FORWARDEDGE

OCTANS SPACE AFRICA

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

COMMERCIAL INTRODUCTION

Date: APRIL 2026

Forward Edge-AI, Inc. | Octans Space | www.octanspace.com | forwardedge.ai
POC: octans@inhub.world

PROBLEM: Organizations delay PQC adoption, leaving critical data exposed to today's breaches and tomorrow's quantum threats

- **Immediate Risk:** Current encryption is already vulnerable to advanced AI-driven and state-sponsored cyberattacks.
- **Harvest-Now, Decrypt-Later:** Adversaries are capturing encrypted data today for future quantum decryption.
- **Quantum Imminence:** Quantum breakthroughs may arrive sooner than expected—making delayed PQC adoption a critical liability.

> "There is nothing in our portfolio that is high assurance, low cost, easy to own, future proof, easy to certify, scalable to multiple form factors, and non-Controlled Cryptographic Item (CCI)"
>
> Andy White
> National Security Agency, June 2022

60%	$4.9M	80%	70%	<5
Global organizations experienced a data breach	Average cost of a data breach	Encrypted traffic can be captured and stored for future decryption	C-suite security leaders acknowledge they do not have a post quantum transition plan	Years before quantum computers can break RSA-2048 and ECC

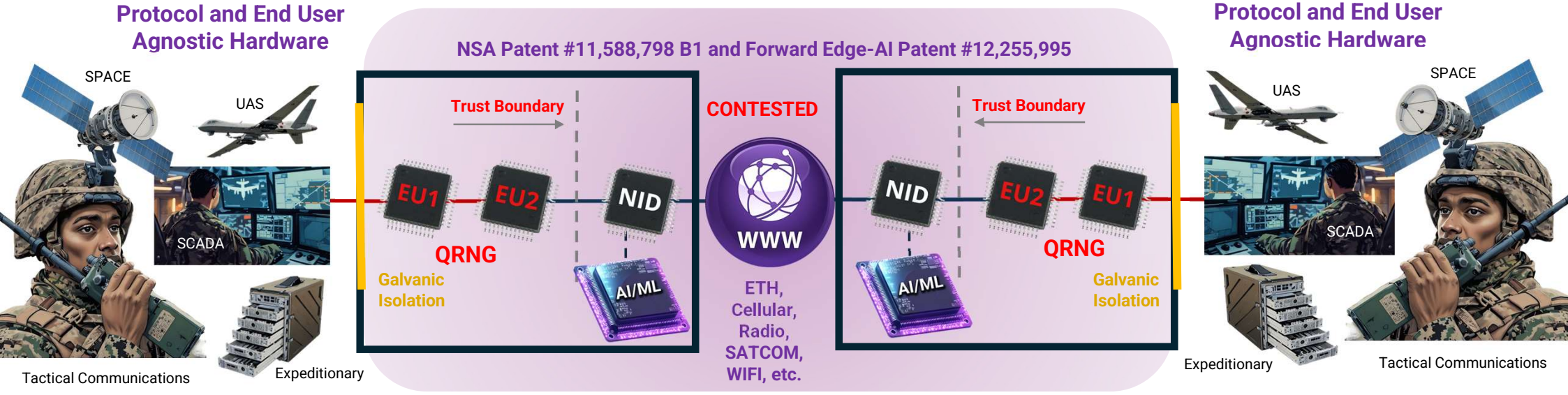
SOLUTION: Isidore Quantum®

Isidore Quantum® is an all-in-one cybersecurity and post-quantum encryption platform that unifies Zero-Trust defense, autonomous threat response, and future-proof cryptography in a single drop-in solution. Designed for commercial, government, and military networks alike, it safeguards critical data and communications against today's advanced cyberattacks and tomorrow's quantum threats—without requiring costly infrastructure changes:

- **Comprehensive Protection:** Unifies cybersecurity and post-quantum encryption in one scalable, turnkey solution
- **Future-Proof Security:** Defends sensitive data from today's AI-driven attacks and tomorrow's quantum decryption threats
- **Seamless Integration:** Installs easily into existing IT and cloud infrastructures—no costly redesign required
- **Autonomous Intelligence:** AI-powered monitoring detects and neutralizes threats in real time without human intervention
- **Cost Efficiency:** Reduces cybersecurity spend by up to 60% through unified protection and automated key management

How it Works

(point-to-point shown for simplicity)



Isidore is an NSA CNSA 2.0 compliant, quantum-safe encryption and cybersecurity device that safeguards data through secure hardware and a Zero Trust design, removing the need for traditional key infrastructures. Combining AES-256 encryption with ML-KEM, and Quantinuum's Quantum Random Number Generator (QRNG), the system produces truly unpredictable encryption keys. Operating at Layer 2, the device creates secure and flexible network links that support point-to-point, hub-and-spoke, and mesh configurations. The Network Interface Device (NID) enforces physical and logical red/black separation between trusted and untrusted zones, while built-in Artificial Intelligence (AI) monitors traffic, identifies threats, and adapts in real time to maintain mission continuity. Deployment occurs 70% faster and total cost of ownership is 60% lower than with conventional solutions, delivering a unified, quantum-resilient platform for defense and commercial use.

DIFFERENTIATION

Criteria	Isidore Quantum® - All-In-One	QKD	Software-Only PQC
Integration Costs	**~$700/mo per link** Drop-in, no re-architecture	**$100K+ per link** Requires dedicated fiber, optics, or satellites	**Low upfront, but hidden costs** In patching, latency, and management
Total Cost of Ownership (Over 5 years)	**60%** Less than legacy encryptors; OPEX-friendly	**Highest** Scale limited, cost grows exponentially with distance and nodes	**Moderate** Cheap to deploy, expensive to maintain due to patching & failures
Performance on Legacy Systems	**<0.5ms Latency** Works seamlessly with IPv4/IPv6, SCADA, radio, SATCOM	**Poor** Distance-limited; Incompatible with legacy and mobile systems	**Weak** Breaks performance on constrained / legacy hardware; adds latency
Security Risks	**Minimal** Hardware Red/Black isolation, ephemeral keys, AI-driven resilience	**Fragile** Breaks under physical disruption; Vulnerable to channel loss	**High** Large attack surface, side-channel risks, reliance on patching
Drop-in Suitability	**Excellent** Protocol / hardware agnostic; Plug in and secure immediately	**Poor** Requires custom fiber; Impractical beyond pilots	**Inconsistent across mixed networks** Despite good in theory
Mobile Access Readiness(1)	✓	✗	✗

(1) Isidore meets the requirements of NSA's CSfC Mobile Access Capability Package (MACP), describing how to protect classified mobile data in transit using approved cryptographic algorithms.

VARIANTS

Isidore 1 – SCADA/OT, IoT

Isidore 50 MB/s – 2 GB/s

One Way Data Diode

Isidore Quantum 1701 - Enterprise

	50 MB/s	480 MB/s	1 - 2 GB/s	10 GB/s	68 GB/s	1 TB/s
Size (mm), Weight (g) & Power (w)	~135 × 78 × 27 / 5.3 × 3 × 1, 270g, 8W			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:	<0.5 ms (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™ Fleet Orchestration Suite for provisioning, telemetry, and policy governance across distributed deployments					

23 SUCCESSFUL PROOF OF CONCEPT TESTS: Air, Space, Land, and Sea

VALIDATION: SCADA/OT – USAF PHASE 2 SBIR

- A quantum-resistant cybersecurity platform for ICS/SCADA, OT & IoT environments (US Air Force 688th Cyberspace Wing)
- Enables zero-trust enforcement, end-to-end encryption, role-based access at the physical layer without depending on PKI
- Supports hot-patching, ML anomaly detection, and secure firmware updates without disrupting operations
- Integrates OT-aware analytics with SIEM for correlated security insights across IT/OT domains
- Designed to counter “Harvest Now, Decrypt Later” (HNDL) threats and future quantum attacks

FLC
Fede a Laberstory Consortium
Tor Technology-Tansfer

TECH | SBIR AUTONOMY
WINNER

AFWERX
CHALLENGE

SPACE: USAF AND USSF PHASE II SBIRS

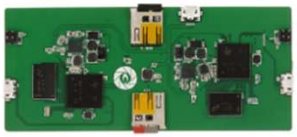
- **Isidore Quantum** was selected as the backbone for the the *High-Throughput Space Router* that embeds quantum-resistant routing into LEO constellations (US Space Force Proliferated Warfighter Space Architecture (PWSA))
- **Isidore Quantum** was selected as a high-throughput, *cross-domain, point-to-multipoint* cryptography device for PWSA
- **Isidore Quantum** is currently on-orbit in a US Air Force Space Communication Security (Space COMSEC) proof of concept

BACKGROUND/HISTORY: NSA Origins as a Secure Phone for the President of the United States

The Protocol Free Encrypting Device (PFED) was developed by the NSA to create a secure, protocol-independent communication system that protects the President's voice and data without relying on complex PKI or VPN infrastructures. Designed for simplicity and modularity, PFED uses commodity hardware in a unique architecture that achieves high-assurance security and meets CNSA 2.0 standards. By separating encryption from network protocols, PFED removes vulnerabilities found in software-based post-quantum transitions and provides a resilient, drop-in solution for national leadership and defense operations. Key advantages of PFED include:

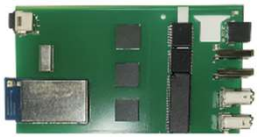
- **CNSA 2.0 Compliance**
- **Protocol Agnostic "Drop-In" Design**
- **Minimal Attack Surface**
- **Autonomous Key Management**
- **Commodity Hardware Integration**
- **Non-Controlled Cryptographic Item (Non-CCI)**

INVENTED BY THE NSA AND BACKED BY 3 YEARS OF USAF AND USSF FUNDED RDT&E: TRL 8 in 2024



TRL 2 - PFED
(2018 - 2020 NSA)

- Beagle Bone & Raspberry Pi modules
- F35, sUAS, REAPER, Tests
- CYBERCOM tests
- NSA OT/SCADA installation/test

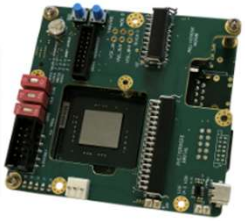


TRL 3 - Isidore
(2022 CRADA)

- Simple ARM processor
- USB, ETH, WIFI interfaces
- Lab-based simulations and tests
- NSA receives patent for PFED

TRL 6 - Isidore
(2023 Phase I SBIRs)

- Upgraded ARM processor
- USB, ETH, WIFI interfaces
- 1,000(+) structured stakeholder interviews
- 50 Mb/s throughput
- Smartphone, expeditionary comms. Tests
- Lab-based simulations and tests
- Lab-tests (Lumen)



TRL 7/8 - Isidore
(2024 Phase II SBIRs)

- Space COMSEC version
- 100 Mb/s throughput/new processor
- PWSA high throughput space crypto award
- PWSA high throughput space router award
- Radiation hardening
- Award of Air Force CSO
- AFGSC and Army Challenge Wins
- AFSOC, AFNWC, Idaho Labs, Lumen, MITRE, CACI tests
- **Achieved TRL-8 December 2024**

TRL 8 - Isidore
(2025 Phase II SBIRs)

- CubeSat launched
- FCC testing
- FIPS 140-3
- Serial and radio interfaces
- Bank, Maritime, Power, Taiwan POCs
- New Neuromorphic Processor (800 Gb/s throughput)
- Forward Edge-AI receives multiple patents
- FLC award winner
- US Army smaller SWaP-C
- Special Customer

TRL 8+
(Private Capital)
(2025/2026)

- Taiwan NSB purchase
- NOMARS and Stiletto
- VITA 46.XX standard bus for JADC2/ ABMS
- **CSfC (planned)**
- **High Assurance (planned)**
- Neuromorphic Processor
- 1Tb/s throughput
- Japan IPA install
- 50 maritime ships

CNSA 2.0 ALGORITHMS: Practical Tradeoffs and Legacy System Risks

AES-256 GCM remains the cornerstone of CNSA 2.0, offering a proven, quantum-resistant, and low-risk encryption baseline that is already well integrated into DoD and NATO systems. ML-KEM and ML-DSA are critical for post-quantum migration but introduce significant performance and integration challenges for legacy infrastructure. LMS/XMSS is well-suited for firmware signing, while SPHINCS+ is impractical, underscoring that AES anchors current security while PQC provides the necessary resilience against future quantum threats.

Algorithm (CNSA 2.0)	Error Rate	Bandwidth Impact	Cost to Implement	Impact on Legacy Infrastructure	Key Takeaway
ML-KEM (Kyber) – Key Exchange	Negligible ($\approx 2^{-165}$ to 2^{-175})	Mid (~1–1.5 KB per handshake, larger than ECC but manageable)	Mid (firmware/lib updates, no HW accel in old gear)	Mid – may break MTU/buffer limits, slows on radios/routers without accel	Most practical PQC KEM; efficient but heavier on legacy buffers/CPU.
ML-DSA (Dilithium) – Signatures	None (deterministic)	High (signatures 3–5 KB vs. ~64B ECDSA)	High (smart card/embedded refresh; HW+firmware upgrades)	High – cert chain bloat, storage/bandwidth stress, slow verify on constrained devices	Standard PQC signature; strong but heavy footprint on legacy PKI.
LMS/XMSS – Hash-Based (Firmware/Code Signing)	None (hash-based; risk in state tracking)	Low–Mid (multi-KB signatures; rare use only)	Mid (state management procedures needed)	Low–Mid – acceptable since used rarely; lifecycle/key tracking must change	Best for firmware/code signing; manageable overhead if lifecycle controls enforced.
SLH-DSA (SPHINCS+) – Hash-Based (Stateless)	None (hash-based)	Very High (8–50 KB signatures; 30–50× larger than ECC)	High (CPU/memory cost; slow verify)	High – overwhelms radios/networks; impractical on legacy systems	Secure but impractical; excluded from CNSA 2.0 NSS use.
AES-256 GCM – Symmetric Encryption (Classical, CNSA 2.0 approved)	None (deterministic)	Low (fixed block size, negligible overhead vs. PQC)	Low (libraries widely available; HW accel common)	Low – already deployed in most DoD/NATO systems; strong HW support	Quantum-resistant symmetric cipher; “gold standard” for TS data, efficient with HW accel; resource limits only matter on very constrained HW.

SOFTWARE ONLY APPROACHES:

Unacceptable Risks

Software-only encryption is inexpensive upfront but performs poorly on legacy tactical systems, introduces latency, and carries high security risk due to weak red/black isolation and side-channel exposure. Hardware-only solutions deliver high throughput, low latency, and strong physical isolation, but at greater procurement and handling costs. Hybrid approaches, such as PFED, balance performance and security with COTS/commodity components, making them the most practical drop-in choice for modernizing tactical edge systems under CNSA 2.0.

Solution Type	Performance on Legacy Systems	Integration Cost / Risk	Security Risks	Drop-In Suitability
Software-Only	Speed tied to CPU power; legacy HW = poor performance and high latency	Low cost (software install), but high risk of integration issues and heavy CPU load	No red/black isolation; OS/app bugs or side-channels break security	Poor – requires installs everywhere, not transparent
Hardware-Only	ASIC/FPGA can run at line rate, but very expensive; not patchable if ASIC	High procurement and certification cost; new device required	Strong isolation but fixed-function hardware limits flexibility; accelerators tied to host offer no isolation	Good – true inline encryptor, but costly and rigid
Hybrid (e.g., PFED/ Isidore)	Up to ~500 Mbps on commodity HW; optimized for tactical edge	Moderate cost; easier integration than Type-1; patchable with commodity parts	Enforces physical red/black separation with independent processors; resistant to side-channels; auto rekey/zeroize built-in	Excellent – plug-and-play, protocol-agnostic, minimal changes needed