



Future-Proofing Data in a Quantum World

CSE: QSE | OTCQB: QSEGF | FSE: VN80

September 2026



Forward Looking Statement

This presentation contains forward-looking statements. These statements relate to future events or future performance and reflect our expectations and assumptions regarding our growth, results of operations, performance and business prospects and opportunities. Such forward-looking statements reflect our current beliefs and are based on information currently available to us. In some cases, forward-looking statements can be identified by terminology such as “may”, “would”, “could”, “will”, “should”, “expect”, “plan”, “intend”, “anticipate”, “believe”, “estimate”, “predict”, “potential”, “continue” or the negative of these terms or other similar expressions concerning matters that are not historical facts. The forward-looking statements in this presentation include, among others, statements regarding (i) future operating results, (ii) revenue generated from the QSE Platform, (iii) the anticipated time frame to complete additional upgrades to the QSE Platform, (iv) the Company’s ability to obtain market share, (v) general economic performance of the Company.

Forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause our actual performance or achievements to differ materially from anticipate results, performance or achievements expressed or implied by such forward looking statements. The risks and uncertainties that affect forward-looking statements include, but are not limited to:

- our expected future losses and accumulated deficit levels;
- our projected financial position and estimated cash burn rate;
- our ability to continue as a going concern;
- our requirement for, and our ability to obtain, future financing on favorable terms or at all;
- our potential sources of financing to fund ongoing operations;
- our assessment of market acceptance of the QSE product suite;
- our plans to market, sell and distribute the QSE product suite;
- our expectations with respect to future corporate alliances and licensing transactions with third parties;
- our strategy with respect to the protection of our intellectual property;
- the regulatory approval process;
- our ability to successfully compete in our targeted markets;
- our ability to adequately protect proprietary information and technology from competitors;
- our ability to attract and retain key personnel;
- the potential for liability claims; and
- the substantial risks involved in early-stage technology development companies related to, among other things, commercialization, capitalization, cost containment, and potential litigation.

A number of factors and assumptions could cause actual events, performance, or results, including those in respect of the foregoing items, to differ materially from the events, performance and results discussed in the forward-looking statements. Material factors and assumptions that could cause actual events, performance, or results to differ materially from those set forth in the forward-looking statements include, but are not limited to:

- the effect of continuing operating losses on our ability to obtain, on satisfactory terms, or at all, the capital required to maintain the Company as a going concern;
- the ability to obtain sufficient and suitable financing to support operations, development and the continued upgrade to the QSE Platform;
- the ability of the Company to retain qualified personnel to continue the upgrades to the Company’s QSE Platform;
- the ability to generate market acceptance of the Company’s product suite under the QSE Platform;
- the loss of the Company’s sole customer on the QSE Platform; and
- the increase in operating costs from additional development and commercialization costs and increased staff.

Although the forward-looking statements contained in this presentation are based on what we consider to be reasonable assumptions based on information currently available to us, there can be no assurance that actual events, performance, or results will be consistent with these forward-looking statements, and our assumptions may prove to be incorrect. These forward-looking statements are made as of the date of this presentation.

Forward-looking statements made in this presentation are made as of the date of the original document and have not been updated by us except as expressly provided for in this presentation. As required by applicable securities legislation, in its capacity as a reporting issuer, it is the Company’s policy to update forward-looking information in its periodic MD&As, as required from time to time, and provide updates on its activities to the public through the filing and dissemination of news releases and material change reports.

A Full Post-Quantum Security Posture Platform

QSE helps organizations identify cryptographic risk, plan the transition and deploy quantum-resilient protection across existing infrastructure

Core Posture Infrastructure

Assess, discover and prioritize cryptographic exposure, then simulate the migration path

Plug and Play Security

Resolve identified vulnerabilities with quantum-resilient protection without replacing existing infrastructure

Growing Commercial Reach

Partner-led access to enterprise, government and regulated markets globally

Scalable Revenue Model

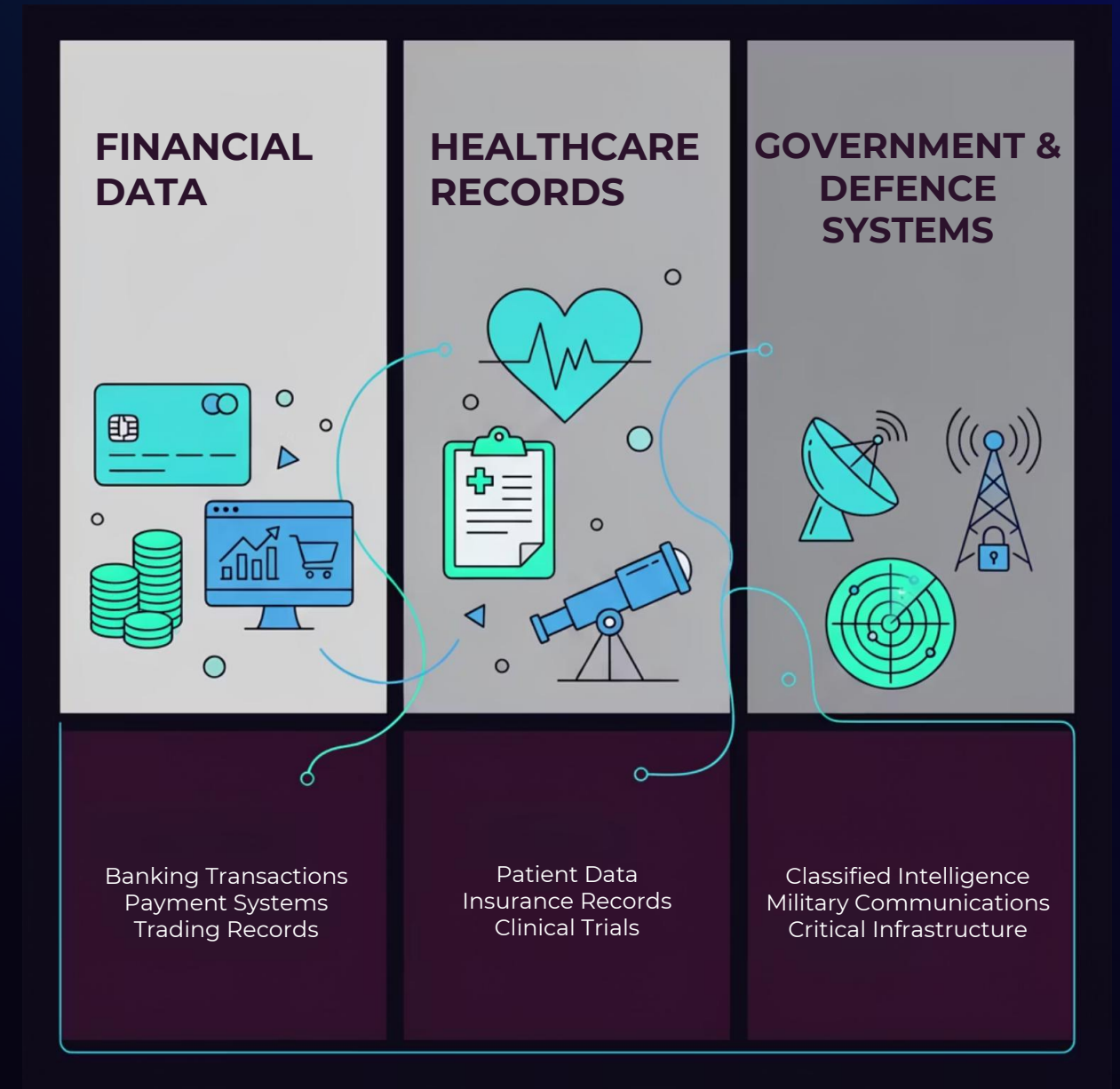
Assessment, integration, recurring reviews, software usage and enterprise deployments



Today's Encryption Has an Expiration Date

RSA & ECC underpin today's identities, certificates and sensitive communications. Quantum computing exposes both a decryption gap & it threatens the infrastructure of digital trust integrity - while many organizations still lack visibility into where vulnerable cryptography sits today.

- 📄 **Harvest now, decrypt later:** adversaries can collect encrypted data today and decrypt it when quantum capability matures.
- 📄 **Forge Now/Act Later:** Quantum-enabled attackers could forge trusted digital identities, signatures, certificates, and software.
- 📄 **Cryptographic blind spots:** certificates, libraries, keys and embedded cryptography are often spread across systems with no complete inventory of what must eventually be migrated.



A Regulatory-Driven Inflection Point

The shift to post-quantum cryptography is no longer a matter of 'if,' but 'when' and 'how,' driven by urgent global regulatory mandates.

This marks the beginning of a multi-decade infrastructure transition, demanding immediate strategic action.

Mandated Standards

Organizations such as NIST have begun to standardize post-quantum algorithms through certifications such as FIPS 203, 204 and 205. FIPS 140-3 defines security requirements for cryptographic modules.

Government Directives

Federal policies such as U.S. EO 14412 are accelerating PQC migration. Malaysia's Act 854 and Directive 9 are driving cryptographic-readiness and migration planning across NCII sectors.

Enterprise Acceleration

Regulated organizations increasingly need cryptographic inventories, evidence-backed readiness and executable migration plans.

Sources: White House EO 14412 (June 22, 2026); NIST FIPS 203/204/205 & FIPS 140-3; NACSA Malaysia Act 854 / Directive 9.



A Paradigm Shift: The Rise of Post-Quantum Cybersecurity

The Big Picture

- Quantum computing will soon **break current encryption standards**. The Global Risk Institute forecasts cryptographically relevant Quantum Computer possible within 5 years (49%), and likely within 7 years (70%).
- This creates an entirely new, critical category: **Post-Quantum Cybersecurity**.

Market Growth

\$2.8B+

Quantum security market in **2023**

\$10.2B+

Projected quantum cryptography market by **2030**

~46%

Annual growth, making it one of the fastest-growing segments in cybersecurity.

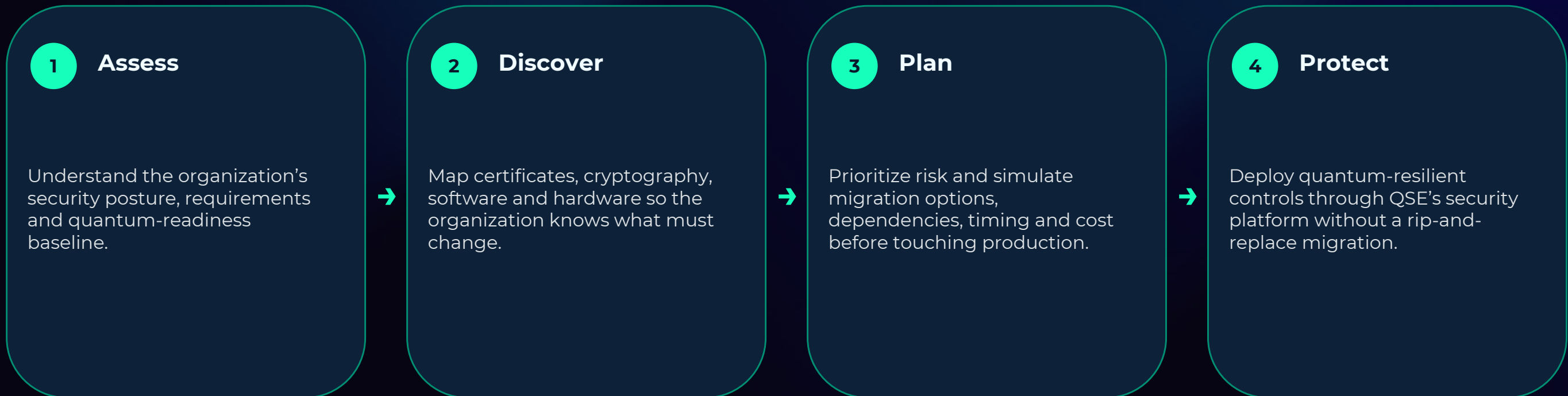
Urgency & Necessity

- More than **70% of high-priority federal systems & organizations** expected to adopt PQC solutions by year-end 2030.
- Cybercrime losses projected to hit **\$10.5 TRILLION globally**.
- Implementing post-quantum solutions is rapidly becoming a **necessity, not a choice**.

The transition to quantum-safe security is inevitable and already starting.

You Can't Protect What You Can't See

Think of enterprise cryptography like a city map: first locate the risks, then plan the route, then protect what matters.



QSE turns a complex cryptographic estate into an executable migration map.

A Plug-and-Play Quantum Security Layer

QSE enables organizations to secure their data today and into the quantum future — **without replacing existing systems.**



Quantum-Resilient Encryption

QSE adds a future-ready encryption layer to existing infrastructure, strengthening post-quantum cryptography with independently truly random QNRG physical entropy.



Comprehensive Data Protection

Safeguards data at rest, in transit, and fortifies identity and access systems.



Flexible Deployment

Delivered via API for enterprise integration or autonomous on-prem for high-security environments.



No rip-and-replace. No disruption. Immediate protection.



Differentiated by Design

Full Posture Platform



Combines assessment, automated discovery, migration simulation and remediation planning with deployable quantum-resilient security.

True Quantum Randomness



Leverages non-deterministic entropy sources to generate keys that are provably secure against even future quantum attacks.

On-Premise Capability



Offers autonomous, on-premises deployment options for critical infrastructure, ensuring full data sovereignty and regulatory compliance.

Plug-and-Play Integration



Seamlessly integrates into existing security frameworks, requiring no rip-and-replace of current infrastructure.

Positioned as core infrastructure, not merely a feature, providing foundational security for the quantum era.



Full-Lifecycle Quantum Security Platform

QSE helps organizations understand the problem, plan the migration and deploy quantum-resilient protection.



One platform spanning readiness, migration planning and deployable security - with multiple entry points into enterprise accounts.

Multiple Recurring Revenue Streams

QSE can enter through readiness and discovery, then expand customers into protection, identity, communications and recurring platform usage.



QPrime Assessments

Initial assessment fee + integration/onboarding + recurring reassessments and workshops.

Malaysia model: two regional readiness workshops per year through 2039.*



Enterprise Deployments

QRek integration and deployment revenue, including remote and autonomous on-premise implementations.



Platform Usage

QAuth, QSEaaS and QWire subscriptions plus entropy, storage and usage-based consumption.



Hardware & Support

On-premise hardware sales, maintenance and future QHSM deployment opportunities for high-security environments.

Land through readiness. Expand into protection, identity, communications and recurring infrastructure usage.

*Management commercial model; subject to customer contracts and applicable regional requirements.

Expanding Customer & Partner Base

Providing clear near-term revenue visibility with significant long-term upside potential.

POS Digicert

NEXTWAVE



Commercial Base

- Revenue-generating enterprise deployments
Expansion opportunities within existing accounts

ENZO PLUS+

fm
FIRST MAJESTIC
SILVER CORP.

netexperts
DESDE 1989

Pipeline Development

- Tens of millions in identified client opportunities
- POS DigiCert channel into Malaysia digital-trust / NCII readiness ecosystem
- Nextwave expands QSE distribution in Thailand
- Additional regional channels under development

nnp NUSA
NETWORK
PRAKARSA

porta



The Muthoot Group

software
COGITO

CYBER QUANTA

coegi

Nacha

Partner-led distribution provides a scalable route into regulated markets while creating multiple paths to recurring revenue.

*Pipeline represents prospective opportunities, not contracted or recognized revenue.

Partner-Led Global Expansion

QSE is accelerating its global reach through **strategic partnerships and targeted sales initiatives**, ensuring efficient market entry and scalable distribution.

Value-Added Distributors

Leveraging established networks across APAC, EMEA, and other key regions for broad market penetration and localized support.

Direct Enterprise & Government Sales

Cultivating high-value relationships with large enterprises and government entities through direct engagement and specialized teams.

Regulated Industry Focus

Prioritizing sectors with urgent compliance needs, such as finance, healthcare, and defense, where quantum security is paramount.

This multi-pronged approach allows QSE to rapidly scale its footprint while addressing critical security mandates in diverse global markets.



NFP & Industry Ecosystem

Positioning QSE as a post-quantum readiness voice across policy, public-interest cyber, defence, and trusted validation.

QSE is building influence where PQC policy, education, regulated buyers, and third-party credibility intersect.

Policy & Standards Access

PTPKM • PEKOM • NUMANA* • QASECDEF*

Early visibility into regulatory language, market requirements, and ASEAN quantum-readiness priorities.

**Planned / shortly pending memberships.*

Public-Interest Cyber Credibility

Malware Village • World Cyber Health

Education-first channels that position QSE as a contributor to cyber resilience, not only a vendor.

Defence & Government Reach

CADSI • MISA

Canadian representation and trusted access points for regulated public-sector and critical-infrastructure audiences.

Validation & Market Enablement

SITG

Supporting validator for workshops, speaking engagements, and buyer-confidence building.

Outcome: stronger regulatory alignment, credible public-sector positioning, and a repeatable workshop-led path into PQC readiness programs.

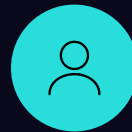
Building a Scalable Revenue Base

QSE's early commercial success provides a robust foundation for rapid expansion and market leadership in the post-quantum era.



262 Enterprise Customers

Demonstrating established market demand and integration.



102,000+ Active Users

Across diverse global markets, highlighting broad acceptance and operational utility.



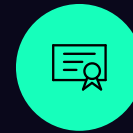
Global Deployments

Active presence in 4 regions and 13 countries, including Asia, Europe, and the United States.



14 Commercial Partners

Strategic alliances expanding reach and accelerating market penetration

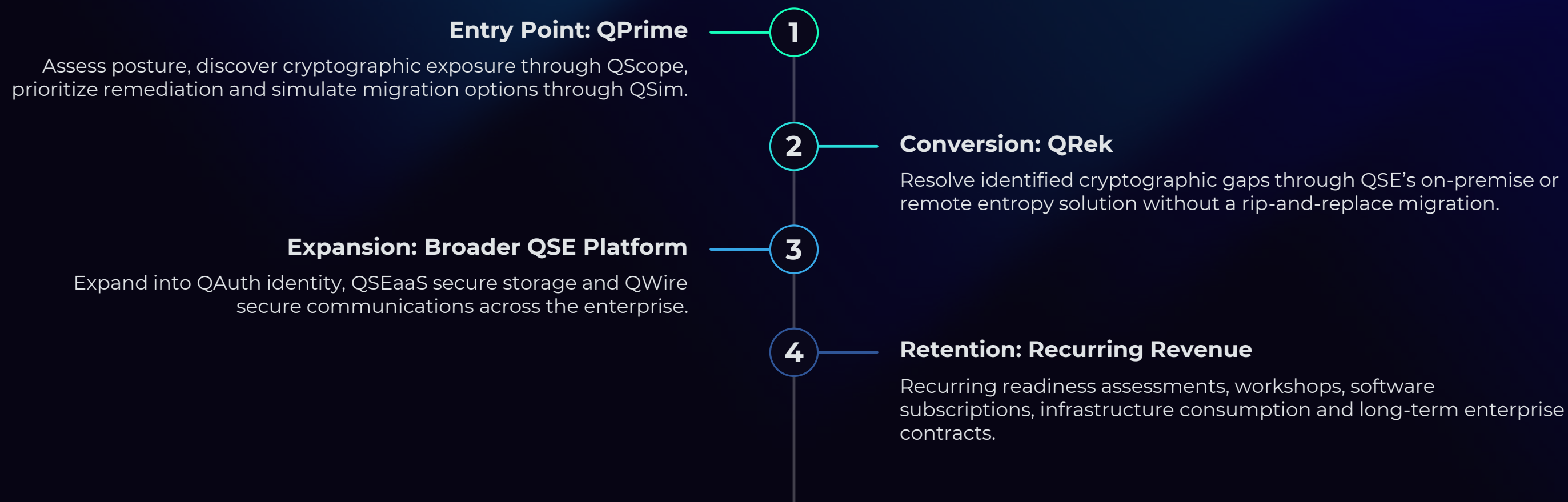


Government Certifications

Key approvals enable access to high-security contracts and critical infrastructure projects.

Designed for Expansion

QSE's customer engagement model is built to move organizations from readiness into deployment and recurring platform usage.



QPrime identifies the problem; QSE's broader platform creates the opportunity to solve it and expand within the account.

Industry-Leading Certifications & Patents

QSE's technology and processes are rigorously validated, meeting the highest global standards for quantum-safe security and data protection.



Global Compliance Frameworks

Alignment with critical standards and frameworks including NIST SP 800-22, SP 800-53 and SP 800-57; FIPS 140-3; and ISO/IEC 15408, 14888, 18033-8 and 20543.



Data Security Assurance

Certified SoC2 Compliant (SSO) and HIPAA Compliant, providing robust data privacy and security for sensitive information across industries.



International Recognition

CyberSecure Canada Level 2 certification supporting access to higher-security government and public-sector opportunities.



Extensive Patent Portfolio

11 patent cases submitted covering QSE's entropy technology and quantum-readiness assessment features.

Our QSE Entropy technology has been independently verified by recognized global standards evaluators including NIST and DIEHARDER, underscoring its foundational strength.

Valuation Disconnect

Despite operating in one of the fastest-emerging areas of cybersecurity, QSE trades at a substantial discount to several higher-valued quantum-security peers.

Company	Ticker / Market	Relevance	Revenue source	Approx. market value	LTM revenue	Market cap / LTM revenue
Quantum Secure Encryption Corp.	CSE: QSE / OTCQB: QSEGF	Post-quantum security posture, migration planning, entropy, identity & secure data	PQC resiliency platform	~C\$44M	~C\$310K	~141x
Quantum eMotion	TSXV: QNC / NYSE: QNC	Canadian quantum cybersecurity / QRNG peer	QRNG / quantum security	~C\$522M	~C\$23K	~22,500x
01 Quantum	TSXV: ONE	Canadian quantum-safe cybersecurity / post-quantum migration peer	Services / engineering	~C\$48M	~C\$1.60M	~30x
Arqit Quantum	NASDAQ: ARQQ	Quantum-safe encryption / cybersecurity peer	Encryption software / services	~US\$354M	~US\$1.09M	~325x

The opportunity is that even a partial narrowing of the valuation gap could represent significant upside as QSE continues converting customer traction, partner relationships, and pipeline opportunities into recognized revenue.

Experienced Leadership Across Technology & Capital Markets

Our leadership team brings deep, multi-disciplinary expertise across cybersecurity, enterprise software, and capital markets, with a proven track record of scaling technology platforms and executing public market strategies.



Ted Carefoot, CEO

Over 20 years leading high-performance product teams, with expertise in AI-driven cloud, digital security, risk management, and software product development. Previously Development Director at EA.



James Young, Director

Seasoned entrepreneur and executive with 25+ years across telecom, print/digital publishing, digital advertising, and software development.



Michael Massing, CTO

Technology executive with 30+ years in cybersecurity, cryptography, AI and advanced computing, including senior roles at Dell SonicWall, TokenX Labs and LifeSite. He holds eight issued patents and experience supporting NASA's SETI initiatives.



Darien Lattanzi, Director

Experienced business associate in junior venture markets (exploration, mining, crypto, cannabis, tech) with active involvement in capital raises exceeding \$70,000,000.



Alan Tam, CFO & Director

Senior executive with over 20 years of experience in structuring, planning, and executing IPOs, RTOs, and CPCs.



Shoukri Kattan, Director

20+ years of experience spanning startups and enterprises in AI, MedTech, and digital health, bringing technology innovation and market strategy expertise.

Strong Capital Structure

Quantum Secure Encryption Corp. maintains an efficient and robust capital structure, providing stability and flexibility for future growth initiatives.

Ticker	CSE:QSE OTCQB:QSEGF FSE:VN80
Share Price (September 8, 2026)	\$0.53
Issued and Outstanding Shares	81,519,445
Warrants	12,137,586
Options & RSU	6,379,333
Fully Diluted Shares	100,036,364
Market Capitalization (September 8, 2026)	C\$43,205,306

✔ **+7.0 Million in Cash | Zero Debt ***

* As at August 31, 2026

Key Investment Highlights

Quantum Secure Encryption Corp. presents a compelling investment opportunity at the forefront of the quantum cybersecurity revolution.



Pioneering Cybersecurity Segment

Positioned in a rapidly emerging cybersecurity segment driven by the imminent risks posed by quantum computing.



Full Posture Platform

Addresses the transition from assessment and automated discovery through migration planning and deployable quantum-resilient protection.



Commercial Revenue Base

Revenue-generating enterprise deployments provide an established base as QSE expands through new partner and regulated-market channels.



Addressing an Immediate Problem

Offers a vital solution as governments and enterprises proactively prepare for new quantum-safe security standards.



Growing Global Customer Base

A rapidly expanding customer base with active enterprise deployments across multiple key regions worldwide.



Large Qualified Pipeline

Growing enterprise and government opportunities provide significant potential for conversion into assessments, migration work and broader platform deployments.



CSE: QSE | OTCQB: QSEGF | FSE: VN80