qnulabs.com

The Quantum Threat: Preparing for a New Era of Cyber Risk

The Quantum Threat

A New Era of Cyber Risk

Quantum Computers are arriving, faster than anticipated!!

Quantum computing promises revolutionary advances in science and innovation. But it also poses a direct threat to current encryption systems such as RSA, ECC, and Diffie-Hellman, which secure the internet today. Quantum algorithms like Shor's and Grover's can crack these within minutes, rendering traditional cryptography obsolete.

What's at Stake?

Defence Systems

Inter-location fiber optic links, command center-to-troops communication, drone control channels, and weapon telemetry are all vulnerable to quantum-enabled interception and spoofing—jeopardizing battlefield advantage, strategic operations, and national security.

Government & Critical Infrastructure

Governments and critical infrastructure face growing quantum-era risks, with sensitive data vulnerable to interception and decryption, threatening blackouts, transport disruptions, and national security.

BFSI

Quantum attacks can decrypt secure financial transactions, compromise digital signatures, expose customer data, and manipulate stock trading systems. Institutions face systemic risks and irreversible breaches.

Cybersecurity is facing a seismic shift. Are you prepared?

Telecom

Core network signaling, 5G/6G communication, and inter-operator data exchanges can be hijacked, leading to surveillance, disruption, or mass-scale data theft.

Healthcare

Sensitive patient records, proprietary drug research, and clinical trial data could be accessed, modified, or leaked -threatening privacy and disrupting innovation.

Enterprise IT

Email systems, collaboration platforms, VPNs, and cloud infrastructure protected by traditional crypto will all be vulnerable—creating massive regulatory, reputational, and financial exposure.

Why Enterprises Must Act Now

Proactive Is the New Secure

With the rise of quantum computing and AI-driven cyberattacks, the urgency to adopt quantum-safe security has never been higher. The cyber threat landscape is evolving faster than ever - organizations must act before vulnerabilities are exploited.

Key Reasons to Act Now

Harvest Now, Decrypt Later Attacks

Adversaries are intercepting sensitive data today to decrypt later with quantum computers, putting intellectual property, financial records, and classified files at risk.

Long-Term Data Privacy

Contracts, health records, legal files, and financial data have retention spans of 10+ years. Only quantum-safe solutions can protect this long-term information horizon.

Future-Proofing Infrastructure

Security upgrades later will cost more. Integrate quantum-safe systems today to reduce future technical debt.

AI-Powered Attacks

Attackers now leverage AI to discover vulnerabilities, automate phishing, and penetrate networks faster than ever—amplifying the threat and reducing the response window.

Global Shift Toward Compliance to Quantum Standards

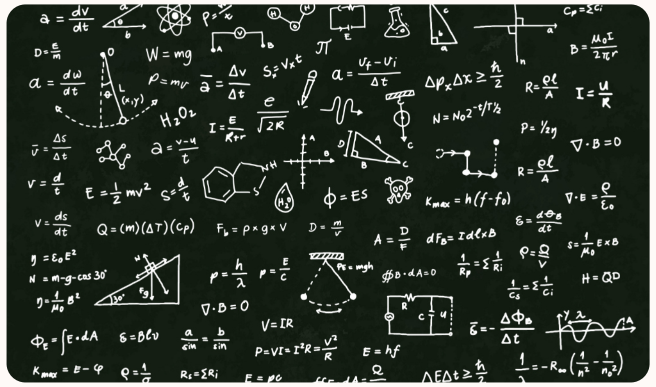
With NIST's PQC standards released and countries like the US, India, and China investing heavily in quantum tech, quantum-safe readiness is becoming a boardroom priority.

Navigating the Quantum Shift

What Are Your Options?

Two Proven Paths to Quantum-Safe Security

The products use quantum principles and technologies like QKD, QRNG, and QHSM to enable unbreakable encryption, secure keys, true randomness, and tamper-proof storage, ensuring unconditional security.



Quantum-safe cryptography uses lattice algorithms to resist classical and quantum attacks, running on existing systems without extra hardware. In August 2024, NIST approved Kyber, Dilithium, and SPHINCS+.

What if you could get the best of both worlds?

The Hybrid Approach

Progressive enterprises are adopting a layered strategy that blends quantum hardware and post-quantum software. By combining QKD for mission-critical links with PQC for scalable applications, organizations achieve comprehensive protection-securing both high-value assets and everyday digital workflows in a cost-effective, future-ready manner.

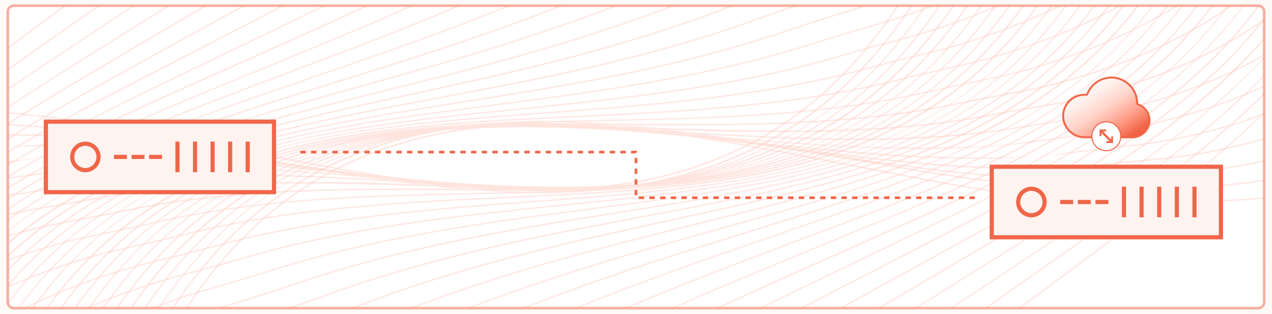
QNu Labs' Quantum-Safe Solutions for Enterprises

Enabling Scalable, Hybrid Security for the Post-Quantum World

At QNu Labs, we deliver integrated, future-proof quantum-safe solutions that secure digital infrastructure end-to-end by combining quantum physics, post-quantum algorithms, and seamless enterprise integration.

Quantum-Safe End-to-End Networks

Secure Your Communications Infrastructure - From Core to Edge



As digital infrastructure underpins national security, finance, and citizen services, protecting communication channels is critical. Classical encryption is increasingly vulnerable, especially across backbone links like data centers, telecom hubs, command centers, satellites, branch offices, and mobile units.

QNu Labs enables enterprises, governments, and telecoms to build hybrid quantum-safe networks combining physical quantum protection and software flexibility. Using **Armos (Terrestrial QKD)**, **Digital QKD**, **Free-Space QKD**, and **QKDN Controller**, we deliver secure, scalable, and future-proof communications across diverse regions and threats.

Key Capabilities:

Establish ultra-secure, physics-backed data links between critical sites using Armos and Digital QKD, eliminating key transmission and preventing interception—even by quantum computers.

Extend secure communication to the last mile with Free-Space QKD-a line-of-sight quantum encryption solution ideal for mobile command posts, naval assets, remote stations, or field units where fiber is unavailable.

Centrally manage key distribution and security policies with QKDN, overseeing both physical and digital QKD nodes while providing continuous monitoring, role-based access, and dynamic threat response.

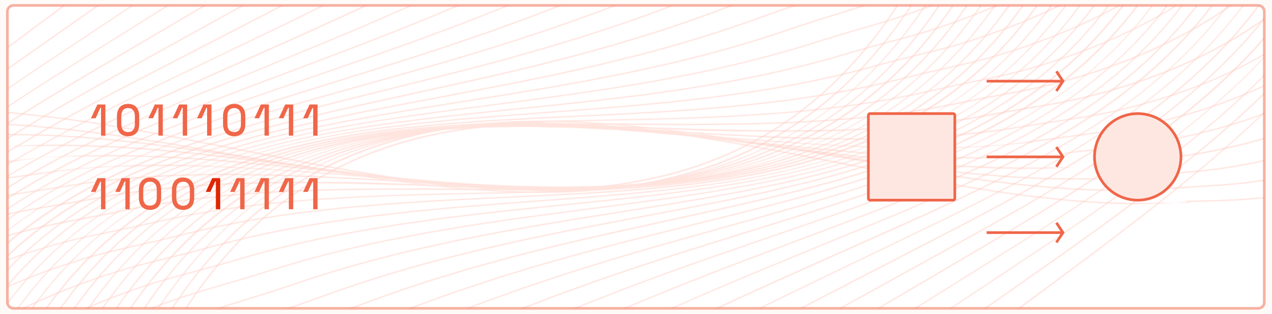
Build layered, high-availability mesh networks that operate across cities and continents. QNu's solutions support hub-and-spoke, ring, and mesh topologies-preventing single points of failure and enabling true end-to-end integrity.

Solution Components: QKD, Digital QKD, Free Space QKD, QKDN

Ideal For: Telecom & Government

Quantum-Safe Enterprise for Data in Transit & at Rest

Secure Your Digital Operations—From Data Centers to Devices



In a digital-first world, enterprises in banking, telecom, and healthcare handle sensitive data protected by classical encryption, soon vulnerable to quantum computing. Transitioning to quantum-safe infrastructure is a proactive business and compliance necessity.

QNu Labs drives this transformation with a modular, crypto-agile security architecture that integrates with existing systems. The QShield platform secures communications, collaboration, storage, and identity using next-gen encryption and true quantum randomness.

Key Capabilities:

Establish post-quantum site-to-site VPNs between data centers, branch offices, and global partner locations using PQC and QRNG-based entropy—ensuring sensitive data (financial, medical, operational) remains protected from interception and future decryption.

Enable secure remote access for employees through quantum-safe encrypted tunnels, safeguarding enterprise systems from credential theft and data leakage in hybrid, remote, or public network environments.

Facilitate secure collaboration and long-term file sharing by encrypting communication channels and file storage systems—protecting sensitive documents such as financial statements, legal contracts, and health records from tampering or unauthorized access.

Deliver future-proof authentication systems by integrating QRNG-enhanced cryptographic keys—ensuring unpredictable, quantum-resilient access controls across user logins, devices, and enterprise apps.

Issue and manage digital certificates using post-quantum cryptography, securing HTTPS, email, code signing, and VPN access—even in the face of quantum-capable adversaries threatening traditional PKI systems.

Centralize encryption key lifecycle management with crypto-agile systems that support key generation, rotation, and revocation across multiple encryption protocols—eliminating gaps in compliance, security posture, and cryptographic hygiene.

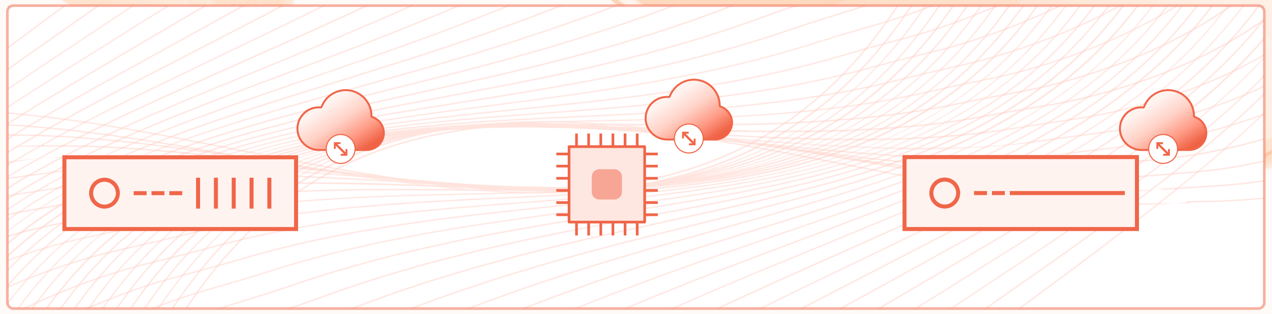
Solution Components: QConnect, QVerse, QSFS, QVault, QHSM, Qosmos, and Tropos

Ideal For: All Enterprises (Gov, BFSI, Telco, Healthcare, Manufacturing, Automobile)

Quantum Safe IoT Connectivity

End-to-End Quantum Security for Edge and IoT Devices

Enterprises and governments deploy billions of IoT devices, pushing the security perimeter from a central point to vulnerable, unattended network edges.



QNu Labs offers a next-generation quantum-safe security stack for IoT and edge devices, ensuring integrity, confidentiality, and identity verification at the device level. This solution is ideal for defense, critical infrastructure, industrial automation, smart surveillance, and next-gen mobility, where traditional security is vulnerable to quantum-enabled threats.

Key Capabilities:

Secure IP phones and video conferencing endpoints in defense, government, and corporate offices by encrypting voice and video traffic with quantum-safe tunnels—protecting sensitive discussions from eavesdropping and tampering.

Secure telemetry and control of drones in disaster relief, and border surveillance—ensuring that communication between unmanned systems and base stations remains tamper-proof and confidential.

Safeguard IP camera feeds in smart cities, critical facilities, and transport hubs by encrypting video streams and preventing hijacking or deepfake injection into monitoring systems.

Protect autonomous vehicles and industrial robots from data spoofing, command injection, and network-based tampering—critical for both safety and operational continuity.

Enable quantum-secure communication between remote sensors and centralized command systems in nuclear plants, oil rigs, or battlefield zones.

Solution Components: QShield RAC, QShield Platform, Tropos, Communication Chip

Ideal For: All Enterprises (Gov, BFSI, Telco, Healthcare, Manufacturing, Automobile)

QNu Labs' Quantum-Safe Product Suite

QNu Labs delivers a comprehensive portfolio of quantum-resilient solutions that safeguard data and communication across critical industries. Our suite combines hardware-grade quantum security with seamless enterprise integration, backed by 10+ patents, global validations, and strategic deployments.

Armos – Quantum Key Distribution (QKD) System

The future of key exchange—no transmission, no interception.

Armos, QNu Labs' flagship QKD system, uses quantum physics to securely generate and distribute encryption keys without transmitting them, preventing interception. It's deployed in mission-critical defense and enterprise fiber-optic networks.

ARMOS - QKD

Key Differentiators:

- TEC Certified
- Supports 200 km point-to-point, scalable via trusted nodes
- Enables secure hub-and-spoke intercity quantum networks
- ETSI-compliant for global interoperability

Tropos – Quantum Random Number Generator (QRNG)

The gold standard of randomness—trusted for critical security

Tropos is a hardware-based QRNG that uses the principles of quantum physics to generate truly unpredictable random numbers. It is available in multiple form factors—PCIe card, chip, and compact USB—for seamless integration across systems.

TROPOS - QRNG

Key Differentiators:

- Complaint to NIST test suite
- Certified by CR Rao & ISI Kolkata
- Low-latency and high-throughput generation

QHSM – Quantum Hardware Security Module

Protecting digital roots of trust— at the edge, in the cloud, and everywhere in between.

QHSM is a tamper-proof module designed to manage, store, and process cryptographic keys using quantum-safe mechanisms. It supports traditional and post-quantum algorithms.

QHSM

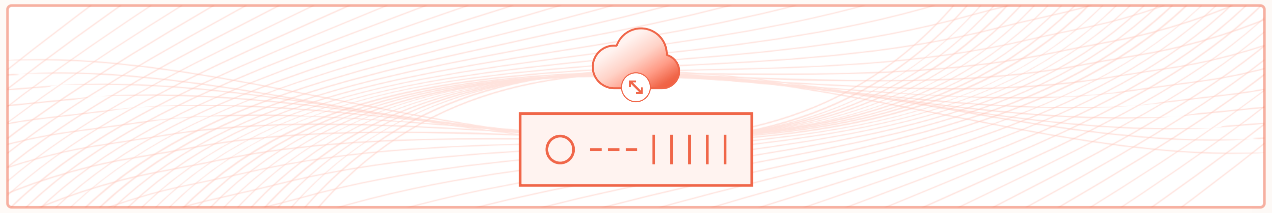
Key Differentiators:

- FIPS Complaint
- Support PQC and QRNG
- High Availability with TPS > 8000

Digital QKD – Software

Scalable quantum key exchange—built for enterprises, tested for the future

Digital QKD is a scalable, software-based Quantum Key Distribution solution that enables quantum-safe key exchange over optical fiber using QRNG and PQC algorithms, offering an affordable and flexible path to quantum-secure communications.



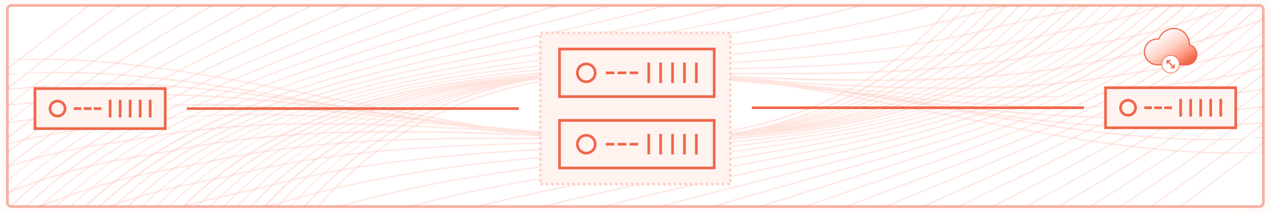
Key Differentiators:

- Software-based QKD
- Plug-and-play with existing optical links
- Compact and cost-effective ideal for enterprises

QKDN – Network Controller & Orchestrator

Orchestrating hybrid QKD deployments across the globe

QKDN is QNu Labs' platform for managing hardware and Digital QKD nodes, enabling scalable, intelligent, and resilient quantum-safe networks for secure key exchanges across any distance.



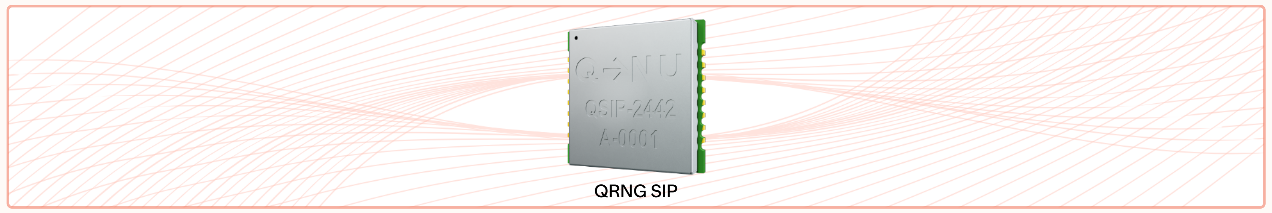
Key Differentiators:

- Complaint to ETSI standards
- Role-based access control
- Device configuration management
- Map & Topology View

Quantum Communication Chip

Taking Quantum Inside

The Quantum Communication Chip is a compact, FPGA-based module that integrates Quantum Random Number Generation (QRNG) and Post-Quantum Cryptography (PQC) capabilities on a single chip. Designed for IoT devices, drones, autonomous systems, and next-gen edge networks, it enables ultra-secure, low-latency communication even in resource-constrained environments.



Key Differentiators:

- Compact, power-efficient, and edge-ready
- NIST PQC and QRNG chip
- Easy to integrate with any OEM providers

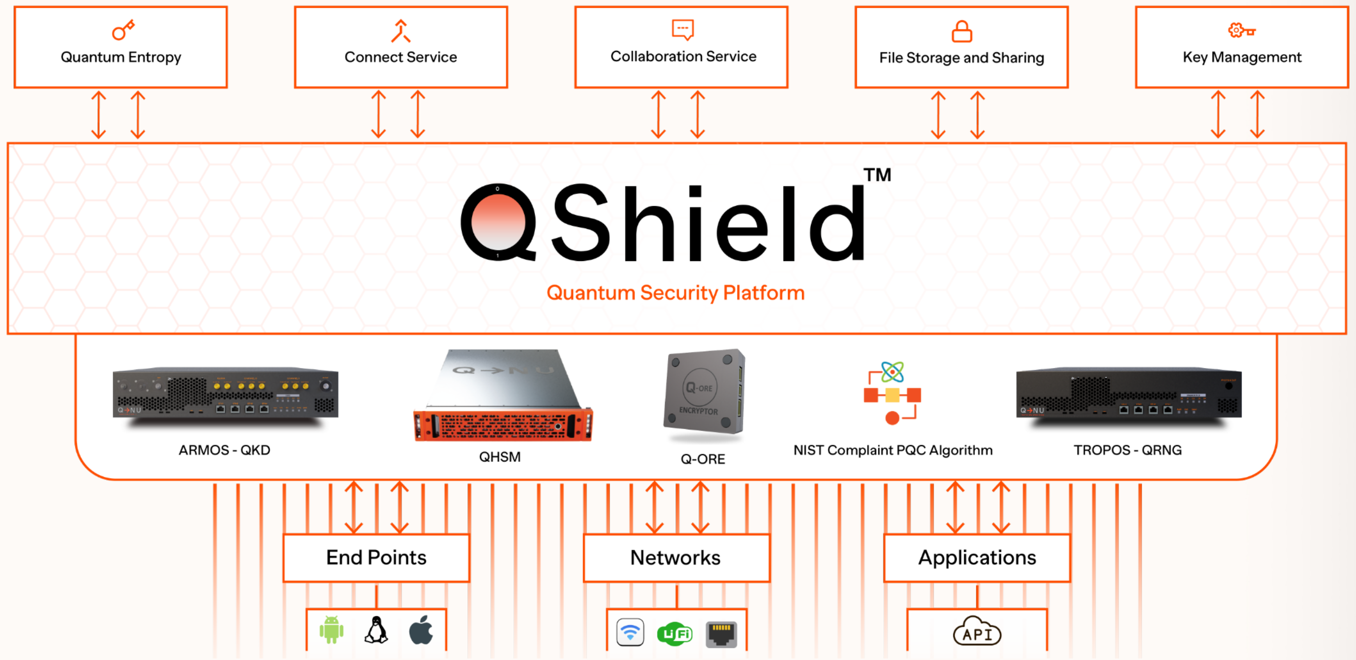
Use Cases:

- Secure drone-to-base and satellite communications
- Quantum-safe IoT device onboarding and telemetry
- Embedded security for autonomous vehicles and defense-grade edge devices

QShield – Your Gateway to Quantum Secure Services

From endpoints to the cloud—quantum-resilient security, simplified

QShield is QNu Labs' cloud-native SaaS platform delivering end-to-end quantum-safe security across VPNs, file sharing, messaging, and key management. Built on NIST-approved post-quantum algorithms and enhanced with QRNG-generated entropy, QShield enables enterprises to adopt quantum-resilient infrastructure without needing specialized hardware. It integrates seamlessly with existing IT systems, offering flexible deployment options, unified control, and plug-and-play scalability.



Key Differentiators:

- NIST-compliant PQC for future-ready encryption
- Built-in crypto agility for evolving threats
- Integrates QRNG, QKD, QHSM as needed
- Flexible pricing: subscription, perpetual, enterprise
- Scalable, secure, multi-tenant, no infrastructure changes

About QNu Labs

Accelerating the World's Transition towards Quantum Secure Future.

QNu Labs, founded in 2016 at IIT Madras Research Park and backed by India's National Quantum Mission, leads in quantum cybersecurity, securing digital infrastructure against quantum threats. It aims to make India a global leader in quantum-secure communications and supports digital sovereignty by 2047.

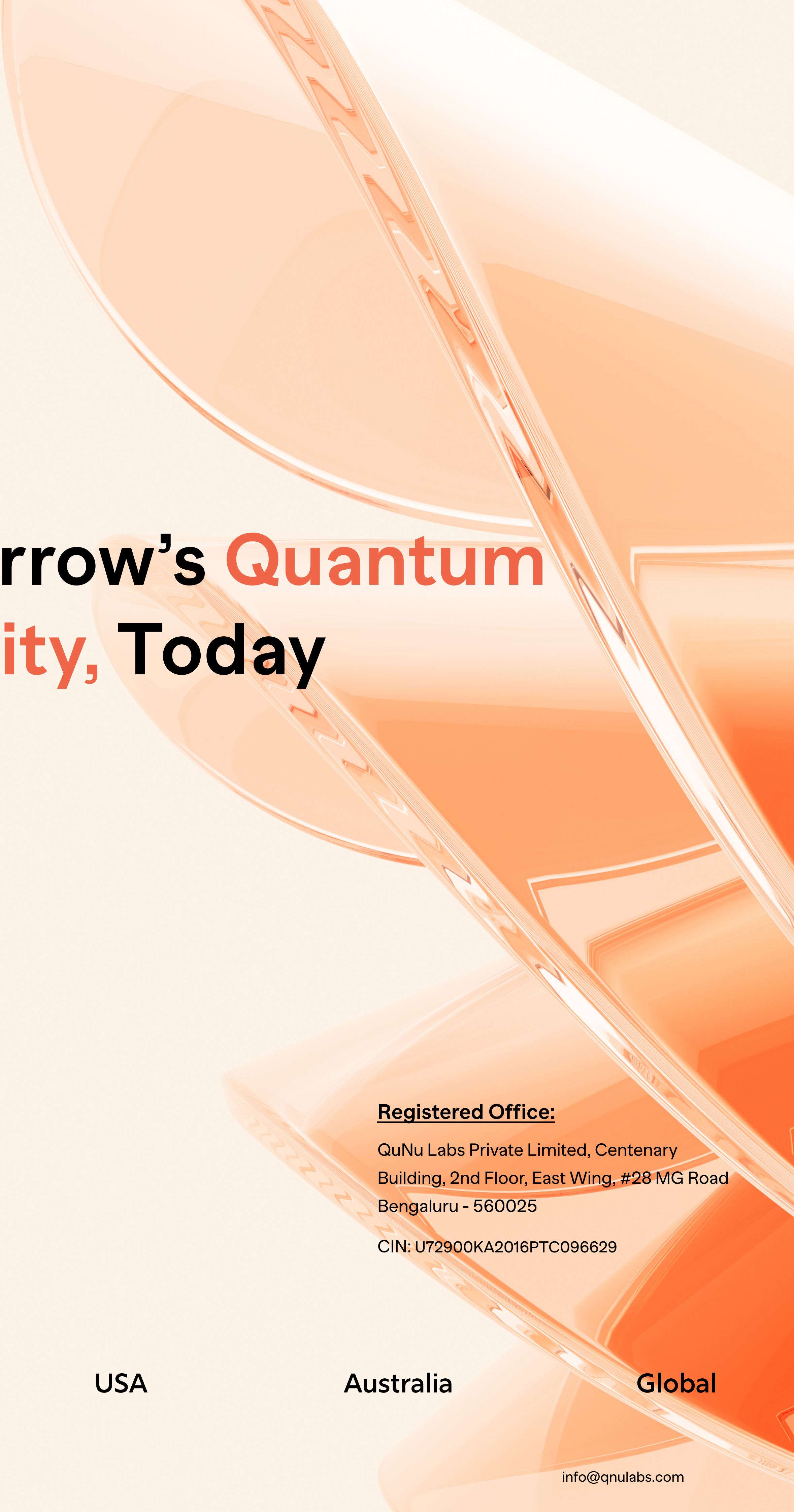
Championing Atmanirbhar Bharat, Make in India, and Digital India, QNu Labs delivers true quantum randomness and tamper-proof protection. Its flagship product, QShield™, is an indigenous, plug-and-play quantum-safe platform with a three-layer stack, meeting NIST, FIPS, and Indian standards. Tested in military-grade environments, it's available on AWS and the GeM portal.

QNu embeds Quantum Random Number Generators in devices and is building a 1,000 km QKD network, plus free-space and satellite QKD. Their portfolio includes a quantum-safe drone communication platform. Trusted by governments, defense, and various industries, QNu offers scalable, flexible, and seamless security solutions.

With offices in the US and Australia, QNu Labs supports global collaboration and has presence across the Middle East, Africa, Far East, APAC, and Europe.

Trusted Partnerships & Global Recognition

Trusted Clients



QNU

Proactively™
Quantum

Tomorrow's Quantum Security, Today

Scan for more details

Registered Office:

QuNu Labs Private Limited, Centenary
Building, 2nd Floor, East Wing, #28 MG Road
Bengaluru - 560025

CIN: U72900KA2016PTC096629

India USA Australia Global

info@qnulabs.com