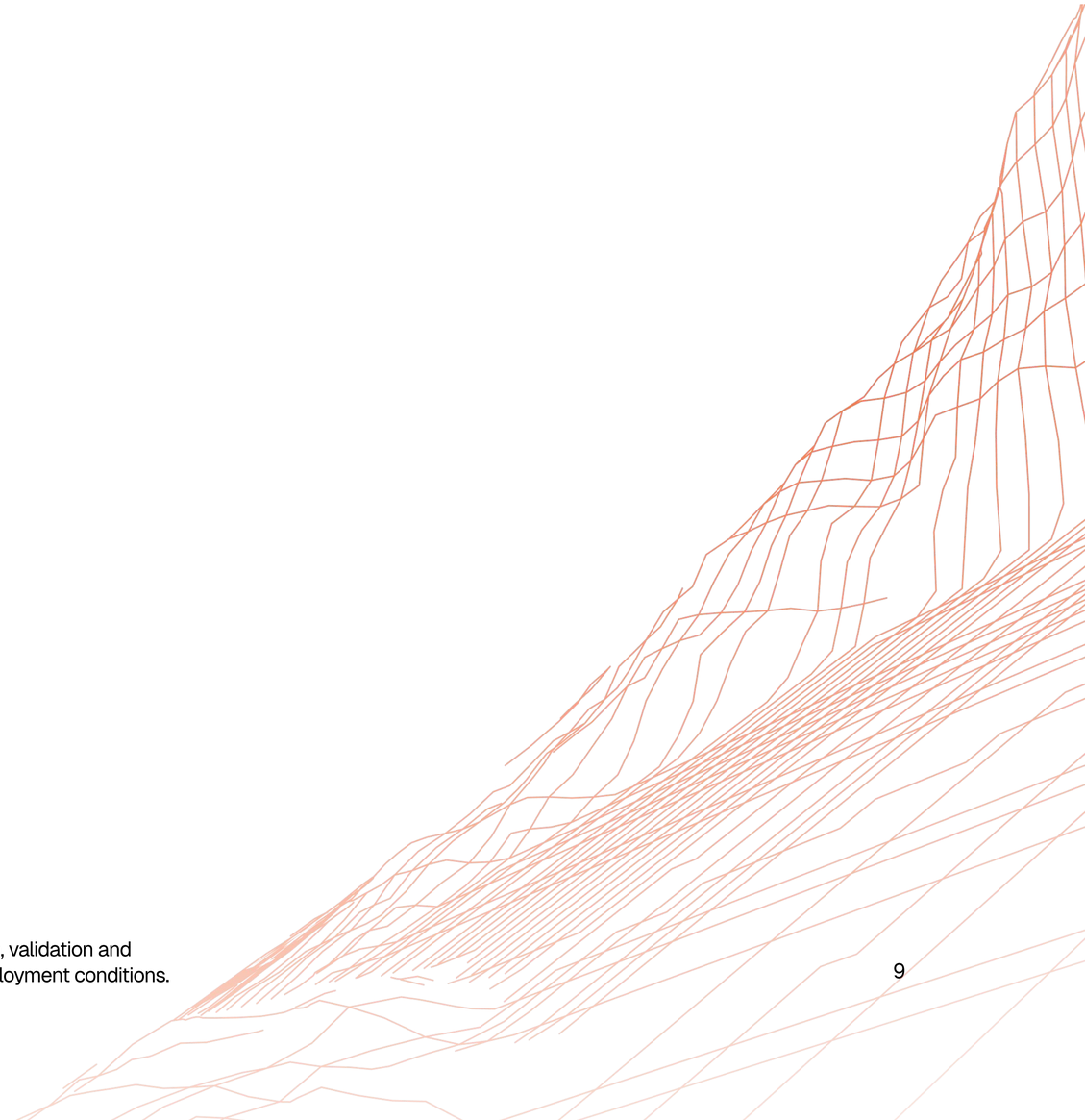
Quantum Resilient AI Security, Optimized for Performance

AIQu VEIL sets a new standard for secure ML, combining unmatched protection, speed, and accuracy so enterprises can deploy AI with confidence at scale.

92.45%	99.25%	+6.80%
Raw Data Test Accuracy	Protected Data Test Accuracy	Difference

Models trained on protected data achieve even higher accuracy than those trained on raw data, delivering an unprecedented advantage for enterprises.

The data can be compressed substantially, reducing storage and processing costs while accelerating overall model performance substantially.



INTEGRATED QUANTUM TECHNOLOGIES

Technical assessments and performance expectations reflect management's current beliefs based on internal research, validation and testing conducted by the Company. Results may vary across customer environments, datasets, configurations and deployment conditions.

WHY AIQU VEIL MATTERS?

AIQu VEIL: Secure, Efficient, and Quantum-Ready

Faster & Smarter ML

Enhances model speed and accuracy while compressing data to lower energy use and storage costs.

Global Deployment:

Centralized ML deployment across global operations reduces duplication, improves consistency, and can enhance model accuracy and operational efficiency.

End-to-End Security:

Protects sensitive data in regulated industries and resists quantum attacks, reducing breach risks and reputational damage.

Cost Efficiency

Consolidates AI teams and pipelines, simplifying deployment, reducing operational complexity, and improving scalability.

Simplified Compliance:

Built-in governance supports compliance with GDPR, HIPAA, and emerging AI regulations while improving oversight and reducing the compliance burden.

Accelerated Time-to-Value:

A streamlined global rollout accelerates deployment, improves time-to-value, and ensures consistent model performance across enterprise environments.

INTEGRATED QUANTUM TECHNOLOGIES

Technical assessments and performance expectations reflect management's current beliefs based on internal research, validation and testing conducted by the Company. Results may vary across customer environments, datasets, configurations and deployment conditions.

OUR TARGET MARKET

Organizations That Need Quantum-Ready AI Protection

Organizations across industries face regulatory, security, and skills challenges that hinder the safe and scalable adoption of AI.

FINANCIAL SERVICES AND BANKING

AIQu enables compliant, quantum-resilient AI model deployment across regions, reducing fraud detection latency and ensuring adherence to GDPR, APRA, and FINRA regulations.

CRITICAL INFRASTRUCTURE

AIQu protects operational ML models across distributed sites, ensures compliance with NERC-CIP and ISO 27019, and mitigates quantum and model-poisoning threats.

GOVERNMENT AND DEFENSE

AIQu Offers secure, region-segregated AI pipelines to meet FedRAMP, GDPR, and national-sovereignty standards ensuring safe AI deployment across jurisdictions.

MEDICAL AND HEALTHCARE

Healthcare organizations use machine learning to improve outcomes and efficiency but face challenges securing models at scale while protecting PHI and meeting HIPAA and GDPR requirements.

Technical assessments and performance expectations reflect management's current beliefs based on internal research, validation and testing conducted by the Company. Results may vary across customer environments, datasets, configurations and deployment conditions.

Unmatched Security:

Competitors either protect data or maintain performance. The AI Protector Model delivers both fully quantum resilient security and high ML performance.

Global Scalability:

Unlike siloed or regional solutions, the Protector Model enables secure and compliant AI deployments at enterprise scale.

Flexible & Future-Proof:

Immune to quantum threats and adaptable to multiple ML deployment patterns, it provides a unique combination of security, performance, and flexibility.

No Comparable Solution Exists

Performance Without Compromise:

Other solutions reduce model speed or accuracy when protecting data. The Protector Model compresses and secures data without sacrificing quality.

Regulatory & Industry Ready:

Built in compliance for GDPR, HIPAA, CPRA, the EU AI Act, and other frameworks. Competitors often require custom integrations.

Technical assessments and performance expectations reflect management's current beliefs based on internal research, validation and testing conducted by the Company. Results may vary across customer environments, datasets, configurations and deployment conditions.

INTELLECTUAL PROPERTY & INNOVATION

We Don’t Just Protect AI, We Enhance It.

Our patent pending AIQu VEIL infrastructure redefines how intelligence is protected, setting new standards for performance, trust, and scalability. Each breakthrough reinforces our position at the intersection of AI, privacy-preserving innovation, and quantum resilience.

Supervised ML (classification, regression, anomaly detection)

Optimized parameter protection

Cloud-Agnostic - AWS, Azure, GCP, OCI.

End-to-end secure training and inference

On-Premise - Full control, local residency.

Hybrid - Split workloads securely.

INTEGRATED QUANTUM TECHNOLOGIES

Technical assessments and performance expectations reflect management’s current beliefs based on internal research, validation and testing conducted by the Company. Results may vary across customer environments, datasets, configurations and deployment conditions.

PERFORMANCE

The Results (AIQu VEIL): Secure, Fast, Accurate

Metric	Traditional Secure ML	AIQu VEIL
Inference Speed [2, 4, 5, 6]	60–90% slower	Near real time
Model Accuracy [1, 2, 4, 5]	4–10% drop	99%+ preserved
Data Protection [3, 4]	Only at rest or in transit	Full pipeline protection
Quantum Safety [3, 4]	Not future-proof	Quantum-Resilient
Scalability [2, 3, 4, 7]	Expensive, fragile	Enterprise-grade, global

INTEGRATED QUANTUM TECHNOLOGIES

Supporting technical references and source materials are in the appendix. Technical assessments and performance expectations reflect management's current beliefs based on internal research, validation and testing conducted by the Company. Results may vary across customer environments, datasets, configurations and deployment conditions.

UNIFIED CYBERSECURITY

Managed Cybersecurity & SecureGuard360™

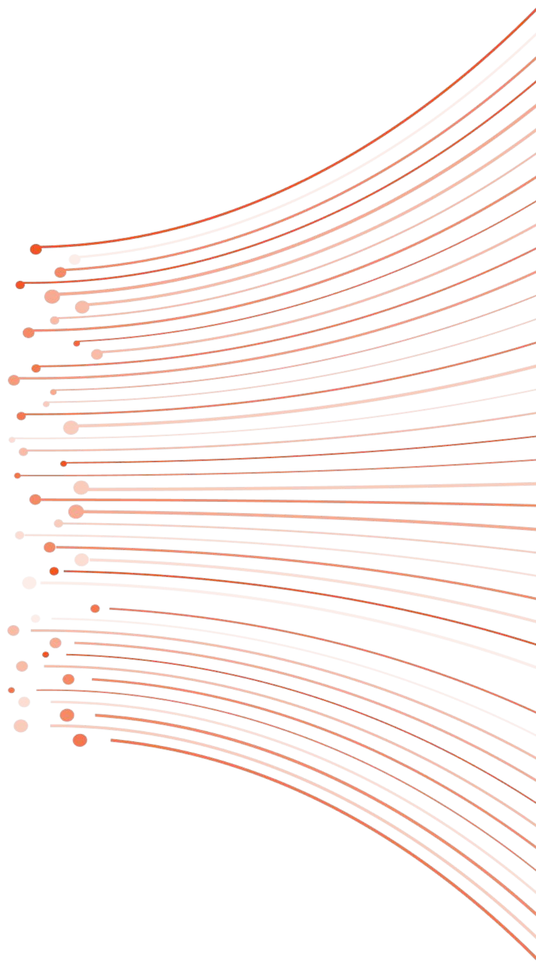
Integrated Quantum Technologies provides managed cybersecurity services to SMB and mid-market organizations across North America while developing proprietary cybersecurity software solutions.

Managed Security Services (MSSP)

- Recurring cybersecurity services: assessments, awareness training, and managed detection & response
- Established cybersecurity service delivery and customer relationships.

SecureGuard360™ : Unified Cybersecurity Visibility Platform

- SaaS platform intended to consolidate data from multiple cybersecurity tools into a single environment.
- Unified visibility across users, devices, and security systems.
- Identification and monitoring of high-risk users, endpoints, locations, and potential threats.
- Actionable insights to strengthen cybersecurity posture and work with existing security infrastructure.



Why Invest in ICS: Research Driven AI Security

ICS is focused on research and innovation, developing quantum-resilient AI security, architecture, and infrastructure solutions

Pioneering AI Infrastructure	Integrated Quantum drives breakthrough research, developing quantum-resilient, privacy-preserving AI architectures that set new industry standards and solve tomorrow's enterprise challenges today.
Industry First	Integrated Quantum is pioneering AIQu Veil, the first quantum-resilient, high-performance platform for AI pipelines—setting a new standard for secure, scalable, enterprise-ready AI.
Unlocking Enterprise AI	We tackle critical enterprise obstacles—data privacy, global deployment, and operational complexity—so organizations can run AI pipelines securely, efficiently, and at scale.
High-Growth Potential	Integrated Quantum operates at the intersection of AI, cybersecurity, and quantum resilience, addressing rapidly growing enterprise and regulated AI markets with high demand for secure solutions.
Innovation in Progress	AIQu VEIL is just the beginning— Integrated Quantum is building a pipeline of next-generation solutions that extend privacy-preserving, quantum-resilient capabilities across AI workflows.
Differentiated Advantage	Integrated Quantum combines proprietary quantum-resilient technology, privacy-preserving methods, and high-performance AI infrastructure, giving enterprises unmatched trust, speed, and compliance.

74,265,314
Shares Outstanding

8,950,000
Options and RSUs Outstanding

7,320,000
Warrants Outstanding

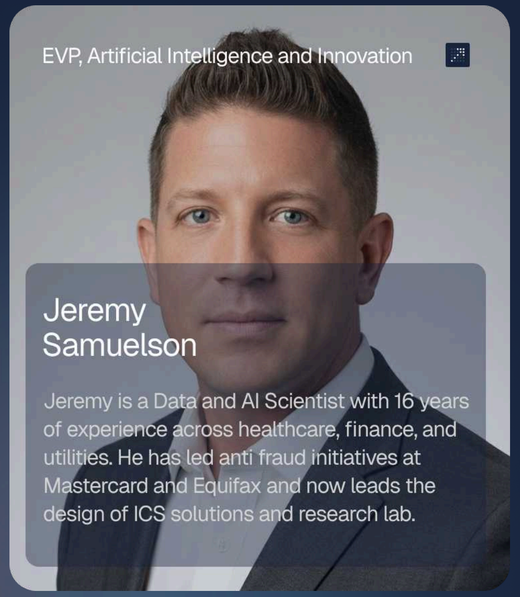
Insider Ownership: Over 50% with voluntary escrow

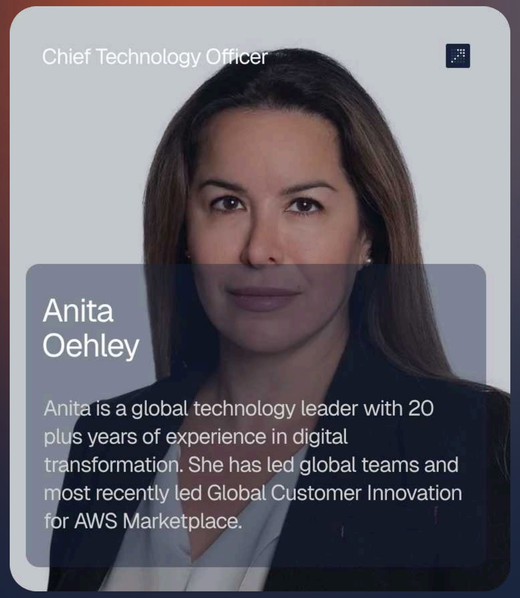
INTEGRATED QUANTUM TECHNOLOGIES

OUR TEAM

Behind Integrated Quantum Technologies is a Multidisciplinary leadership team

We bring together leading researchers, engineers, and strategists united by a single goal: to secure the world's most powerful technologies.



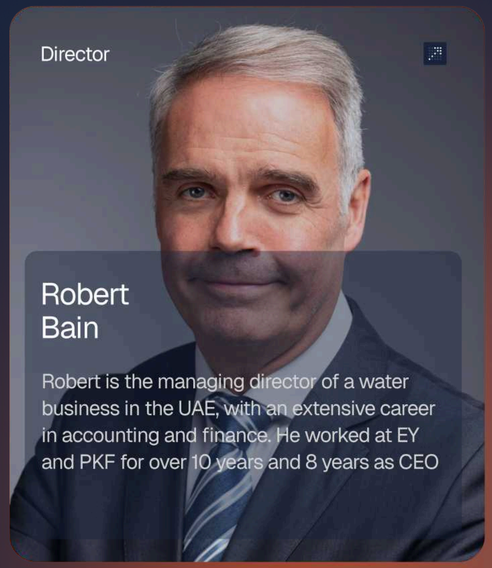


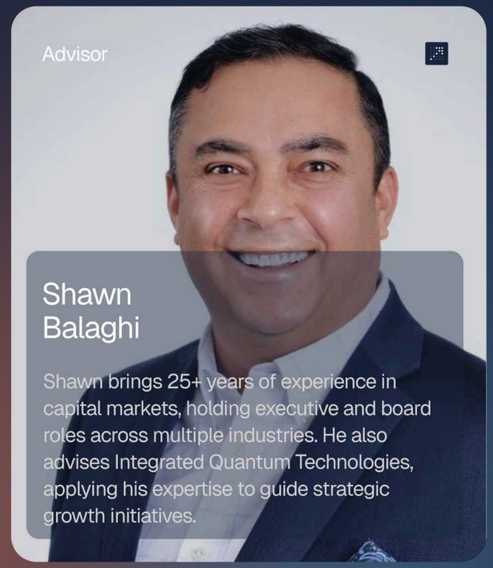
INTEGRATED QUANTUM TECHNOLOGIES

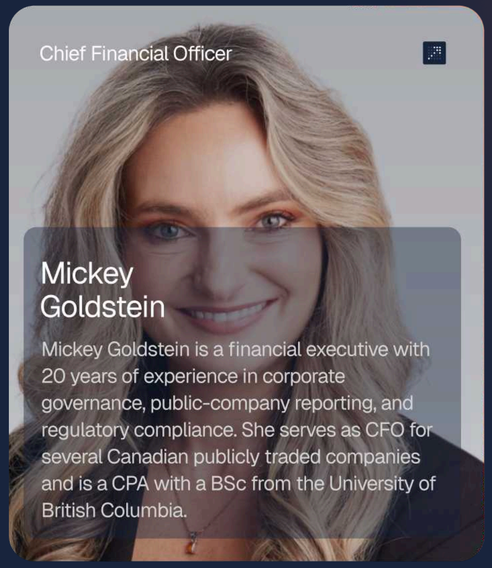
OUR TEAM

Board and Advisors

We bring together leading researchers, engineers, and strategists united by a single goal: to secure the world's most powerful technologies.







INTEGRATED QUANTUM TECHNOLOGIES

Thank You

Email: investors@integratedquantum.com

INTEGRATED QUANTUM TECHNOLOGIES

APPENDIX

References & Supporting Research

[1] Mohammadi, M., Vejdanihemmat, M., Lotfinia, M., Rusu, M., Truhn, D., Maier, A., & Tayebi Arasteh, S. (2026). Differential privacy for medical deep learning: methods, tradeoffs, and deployment implications. npj Digital Medicine, Nature Portfolio. DOI: 10.1038/s41746-025-02280-z. https://www.nature.com/articles/s41746-025-02280-z

[2] Gong, Y., Chang, X., Mišić, J., Mišić, V.B., Wang, J., & Zhu, H. (2024). Practical solutions in fully homomorphic encryption: a survey analyzing existing acceleration methods. Cybersecurity, Springer Nature. DOI: 10.1186/s42400-023-00187-4.https://cybersecurity.springeropen.com/articles/10.1186/s42400-023-00187-4

[3] National Institute of Standards and Technology (NIST) (2024). FIPS 203 / 204 / 205: First Post-Quantum Cryptographic Standards. U.S. Department of Commerce. Published August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[4] Samuelson, J.J. (2026). Informationally Compressive Anonymization: Non-Degrading Sensitive Input Protection for Privacy-Preserving Supervised Machine Learning. arXiv:2603.15842 [cs.LG]. Endorsed by Dr. Mohammad Tayebi, Simon Fraser University. https://arxiv.org/abs/2603.15842

[5] Fan, S., Deng, X., Tang, X., Xu, W. & Zhang, M. (2026). Understanding and boosting fully homomorphic encryption applications on GPU. Cybersecurity, Springer Nature. DOI: 10.1186/s42400-025-00482-2.https://link.springer.com/article/10.1186/s42400-025-00482-2

[6] Reagen, B., Choi, W., Ko, Y., Lee, V.T., Lee, H.S., Wei, G.Y. & Brooks, D. (2021). Cheetah: Optimizing and Accelerating Homomorphic Encryption for Private Inference. IEEE International Symposium on High-Performance Computer Architecture (HPCA). arXiv:2006.00505. https://arxiv.org/abs/2006.00505

[7] Zhang, J. et al. (2024). SoK: Fully Homomorphic Encryption Accelerators. ACM Computing Surveys, Vol. 56, No. 12. https://arxiv.org/abs/2212.01713