SYNERGY QUANTUM

SYNERGY QUANTUM

AT THE CONVERGENCE OF AI, QUANTUM, AND SOVEREIGNTY

Confidential | July 2026

16/07/26

STRATEGIC ROADMAP

A Strategic Roadmap to Sovereign Quantum Security

ALIGNING THE SYNERGY QUANTUM STACK TO PQC, SECURE COMMUNICATIONS & NATIONAL CYBER RESILIENCE

PHASE 01 · ASSESS & PRIORITISE

PHASE 02 · DEPLOY & INTEGRATE

PHASE 03 · SUSTAIN & ASSURE

Sovereign Post-Quantum Security

NIST-standard PQC and crypto-agility deployed across the stack — protecting data with decades-long secrecy needs against harvest-now-decrypt-later.

Indigenous Secure Communications

Sovereign quantum-safe cores, transport and key management — with hybrid PQC and QKD where it delivers operational value.

National Cyber Resilience

Continuous cryptographic visibility and assurance across Defence, Telecom, BFSI and Critical Infrastructure — one governed, sovereign posture.

Eight integrated layers translate these principles into one sovereign quantum-safe architecture — examined next.

The Synergy Quantum Sovereign Stack

Eight deployed capabilities behind the architecture: AI, quantum and cybersecurity, proven at TRL 9.

16/07/26

Eight layers, *one sovereign fortress.*

SynQ Full-stack AI · Quantum · Cybersecurity — proven and deployed at TRL 9

SynQ Connect
Encrypted messaging, voice & video

SynQ-HRoT
Hardware root of trust & secure elements

SynQ-5G Core and RAN
Quantum-safe private 5G networks

SynQ-MobileOSGuard
Hardened post-quantum mobile OS

SynQ-MythGuard
AI-driven exposure management at machine speed

SynQ-HSM
Quantum-safe hardware key storage

SynQ Quantum Shield
Quantum-resilient secure tunnels

SynQ TIP
Real-time Quantum and Cyber threat detection & analytics

Layer 8 Mission-Critical & Tactical Applications

Layer 7 Command, Control & Coordination (C3)

Layer 6 AI Workspace & AI-Assisted Cyber Threat Intelligence

Layer 5 Data & Storage Security

Layer 4 Identity Authentication & Authorization

Layer 3 Post-Quantum Cryptography & Key Lifecycle

Layer 2 Secure Communications Backbone

Layer 1 Foundational Trust & Physical Security

Your Cryptographic Bill of Materials

A single inventory of every cryptographic asset in your organization: where it lives, what it protects, and whether it survives the quantum era.

WHAT'S INSIDE

- Algorithms in use and where
- Key inventory: type, length, rotation status
- Certificate inventory and lifecycle
- Protocol versions and configurations
- Library versions and dependencies
- Hardware crypto modules (HSMs, TPMs, smart cards)
- Third-party and SaaS cryptographic dependencies

WHY IT MATTERS

Visibility

You can't migrate what you can't see. The QCBOM is the map.

Prioritization

Risk-rank every asset by exposure window and data sensitivity.

Compliance

Demonstrate quantum-readiness against NIST, CNSA, and sector mandates.

Crypto-agility

Swap algorithms without rebuilding systems. The QCBOM is the control plane.

Migration Is Not a Single Switch

Quantum-safe transition is a multi-year program. Done right, it's phased, prioritized, and reversible.

> The hardest part isn't the algorithms. It's finding every place cryptography lives, untangling decade-old dependencies, and changing them without breaking production.

DISCOVERY

Finding It All

Cryptography hides in code, libraries, certs, HSMs, third-party services. Manual inventory takes months and is stale on day one.

DEPENDENCIES

Untangling the Web

One algorithm change can break dozens of downstream systems. Hybrid deployments require running old and new in parallel.

PERFORMANCE

Bigger Keys, Bigger Cost

PQC keys and signatures are larger. Handshake latency rises. TLS, certificates, and storage all need re-sizing.

GOVERNANCE

Provable Progress

Boards, regulators, and auditors want measurable readiness. Without a QCBOM, you can't prove what's done or what's left.

Discover. Build. Assess. Migrate.

An end-to-end platform for cryptographic visibility, governance, and post-quantum readiness.

01

DISCOVER

Cryptographic Asset Discovery

Seven specialized scanners find every algorithm, key, cert, and library across code, networks, containers, HSMs, files, and quantum channels.

02

BUILD

CBOM Generation

Consolidate every discovered asset into a single, queryable cryptographic bill of materials. Live, versioned, and exportable.

03

ASSESS

Risk Classification

Every asset scored against quantum exposure, data sensitivity, and migration urgency. Red, amber, green readiness states.

04

MIGRATE

Phased PQC Roadmap

Seven-phase migration: Discovery, Assessment, Prioritization, Planning, Migration, Monitoring, Optimization. With rollback at every step.

PRODUCT ONE

SynQ TIP

Synergy Quantum Threat Intelligence Platform.

16/07/26

QCBOM SYSTEM ARCHITECTURE

Quantum-Safe Cryptographic Bill of Materials Platform

Unified PQC Console Layer

ENTITY NAME
- Organization ID
- Display Name
- Contact Information
- Tenant Identifier

COMPONENT SERVICES
- Service Registry Management
- Module Activation Controls
- License Management

ALLOW POLICY
- Access Control Lists (ACL)
- Role-Based Permissions
- Compliance Rules

REPORTING
- Dashboard Configuration
- Report Templates
- Export (PDF, CSV, JSON)

MIGRATION PLAN
- Timeline & Phases
- Priority Matrix
- Risk Assessment

AUDIT TRAIL
- Activity Logging
- Change History
- User Action Records

CONFIGURATION
- System Settings
- Integration Config
- Notification Rules

▼ Configuration & Policy Layer ▲ Status Updates

Unified Aggregator Layer

AUTH SERVICE
- OAuth 2.0 / OIDC
- JWT Validation
- RBAC Enforcement
- Session Management
- MFA Support

DATA TRANSFORM
- JSON/XML
- Format Conversion
- Schema Validation
- Data Normalization
- CycloneDX Support

API GATEWAY
- Route Management
- Load Balancing
- Rate Limiting
- SSL/TLS Termination
- Request Transform

API MONITOR
- Health Checks
- Performance Metrics
- Error Tracking
- Distributed Tracing

AUDIT LOG
- Request Logging
- Response Logging
- Compliance Records
- Immutable Store

▼ Analysis Request ▲ Reports

QCBOM Scanner Layer

Source Code Scanner
Overview Stats:
- Repository Scans
- Source Code Scans
- Quantum Readiness Score
- Vulnerability Summary

Visualisations:
- Algorithm Distribution
- Risk Level

Reports:
- CBOM Export (CycloneDX)
- JSON,PDF

.json .go .py .js .ts .java .c .cpp .rs

NETWORK
Overview Stats:
- Packets Analyzed
- Encrypted Traffic %
- Protocol Distribution

Visualisations:
- Protocols Counts
- Weak Cipher Alerts

Reports:
- PDF, Excel

.pcap .pcapng

FILESYSTEM
Overview Stats:
- Compliance Score
- Risk Level
- Libraries Found

Visualisations:
- Crypto Library List
- Secrets Detected
- Vulnerability Map

Reports:
- PDF, JSON

.elf, exe .dll .dylib

CONTAINER
Overview Stats:
- CVE by Severity
- Quantum Safe Score
- Algorithm Counts

Visualisations:
- Package Inventory
- Vulnerabilities

Reports:
- Vulnerability Report (PDF)

.Dockerfile

HSM
Overview Stats:
- Hardware RNG Sources
- HSM Health
- Compliance Score

Visualisations:
- Hardware Inventory
- HSM Vendor Detection
- HSM Health

Reports:
- PDF

.pem .key

ENTROPY
Overview Stats:
- Shannon Entropy (0-8)
- Quality Badge
- Tests Passed Count

Visualisations:
- Entropy Distribution
- Source Type (QRNG/TRNG)
- Byte Frequency Chart

Reports:
- NIST Test Results , Recommendations (PDF)

.bin .raw .dat .elf

QKD
Overview Stats:
- Protocol (BB84/E91/etc)
- QBER % Gauge
- Key Rate (bps)

Visualisations:
- Security Score (0-100)
- Distance vs Key Rate
- QBER Trend Chart

Reports:
- Key Quality Metrics
- Protocol Comparison

.pickle

01 MODULE 01

Source Code Scanner

Static analysis across your codebase for cryptographic usage.

WHAT IT SCANS

Source repositories, build artifacts, dependency manifests.

WHAT IT DETECTS

Algorithm calls (RSA, ECC, AES), key generation, cert handling, weak constructs, hardcoded keys.

OUTPUT

Per-file findings, dependency graph, prioritized remediation list with PQC-equivalent suggestions.

WHY IT MATTERS

Cryptography is woven into application logic. The only way to find every usage is to read the code.

02 MODULE 02

Network Scanner

Live discovery of cryptographic protocols and certificates in transit.

WHAT IT SCANS

Live traffic via SQANA agent, PCAP analysis, and active enumeration across enterprise and OT networks.

WHAT IT DETECTS

TLS/DTLS, SSH, IKE/IPsec, WireGuard, QUIC, MACsec, including weak ciphers, expired certs, deprecated versions.

OUTPUT

Endpoint and protocol inventory, certificate lifecycle status, prioritized network migration list.

WHY IT MATTERS

Network crypto is exposed to harvest-now-decrypt-later. Continuous visibility is the only defence.

03 MODULE 03

File System Scanner

Catalogue cryptographic material stored at rest.

WHAT IT SCANS

Local and networked file systems, object stores, backup volumes.

WHAT IT DETECTS

Certificates, private keys, keystores (JKS, PKCS#12), encrypted archives, signed binaries.

OUTPUT

Inventory of crypto-bearing files, expiry calendar, orphaned-key alerts.

WHY IT MATTERS

Stored keys outlive the systems that created them. Most organizations cannot answer where their private keys actually live.

04 MODULE 04

Container Scanner

Cryptographic discovery inside container images and orchestrated workloads.

WHAT IT SCANS

Container images (Docker, OCI), Kubernetes secrets, service mesh certificates, sidecar configs.

WHAT IT DETECTS

Embedded keys, baked-in certs, crypto libraries in base images, weak default ciphers.

OUTPUT

Image-level CBOM, secrets-in-image alerts, registry-wide PQC readiness score.

WHY IT MATTERS

Containers package crypto into immutable artifacts. Without scanning, weak crypto ships with every deployment.

HSM Scanner

Inventory of hardware-anchored keys and crypto operations.

WHAT IT SCANS

Hardware Security Modules, network HSMs, cloud KMS, TPMs, smart cards.

WHAT IT DETECTS

Key types and lengths, key usage policies, supported algorithm sets, firmware versions.

OUTPUT

HSM inventory, PQC-capability matrix, key-rotation calendar, hardware migration plan.

WHY IT MATTERS

HSMs hold the root of trust. They are the longest-lived crypto in the enterprise and the hardest to migrate.

06 MODULE 06

QKD Scanner

Visibility into quantum key distribution links and quantum-channel deployments.

WHAT IT SCANS

QKD endpoints, key managers, trusted-node networks, quantum-network controllers.

WHAT IT DETECTS

Active QKD sessions, key-rate metrics, link integrity, integration with classical KMS.

OUTPUT

QKD topology map, session telemetry, hybrid classical and quantum key flow audit.

WHY IT MATTERS

Organizations deploying QKD need the same level of governance as classical crypto. SynQ TIP provides it.

07 MODULE 07

Entropy Scanner

Audit the quality of randomness underpinning every cryptographic operation.

WHAT IT SCANS

OS entropy sources, RNG hardware, library RNGs, application-level random pools. (QRNG, PRNG)

WHAT IT DETECTS

Low-entropy sources, predictable seeds, weak PRNGs, kernel-pool starvation.

OUTPUT

Entropy-quality report by source, NIST SP 800-90B compliance status, hardening recommendations.

WHY IT MATTERS

Strong algorithms with weak randomness are worthless. Entropy is the foundation no other scanner sees.

Dashboard

Synergy Quantum — SynQ Threat Intelligence Platform — v2.0 — admin — Logout

- Dashboard
- CODE SCANNER
  - Upload CBOM
  - Repo Scan
  - Direct Scan
  - Recent Scans
- FILE SYSTEM
  - Filesystem Scan
  - Filesystem Archive
- NETWORK ANALYSIS
  - Overview
  - Network Scan
  - Live Monitor
  - Network Inventory
- CONTAINER ANALYSIS
  - Container Insights
  - Container Archive
- HSM
  - Overview
  - HSM Agents
  - HSM Jobs
- ENTROPY
  - QRNG/PRNG Scan

Security Overview

Your quantum-safe security at a glance

Download Report

Time Range: 7 Days | 30 Days | 90 Days | All Time

View: Overview | Code Scanner | Filesystem | Network | Container | HSM | Entropy | QKD

Your quantum-safety journey

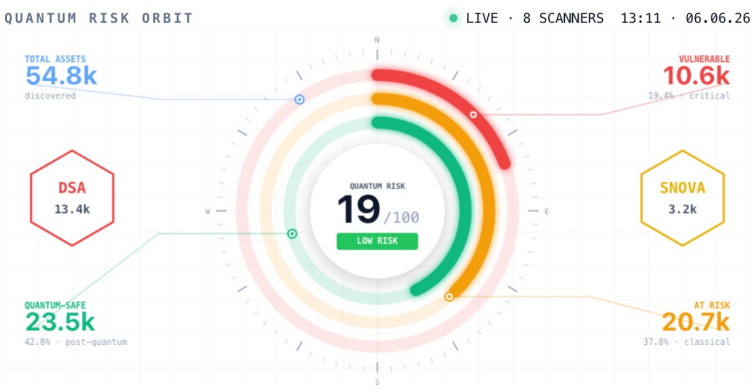
From discovery to verified compliance — every asset, end to end

4-STAGE WORKFLOW

STEP 1	STEP 2	STEP 3	STEP 4
Discovery	**Prioritization**	**Remediation**	**Compliance**
What we found in your environment	Top algorithms ranked by exposure	Migrate to post-quantum security	Quantum-safe across all standards
54.8k	13.4k	10.6k	43%
assets discovered	in highest-risk algorithm	awaiting migration	overall compliant

1. Discovery

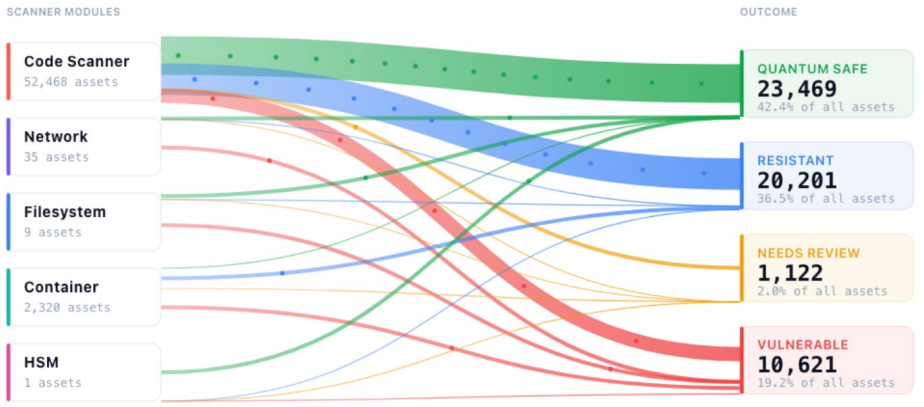
What we found in your environment



Live pipeline

Every asset streamed through its scanner into a quantum-safety outcome

STREAMING



Hover a module or outcome to highlight its flows · click an outcome to isolate

2. Prioritization

3. Remediation

Compliant Breakdown Summary — LIVE · 5 STANDARDS

01 PHASE 01 – 02

Discovery & Assessment

Find every cryptographic asset, then quantify its quantum risk, sensitivity, and urgency.

PHASE 01 · DISCOVERY

Multi-source scan — All 7 scanners run concurrently across the in-scope estate.

Continuous monitoring — Live agents stay on after the sweep to catch drift.

Asset normalization — Findings consolidated into a single QCBOM schema.

Coverage validation — Gap analysis against known asset inventory and CMDB.

PHASE 02 · ASSESSMENT

Quantum risk scoring — Per-asset score against Shor and Grover exposure windows.

Data classification — Map assets to the data they protect and its sensitivity.

Compliance gap — Current state vs. NIST, CNSA 2.0, and sector mandates.

Threat modelling — Harvest-now-decrypt-later exposure for long-lived secrets.

02 PHASE 03 – 04

Prioritization & Planning

From a risk-ranked backlog to a concrete, resource-loaded migration plan.

PHASE 03 · PRIORITIZATION

Risk-impact matrix — 2D scoring: quantum exposure vs. business criticality.

Effort estimation — Migration complexity per asset class with dependencies.

Sequencing — Order assets into waves that respect risk and dependencies.

Stakeholder review — Sign-off from CISO, app owners, and compliance.

PHASE 04 · PLANNING

Roadmap construction — Multi-year plan aligned to NIST and regulatory deadlines.

Algorithm selection — Map each asset class to its target PQC algorithm.

Pilot scoping — Choose representative workloads for hybrid-mode pilots.

Resourcing & budget — Headcount, vendor, and capex/opex by wave.

03 PHASE 04 – 05

Planning & Migration

Turn priorities into a resourced plan, then execute the waves and replace crypto in production.

PHASE 04 · PLANNING

Roadmap construction — Multi-year plan aligned to NIST and regulatory deadlines.

Algorithm selection — Map each asset class to its target PQC algorithm.

Pilot scoping — Choose representative workloads for hybrid-mode pilots.

Resourcing & budget — Headcount, vendor, and capex/opex by wave.

PHASE 05 · MIGRATION

Hybrid deployment — Run classical and PQC in parallel for safe cutover.

Cert & key reissue — PQC certs and keys issued from upgraded PKI.

Library upgrades — Swap OpenSSL/BoringSSL/BC for PQC-capable builds.

Rollback drills — Each wave includes a tested rollback path.

04 PHASE 06 – 07

Monitoring & Optimization

Operate the migrated estate with continuous visibility, then tune for performance and cost.

PHASE 06 · MONITORING

Continuous QCBOM — Always-on inventory keeps the crypto bill-of-materials live.

Drift alerts — Automated flags when assets diverge from target posture.

Compliance reporting — Evidence packs generated against NIST and CNSA 2.0.

Threat-intel feed — Live signals on new quantum and algorithm risks.

PHASE 07 · OPTIMIZATION

Performance tuning — Reduce PQC latency and handshake overhead at scale.

Cost optimization — Right-size compute, HSM, and vendor spend by wave.

Crypto-agility upgrades — Make algorithm swaps routine and low-risk going forward.

Lessons learned — Capture findings to refine the program annually.

05 DEPLOYMENT

Three Ways to Deploy SynQ TIP

Choose the model that fits your security posture, data residency, and operational constraints.

01

SAAS

Synergy Cloud

Fully managed. Fastest time to value.

- No infrastructure to manage
- Continuous updates and threat intel
- Multi-tenant with strong isolation
- Recommended for greenfield programs

02

PRIVATE CLOUD

Dedicated Tenant

Single-tenant deployment in your cloud account.

- Your AWS, Azure, or GCP account
- Customer-managed keys end to end
- VPC isolation, private endpoints
- Recommended for regulated industries

03

ON-PREMISES

Air-Gapped Install

Full on-prem deployment for sovereign control.

- Runs entirely inside your perimeter
- No external dependencies at runtime
- Offline update channel
- Recommended for defence and critical national infrastructure

06 CALL TO ACTION

Post-quantum starts with visibility.

Map the invisible. Govern what you find. Migrate with confidence.

01

WEEK 1

Run a Discovery Pilot

Deploy SynQ TIP scanners against a representative slice of your estate. Receive a baseline QCBOM and risk report within ten business days.

02

WEEK 4

Build the Roadmap

We work with your team to translate findings into a prioritized, time-bound migration plan aligned to NIST and your sector mandates.

03

ONGOING

Operate with Confidence

Continuous QCBOM, drift alerts, compliance reporting, and phased PQC migration with rollback at every wave.

PRODUCT TWO

SynQ Connect

Post-Quantum Secure Messaging & Collaboration Architecture

16/07/26

01 OVERVIEW

A Unified Secure Communication Platform

A server-controlled, key-managed architecture using trusted-device authentication, PQ-mTLS transport, protected QRSKM key management, and AES-256-GCM protection — encrypted, centrally governed, and quantum-resilient.

Communicate

1:1 & group messaging, voice/video calling, event notifications, and broadcast alerts.

Protect

message protection, encrypted storage, and ciphertext-only persistence.

Govern

Trusted-device enforcement, policy-based access, audit logging, and key revocation.

02 PURPOSE

Built for High-Security Environments

Designed for government-grade environments where communication must resist both classical cyber threats and future quantum-era risks.

- Secure 1:1 messaging
- Secure voice / video calling
- File & attachment handling
- Trusted device enforcement
- Audit logging
- Secure group communication
- Event notifications
- Encrypted storage
- Policy-controlled access
- Session revocation & key rotation

KEY MESSAGE Sensitive communication is encrypted, centrally governed, and protected against cryptographic obsolescence.

03 CORE PRINCIPLE

Server-Controlled Protected Key Model

No client-side AES key delivery. Long-term keys never touch user devices — they stay protected in the KMS.

Protected custody

Long-term QRSKM stays inside a KMS, never stored on devices.

Policy-gated derivation

Session-root keys are derived only after policy approval.

Per-operation keys

AES-256-GCM working keys derived only for approved operations.

Ciphertext-only

Messages and attachments are stored solely as ciphertext.

Transient plaintext

Plaintext exists only briefly during authorized rendering.

Identity, not keys

Devices hold session credentials — not communication keys.

04 DEPLOYMENT

Flexible Deployment Across Networks

The same secure architecture adapts to three deployment models, set by organizational security policy.

01

Captive Network

Isolated or air-gapped environment, physically separated from public networks. For the most sensitive communication domains.

02

Public Network + Isolated VPN

Operates over public infrastructure with an isolated VPN or secure overlay, per organizational policy.

03

Public Network

Runs across wired, radio, satellite, and 4G/5G networks, subject to security rules and availability.

Secure Communication Modules

QChat

1:1 messaging, voice notes, replies, attachments, low-latency chat.

QRoom

Group collaboration, room messaging, video/audio briefings.

QMail

Secure internal email for formal communication & documents.

QSpace

Encrypted file sharing & controlled folders — no local storage.

Broadcast

Rapid alerting & dissemination to selected or all participants.

Monitoring

Dashboards, tracking, anomaly detection, reports, policy control.

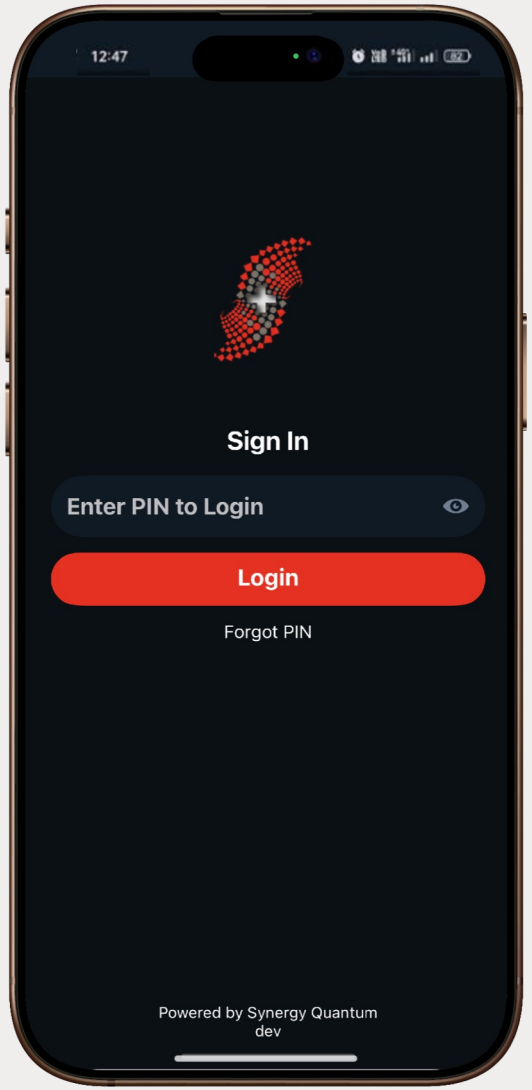
SUMMARY

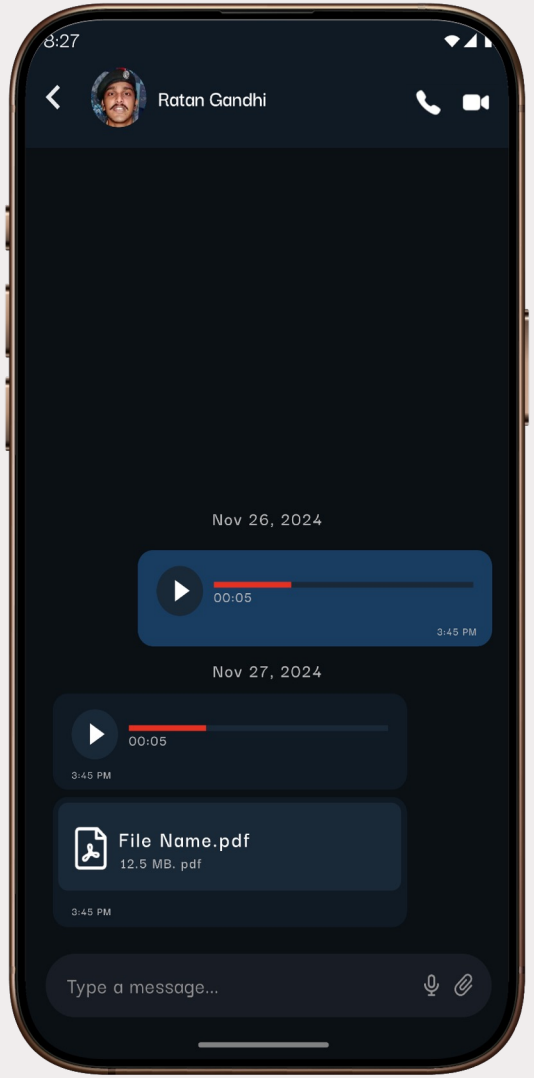
Server-Controlled, Quantum-Resilient Communication

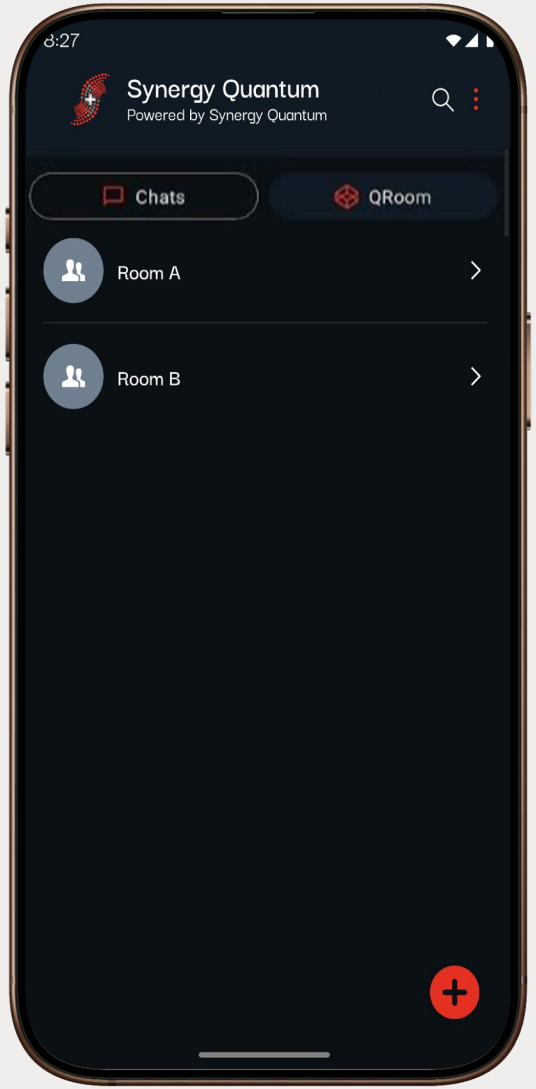
- ✓ Trusted devices authenticate first
- ✓ PQ-mTLS protects the transport
- ✓ QRSKM stays protected in the KMS
- ✓ Session & working keys are short-lived
- ✓ AES-256-GCM protects messages & files
- ✓ Storage remains ciphertext-only
- ✓ Policy controls access & rendering
- ✓ Revocation & rotation contain compromise
- ✓ Audit & monitoring give assurance

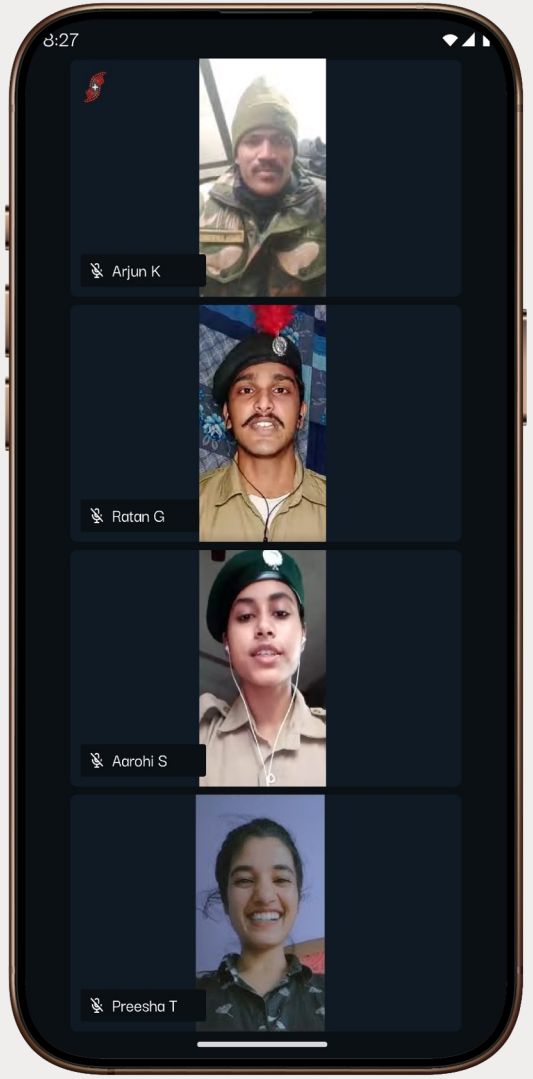
Secure messaging, collaboration and file exchange — with protected key custody, encrypted storage, and quantum-resilient architecture.

Client Interface (Mobile)



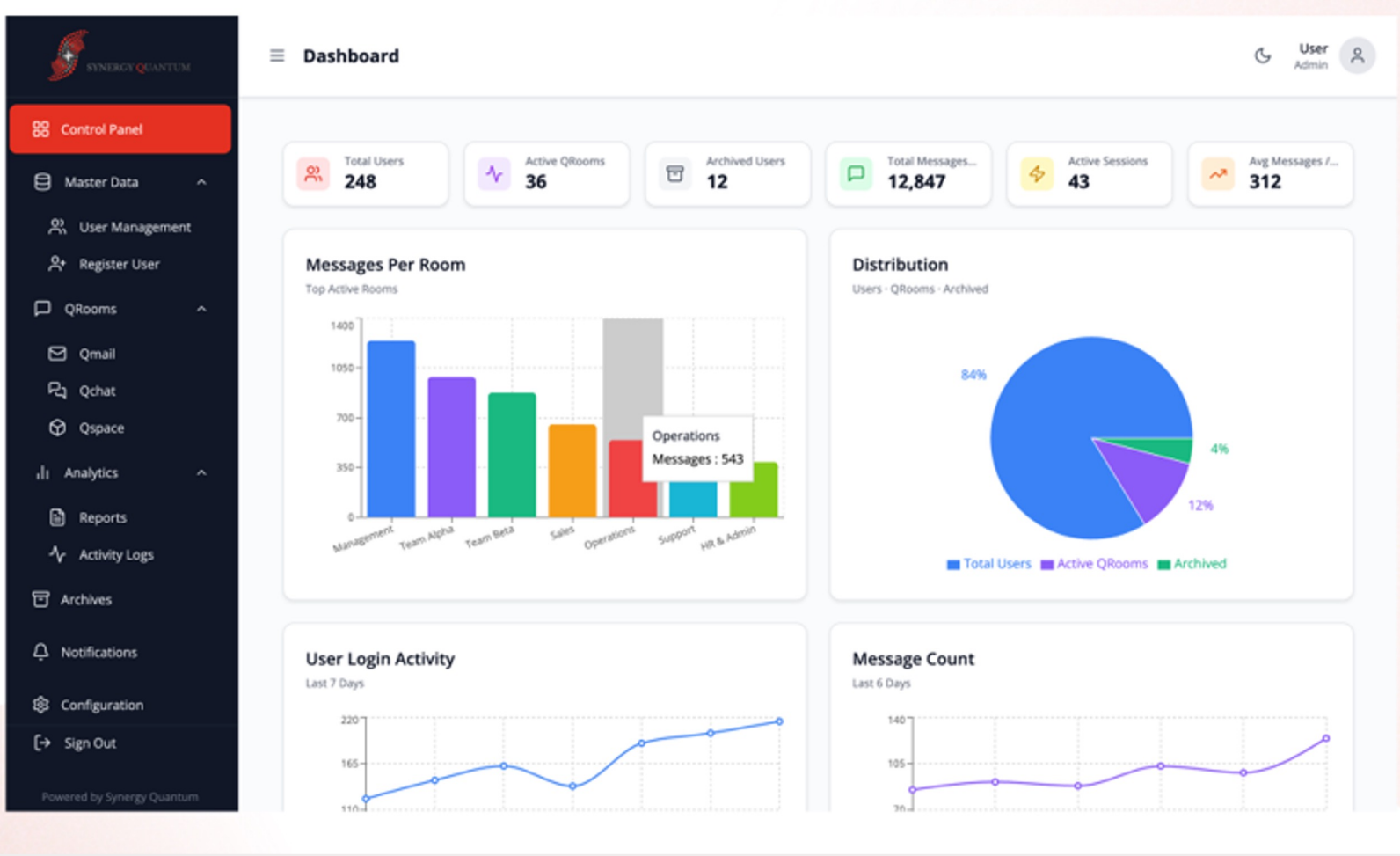






Monitoring and Management System

SynQ Messenger is designed to **integrate with existing IT infrastructure** & databases.



- Custom dashboards
- Integrated communication tracking
- Real-time communication monitoring
- Anomaly detection and threat analysis
- Automated situational reports
- Use Case: Force tracking and mission coordination

PRODUCT THREE

SynQ Quantum Shield

Post-Quantum Resilient VPN & Secure Network Access

16/07/26

01 OVERVIEW

Post-Quantum Resilient VPN

SynQ Quantum Shield protects data in transit using post-quantum cryptography and hybrid secure key exchange — built on standard VPN technology, deployable across servers, VMs, containers, and embedded systems.

The Problem

Classical VPNs rely on cryptography that may break in the quantum era. Enterprises need a migration path to quantum-resilient tunnels — without abandoning standard VPN architectures.

The Solution

Hybrid key exchange combines a classical and a post-quantum KEM, so tunnels stay secure today and resist future quantum attacks — a practical, standards-based transition.

02 KEY CAPABILITIES

What SynQ Quantum Shield Delivers

Post-quantum cryptography

ML-KEM for quantum-resistant key encapsulation.

Hybrid key exchange

X25519 + PQ KEM — classical and post-quantum combined.

Standard VPN technology

Built on IPsec; no proprietary tunnel stack.

AES-GCM tunnel traffic

Authenticated encryption for all payloads in transit.

Verifiable security

Validated with Wireshark and cryptographic tooling.

Flexible deployment

Servers, VMs, containers, and embedded environments.

Private subnet access

Secure, policy-controlled reach into private networks.

Risks SynQ Quantum Shield Mitigates

Man-in-the-middle

Mutual authentication and encrypted tunnels block interception and tampering.

Public Wi-Fi exposure

Traffic stays encrypted on untrusted and shared networks.

Data surveillance

AES-GCM tunnels prevent passive monitoring of payloads.

Credential interception

Certificate, PSK, and PPK auth resist credential theft.

Untrusted network access

Only authenticated, policy-approved devices reach private subnets.

Future quantum decryption

Hybrid PQ key exchange defends against harvest-now-decrypt-later.

04 DEPLOYMENT

Deploy Anywhere, Validate Everywhere

The same hybrid post-quantum tunnel runs across every environment — from data-centre servers to embedded devices.

Servers

Physical and cloud server estates

Virtual Machines

Hypervisor and cloud VM workloads

Containers

Docker and orchestrated environments

Embedded

Edge, IoT, and embedded systems

STANDARDS-BASED & VERIFIABLE

Built on IPsec with ML-KEM hybrid key exchange and AES-GCM tunnels — security can be inspected and confirmed with Wireshark and standard cryptographic tooling.

BUSINESS OUTCOME

Practical VPN Modernization for the Quantum Era

Secure today

AES-GCM tunnels and mutual authentication protect every session on untrusted networks.

Ready for tomorrow

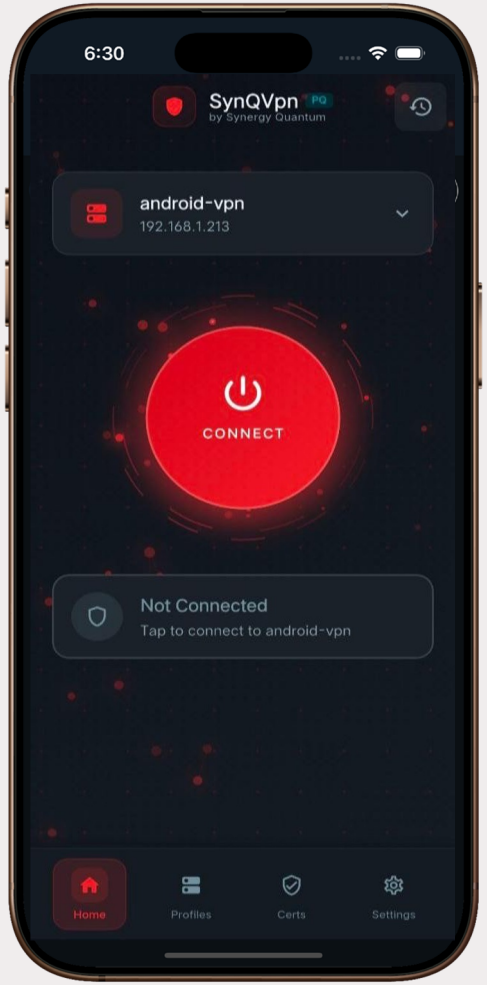
Hybrid ML-KEM key exchange defends against future quantum decryption.

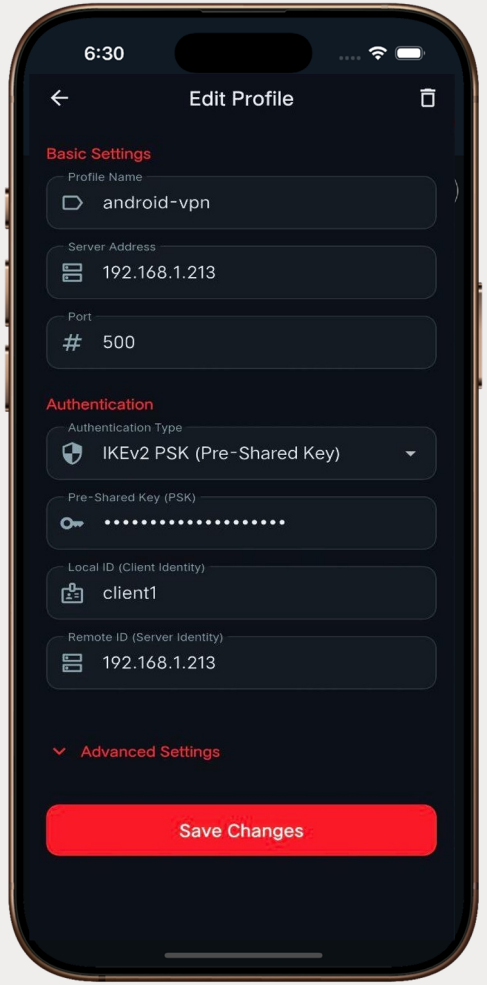
No rip-and-replace

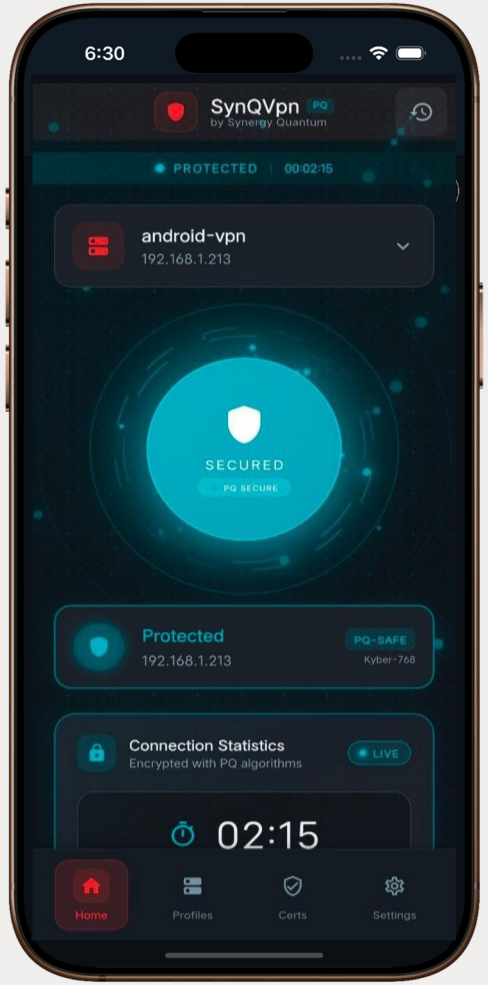
Built on standard IPsec VPN — a practical migration path, not a rebuild.

> *SynQ Quantum Shield enables secure network access and VPN modernization through a practical, standards-based hybrid post-quantum transition.*

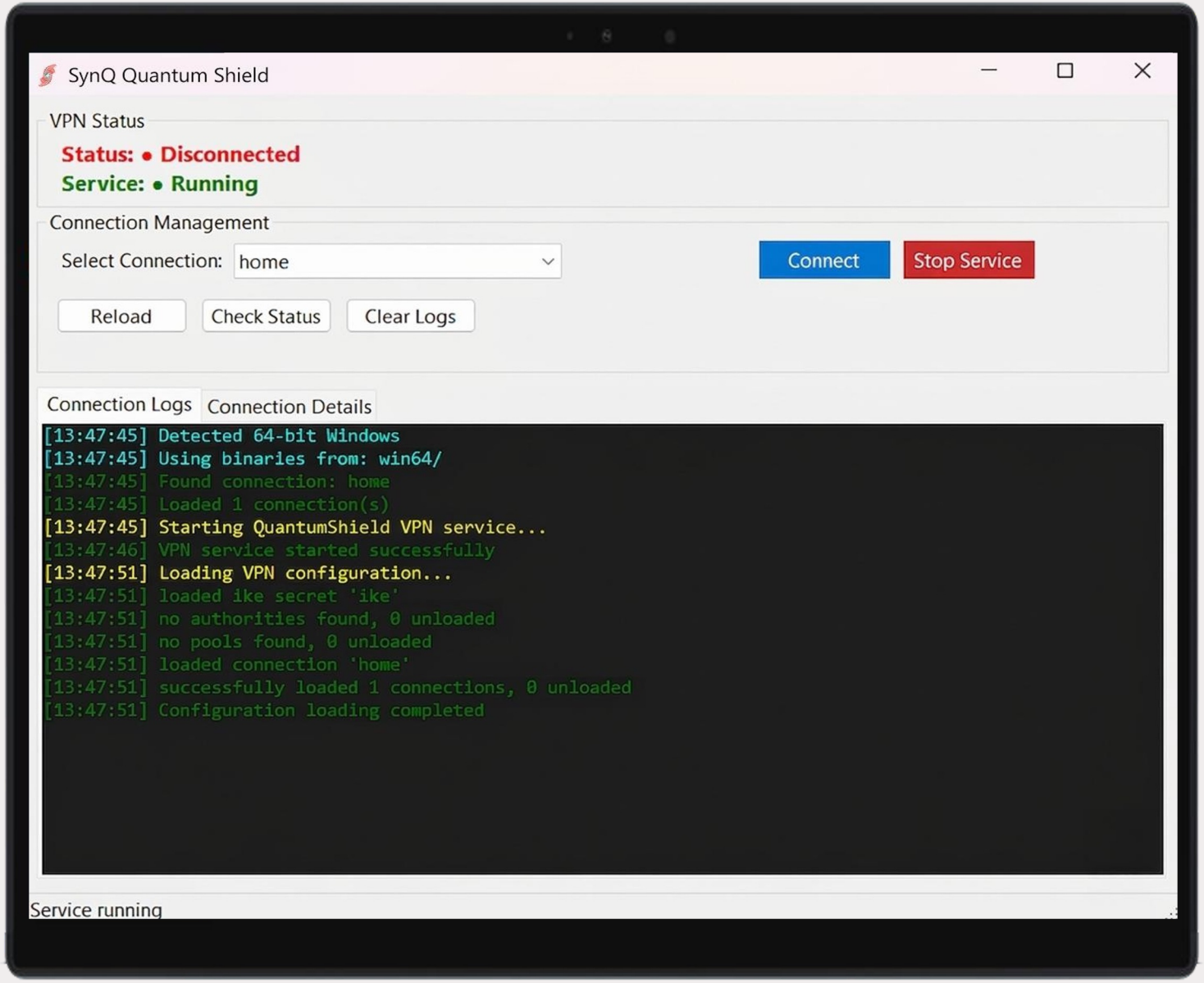
Client Interface (Mobile)







Client Interface (Windows)



PRODUCT FOUR

SynQ-HRoT

Sovereign Hardware Root of Trust — SQ-HRoT-01 Quantum-Safe ASIC

16/07/26

One Indigenous Chip, Sovereign Trust

SQ-HRoT-01 establishes the foundational layer of trust for a quantum-safe nation — from devices to data centres, from cities to strategic systems. Sovereign, quantum-safe, and secure by design.

Sovereign by Design

Indigenously designed and fabricated silicon — ending dependence on foreign TPM, HSM, and HRoT chips and the supply-chain risk that comes with them.

Quantum-Safe at the Root

Post-quantum cryptography embedded in hardware, so the root of trust resists both classical attack and the quantum threat to today's algorithms.

Why a Sovereign Root of Trust

Foreign dependence

Critical infrastructure relies on imported security chips — TPM, HSM, and HRoT — from foreign vendors.

Supply-chain risk

That dependence carries the risk of supply-chain attacks, backdoors, side-channel vulnerabilities, and kill switches.

Quantum threat

Quantum computing simultaneously threatens the cryptographic algorithms those chips implement.

The answer

SQ-HRoT-01 resolves both: a sovereign, indigenously fabricated, quantum-safe hardware root of trust.

Five Capabilities on One ASIC

PQC Algorithms

Quantum-safe post-quantum cryptography built directly into silicon.

PUF Identity

A physical unclonable function gives every chip a unique, unforgeable identity.

TRNG Entropy

A true random number generator supplies high-quality cryptographic entropy.

Chain of Trust

A hardware chain-of-trust engine anchors and verifies every boot stage.

Tamper-Resistant

Tamper-resistant design protects secrets against physical and side-channel attack.

Five-Layer Silicon Security Stack

TRUST FLOWS UPWARD

Host Interface Layer	Secure bus and API exposure to the host system
Cryptographic Services	PQC engines, signing, and key operations
Identity & Entropy	PUF device identity and TRNG entropy source
Chain-of-Trust Engine	Verified, measured boot across every stage
Immutable Trust Anchor	Tamper-resistant hardware root — the foundation

From Design to Sovereign Deployment

RTL Design & Verification → FPGA Prototype & Validation → Tape-Out (Domestic Fab) → Packaging & Testing → Deployment & Certification

Executed as a fully indigenous programme aligned to national design-linked-incentive support.

STRATEGIC IMPACT

Sovereign security
Eliminates dependence on foreign security silicon.

Indigenous capability
Strengthens the national semiconductor ecosystem.

Quantum-resilient future
Protects digital infrastructure against quantum threats.

Strategic advantage
Secures critical national assets, defence, and citizen data.

PRODUCT FIVE

SynQ-HSM

FPGA Hardware Security Module & Quantum-Ready HSM Enablement

16/07/26

01 OVERVIEW

Two Paths to Quantum-Ready Key Management

SynQ-HSM delivers quantum-resilient authentication and cryptographic key management two ways — a sovereign FPGA-based HSM, and a path to make the HSMs you already own quantum-ready today.

Sovereign FPGA HSM

A new, tamper-resistant FPGA platform that securely manages keys and accelerates cryptographic operations — secure, scalable, and quantum-ready by design.

Enable Your Estate

A lightweight, vendor-neutral PKCS#11 bridge makes the HSMs you already run PQC-ready — with reporting and migration workflows, and no rip-and-replace.

A Sovereign Hardware Security Module

A tamper-resistant FPGA platform that securely manages cryptographic keys and accelerates secure operations — delivering scalable, quantum-ready cryptographic infrastructure.

Tamper-Resistant

Hardware-protected key storage that resists physical and side-channel attack.

FPGA Acceleration

Reconfigurable silicon accelerates cryptographic operations at scale.

Secure Key Management

Full lifecycle custody — generation, storage, rotation, and destruction.

Quantum-Ready

Hybrid classical and post-quantum operation built in from day one.

03 HSM ENABLEMENT

Make Your Existing HSMs Quantum-Ready

A lightweight, standards-based, vendor-neutral path delivers PQC-enabled keys without ripping out the HSM estate you already own.

SQTIP Agent

Lightweight agent on the host

→

Encrypted Channel

Signed, encrypted link

→

PKCS#11 Bridge

Fronts the existing HSM

→

Existing HSM

Your current estate — now PQC-enabled

Result: PQC-enabled keys across the estate, with reporting and migration workflows — and no rip-and-replace.

Proven in the QEC: demonstrated against widely deployed enterprise HSMs, including the Thales Luna network HSM family — one platform, every HSM, vendor-neutral.

Open, Vendor-Neutral, Standards-Based

PKCS#11

Industry-standard interface for integrating with any HSM estate.

Hybrid Operation

Runs classical and post-quantum cryptography side by side.

FIPS 140-Series

Aligned with hardware key-protection assurance expectations.

NIST PQC Suite

Implements the FIPS 203 / 204 / 205 post-quantum algorithm set.

SECTOR VALUE

Sovereign Key Protection, Every Sector

Banks & Financial

Quantum-ready key custody for payments, signing, and long-lived financial records.

Government

Sovereign control of cryptographic keys for citizen and state data.

Defence

Hardened, tamper-resistant key management for mission and weapons systems.

Critical Infrastructure

Protects keys across energy, telecom, and transport control systems.

One platform, every HSM — a vendor-neutral path to quantum-ready key protection, with or without rip-and-replace.

PRODUCT SIX

SynQ-5G Core

Post-Quantum 5G & Beyond-5G Core for National Critical Infrastructure

16/07/26

01 OVERVIEW

A Sovereign, Quantum-Resistant 5G Core

An enterprise-grade, cloud-native 5G and beyond-5G core for national critical infrastructure — standards-aligned today and quantum-resistant for decades.

Cloud-Native & Sovereign

Containerised, owner-controlled core built for national deployment.

3GPP Release 17 SBA

Standards-based service-based architecture with HTTP/2 interfaces.

CP/UP Separation + Slicing

Control- and user-plane separation with full network-slicing support.

Carrier-Grade HA

High-availability design engineered for always-on critical networks.

02 ARCHITECTURE

3GPP Release 17 Service-Based Core

CONTROL PLANE — NETWORK FUNCTIONS

AMF	SMF	AUSF	UDM	PCF	NRF	NSSF	UDR

Service-Based Interface Bus • HTTP/2 • PQ-OAuth 2.0 secured

USER PLANE

UPF
User Plane Function — high-throughput packet forwarding & routing

NMS
Network Management System — orchestration & operations

Cloud-native foundation
Control/user-plane separation, network slicing, and carrier-grade high availability.

Ten Network Functions, One Sovereign Core

AMF
Access & Mobility Management

SMF
Session Management

UPF
User Plane Function

AUSF
Authentication Server

UDM
Unified Data Management

UDR
Unified Data Repository

PCF
Policy Control

NRF
Network Repository

NSSF
Slice Selection

NMS
Network Management System

Control Plane User Plane Management

Post-Quantum Innovations in the Core

Two innovations harden where classical 5G cores stay vulnerable — the machine-to-machine layer and key generation itself.

PQ-OAuth 2.0

Quantum-resistant API authorization

A notable first: post-quantum authorization across the service-based interfaces, hardening the machine-to-machine calls between network functions that classical 5G cores leave on conventional cryptography.

QRNG Integration

Quantum entropy at the source

Quantum random number generation strengthens key generation at the source, so every key in the core is rooted in true quantum entropy rather than deterministic pseudo-randomness.

STANDARDS & SECTOR VALUE

Standards-Aligned, Sovereign by Design

COMPLIANCE ALIGNMENT

NIST FIPS 203 / 204 / 205	**NSA CNSA 2.0**	**3GPP Release 17**
TS 33.501 (5G Security)	**ETSI Quantum-Safe**	**ISO/IEC 27001**

Telecom

Sovereign, quantum-resistant core for national carriers and private 5G.

Government

A cloud-native core under sovereign control for public networks.

Defence

Secure machine-to-machine signalling for tactical and base networks.

Critical Infrastructure

Quantum-safe connectivity for energy, transport, and utilities.

A sovereign, cloud-native 5G core that stays quantum-resistant for decades.

PRODUCT SEVEN

SynQ-MobileGuard

Quantum-Secure Android — Post-Quantum Trust from the OS to the Network Edge

16/07/26

The Most Exposed Surface, Hardened

Voice, messages, signalling, and data travel across networks never designed to withstand quantum-era threats — and adversaries are already capturing that traffic to decrypt later. MobileGuard hardens the operating system itself and the entire link between the device and every network it touches.

Hardened at the OS

Post-quantum protection built into the operating system and telephony stack — not bolted onto a single app.

Familiar Experience

Looks and behaves like a standard Android phone, with zero change to how users call, message, or use apps.

Security Built Into the Phone Itself

Hardened OS & Telephony

Post-quantum protection built into the operating system and the telephony stack — not bolted onto a single app.

Hybrid Cryptography

Classical and post-quantum algorithms combined: secure today, resilient against tomorrow's quantum adversary.

Familiar Experience

Looks and behaves like a standard Android phone, with zero change to how users call, message, or use apps.

One Trust Model, Three Tiers

A single post-quantum trust model runs from the application surface down to every radio interface.

Tier 1 — Application Surface

Voice, messaging, and apps — the user-facing experience, unchanged.

Tier 2 — Operating System

Hardened OS and telephony stack with post-quantum protection embedded.

Tier 3 — Network Edge

Every radio interface — mobile, Wi-Fi, and enterprise — under one PQ model.

Connectivity Fabric, Extended to the OS

SynQ Connect

THE SECURE-CONNECTIVITY FABRIC

Establishes cryptographically protected channels between trusted devices and the secure vault.

+

SynQ-MobileGuard

EXTENDS PROTECTION OUTWARD

Carries that protection into the OS and out through every radio interface — mobile, Wi-Fi, and enterprise.

One unified post-quantum trust model — closing the gap between the devices people carry and the post-quantum future.

SECTOR VALUE

Securing the Most Exposed Surface

Defence

Quantum-secure handsets for tactical voice, messaging, and signalling in the field.

Government

Hardened mobile devices for officials, with no change to everyday usability.

Intelligence & Diplomatic

Protected communications for missions operating on untrusted foreign networks.

Enterprise Mobility

Post-quantum protection for executive and BYOD fleets across mobile and Wi-Fi.

MobileGuard closes the gap between the devices people already carry and the post-quantum future the world is moving towards.

PRODUCT EIGHT

SynQ-MythGuard

Machine-Speed Exposure Management Against AI-Driven Attack Surfaces

16/07/26

01 OVERVIEW

The Problem Is Exposure Velocity

Frontier-class AI discovers, chains, and weaponises weaknesses across code, identity, cryptography, cloud, and AI agents at machine speed — while defenders still patch on quarterly cadences. MythGuard collapses that asymmetry.

73%
expert-task success rate for a frontier system on hardened cyber ranges

32
steps to a simulated corporate-network takeover — in 3 of 10 runs

271
bugs patched in a single browser release via frontier-AI discovery

Illustrative figures cited by Synergy Quantum to frame the shift in attacker capability.

Five Stages, Run at Machine Speed

1. Discover	2. Correlate	3. Prioritise	4. Validate	5. Remediate
Continuous discovery across code, binaries, containers, APIs, certificates, and agents.	Build the Exposure Graph linking code, service, identity, data, and exploit paths.	Score each finding by exploitability, reachability, privilege, and patch age.	Filter AI-generated noise by confirming deployed versions and runtime reachability.	Route to owners, track patch SLAs, and escalate aged criticals to leadership.

A continuous loop — outcomes feed back into discovery, so defenders outpace machine-speed attackers.

How MythGuard Ranks What Matters

THE RISK SCORE

Risk = Exploitability × Reachability × Privilege × Patch Age

SEVEN BILLS OF MATERIALS

- SBOM
- LBOM
- CBOM
- AIBOM
- NCBOM
- QCBOM
- KBOM

One Exposure Graph

All seven inventories link code, service, identity, data, and exploit paths into a single graph — so every finding is scored in context, not in isolation.

Ten Attack Surfaces Defended

1	Old or copied code
2	Known CVEs in dependencies
3	Memory corruption
4	Browser, parser & JIT chains
5	Multi-step exploit chaining
6	Weak cryptography
7	Hardcoded secrets
8	Cloud & Kubernetes misconfig
9	AI-agent trust-boundary abuse
10	External attack surface

OPERATIONAL ROLLOUT

From Backlog to Machine-Speed in 90 Days

DAYS 1–30	DAYS 31–60	DAYS 61–90
Discover	**Prioritise**	**Remediate & Govern**
Connect code, container, cloud, and binary sources. Run SBOM, LBOM, CBOM, and AIBOM inventories, stand up NCBOM external discovery, and build the first Exposure Graph.	Tune the attack-surface score, map owners to top exposed assets, identify the most reachable assets per business unit, and validate chains to suppress noise.	Enforce the 7-day SLA for internet-facing criticals, roll out the patch-SLA and executive dashboards, review AI-agent trust boundaries, and begin the PQC-readiness roadmap.

> *MythGuard doesn't out-hack frontier AI — it removes the backlog those systems depend on, so patching, hardening, and governance run faster than AI can chain weaknesses.*

SYNERGY QUANTUM