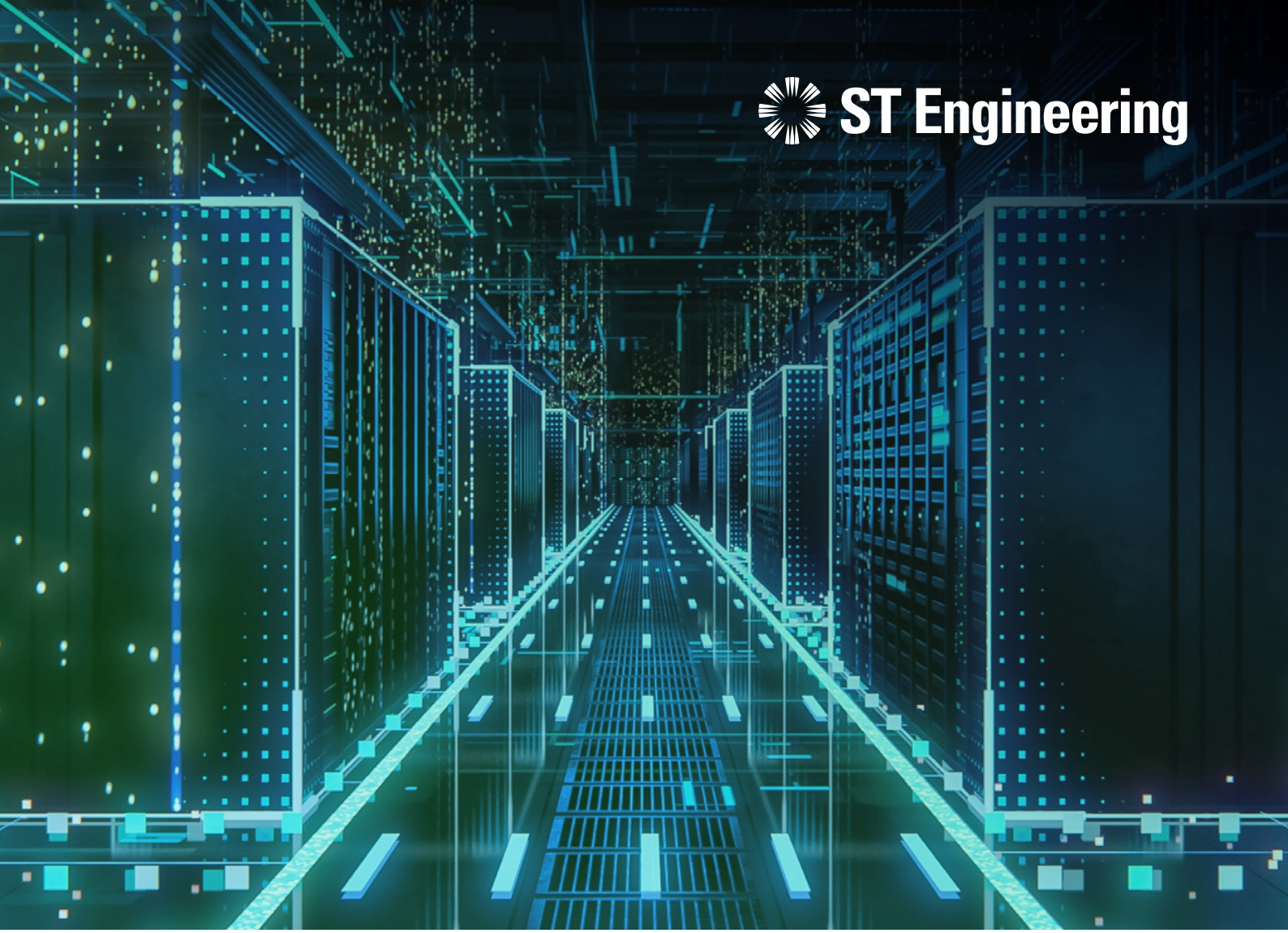


Quantum-Safe Encryptor

Post-Quantum Security

The threat landscape is evolving. Cybercriminals are increasingly preparing for the rise of quantum computing, rendering data in transit more vulnerable than ever. Governments and critical infrastructure operators must act now to defend against current cyber threats and the looming risk of Harvest Now, Decrypt Later (HNDL) attacks.

The Quantum-Safe Encryptor is engineered to deliver quantum-resistant encryption, safeguarding data integrity and confidentiality for governments and critical sectors in an unpredictable digital landscape.

The Rising Quantum Threat

Quantum computing is advancing rapidly, posing a serious threat to current encryption methods like RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography), which protect most global communications. Once quantum capabilities mature, these algorithms will be easily broken.

This has sparked attacks, where adversaries collect encrypted data with the intent to decrypt it once quantum power becomes available. A survey found that over 60% of organisations are concerned about their preparedness for the risks of a post-quantum computing future, with many taking decisive action to implement solutions to mitigate the risks.[1] Meanwhile, the Global Risk Institute reports a 31% chance of quantum decryption capabilities emerging within 10 years.[2]

Without immediate action to adopt quantum-safe encryption, organisations risk the long-term confidentiality, integrity, and trust of their most sensitive communications and national security assets.

The urgency is real:

Imminent Decryption Risk

RSA and ECC encryption currently secure the majority of global communications. However, they may be broken within 10–15 years[2], placing long-term data confidentiality at immediate risk.

Global Unpreparedness

Despite rising awareness, most organisations have no migration roadmap to post-quantum cryptography, creating a widening vulnerability gap.

Nation-State Acceleration

Government-funded quantum programmes exceed $30 billion globally[3], accelerating the timeline for quantum decryption capabilities.

The Quantum Countdown Is Ticking

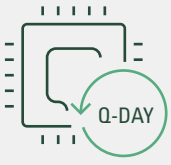
> $1 Trillion

in encrypted digital assets are at risk of decryption once quantum computers reach sufficient power.[4]

99%

of Fortune 500 companies are not adequately prepared for the imminent threats posed by quantum computing.[5]

1-in-3



chance of a quantum computer capable of breaking today's encryption will emerge by 2035, a tipping point known as 'Q-Day'.[6]

48%

of executives believe quantum computing will play a significant role in their industries by 2025.[7]

[1] ZDNET. (2023, October 19). 61% of firms worry they are unprepared for security risks in quantum era.

[2] Global Risk Institute (2024, December 6). Quantum threat timeline report 2024

[3] World Economic Forum. (2022, September 13). State of quantum computing: Building a quantum economy

[4] World Economic Forum. (2025, January). Embracing the quantum economy: A pathway for business leaders

[5] India Technology News. (2024, December 27). 99% of Fortune 500 firms are not quantum-ready

[6] Wired. (2025, March 24). The quantum apocalypse Is coming. Be very afraid

[7] EY. (2022, June 27). How can you prepare now for the quantum computing future?

Becoming Quantum-Safe

The Quantum-Safe Encryptor is purpose-built to secure critical data flows in today's increasingly complex threat landscape. Designed for the future, it delivers high-assurance, low-latency Layer 2 encryption for sensitive data in transit, with support for Post-Quantum Cryptography (PQC) and third-party Quantum Key Distribution (QKD) readiness. The centralised monitoring enables remote health monitoring system of the encryptors within the network. Empowering organisations to remain secure, adaptable, and ready for tomorrow's challenges.

The encryptor's advanced capabilities make it a trusted foundation for implementing quantum-safe cybersecurity strategies:

Quantum-Safe Encryption

Combining PQC and third-party QKD readiness provides quantum resilience for data at transits. It ensures data remains protected against classical and quantum computing threats, providing unmatched security confidence in mission-critical government and infrastructure environments.

Certified for Global Security Compliance

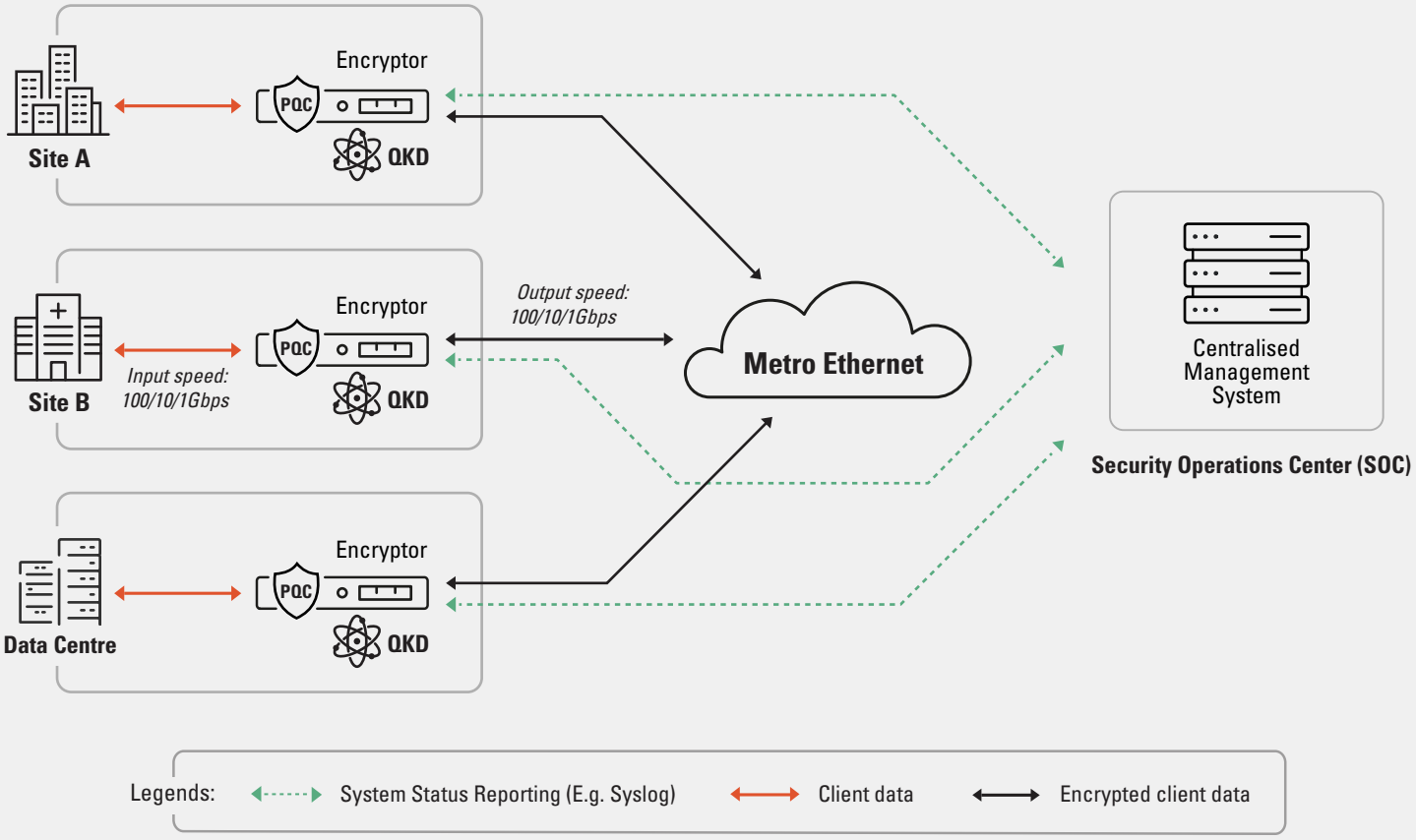
Design to comply with FIPS 140-3 Level 3 standards, it provides globally recognised security assurance. Meeting strict federal requirements, it enables organisations to confidently deploy in highly sensitive and regulated environments without risking compliance.

FPGA-Based Encryption

Built on Field Programmable Gate Array (FPGA) architecture, the encryption engine ensures hardware-level security with high performance. This architecture provides flexibility, low latency, and cryptographic agility in environments demanding real-time secure data transmission and future-proof encryption.

Unified Security Intelligence for a Quantum-Safe Future

With full integration into Security Operations Centres (SOCs) and a Centralised Management System, the Quantum-Safe Encryptor provides unified visibility and control, proactive threat detection, streamlined incident response, and real-time analytics and logging, all within a secure 1U encryptor designed for mission-critical environments.



Quantum-Safe Encryptor

Key Features

Scalable bandwidth (100/10/1Gbps) that dynamically adjusts throughput to meet changing workloads ensuring seamless, high-speed secure data transmission.

Real-time encryptor health monitoring to track device status and performance continuously ensuring uptime and proactive fault response.

Versatile network interfaces to support multiple connectivity speeds within a single device enabling flexible, future-ready infrastructure integration.

Real-time traffic anomaly detection analyses live data flows to identify unusual activity and trigger immediate security actions.

Point-to-point and multi-point deployments that facilitate secure data exchange across direct links or distributed networks with consistent integrity.

Compact 1U rack-mount design, a space-saving form factor optimised for data center efficiency and easy deployment.

Tamper-resistant with zeroisation, which automatically erases sensitive data in the event of a breach, ideal for high-security and government use.

Integration with Security Operations Centres (SOCs) delivers centralised control, faster incident response, automated enforcement, and unified monitoring for stronger cybersecurity.

Key Benefits

Ultra-low latency & high-speed encryption deliver maximum data throughput with minimal delay for mission-critical, time-sensitive operations.

Consistent performance at scale ensures stable encryption and network efficiency regardless of data volume or complexity.

Unified network-wide security visibility centralises threat monitoring across all endpoints for faster incident response and reduced risk exposure.

Streamlined security operations simplify administration through integrated monitoring, configuration, and control tools, all from one console.

Use Cases for Quantum-Safe Encryptor

In an era defined by rising quantum computing threats, the Quantum-Safe Encryptor empowers governments, critical infrastructure sectors with uncompromised data protection. Its advanced encryption capabilities and centralised security management enable organisations to maintain mission continuity, ensure regulatory compliance, and achieve future-ready resilience across mission-essential environments.

Government

Classified Communications Protection

Secure highly sensitive communications between government agencies, military command centres, and allied networks to prevent espionage, block data interception, and ensure mission-critical operations remain confidential in a quantum-threat environment.

Benefits

- **Protects classified and mission-critical data** from unauthorised access, safeguarding national security and sovereign information control.
- **Enables real-time threat detection** by integrating with SOCs for faster, coordinated incident response and forensic analysis.
- **Ensures compliance with defence-grade standards** such as FIPS 140-3 delivering tamper-resistant protection across government and critical infrastructure.

Critical Infrastructure

Securing National Operational Systems

Protect industrial control systems and SCADA networks across national infrastructure from cyber intrusions, data manipulation, and outages that could disrupt essential services or compromise national stability.

Benefits

- **Safeguards operational data integrity** by encrypting Layer-2 communication between critical nodes in real time.
- **Prevents service disruption** from cyber attacks by ensuring encrypted, uninterrupted operations across power grids and water systems.
- **Provides centralised visibility** with integrated monitoring for early detection of anomalies across distributed environments.

Finance & Banking

Financial Data Security

Safeguard high-value transactional data between banks, financial institutions, and regulators to maintain confidentiality, support compliance, and protect against quantum-era breaches targeting encryption and real-time financial operations.

Benefits

- **Mitigates risk of data breaches** by encrypting financial data against both current and future quantum decryption threats.
- **Ensures transaction integrity** with hardware-enforced encryption that prevents tampering and protects high-value transfers end-to-end.
- **Delivers ultra-low latency performance** ideal for high-speed transactions and uninterrupted financial service operations.

Enterprise & Data Centre

Enterprise & Data Centre

Secure high-volume, multi-site data flows with ultra-low latency, quantum-safe encryption, supporting operational resilience, data integrity, and uninterrupted performance across mission-critical workloads and geographically distributed environments.

Benefits

- **Safeguards interconnects** with hardware-based PQC/QKD encryption for current and future threats.
- **Centralises security management** for faster response and unified policy enforcement.
- **Maintains efficiency** with microsecond latency for mission-critical workloads.

SECURE WHAT MATTERS

ST Engineering Cybersecurity

With over two decades of cybersecurity expertise, ST Engineering's Cyber business has evolved from a focus on cryptography to leading in end-to-end cybersecurity solutions. We protect government entities, critical infrastructure, and enterprises against evolving threats. Our capabilities include operating over 20 global Cybersecurity Operation Centres (SOCs), training 2,500 professionals, and driving innovation through R&D. Leveraging deep engineering expertise, we integrate advanced cybersecurity into communications and industrial systems, empowering organisations to achieve cyber resilience through a comprehensive approach encompassing people, processes, and technology. We secure what matters.

www.stengg.com/en/cybersecurity sg.linkedin.com/showcase/st-engineering-cybersecurity/

ST Engineering