FORWARDEDGE

OCTANS SPACE AFRICA

White Paper

Isidore Quantum®

Solución Integral de Ciberseguridad y PQC de Fácil Integración.

Garantizando la Última Frontera: Resiliencia Cibernética y Cuántica para la Infraestructura Espacial.

¿Por qué Isidore Quantum?

Alto Rendimiento: Ofrece cifrado de alto rendimiento con baja latencia.

Ultra-Bajo SWaP-C: Proporciona cifrado de alta seguridad con menos de 8 vatios para plataformas con restricciones de espacio.

Claves Autónomas: Rekeying en órbita y seguridad autorreparable sin intervención desde tierra, certificados, PKI ni firmas.

Defensa Impulsada por IA: Predice, detecta y mitiga amenazas cibernéticas en tiempo real en redes de flotas.

La dependencia global de los satélites para comunicaciones, navegación, inteligencia y comercio ha convertido el espacio en la columna vertebral de la infraestructura moderna y en el próximo frente crítico de la ciberseguridad. A medida que las redes orbitales continúan creciendo, la vulnerabilidad a intrusiones cibernéticas, manipulación de datos y compromisos en la cadena de suministro ha aumentado rápidamente. Muchos sistemas espaciales aún dependen de protocolos de cifrado obsoletos como RSA y ECC, que dejarán de ser efectivos cuando las computadoras cuánticas alcancen plena capacidad operativa. Los adversarios estatales ya se están preparando para ese momento mediante campañas de “Harvest Now, Decrypt Later” (HNDL), capturando hoy comunicaciones satelitales cifradas para su futura descifrado y uso como arma. La convergencia de los ciberataques convencionales con la amenaza emergente de descifrado cuántico pone en riesgo no solo misiones individuales, sino constelaciones enteras y redes de mando, colocando las comunicaciones globales, los sistemas de defensa y la infraestructura espacial comercial en una situación de alto riesgo. No actuar ya no representa paciencia estratégica, sino una cuenta regresiva hacia una vulneración inevitable.

La familia espacial Isidore Quantum, que incluye Space COMSEC, el High Throughput Space Router (HTSR) y el High Throughput Space Crypto (HTSC), ofrece una solución unificada de ciberseguridad resistente a la computación cuántica, diseñada específicamente para el dominio espacial. Desarrollado en colaboración con la NSA y totalmente alineado con los estándares CNSA 2.0, el sistema proporciona cifrado post-cuántico de confianza cero impulsado por IA en todas las capas de la comunicación espacial: desde enlaces satélite a satélite y enrutamiento de datos en órbita hasta interfaces de comando en tierra. Diseñado con bajo tamaño, peso, potencia y costo (SWaP-C) y con integración plug-and-play, cada componente funciona de manera autónoma con detección de anomalías en tiempo real, autorreparación criptográfica y generación de claves aleatorias cuánticas. Validado mediante pruebas con la Fuerza Espacial de EE. UU., la NASA y socios de defensa, la suite Isidore Quantum® permite a los operadores proteger activos orbitales críticos, asegurando las misiones actuales y reforzando la próxima generación de infraestructura espacial frente a amenazas cuánticas futuras.

La Situación

60%	98%	70%	USD$500Mil Millones
De los operadores de satélites reportaron intentos o intrusiones cibernéticas exitosas.	De los satélites activos dependen de cifrado RSA o ECC.	De las estaciones terrestres se conectan a redes públicas sin segmentación.	Valor económico global derivado de las comunicaciones basadas en satélites.

El dominio espacial, antes considerado un santuario tecnológico, se ha convertido en uno de los entornos más disputados y vulnerables digitalmente en la defensa y el comercio modernos. Satélites, sistemas de lanzamiento y redes de control terrestre permiten comunicaciones globales, observación de la Tierra, navegación GPS, reconocimiento de defensa y alerta de misiles. A pesar de su importancia, muchos de estos sistemas dependen de cifrados obsoletos, arquitecturas de confianza débiles y flujos de datos no supervisados diseñados para la fiabilidad operativa más que para la resiliencia en ciberseguridad.

Isidore Quantum®: Solución integral de ciberseguridad PQC

Isidore Quantum representa un ecosistema de próxima generación en ciberseguridad y cifrado post-cuántico diseñado para proteger el sector espacial global frente a amenazas actuales y emergentes. El sistema incluye Space COMSEC, HTSR y HTSC, ofreciendo protección de confianza cero conforme a CNSA 2.0 para satélites, estaciones terrestres y redes multidominio. Cada módulo integra detección de anomalías impulsada por IA, gestión autónoma de claves y cifrado aleatorio cuántico para contrarrestar intrusiones en tiempo real y futuras capacidades de descifrado cuántico. Ligero, eficiente en consumo energético y validado en colaboración con la Fuerza Espacial de EE. UU. y la NASA, la familia espacial Isidore Quantum® permite comunicaciones resilientes y seguras frente a la computación cuántica desde la órbita hasta la Tierra, reforzando la infraestructura espacial moderna.

Cada sistema comparte un núcleo mejorado con IA conforme a CNSA 2.0, capaz de operación autónoma, criptografía post-cuántica y defensa autorreparable frente a amenazas en evolución.

Capacidades	Impacto en la Misión
Cifrado Conforme a CNSA 2.0	Cumple con los estándares de la NSA para resiliencia post-cuántica y seguridad multidominio.
Arquitectura de Confianza Cero	Garantiza que los dispositivos solo se comuniquen cuando estén emparejados criptográficamente (sin confianza implícita)
Defensa Impulsada por IA	Predice, detecta y mitiga anomalías cibernéticas en flotas satelitales en tiempo real.
Gestión Autónoma de Claves	Elimina PKI y la carga operativa mediante rekeying autónomo en órbita.
Aislamiento Rojo/Negro y Entropía Cuántica	Segmentación reforzada por hardware + generación de ruido cuántico para claves verdaderamente aleatorias y de un solo uso.
Integración Plug-and-Play (Conectar y Usar)	Integración inmediata sin rediseño de satélites o estaciones terrestres.

Ventaja unificada

La familia espacial Isidore Quantum integra cifrado post-cuántico, redes de confianza cero y defensa impulsada por IA en un único ecosistema listo para misión. Al combinar criptografía conforme a CNSA 2.0, gestión autónoma de claves y detección de anomalías en tiempo real, ofrece protección autorreparable y resistente a la computación cuántica en constelaciones satelitales, estaciones terrestres y enlaces multidominio. Su arquitectura plug-and-play permite una integración fluida en sistemas existentes, proporcionando seguridad inmediata, escalable y preparada para el futuro frente a las amenazas actuales y las cuánticas emergentes.

Confiar únicamente en AES-256 crea una peligrosa ilusión de seguridad. El cifrado sigue siendo fuerte, pero su entorno ya se está desmoronando. Los algoritmos cuánticos romperán los intercambios de claves, los ataques de canal lateral extraerán secretos en tiempo real y los exploits impulsados por IA evolucionarán más rápido que cualquier parche. Quienes se aferran a la idea de que 'AES-256 es suficiente' corren el riesgo de proteger una bóveda vacía mientras los intrusos entran por puertas invisibles. La nueva era exige más que resistencia por fuerza bruta; exige arquitecturas diseñadas para resistir la velocidad cuántica, las fugas físicas y adversarios con inteligencia artificial.

Urgencia Estratégica en Órbita

La próxima gran brecha comenzará en órbita, no en la Tierra. Los adversarios ya han infiltrado redes satelitales, recopilando datos cifrados e identificando vulnerabilidades en preparación para el momento en que la computación cuántica haga obsoletas las defensas actuales. Cuando llegue ese momento, cada comando, imagen y transmisión podría quedar expuesto. La cuenta regresiva hacia el "Q-Day" ya ha comenzado, exigiendo acción inmediata para mantener el control del espacio.

Actúe ahora:

La guerra cibernética ya se ha extendido al espacio, y la computación cuántica está a punto de redefinir todos los supuestos sobre seguridad espacial. La familia Isidore Quantum, que incluye Space COMSEC, HTSR y HTSC, ofrece la primera arquitectura de confianza cero, impulsada por IA y resistente a la computación cuántica, diseñada para integrarse sin fricción en todo el ecosistema espacial. Probada con la NASA, la Fuerza Espacial de EE. UU. y la NSA, proporciona protección segura frente a la computación cuántica y autorreparable para satélites, constelaciones y redes de comando en entornos militares y comerciales.

Dispositivo Espacial COMSEC Isidore Quantum® —un módulo de cifrado compacto y resistente a la radiación. El diseño de la carcasa es idéntico en toda la familia Isidore Quantum HTSR y HTSC, con variaciones de tamaño según la función.

Variantes y Especificaciones:

Especificación	COMSEC en el Espacio	Enrutador Espacial de Alto Rendimiento	Criptografía Espacial de Alto Rendimiento
Tamaño (mm), Peso (g) y Potencia (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
Función Primaria	Cifrado resistente a la computación cuántica y seguridad de comunicaciones para comando, control y telemetría satelital.	Enrutamiento y conmutación seguros frente a la computación cuántica para constelaciones multisatélite y redes espaciales híbridas	Cifrado post-cuántico de alta velocidad para comunicaciones espaciales intensivas en datos y multidominio.
Rendimiento	Hasta 2 Gb/s de velocidad de datos segura con <90 µs (estimado).	Hasta 2 Gb/s con 10 µs de retardo de reenvío; <1 ms de retardo total de extremo a extremo	Cifrado de 10 Gb/s con <10 µs de retardo de reenvío; <90 µs (estimado).
Estándares de Cifrado	Compatible con CNSA 2.0 (AES-256 GCM, ML-KEM), con Generador de Números Aleatorios Cuánticos (QRNG) integrado.	En conformidad con CNSA 2.0, con cifrado adaptativo a través de dominios clasificados/no clasificados, con QRNG integrado.	Compatible con CNSA 2.0, con QRNG integrado.
Defensa impulsada por IA	Detección de amenazas asistida por IA y reconocimiento de patrones en canales de datos, y respuesta cibernética automatizada.	Detección de amenazas asistida por IA y reconocimiento de patrones en canales de datos, y respuesta cibernética automatizada.	Detección de amenazas asistida por IA y reconocimiento de patrones en canales de datos, y respuesta cibernética automatizada.
Gestión Autónoma de Claves	Rekeying continuo en órbita y seguridad autorreparable—sin PKI, certificados ni cargadores manuales.	Rekeying continuo en órbita y seguridad autorreparable—sin PKI, certificados ni cargadores manuales.	Rekeying continuo en órbita y seguridad autorreparable—sin PKI, certificados ni cargadores manuales.
Arquitectura	Confianza-Cero, independiente de protocolo; opera en enlaces Ethernet, SATCOM y RF; enrutamiento en malla, punto a multipunto y hub-and-spoke.	Enrutamiento definido por software en malla y punto a multipunto; segregación multidominio con reconocimiento de VLAN.	Confianza-Cero, independiente de protocolo; opera en enlaces Ethernet, SATCOM y RF; enrutamiento en malla, punto a multipunto y hub-and-spoke.

1. Las especificaciones indicadas están sujetas a cambios sin previo aviso.

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
Tamaño, Peso y Potencia	~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	Disponible Q3 2026	Disponible Q3 2026	Disponible Q4 2026
Ambiental	–40 °C a +85 °C; calificado para choques y vibraciones.					
Criptografía	AES-256 GCM y ML-KEM					
Entropía Cuántica	Subsistema integrado de Generador de Números Aleatorios Cuánticos (QRNG); validado según NIST SP 800-90 A/B/C y BSI AIS-31.					
Topologías	Punto a punto, punto a multipunto, malla y hub-and-spoke; compatible con topologías cableadas, inalámbricas e híbridas.					
Certificaciones y Cumplimiento	NSA CNSA 2.0, FIPS 140-3 (Nivel 3), NIST SP 800-90 A/B/C, BSI AIS-31, ECCN 5A002 (Excepción de Licencia ENC)					
Latencia	<90 µs (estimado)					
Arquitectura de Seguridad	Separación Rojo/Negro (Red/Black) aplicada por hardware con aislamiento galvánico; operación de confianza cero (zero-trust) y sin intervención (zero-touch); postura encubierta (sin anuncios de red ni respuestas a sondas)					
IA / Autonomía	Motor de IA embebido entrenado para la detección de anomalías en tiempo real y respuesta auto-reparadora.					
Sistema de Gestión	Cassian™ para la orquestación de flotas, aprovisionamiento, telemetría y gobernanza de políticas en implementaciones distribuidas.					

1. Las especificaciones indicadas están sujetas a cambios sin previo aviso.