

Quantum-Ready Today: A Comprehensive Guide to Securing Digital Infrastructure in the Post-Quantum Era

August, 25

Executive Summary: Pioneering Quantum-Resilient Security

Addressing the Imminent Quantum Disruption

The advent of quantum computing poses a fundamental threat to classical cryptography. Moontrace confronts this disruption head-on with a full-stack platform designed to manage the entire cryptographic lifecycle, safeguarding sensitive data against future threats like "Harvest Now, Decrypt Later" attacks.

A Global-First, Transparent Foundation

As a global-first organization founded in India, our core philosophy is to make advanced security accessible. We are committed to being developer-friendly, cost-efficient, and operationally transparent, accelerating time-to-market and reducing implementation friction for our partners.

Our Unified Suite for End-to-End Assurance

We provide a cohesive suite of cutting-edge tools—VANTAGE, APX, Moontrace VPN, and QUBEx. Together, they form an integrated solution for discovery, migration, secure transport, and hardware-based key management, ensuring a seamless transition to a quantum-safe posture.

Empowering the Post-Quantum Era

Our ultimate goal is to empower organizations to navigate the post-quantum world with confidence. We provide the tools and expertise necessary to gain complete visibility, migrate securely, and manage cryptographic assets effectively, future-proofing digital infrastructure for decades to come.

The Quantum Imperative: Threat & Opportunity

The Imminent Quantum Threat

Shor's Algorithm: The development of a cryptographically-relevant quantum computer capable of running Shor's algorithm poses an existential threat to current public-key cryptography, such as RSA and ECC. These algorithms form the foundation of today's digital security infrastructure.

'Harvest Now, Decrypt Later' (HNDL): This critical threat involves adversaries collecting and storing encrypted data today with the intention of decrypting it once powerful quantum computers become available. This makes the threat immediate, as today's data is retroactively vulnerable.

Mosca's Theorem: A Call for Proactive Migration

This theorem frames the urgency of quantum risk. It states that if the time required to migrate to new quantum-safe systems (Y) plus the time your data needs to remain secure (Z) is greater than the time until a quantum computer can break current encryption (X), you are already at risk.

If $(Y + Z) > X$, you are vulnerable.

Given the significant time needed for migration (Y), proactive and immediate action is essential to prevent future security breaches.

Core Challenge for Enterprises

Enterprises face the enormous task of protecting sensitive customer data, intellectual property, and trade secrets from retroactive decryption. They must also manage complex supply chains and adhere to evolving data protection laws, making the transition to PQC a significant operational and compliance challenge.

Core Challenge for Governments

For government and defense sectors, the challenge is one of national security. Ensuring the long-term confidentiality of state secrets, intelligence, diplomatic communications, and safeguarding critical infrastructure like energy grids and financial systems is paramount and requires an immediate shift to quantum-resistant technologies.

Core Challenge for Developers

Developers face the complex technical task of integrating new, standardized PQC algorithms into existing and future systems. This requires ensuring system compatibility, managing new cryptographic libraries, and upskilling the workforce in quantum-safe development practices, all while maintaining agile development cycles.

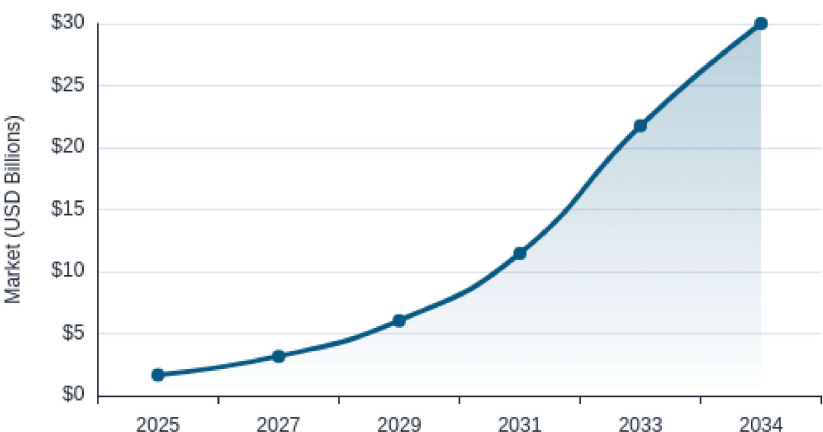
Accelerating Market Growth & Opportunity

The confluence of these threats and challenges is driving an unprecedented and rapidly accelerating global market for Post-Quantum Cryptography solutions. Standardization efforts and rising awareness are creating a significant opportunity for platforms that can simplify and secure the migration to a quantum-safe future.

Massive Market Opportunity & Growth Projections

Global PQC Market Forecast

Surging from **\$1.68B** (2025) to **\$30B** (2034)



Projected 37.72% CAGR

High Growth

Global Demand

Quantum Urgency

Indian PQC Market: Strategic Importance

As a global-first company founded in India, we recognize the nation's pivotal role. India's rapid digitalization and focus on data sovereignty create a significant growth vector for PQC, particularly within its critical national infrastructure.

Critical Sector Growth Opportunities in India



Defense Sector

Essential for safeguarding national security, classified communications, and strategic digital assets from advanced quantum attacks.

National Security

Secure Comms



Finance Sector

Crucial for protecting sensitive financial transactions and ensuring long-term integrity of records against quantum-enabled fraud.

Financial Integrity

Data Protection



Health Sector

Imperative for securing patient privacy, sensitive medical records, and valuable research data in compliance with regulations.

Patient Privacy

Regulatory Compliance

Market Opportunity & Key Drivers



Urgent Global Demand for PQC

The "Harvest Now, Decrypt Later" threat makes quantum-resilience an immediate necessity. Adversaries are storing encrypted data today to be broken by future quantum computers, forcing a global proactive transition to PQC to protect long-term data confidentiality.

HNDL Threat

Proactive Migration

Data Confidentiality



Rising Threats & Regulatory Push

Heightened awareness of quantum threats is driving governments and regulatory bodies like NIST and ANSSI to establish clear PQC standards and migration roadmaps. This regulatory push creates a compliance-driven imperative for organizations worldwide to adopt quantum-safe technologies.

Cybersecurity Risk

Regulatory Mandates

Global Standards



Strategic Importance of India

As a rapidly expanding digital economy and technology hub, India represents a critical landscape for PQC adoption. The "Digital India" initiative and the need to secure national infrastructure and a vast user base make it a strategic market for quantum-resilient solutions and innovation.

Digital India

Emerging Market

Innovation Hub



Broader Quantum Market Expansion

The PQC market is part of a larger quantum technology ecosystem. The expansion includes complementary technologies like Quantum Key Distribution (QKD) for secure communication channels and Quantum Random Number Generators (QRNGs) for superior cryptographic key entropy, creating a holistic security market.

Quantum Ecosystem

QKD & QRNG

Future-Proofing

Vision, Mission & Core Philosophy

OUR VISION

Secure Cryptography for All, Globally

OUR MISSION

**Making Global Cryptographic Infrastructure
Visible, Agile, and Quantum-Secure**

FOUNDATIONAL PHILOSOPHY

**Global-First, Developer-Friendly, Cost-Efficient,
Transparent**

Moontrace Core Solutions: Discovery & Migration

Moontrace VANTAGE

Comprehensive Cryptographic Visibility

Holistic Cryptographic Discovery: Moontrace VANTAGE serves as the critical first step in achieving quantum resilience by providing deep, real-time visibility across your entire IT infrastructure. It automatically discovers and inventories all cryptographic assets, including certificates, keys, and algorithms, irrespective of their deployment location—on-premise, in the cloud, or hybrid environments.

Precision Risk Assessment: This comprehensive inventory enables immediate identification of quantum-vulnerable cryptography and legacy systems. By leveraging advanced analytics, VANTAGE allows for precise quantum risk assessments and the strategic prioritization of at-risk data and systems.

Real-time Inventory

Vulnerability Mapping

Risk Prioritization

Automated Discovery

Compliance Readiness

Moontrace APX

Simplified PQC Migration and Agility

Streamlined PQC Transition: Beyond discovery, Moontrace APX streamlines the often-complex transition to post-quantum cryptography. It offers an agile platform designed for seamless migration and continuous cryptographic security, minimizing operational disruption and ensuring compliance with evolving security directives and standards.

Future-Proof Agility & Management: APX automates the deployment of new, standardized PQC algorithms, facilitating the necessary transition away from existing data security frameworks. Its inherent agility allows organizations to adapt rapidly to new threats and cryptographic advancements, ensuring secure key management and simplified updates across diverse digital ecosystems.

Automated Migration

Agile Deployment

PQC Standard Integration

Secure Key Management

"There will be disruption from both the transition away from existing data security frameworks and the deployment of entirely new technologies, platforms, and systems in the post-quantum cryptography world."

— Arit Kumar Bishwas, Quantum Computing Research Director

Moontrace Solution Suite: Secure Transport & Key Management

Moontrace VPN: Quantum-Resilient Secure Tunneling Solution

Moontrace VPN is a next-generation virtual private network engineered from the ground up with Post-Quantum Cryptography (PQC). It addresses the critical need for secure data-in-transit in the quantum era.

By employing a hybrid cryptographic model, it encrypts traffic using both classical and NIST-standardized PQC algorithms. This dual-layer approach provides immediate protection against "Harvest Now, Decrypt Later" threats while ensuring a seamless transition for existing infrastructure.

The core value lies in providing robust, quantum-safe tunneling for all network traffic, securing remote access and sensitive data against both current and future adversaries.

Data-in-Transit Security

Hybrid PQC Mode

HNDL Protection

Moontrace QUBEx: Hardware-Based Quantum Key Management System

Moontrace QUBEx is a robust hardware appliance that forms the foundation of a quantum-resilient trust infrastructure, providing an advanced system for secure quantum key management.

The system integrates with Quantum Random Number Generators (QRNGs) to guarantee true, unpredictable randomness for cryptographic key generation and performs secure, out-of-band key exchange, isolating key management from software vulnerabilities.

Its value lies in establishing the strongest possible root of trust, ensuring superior key randomness and scalable, secure key delivery to future-proof an organization's cryptographic ecosystem.

Hardware Root of Trust

Quantum Randomness (QRNG)

Secure Key Lifecycle

Platform Architecture & Technical Foundations

Holistic Cryptographic Lifecycle

From discovery to migration and continuous operation, Moontrace's platform provides a seamless, integrated approach to cryptographic lifecycle management. This ensures a consistent security posture, agile adaptation to new threats, and comprehensive oversight.

Our solutions automate processes from initial vulnerability identification (VANTAGE) to rapid deployment of new algorithms (APX), guaranteeing an always-on, future-proof security ecosystem.

Discovery

Migration

Monitoring

Automation

Standards-Compliant Quantum Security

Our architecture strictly adheres to the latest Post-Quantum Cryptography (PQC) algorithms standardized by NIST. This commitment ensures compliance with evolving federal and industry security mandates, providing proven quantum-resistance.

We actively implement and support algorithms like ML-KEM, ensuring our platform provides cryptographic strength that is recognized and validated by leading global authorities, future-proofing your data.

NIST Compliance

Quantum-Resistant

ML-KEM Ready

Industry Standard

Quantum-Enhanced Randomness

At the core of robust cryptographic security lies true randomness. Moontrace's platform supports interfaces for Quantum Number Generation (QNG), leveraging the inherent unpredictability of quantum mechanics to produce truly random numbers.

This provides the strongest possible foundation for cryptographic key generation and secure protocol operation, fortifying against even the most sophisticated predictive attacks.

Cryptographic Strength

Unpredictable

QNG Supported

Key Foundation

Engineered for High-Stakes Environments

Every component of the Moontrace platform is engineered with a 'mission-critical' mindset. This means designing for extreme resilience, high availability, and the protection of the most sensitive data and national security assets.

Our architecture minimizes attack surfaces and ensures operational continuity, making it suitable for environments where failure is not an option.

High Resilience

Zero Trust

Operational Continuity

Data Sovereignty

"Echoing the National Cyber Security Centre Finland, we urge all organizations handling sensitive data to begin planning their transition to quantum-safe algorithms."

— Bittium Blog

Strategic Use Cases & Target Audiences

Enterprises

For corporations, the focus is on a seamless transition away from vulnerable legacy systems. Our platform facilitates complex PKI migration, ensures adherence to evolving data protection regulations, and provides robust security for long-term intellectual property and sensitive customer data.

PKI Migration

Compliance

Data Security

Governments & Defense

National security hinges on the long-term confidentiality of state secrets and the integrity of critical infrastructure. We provide the tools to protect classified intelligence and secure essential communications against sophisticated, state-level quantum threats.

Long-Term Secrets

Critical Communications

National Security

Developers & Innovators

We empower developers to be at the forefront of the quantum-safe transition. Our developer-friendly tools and APIs enable the integration of PQC from the ground up, fostering a new generation of inherently secure, future-proof applications and systems.

Future-Proof Systems

Secure by Design

PQC Integration

Business Model & Monetization Strategy

SaaS Licensing

A recurring revenue model based on flexible subscriptions for our core software suite. This ensures predictable income and continuous value delivery to our clients through ongoing updates and support.

This includes licenses for **VANTAGE** (visibility), **APX** (migration), and the **Moontrace VPN** (secure transport).

Recurring Revenue

Scalable Tiers

Continuous Updates

Hardware Sales with Subscription

Direct sales of our robust **QUBEx** hardware appliances, which provide the physical root of trust for quantum key management.

Hardware sales are coupled with a mandatory recurring subscription for essential firmware updates, maintenance, and technical support, creating a hybrid revenue stream.

One-Time Sale

Mandatory Support Subscription

Firmware & Security

Professional Services

High-value consulting and implementation services to guide clients through their PQC transition. This generates revenue while ensuring successful customer adoption and long-term partnership.

Services include comprehensive quantum risk **audits**, custom **integration** support, and strategic **advisory** on PQC roadmaps.

Consulting Fees

Bespoke Solutions

Expert Guidance

Product & Certification Roadmap



Team, Advisors & Future Outlook

Founding Team: Visionaries Driving Quantum Innovation

Moontrace is driven by a core team of visionaries with a singular focus: to solve the complex challenges of the post-quantum era. Our founders possess a deep understanding of cryptography and cybersecurity, and are committed to building a platform that is not only technologically advanced but also accessible and developer-friendly. Our early-stage structure allows for agility and a relentless focus on our mission to secure global digital infrastructure.

Mission-Focused

Agile & Lean

Deep Expertise

Strategic Advisors: Guiding Our Path to Market Leadership

We recognize that navigating the nascent PQC market requires diverse expertise. We are actively seeking strategic advisors from academia, industry, and government to help shape our product roadmap, guide our market strategy, and ensure our solutions meet the highest standards of security and compliance. Your insights will be invaluable in our journey to become a market leader.

Seeking Guidance

Industry Foresight

Technical Validation

Join Us: Inviting Contributors, Investors, and Partners

Building a quantum-resilient world requires a collective effort. Moontrace is extending an open invitation to passionate contributors, forward-thinking investors, and strategic partners to join us. Whether you are a cryptography expert, a talented engineer, an investor seeking the next frontier in cybersecurity, or an organization looking to build a quantum-safe future, we want to hear from you.

Seeking Talent

Investment Opportunity

Strategic Alliances

Future Outlook: Building a Quantum-Resilient Tomorrow, Together

Our vision is to build an enduring company that stands as a pillar of trust in the digital economy. By combining our foundational expertise with the collective intelligence of our future team, advisors, and partners, we will develop the critical infrastructure needed for a secure post-quantum world. Together, we will not only address a pressing security need but also shape the future of digital trust.

Long-Term Vision

Collaborative Growth

Shaping the Future

Frequently Asked Questions

Why is addressing PQC urgent now?

The primary driver is the "**Harvest Now, Decrypt Later**" (**HNDL**) threat. Adversaries are collecting encrypted data today, knowing future quantum computers could "crack the best current encryption in hours or minutes" (PwC).

With 60-78% of organizations expecting quantum mainstream by 2030 (KPMG), it's crucial to "begin planning their transition to quantum-safe algorithms" now (Bittium).

Harvest Now Decrypt Later

Imminent Threat

Proactive Planning

How do you mitigate hybrid crypto risks?

Moontrace enables a phased, secure transition with hybrid approaches, avoiding disruptive "rip and replace" strategies. This allows current systems to operate securely alongside new quantum-safe algorithms.

Our platform facilitates seamless integration of NIST-standardized PQC algorithms (e.g., ML-KEM), minimizing interoperability risks and ensuring cryptographic agility for engineers managing this complex shift (IETF).

Phased Transition

Interoperability

NIST-Aligned

What are your key differentiators?

- **Integrated End-to-End Platform:** Full-stack solution from discovery to hardware-based key management.
- **NIST-Aligned & Quantum-Enhanced:** Uses NIST-standardized algorithms and true randomness via Quantum Number Generation (QNG).
- **Mission-Critical Design:** Engineered for high-stakes environments ensuring resilience and operational continuity.
- **Global & Developer-Friendly:** Solutions built for broad adoption and ease of integration by developers.

Full-Stack

NIST-Certified

QNG

Resilience

How do you support compliance?

Our solutions adhere to global PQC standards from NIST, ANSSI, and the European Commission. We help organizations perform quantum risk assessments (Capgemini, KPMG) to meet compliance needs.


We also align with national initiatives (e.g., PQC Finland), ensuring our algorithms are tailored for specific national security and industry practices.

NIST Compliance

Risk Assessment

Strategic Roadmap

The Immediate Impact: Quantum Threat Perception


78%

US organizations expecting Quantum mainstream by 2030


95%

German leaders seeing high relevance/impact of Quantum on security


65%

German leaders perceiving high risk to their own data from Quantum