ISIDORE
QUANTUM

Isidore Quantum® is like LTE. It works everywhere, is already deployed, and meets real-world demands right now.

Isidore Quantum® vs. Quantum Key Distribution (QKD)

In the race for **quantum-era dominance**, Isidore Quantum wins on:

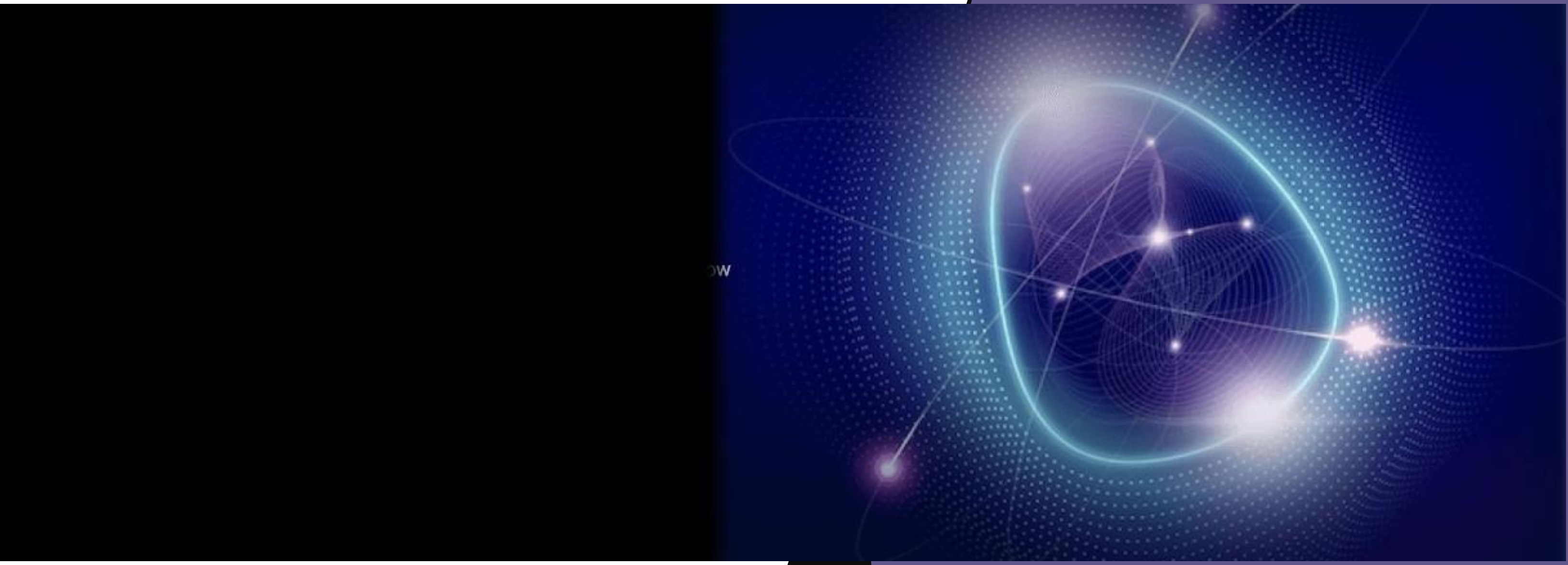
- **Ubiquity**: No infrastructure overhaul required.
- **Speed to Market**: Already deployed in air, land, sea, and space.
- **Resilience**: Hardware-secured, AI-adaptive, and built to scale.

The cybersecurity threat landscape is moving fast toward a post-quantum reality. As nation-state actors carry out "Harvest Now, Decrypt Later" campaigns, waiting for QKD infrastructure to catch up creates real and immediate risk.

Isidore Quantum is a field-tested, CNSA 2.0-compliant encryption platform co-developed with the NSA. It offers scalable, post-quantum protection without the need for new fiber or complicated certificate management. Unlike QKD, which relies on delicate optical systems and cannot function effectively in mobile or edge environments, Isidore delivers protocol-agnostic, zero-trust encryption that works across cellular, satellite, space, and operational technology (OT) networks.

From a cryptographic standpoint, QKD is based on quantum entanglement and Heisenberg's uncertainty principle, allowing for theoretically unbreakable key exchanges, but only if the quantum channel remains perfectly secure. That same dependency on fragile infrastructure limits its usefulness beyond controlled, stationary deployments. Isidore takes a more practical approach. It uses post-quantum cryptographic algorithms. CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium for digital signatures. both endorsed by NIST and adopted in the NSA's CNSA 2.0 suite. These algorithms are supported by an AI-driven rules engine that automatically detects anomalies, initiates a cyber immune response, and rekeys or zeroizes in real time. The result is a system that is not only quantum-resistant, but also intelligent, adaptive, and operational today.

Contents



For CISOs, the message is clear. Waiting for QKD is a gamble on a brittle, fiber-dependent future that may never scale beyond controlled lab environments. Meanwhile, the attack surface continues to grow, and the timeline to quantum risk keeps getting shorter. Isidore Quantum offers a decisive, compliant, and cost-effective solution today. Organizations that move early will not only strengthen their infrastructure, they will gain a first-mover advantage in post-quantum resilience. The next breach will not wait for QKD. Your security stack should not either.

QKD remains largely academic. While it can function in tightly controlled environments, it is unlikely to scale commercially before quantum-era threats become a mainstream reality.

Feature	Isidore Quantum® (VHS)	QKD Solutions (Betamax)
Deployment Flexibility	Operates over wireless, fiber, SATCOM, CAN Bus, MIL-STD-1553, and Ethernet. Ideal for mobile, disconnected, and tactical environments.	Requires dedicated fiber optic networks. Not viable for mobile or low-power deployments.
Form Factor	Compact, credit card-sized hardware (350g). Power efficient (7–10W), deployable at edge and in space (e.g., CubeSats, drones, ships).	Large, fixed systems with specialized receivers. Power-intensive and difficult to deploy.
Scalability	Supports mesh, point-to-point, and hub-and-spoke configurations. Ephemeral keying makes each node cryptographically independent.	Hard to scale. Each connection requires line-of-sight quantum channels. No dynamic rekeying.
Key Management	Fully autonomous key lifecycle. No PKI or KMI. No certificates. Self-rekeys and zeroizes when tampered.	Centralized control. Requires trusted setup and classical authentication. Prone to side-channel attacks.
Cost & TCO	$1,600–$10,000 per device. Optional SaaS ($368–$500/month). Up to 60 percent lower total cost of ownership.	High upfront and ongoing costs due to fiber and optical hardware. Requires expert integration teams.
Regulatory Compliance	No ITAR or EAR restrictions. Built from commercial off-the-shelf parts. Compliant with NSA CNSA 2.0.	Restricted for export. Often delayed by national security review processes.
Threat Model Adaptability	AI-powered anomaly detection, self-healing, and rule-driven automation. Cyber immune response trained on 8 trillion signals from Microsoft.	Static. No built-in anomaly detection or real-time mitigation.
Industry Adoption	Pipeline of over 150,000 units across land, sea, air, and space. Plug-and-play ready across domains.	Limited to research labs or specialized government sites. Minimal commercial traction.

The readiness gap is clear.

Isidore Quantum consistently outperforms QKD across every category that matters: deployment speed, cost, mobility, and adaptability.

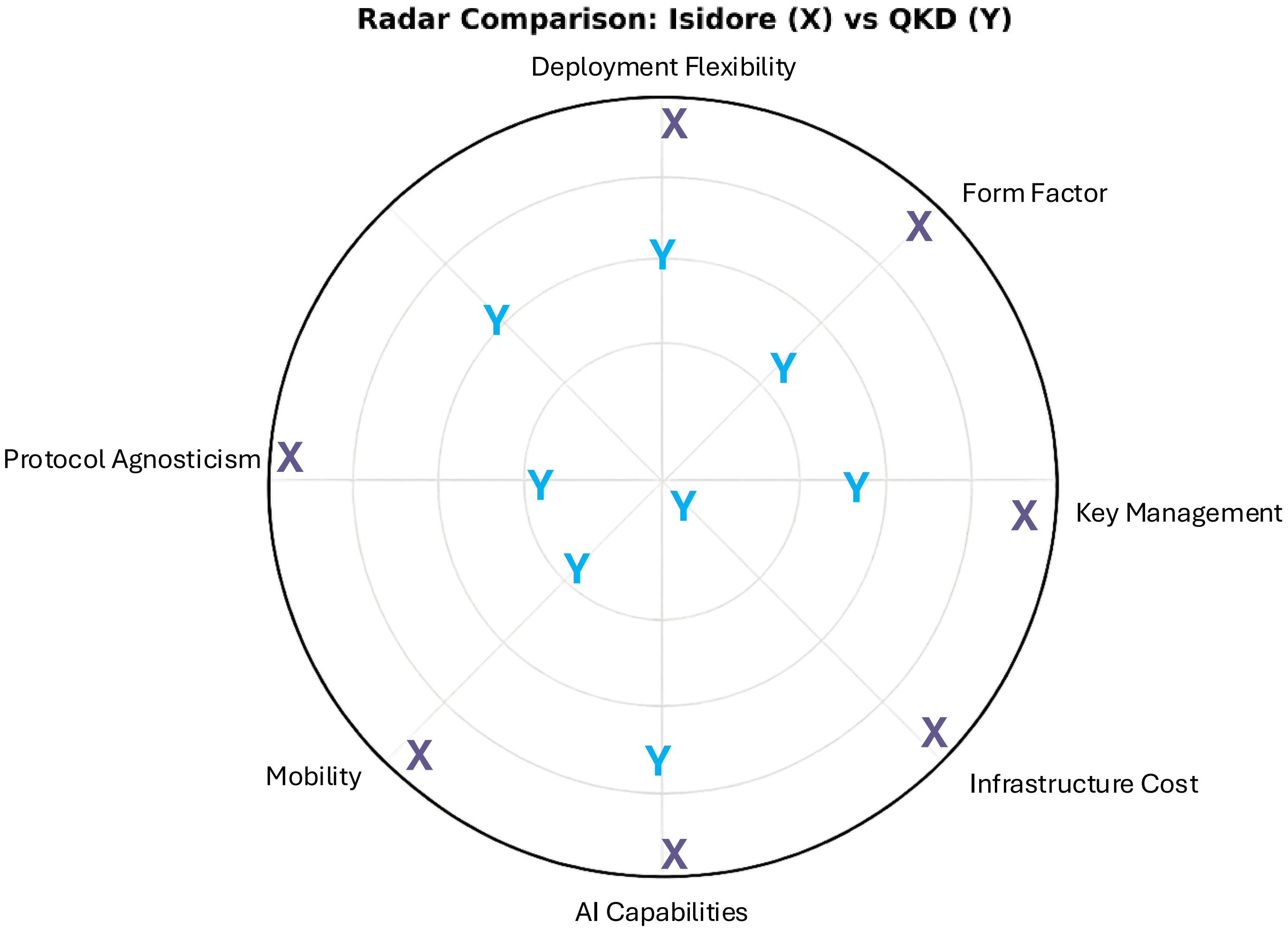
While QKD can take months to install and millions to implement, Isidore is plug-and-play, deploys in minutes, and draws just 10 watts of power. It is already in use across defense and telecom networks, validated in orbit, and operational in active military environments.

Two paradigms are emerging in quantum-safe cybersecurity. On one side is Isidore Quantum, a CNSA 2.0-compliant, AI-enhanced platform built for scale and deployment today. On the other is QKD, still locked behind physical limitations, fragile infrastructure, and narrow use cases.

Isidore Quantum represents a shift in encryption architecture built for real-world deployment. Designed to operate across air, land, sea, and space, its compact, low-SWaP (Size, Weight, and Power) form factor and protocol-agnostic design make it highly adaptable to a wide range of environments. Unlike QKD, which depends on dedicated fiber optic infrastructure for photon-based key exchange, Isidore Quantum works over standard communications channels. These include IP, Ethernet, SATCOM, MIL-STD-1553, and wireless links. This flexibility allows it to function in mobile, disconnected, and adversarial settings where QKD cannot be deployed. Its plug-and-play configuration supports rapid setup without the need for major infrastructure changes, setting a new standard for field-ready cryptographic resilience.

Technology Radar

The following radar chart illustrates the comparative capabilities of Isidore Quantum versus traditional Quantum Key Distribution (QKD) solutions across key performance and deployment metrics.



While QKD aims to offer secure key distribution, it still depends on classical communication channels and is vulnerable to man-in-the-middle and infrastructure-level attacks. QKD also lacks dynamic key lifecycle management and often requires manual oversight or trusted intermediaries. Isidore Quantum solves these issues through ephemeral keying and autonomous lifecycle control. It does not require a Public Key Infrastructure, Key Management Infrastructure, or any human input. The system automatically rekeys and zeroizes in response to detected threats.

This level of independence is reinforced by a zero-trust architecture. No node or device is implicitly trusted, and all access is continuously verified. This eliminates many of the traditional failure points found in manual or centralized systems.

Scalability and economics reveal the divide between theory and deployment

QKD systems require significant capital investment in custom optics, amplifiers, and dedicated fiber installation. These costs, combined with high complexity and limited scalability, have kept QKD largely confined to academic labs and a few specialized government installations. Isidore Quantum is priced between $1,600 and $10,000 per device, depending on configuration. A SaaS model is also available, ranging from $368 to $500 per month. Its total cost of ownership is up to 60 percent lower than traditional systems. Because Isidore uses commercial off-the-shelf components and is free of ITAR and EAR export restrictions, it can scale globally with greater speed and flexibility. This positions it to meet growing demand in a post-quantum security market projected to reach $1.2 trillion by 2027.

Isidore Quantum is already active in real-world operations. It has flown aboard SpaceX's Transporter-13 mission, been integrated into DARPA's NOMARS autonomous vessel, and completed testing across 23 pilot programs with telecom and defense leaders. These results confirm that Isidore is resilient, adaptable, and ready for deployment in diverse mission-critical environments. QKD remains mostly theoretical beyond small-scale fiber deployments between data centers. It is not suited for use in mobile or disconnected environments, and its reliance on environmental stability makes it vulnerable to optical tampering and difficult to operate in defense or infrastructure-critical settings.

Isidore Quantum is like LTE. It is not the most exotic technology, but it is practical, scalable, and already changing how systems secure data. It works across existing infrastructure, adapts to varied use cases, and is built to meet today's demands. QKD is more like Google Fiber. It sounds ideal on paper but remains locked behind fragile infrastructure and narrow deployment scenarios. Where Isidore removes the limitations of PKI and certificate management, QKD tries to solve them with quantum mechanics while introducing fragilities of its own.

Isidore Quantum is a tested, AI-enhanced, hardware-secured platform that closes the operational gaps QKD cannot. It delivers on the core needs of post-quantum protection — scalability, resilience, and cost efficiency — all in a package that is deployable now.

QKD is still waiting at the starting line. Isidore is already on the field. If you need quantum-grade security that works today, this is your answer.

Purpose-built for dual-use and broad adoption, Isidore Quantum delivers enterprise-grade scalability across a range of form factors and mission-critical environments. It gives organizations the ability to act now, not later.

Air	Land	Sea	Space
US Air Force, US Navy	US Air Force, US Army	DARPA, US Navy	Air Force, National Science Foundation, US Space Force

Contact Us:

Brandon Chapman
Brandon@Forwardedge.ai

Appendix A

Acronyms

AES	Advanced Encryption Standard CQTS Cross-Quantum Technology Systems
CRQC	Cryptoanalytically-Relevant Quantum Computer CSfC Commercial Solutions for Classified
HiPS	High-Performance Superconducting Qubit Systems HNDL Harvest Now, Decrypt Later
LPS	Laboratory for Physical Sciences LWE learning-with-errors
NEQST	New & Emerging Qubit Science & Technology NIST National Institute of Science and Technology NQCO National Quantum Coordination Office
NSA	National Security Agency NSS National Security Systems
PKI	Public-key Infrastructure, asymmetric encryption scheme, two different keys are used to encrypt/decrypt PQC Post-Quantum Cryptography
PSK	Pre-shared key, symmetric encryption scheme, same key is used to encrypt/decrypt QC Quantum Computer
QCISS	Quantum Characterization of Intermediate-Scale Systems QIS Quantum Information Science
QiS	Qubits in Silicon Program
QR	Quantum-Resistant (algorithms)
QRC	Quantum-Resistant Cryptography
SHiFT	Stable High Fidelity Trapped Ion Systems SIS short integer solution

.