Your Data Is Safe Today. Not Tomorrow.

Future quantum computers will break today's encryption - making data stolen now decryptable later.

What is Quantum-Safe Networking

Quantum-Safe Networking (QSN) encrypts data at the optical layer, securing critical links against current and future quantum threats - particularly for industries with strict data protection and sovereignty requirements.

Why It Matters

The threat is already active.

- Quantum computers will break current encryption standards in minutes
- Data stolen today will be decrypted once quantum computing matures
- Current RSA/ECC encryption is mathematically vulnerable to quantum attacks
- Banking, healthcare, and public sector face the highest exposure

True quantum-safe security requires a layered and combined approach of QSN and PQC

QSN

Quantum-Safe Networking (QSN) - Network-Native Protection

Protects the entire highway, so every car is safe.

- ✓ Integrates Post-Quantum Cryptography (PQC) into the network backbone
- ✓ Protects all traffic between sites - no app changes needed
- ✓ Secures legacy and modern apps with a single deployment

PQC

Post-Quantum Cryptography (PQC) - Application-Specific Protection

Armours the specific high-value car, wherever it goes.

- ✓ Directly encrypts high-value data assets (files, databases, credentials)
- ✓ Ensures data remains secure wherever it is stored – on any device or cloud
- ✓ Provides granular, application-level control over security policies

How it Works

Protects against fibre tapping and untrusted network paths

Encrypts all traffic, regardless of protocol - nothing passes unprotected

Zero bandwidth penalty, no latency impact

No changes to existing routers, servers, or cloud systems required

How QSN Protects Against Threats

Attacks today impact communication, infrastructure, privacy and safety

Healthcare

2019 - SingHealth 1.5M Records Exposed

Est. loss: $20 mil

Prevents stolen traffic from being replayed or decrypted ✓

Banking & Financial Services

2025 - Santander & DBS Breach

Est. loss: $250 mil

Encrypts all traffic across financial networks - partners, vendors, payment gateways ✓

Government & Public Sector

2024 - US Treasury Hack

Est. loss: $250 mil

Captured traffic cannot be read or altered ✓

Oil & Gas

2021 - Colonial Pipeline Ransomware

Est. loss: $5 bil

Isolates critical control networks from interference ✓

Problems	Outcomes
Current encryption breaks under quantum attack	Optical-layer encryption quantum computers can't crack
Data stolen now, decrypted later	Harvest-now-decrypt-later threat eliminated
Every app needs individual security updates	One deployment protects all traffic on the link
Infrastructure changes disrupt operations	Transparent - no hardware replacement needed

Why Choose QSN with Maxis

99.999% SLA Across 40+ Data Centres
Under 5 minutes downtime annually

No Hardware Replacement
Transparent to all existing infrastructure

Enterprise-grade Support
Proactive monitoring and rapid restoration for businesses

Future-proof your network before the quantum threat arrives.

Maxis Business