FORWARDEDGE

OCTANS SPACE AFRICA

White Paper

Isidore Quantum®

All-in-One Cybersecurity and Drop in PQC Solution

Securing the Final Frontier: Cyber and Quantum Resilience for Space Infrastructure.

Why Isidore Quantum:

High-Throughput Performance: Delivers high throughput encryption with low latency

Ultra-Low SWaP-C: Delivers high assurance encryption under 8 watts for space-constrained platforms

Autonomous Keying: On-orbit rekeying and self-healing security without ground intervention, certificates, PKI, or signatures

AI-Driven Defense: Predicts, detects, and mitigates cyber threats in real time across fleet networks

Global dependence on satellites for communication, navigation, intelligence, and commerce has turned space into the backbone of modern infrastructure and the next critical front in cybersecurity. As orbital networks continue to grow, vulnerability to cyber intrusion, data manipulation, and supply chain compromise has expanded rapidly. Many space systems still rely on outdated encryption protocols such as RSA and ECC, which will become ineffective once quantum computers reach full operational capability. Nation-state adversaries are already preparing for that moment through Harvest Now, Decrypt Later (HNDL) campaigns, capturing encrypted satellite communications today for future decryption and weaponization. The merging of conventional cyberattacks with the approaching quantum decryption threat endangers not only individual missions but entire constellations and command networks, placing global communications, defense systems, and commercial space infrastructure at serious risk. Failing to act no longer represents strategic patience but a countdown to inevitable compromise.

The Isidore Quantum space family, which includes Space COMSEC, the High Throughput Space Router (HTSR), and the High Throughput Space Crypto (HTSC), delivers a unified and quantum-resilient cybersecurity solution engineered specifically for the space domain. Developed in collaboration with the NSA and fully aligned with CNSA 2.0 standards, the system provides AI-driven, zero-trust, post-quantum encryption across every layer of space communication—from satellite-to-satellite links and on-orbit data routing to ground command interfaces. Designed for low Size, Weight, Power, and Cost (SWaP-C) with plug-and-play integration, each component functions autonomously with real-time anomaly detection, cryptographic self-healing, and quantum-random key generation. Proven through testing with the U.S. Space Force, NASA, and defense partners, the Isidore Quantum® suite equips operators to secure vital orbital assets, safeguarding current missions while reinforcing the next generation of space infrastructure against future quantum threats.

The Situation

60%	98%	70%	$500B
Satellite operators reported attempted or successful cyber intrusion	Active satellites rely on RSA or ECC encryption	Ground stations interface with public networks lacking segmentation	Global economic value derived from satellite-based communications

The space domain, once considered a technological sanctuary, has become one of the most contested and digitally vulnerable environments in modern defense and commerce. Satellites, launch systems, and ground control networks enable global communications, Earth observation, GPS navigation, defense reconnaissance, and missile warning. Despite their importance, many of these systems depend on outdated encryption, weak trust architectures, and unmonitored data flows designed for operational reliability rather than cybersecurity resilience.

Isidore Quantum®: All-in-One Cybersecurity PQC Solution

Isidore Quantum represents a next-generation cybersecurity and post-quantum encryption ecosystem designed to safeguard the global space enterprise from both current and emerging threats. The system includes Space COMSEC, the HTSR, and the HTSC, delivering zero-trust, CNSA 2.0-compliant protection for satellites, ground stations, and cross-domain networks. Each module integrates AI-powered anomaly detection, autonomous key management, and quantum-random encryption to counter real-time cyber intrusions and future quantum decryption. Lightweight, power-efficient, and proven through collaboration with the U.S. Space Force and NASA, the Isidore Quantum® Space Family enables resilient, quantum-secure communications from orbit to ground, reinforcing the backbone of modern space infrastructure.

Each system shares a CNSA 2.0-compliant, AI-enhanced core capable of autonomous operation, post-quantum cryptography, and self-healing defense against evolving threats.

Capability	Mission Impact
CNSA 2.0-Compliant Encryption	Meets NSA standards for post-quantum resilience and cross-domain security
Zero-Trust Architecture	Ensures devices only communicate when cryptographically paired—no implicit trust
AI-Driven Defense	Predicts, detects, and mitigates cyber anomalies across satellite fleets in real time
Autonomous Key Management	Eliminates PKI and operator overhead with on-orbit self-rekeying
Red/Black Isolation & Quantum Entropy	Hardware-enforced segmentation + Quantum Random Noise Generation for provably random, one-time keys
Plug-and-Play Integration	Drop-in retrofit—no redesign required for satellite buses or ground stations

Unified Advantage

The Isidore Quantum space family unifies post-quantum encryption, zero-trust networking, and AI-driven defense into a single, mission-ready ecosystem for space infrastructure. By combining CNSA 2.0–compliant cryptography, autonomous key management, and real-time anomaly detection, it delivers self-healing, quantum-resilient protection across satellite constellations, ground stations, and cross-domain links. Its plug-and-play architecture enables seamless integration into existing systems, providing operators with immediate, scalable, and future-proof security against both today's cyberattacks and tomorrow's quantum threats.

Relying on AES-256 alone creates a dangerous illusion of safety. The cipher itself remains strong, but the scaffolding around it is already crumbling. Quantum algorithms will tear through key exchanges, side-channel attacks will siphon secrets in real time, and AI-driven exploits will adapt faster than any patch. Defenders who cling to "AES-256 is enough" risk guarding an empty vault while intruders walk through unseen doors. The era ahead demands more than brute-force resistance; it demands architectures built for resilience against quantum speed, physical leakage, and machine-intelligent adversaries.

Strategic Urgency On Orbit

The next major breach will begin in orbit, not on Earth. Adversaries have already infiltrated satellite networks, collecting encrypted data and identifying weaknesses in preparation for the day quantum computers make current defenses obsolete. Once that moment arrives, every command, image, and transmission ever sent could be exposed. The countdown to Q-Day has already started, demanding immediate action to maintain control of the skies.

Act now:

Cyber warfare has extended into orbit, and quantum computing is poised to overturn every existing assumption about space security. The Isidore Quantum space family, which includes Space COMSEC, HTSR, and HTSC, offers the first AI-powered, post-quantum, zero-trust architecture engineered for seamless integration throughout the space enterprise. Proven through testing with NASA, the U.S. Space Force, and the NSA, these systems provide quantum-safe, self-healing protection for satellites, constellations, and command networks across both military and commercial domains.

Isidore Quantum® Space COMSEC Device — a compact, radiation-hardened encryption module. Identical casing design used across the Isidore Quantum HTSR and HTSC family with size variations by function.

Variants and Specifications:

Specification	Space COMSEC	High Throughput Space Route	High Throughput Space Crypto
Size (mm), Weight (g) & Power (W)	~91 x 96 x 25 mm (3.6 x 3.8 x 1 in); 218 g (9 oz); ~5 W	~91 x 96 x 25 mm (3.6 x 3.8 x 1 in); 218 g (9 oz); ~5 W	~ 91 × 96 × 25 / 3.6 × 3.8 × 1, 220g, 10W
Primary Function	Quantum-resilient encryption and communications security for satellite command, control, and telemetry	Quantum-secure routing and switching for multi-satellite constellations and hybrid space networks	High-speed, post-quantum encryption for data-intensive and cross-domain space communications
Throughput	Up to 2 Gb/s secure data rate with <90 µs (estimated)	Up to 2 Gb/s with 10 µs forwarding delay; <1 ms total end-to-end delay	10 G/bs encryption with <10 µs forwarding delay; <90 µs (estimated)
Encryption Standards	CNSA 2.0–compliant (AES-256 GCM, ML-KEM), with integrated Quantum Random Number Generator (QRNG)	CNSA 2.0–compliant, with adaptive encryption across classified/unclassified domains, with integrated QRNG	CNSA 2.0–compliant, with integrated QRNG
AI-Driven Defense	AI-assisted threat detection and pattern recognition across data channels, and automated cyber response	AI-assisted threat detection and pattern recognition across data channels, and automated cyber response	AI-assisted threat detection and pattern recognition across data channels, and automated cyber response
Autonomous Key Management	Continuous on-orbit rekeying and self-healing security—no PKI, certificates, or manual loaders	Continuous on-orbit rekeying and self-healing security—no PKI, certificates, or manual loaders	Continuous on-orbit rekeying and self-healing security—no PKI, certificates, or manual loaders
Architecture	Zero-trust, protocol-agnostic; operates across Ethernet, SATCOM, and RF links; mesh, point to multi-point, and hub and spoke routing	Software-defined mesh and point-to-multipoint routing; VLAN-aware multi-domain segregation	Zero-trust, protocol-agnostic; operates across Ethernet, SATCOM, and RF links; mesh, point to multi-point, and hub and spoke routing

1. Specifications listed are subject to change without prior notice.

Contact: octans@inhub.world | forwardedge.ai | octanspace.com

Isidore-1: IoT/OT/SCADA

Isidore 50MB/s – 2 GB/s

One-Way-Data Diode

CubeSat

Enterprise

	50 Mb/s	480 Mb/s	1 - 2 Gb/s	10 Gb/s	68 Gb/s	1 Tb/s
Size, Weight & Power	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~7 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~10 W	~140 x 89 x 39 mm (5.5 x 3.5 x 1.5 in); 450 g (16 oz); ~12 W	Available Q3 2026	Available Q3 2026	Available Q4 2026
Environmental:	–40 °C to +85 °C; shock and vibration qualified					
Cryptography:	AES-256 GCM and ML-KEM					
Quantum Entropy:	Integrated Quantum Random Number Generator (QRNG) subsystem; validated per NIST SP 800-90 A/B/C and BSI AIS-31					
Topologies:	Point-to-point, point-to-multipoint, mesh, and hub-and-spoke; supports wired, wireless, and hybrid topologies					
Certifications and Compliance:	NSA CNSA 2.0, FIPS 140-3 (Level 3), NIST SP 800-90 A/B/C, BSI AIS-31, ECCN 5A002 (License Exception ENC)					
Latency:	<90 µs (estimated)					
Security Architecture	Hardware-enforced Red/Black separation with galvanic isolation; zero-trust, zero-touch operation; covert posture (no network announcements or responses to probes)					
Certifications and Compliance:	NSA CNSA 2.0, FIPS 140-3 (Level 3), NIST SP 800-90 A/B/C, BSI AIS-31, ECCN 5A002 (License Exception ENC)					
AI / Autonomy	Embedded AI engine trained for real-time anomaly detection, and self-healing response					
Management System:	Cassian™ for fleet orchestration, provisioning, telemetry, and policy governance across distributed deployments					

1. Specifications listed are subject to change without prior notice.

Contact: octans@inhub.world | forwardedge.ai | octanspace.com