FORWARDEDGE

Isidore Quantum®

All-in-One Cybersecurity and Drop in PQC Solution

The industry's first and only cybersecurity solution to combine Red/Black isolation, a QRNG, NIST approved PQC algorithms and ephemeral key generation and management system into an edge device.

Why Isidore Quantum®:

Affordable: 70% faster to implement and 60% lower total cost of ownership

Autonomous Cyber Resilience: AI-driven system detects, adapts, and self-heals against evolving threats

Drop-In Integration: Protocol, hardware, interface-agnostic design modernizes legacy networks without infrastructure overhaul

Low-SWaP Advantage: Compact, efficient, and scalable for enterprise, defense, and critical infrastructure use

Emerging Cybersecurity Threats

Picture a lock that protected the world for decades, then imagine a silent skeleton key that opens it without effort. Quantum risk comes down to that image: once quantum computers become practical, they will dismantle today's public-key foundations (RSA/ECC), converting years of "secure" traffic into tomorrow's readable archives, the classic "harvest-now, decrypt-later" scenario. Critical infrastructure faces the greatest danger because Operational Technologies (OT), PLC, and SCADA systems were designed for uptime, not cryptographic agility. Many still rely on flat networks and legacy protocols with minimal authentication, where a single intrusion can spread unchecked. Industry and government briefings emphasize the same message: adopt post-quantum protections and build resilience before Q-Day arrives, not afterward.

Quantum computing is not the only disruptive factor. Side-channel attacks bypass mathematics by exploiting physics such as timing variations, power consumption, electromagnetic emissions, and even acoustic signals to extract keys from supposedly "unbreakable" ciphers. PowerHammer illustrates the extreme by using CPU load modulation to send secrets across building power lines, escaping even air-gapped environments. Artificial Intelligence introduces another dimension of risk, with models that analyze traffic patterns, generate exploits automatically, and adapt more quickly than human defenders, aligning with the AI-enabled battlespace envisioned by the DoD. Combined, these threats make perimeter firewalls and clean code necessary but no longer sufficient.

That's why software-only fixes and "we use AES-256" won't save you. AES-256 remains robust against brute force, but real systems fail at the seams: quantum breaks the key-exchange scaffolding around AES, side-channels steal keys during use, and OT stacks leak across poorly segmented, legacy links.

Introduction to Isidore Quantum®

There's an old truth about security: every lock eventually meets its key. For decades, the RSA was the lock that no one could break. But quantum computing will change that. Suddenly, the world's strongest defenses look fragile. Out of that threat, a new vision, not simply a tool but a philosophy: Isidore Quantum®.

At first glance, Isidore Quantum seems unassuming, approximately the size of a credit card. But inside, it is a kind of symphony. Three processors share the work. One encrypts, another re-encrypts, while a third stands guard at the border. The result is a dual tunnel of protection. Keys appear for a moment, used once, then vanish forever. Nothing lingers, nothing remains to be stolen.

What makes Isidore remarkable is not just its power, but its simplicity. It speaks every digital language: voice, video, legacy systems, and all protocols without asking for translation. It requires no reconfiguration, no elaborate setup. Plug it in, turn it on, and your data is safe.

The numbers tell part of the story. Less than eight watts of power. Latency below half a millisecond. Throughput measured in megabits, gigabits, and soon terabits. It can run on a drone battery, secure an entire building, or safeguard a satellite link. Yet its most important trait is what it refuses to do: no announcements on the network, no responses when probed, and no signals that reveal its presence. When cornered, the device defends itself. Antifragility, powered by Artificial Intelligence, defines its strength.

The philosophy extends through a principle as old as cryptography itself: Red/Black separation. Trusted data remains isolated from the untrusted world through physical barriers rather than software tricks, including hardware divides, one-way bridges, and galvanic separation. Even sophisticated side-channel attacks encounter resistance.

Variants and Specifications:

IoT/OT/SCADA

Isidore 1

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 (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 1 Compliant), 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 1 Compliant), 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					

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.

Oversight comes from the Network Interface Device, functioning as a rule-of-one firewall, supported by an AI trained on eight trillion attack patterns that adapts in real time. Above every layer, a system called CASSIAN provides coordination, operating like air traffic control to manage thousands of devices across networks, clouds, and continents.

Developed under the NSA CNSA 2.0 framework and to FIPS 140-3 compliant, Isidore combines hardware-enforced Red/Black separation, zero-trust architecture, and post-quantum cryptography to deliver exceptional security. The hybrid cryptographic engine integrates AES-256-GCM with ML-KEM, powered by quantum entropy generated from embedded Quantum Random Number Generators, ensuring every encryption key is both unpredictable and short-lived.

Isidore Quantum is already compliant with the National Security Agency's CNSA 2.0 requirements and FIPS 140-3 Level 1 compliant. And it has already been tested in the hardest places by the U.S. Army, Air Force, Navy, Space Force, DARPA, and industry giants like Microsoft and Lumen. Each confirmed the same conclusion: it works, everywhere it matters.

The result is a dual-layer protection system capable of safeguarding operational technologies, SCADA environments, space systems, and critical communications networks against harvest-now-decrypt-later threats while supporting easy modernization and drop-in integration with existing infrastructure.

The lesson is simple. In an age where quantum computers threaten to unravel the established order of encryption, Isidore Quantum stands as more than a tool. Isidore Quantum defines a new set of rules. Hospitals, banks, utilities, command centers, and satellites—any environment where trust cannot be compromised—gain a defense designed for tomorrow rather than yesterday.

At its core, Isidore Quantum focuses less on secrecy and more on confidence. Protection extends beyond safeguarding data, restoring faith that even in a quantum future, the most critical information will remain secure.