

Quantum Safe Optical Encryptor

Secure Optical Communications



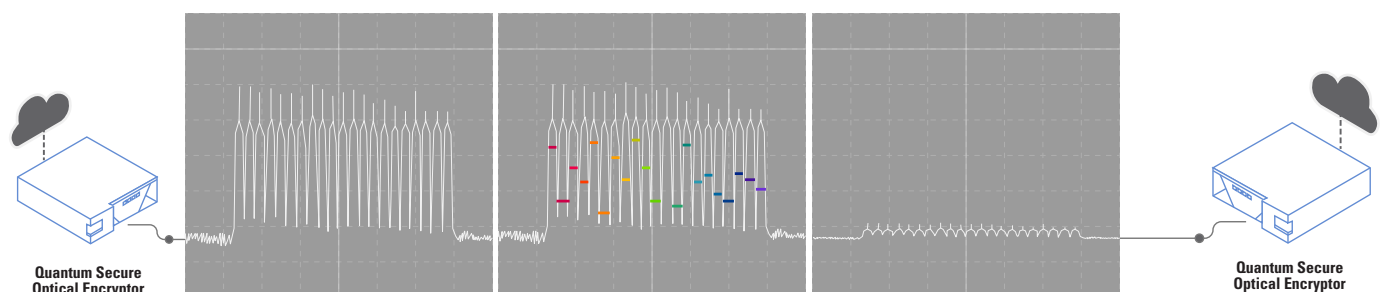
The Quantum Threat Is Already Here

Sensitive communications transmitted over public infrastructure face an increasing Harvest Now, Decrypt Later (HNDL) threat. Adversaries can intercept and store encrypted communications today, with the expectation that future quantum computers could decrypt data protected by current public key cryptography. As a result, government communications, defence information, financial transactions, critical infrastructure operations and intellectual property remain exposed long after transmission.

Harvest-Proof Protection

Quantum Secure Optical Encryptor introduces a fundamentally different approach to protecting data in transit. Instead of relying solely on stronger cryptography, Quantum Secure Optical Encryptor transforms digital payloads into spectrally distributed optical noise before transmission, preventing unauthorised optical receivers from sampling, recording or reconstructing transmitted information. By eliminating opportunities for data harvesting at the optical transmission layer, Quantum Secure Optical Encryptor complements Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD), strengthening long-term confidentiality.

Photonic Protection in Action



Spread

Disperses optical signals across multiple wavelengths.

Encrypt

Embeds continuously changing photonic keys within light.

Bury

Creates an unrecordable transmission scheme using optical noise.

Reconstruct

Only the authorised receiver reconstructs the original information.



A Different Security Paradigm

Quantum Secure Optical Encryptor delivers capabilities beyond conventional encryption, combining physics-based protection, quantum readiness and operational performance to safeguard mission critical communications.



Harvest Proof Protection

Transforms data into optical noise.



Complements PQC & QKD

Strengthens defence-in-depth.



Physics-Based Security

Protects communications at the optical transmission layer.



High Performance

Delivers 100–200 Gb/s with zero added latency.

Benefits

Quantum Secure Optical Encryptor enables organisations to strengthen long-term cyber resilience while protecting mission-critical communications without compromising operational performance.



Harvest Proof Communications

Eliminates opportunities for data harvesting and future decryption.



Long-Term Cyber Resilience

Supports future migration to quantum-safe security architectures.



Zero Added Latency

Protects communications without impacting network performance.



Mission Critical Confidence

Designed for environments where security, resilience and availability are paramount.



Operational Simplicity

Integrates seamlessly with existing optical infrastructure.

Deployment Scenarios

Quantum Secure Optical Encryptor secures mission-critical communications across environments where long-term confidentiality, resilience and trusted data transmission are essential.



Government & Defence

- Classified communications
- Defence command & control
- Intelligence networks



Data Centre Interconnect

- Data centre interconnect (DCI)
- Storage replication
- Disaster recovery



Critical Infrastructure

- Electricity transmission
- Water utilities
- Industrial control systems



Telecommunications Networks

- Metro optical networks
- Long-haul fibre networks
- Telecommunications backbone

