Octans Space Africa (OSA)

In partnership with Forward Edge-AI, Inc.

Isidore Quantum®

The First All-Domain, Quantum-Resistant Encryption Platform – From Space to Server Rack

Born from NSA ingenuity, raised by Forward Edge-AI. Scalable for the Free World.

SECTION 1

The Problem

- **“Q-Day” is fast approaching**
  - Quantum computers will instantly break today’s encryption systems
  - By 2026, asymmetric encryption will be vulnerable to classical computers operating in tandem
- **State-of-the-art encryption (PKI, RSA, ECC) cannot protect critical systems**
  - Defense, finance, energy and healthcare all vulnerable
- **Export controls will severely limit global access to most solutions**

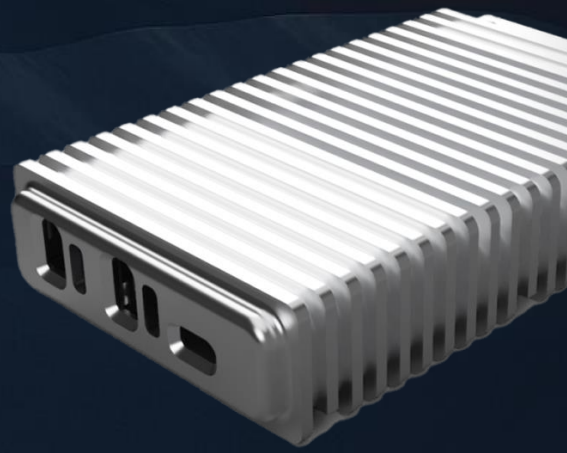
> **“There is nothing in our portfolio that is high assurance, low cost, easy to own, future proof, easy to certify, scalable to multiple form factors, and non-Controlled Cryptographic Item (CCI)”**
>
> Andy White
> National Security Agency, June 2022

56%	200	20 billion	$5.56 million
Organizations experienced a security breach in 2024	Average number of days it took organizations to recover from a cybersecurity breach	Quantum-resistant devices the National Institutes of Science and Technologies estimates is needed before 2027	The average cost of a security breach and growing annually

SECTION 2

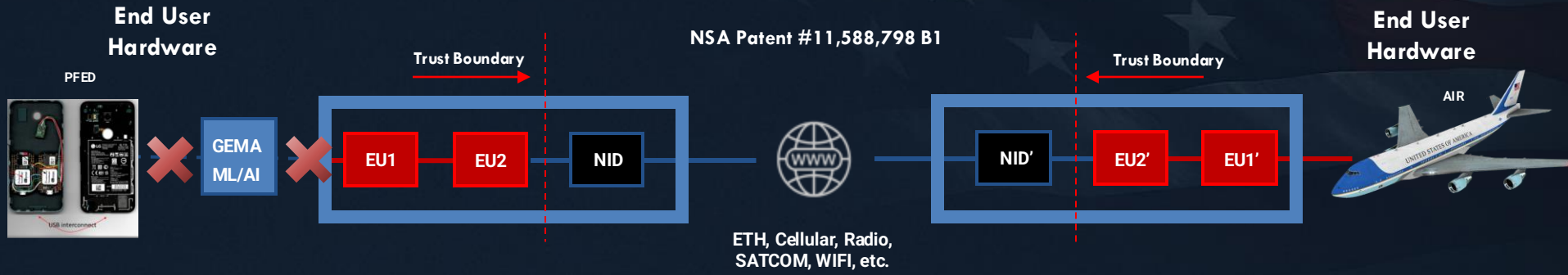
The Solution - Isidore Quantum®

- **National Security Agency (NSA) joint design and license**
- **Quantum cybersecurity protection at mass market scale**
- **Broad applications from satellites to IoT devices**
- **AI driven, commodity off-the-shelf (COTS) hardware**
- **Zero-Trust be default, crypto agile today**
- **The *only* CNSA 2.0 compliant, quantum-resistant encryption device authorized for export**
- **Robust IP Protection**
  - Augmented NSA technology with patented architecture and AI software

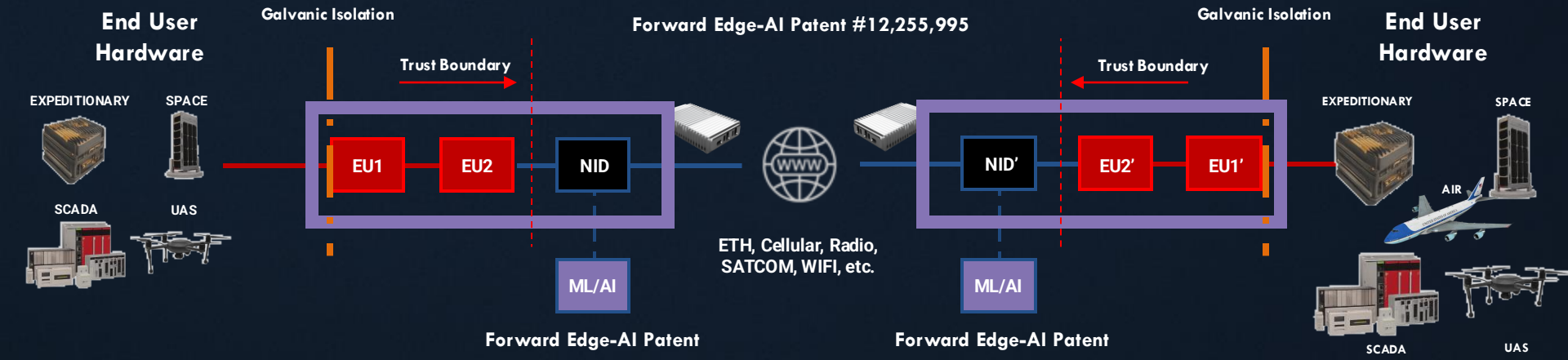


SECTION 3

How it Works



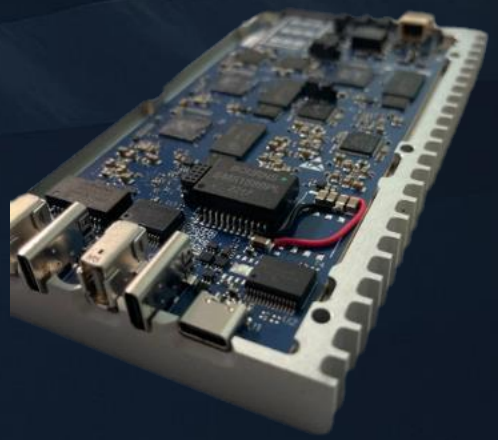
Isidore Quantum®



SECTION 4

Competitive Advantages

- ***Only*** **quantum-resistant platform deployed across all domains (space, air, land and sea)**
- **Cost-effective, plug-and-play architecture**
  - Hardware, software and network agnostic (layer 2 device)
  - 75% faster to implement / 60% lower cost to own and operate
  - No expensive infrastructure overhauls or integration / retrofit challenges
  - Zero-trust by default, crypto agility by design



- **Fully Autonomous**
  - Zero-trust architecture, ephemeral keying and galvanic isolation (IP moat)
- **No reliance on centralized infrastructure or PKI systems**
- **Strategically engineered to be authorized to export under ITAR and EAR**

SECTION 6

Validation

- **NSA collaboration**
  - Federal Lab Consortium Best Technology Transfer Award
- **DoD challenge wins / DoD top secret facility clearance**
  - XTECH, Air Force Expeditionary Challenge
- **Independently 3rd party validated**
  - Rigorous validation by Cubic, Microsoft, and Lumen Technologies using industry-leading equipment from Juniper, Nokia, and Spirent
  - Independently tested and validated by Taiwan's National Security Bureau (NSB)
- **Field-tested under classified and expeditionary scenarios across land, air, sea, and space**
  - USAF (NC3 Community), SOCOM, Space Force, Rogue Space Systems, DARPA (NOMARS), US Navy (M80 Stiletto drone ships)
- **2025: Completed accounting system audit by the Defense Contract Audit Agency (DCAA)**

Lumen Independent Testing

- **Lumen Technologies rigorously tested Isidore across both traditional and commercial real-world environments for classified (CSfC) architectures confirming:**
  - End-to-end encryption performance
  - Protocol Independence Across IPv4 and IPv6
  - CNSA 2.0 Encryption Performance with 0.5ms Latency
  - Dual-VLAN and Zero Trust Architecture in CSfC Setup
  - Substantial Overhead Reduction and Throughput Efficiency
  - Simple, Secure, Low-Cost Deployment
  - Outperformance of legacy IPsec and MACsec devices in both agility and affordability

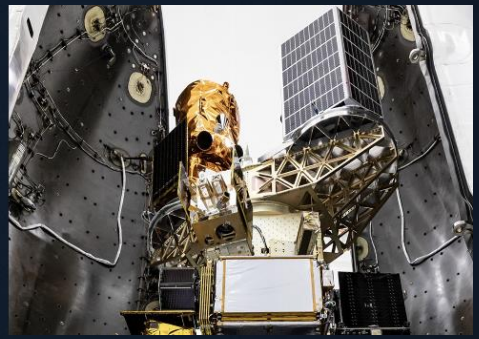
Penetration to Date

Air
US Air Force (1)
US Navy (1)

Land
US Air Force (5)
US Army (1)
Cubic
Lumen
Microsoft
Taiwan National Security Bureau (1)

Sea
DARPA (1)
US Navy (4)
Panasonic (2)
SERCO (1)

Space
Air Force (1)
National Science Foundation (1)
US Space Force (2)
Rogue Space

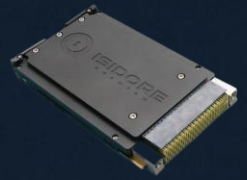


Technology & Product Portfolio

A unified, AI-powered, quantum-resistant cybersecurity portfolio that secures critical infrastructure across air, land, sea, and space — ensuring resilient, zero trust protection in the post quantum-era

Land crypto

Air & sea crypto



Space crypto

Space router

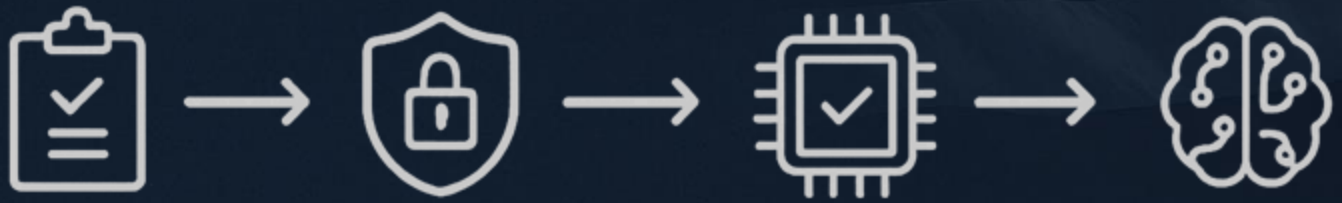
Proprietary hardware and AI software innovations

Dual use solutions address military, government and enterprise customer requirements

Patented CNSA-2.0 compliant, quantum-resistant solution

Leadership in AI-enabled edge devices

Technology Roadmap



Technology Readiness Level 8, VAR Agreements Lumen, Cubic, Microsoft

FIPS-140-3 and CSfC Approvals, GEN 3.0 Release, Low Rate of Initial Production

GEN 3.0 NSA High Assurance Approval, Full Rate Production, 10,000 Devices/Mo

Hondo Neuromorphic Processor Introduced; High-throughput/Space Hardened/Low Cost

SECTION 8

Competitive Differentiation

Authorized to export

NSA licensed and CNSA 2.0 compliant

Proven in LEO in 2025

No PKI-eliminates cognitive load

Forward Edge-AI patented galvanic isolation – patent moat

Proprietary AI-enhanced solution

Competitive Differentiation (2)

FLC

TECH SBIR AUTONOMY WINNER

AFWERX CHALLENGE

Competitive Differentiation (3)

Feature	Isadore Quantum®	Legacy PKI Systems
Deployment Time	<30 minutes	Weeks to months
Total Cost of Ownership	60% reduction	High (certificates, PKI management)
Mobile Banking Support	Fully integrated	Partial/complex
AI-Powered Defence	Built-in	None
Quantum Resistance	CNSA 2.0 compliant	Vulnerable
Zero Trust	Default architecture	Retrofit required
Power Consumption	3-5W	30-70W
Form Factor	Credit card size (218g)	Rack-mounted systems
Price Point	From $1,900 USD (34,000 ZAR) *depending on network topology	$7,600 USD - $75,000 USD (135,000 ZAR - R1.3M ZAR)

Join Us in Leading the Quantum Security Revolution!