WHITE PAPER

Building Telecom Resilience in the Quantum Era

ENTRUST

SECURING A WORLD IN MOTION

Contents

Introduction

Telecom operators are facing an increasingly hostile cyber environment. As critical infrastructure providers, they are prime targets for ransomware, AI-driven attacks, and state-sponsored espionage. In 2025, ransomware featured in 75% of system-intrusion breaches, according to the Verizon Data Breach Investigations Report (DBIR). For example, SK Telecom suffered a major cybersecurity breach in April 2025, potentially exposing USIM authentication data for its entire subscriber base – about 27 million users. At the same time, supply chain compromises, such as the Snowflake breach that impacted AT&T, exposed millions of records. State-backed attacks such as Salt Typhoon against U.S. carriers in 2024 and the destructive attack on Kyivstar in 2023 further highlight the geopolitical dimension of telecom threats.

The threat landscape is intensifying: 53% of telecom companies expected breach costs to exceed $3 million, according to the EY 2023 Global Cybersecurity Leadership Insights Study. Further, Ericsson's 2023 report on quantum computing and 5G security highlights that rapid advancements in quantum computing pose a direct threat to mobile network confidentiality, requiring urgent adoption of quantum-resistant cryptography and protocols. Meanwhile, compliance obligations are increasing. Global mandates like NIS2 and DORA in Europe and FCC rules in the U.S. impose strict obligations, with hefty fines up to €10 million or 2% of turnover.

Against this backdrop, quantum computing represents not just a technological evolution but a seismic disruption to the foundations of digital security. The migration to post-quantum cryptography (PQC) is for most organizations extensive and non-trivial; it requires re-engineering deeply embedded cryptographic systems across operating environments, IoT devices, PKI infrastructures, and encryption key management and protection solutions. This process is complex and time-consuming, requiring careful coordination among telecom operators, vendors, regulators, and standards bodies.

Delaying action introduces significant risks. Bad actors are already harvesting encrypted data today with the intent to decrypt it once quantum capabilities mature ("harvest now, decrypt later"). Moreover, the transition period itself creates exposure, as hybrid cryptographic schemes and interim solutions may introduce new vulnerabilities if not carefully implemented.

For telecom operators, the imperative is clear. They must begin strengthening resilience by adopting adaptive security frameworks, initiate structured PQC migration roadmaps aligned with NIST and regional mandates, and ensure compliance strategies are harmonized across diverse regulatory regimes. Early, proactive action not only reduces the risk of quantum-enabled breaches but also positions operators to lead in delivering secure, trusted services in the quantum era.

This white paper explores how telecom operators can address the three critical priorities: strengthening resilience, beginning PQC migration, and aligning compliance strategies. It also provides actionable guidance to help operators move from reactive defense to proactive transformation.

Building Cyber Resilience: Beyond Traditional Defenses

Telecom operators have implemented robust security measures, but the evolving threat landscape demands more than traditional defenses. Traditionally, telecom operators have relied on:

- **Encryption and public key infrastructure (PKI)** for securing data and authenticating devices
- **Hardware security modules (HSMs)** to safeguard cryptographic keys
- **Centralized key management** with rotation and automated certificate management
- **Identity and access management (IAM)** controls such as multi-factor authentication (MFA), Zero Trust architecture, and principle of least privilege (PoLP)

While these measures form the foundation of cyber resilience, gaps persist. Some of the key gaps include:

1. **Key management issues:** Mismanagement, misuse, proliferation, loss, non-rotation, reuse, and weak pseudo-random number generators (RNGs) compromise encryption integrity. Managing PKI effectively across 4G and 5G environments, too, is complex.

> According to one global telco expert, "Managing public key infrastructure (PKI) at scale across 4G and 5G environments is complex. We face challenges in ensuring interoperability between legacy systems and modern cryptographic frameworks, while maintaining high availability and compliance. Frequent updates to certificate policies and automation of key management are critical to avoid service disruptions and reduce operational overhead."

2. **Limitations of passwords and MFA:** MFA adoption is uneven, and passwords remain vulnerable to phishing and credential stuffing.
3. **Inconsistent IAM across networks and supply chain:** Vast, heterogeneous telecom networks lead to fragmented and inconsistent identity governance.
4. **Compliance complexity:** Fragmented regulations, such as FCC mandates in the U.S., NIS2 and DORA in the EU, the UK Telecoms Security Act, and APAC's diverse data laws strain resources and divert focus from proactive defense.

> A UK-based industry subject matter expert noted, "The UK Telecom Security Act introduces stringent requirements for risk assessment, vendor assurance, and cryptographic controls. Aligning our infrastructure and processes with these mandates requires significant investment in governance frameworks and continuous auditing. This is compounded by the need to manage third-party integrations securely across a diverse vendor ecosystem."

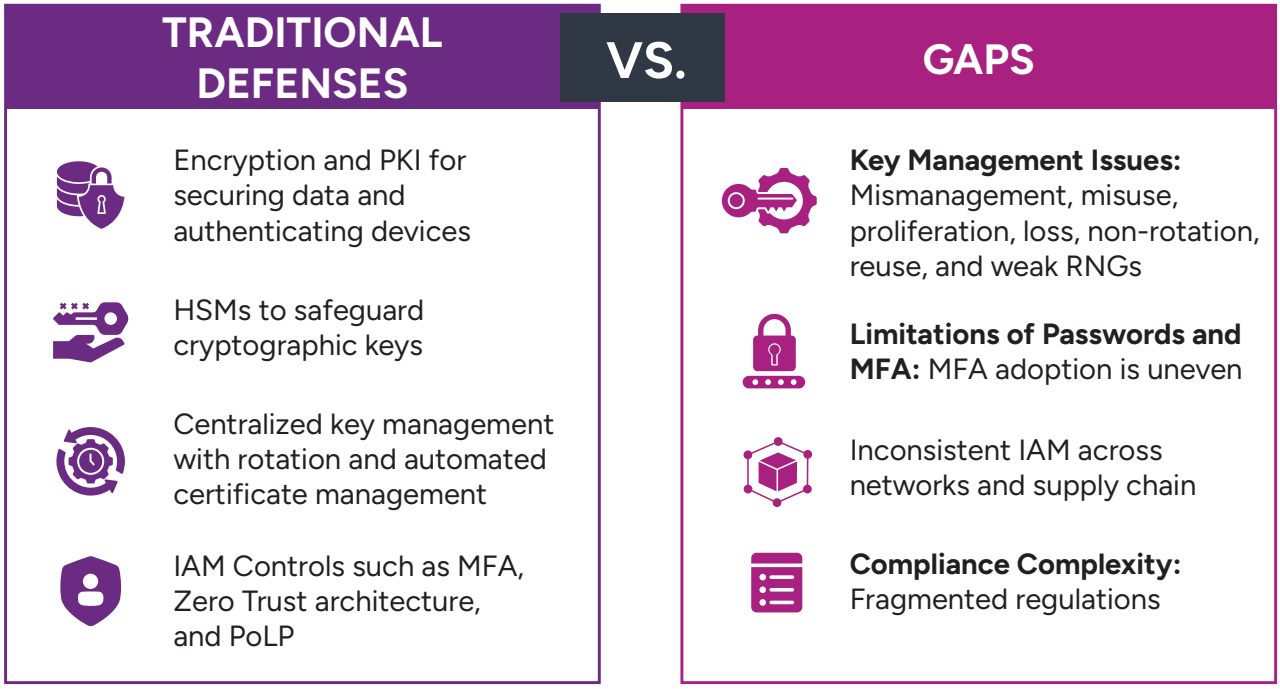


Figure 1: Traditional Defenses vs. Gaps

These gaps give rise to new and evolving challenges and attack vectors. They include:

- **AI-driven threats:** A lack of secure AI processes and deepfake fraud are key challenges telecom companies face. According to Entrust's 2026 Identity Fraud Report, deepfake fraud now drives about 20% of biometric attack attempts. Fraudsters use AI-powered methods like synthetic identities, face swaps, and animated selfies to bypass verification systems. They often pair deepfakes with injection attacks to evade live capture checks.
- **Supply chain exploits:** The telecom infrastructure is complex and relies heavily on third-party vendors, suppliers, and partners, which creates a large attack surface. A vulnerability in a single supplier's hardware, software, or service can cascade and compromise the security of the entire telecom network and its customers. Flaws in third-party or open-source software used in the network can also be exploited to gain unauthorized access.
- **Increased phishing, ransomware, and DDoS attacks:** As the telecom industry is part of critical infrastructure, it is often targeted by well-funded and state-sponsored criminal groups. These attacks range from DDoS attacks, 5G and IoT exploitation, to attacks on operational technology (OT) and industrial control systems (ICS). According to the 2025 Verizon Data Breach Investigations Report (DBIR), ransomware was present in 75% of system-intrusion breaches in 2025, up from 2024. Further, the Verizon 2024 DBIR found that the human element contributed to 68% of breaches.
- **Post-quantum risks:** Quantum computing could break current RSA and ECC asymmetric algorithms, exposing encrypted traffic and stored data as early as 2030–2035. Software update authentication can become vulnerable due to reliance on PKI, digital timestamps for high-value targets like contracts could be attacked, and long-term data storage may become vulnerable due to attacks on wrapping mechanisms used for keys, leading to breach of privacy, network disruption, and reputational damage.

"The quantum threat is very real for the telecom sector – it's firmly on our radar. Quantum computing introduces the risk of "harvest now, decrypt later" attacks, where adversaries store encrypted data today with the intent to break it once quantum capabilities mature. This could have serious implications for the confidentiality and integrity of our networks and customer data," according to one European mobile phone expert.

- **TLS 1.3 visibility and PQC-driven complexity (a new industrial challenge):** TLS 1.3 is essential for PQC-ready security, offering stronger protection, faster performance, and modern cryptographic defaults. It encrypts more of the handshake and removes legacy algorithms, improving privacy, performance, and security for users.
- However, this enhanced encryption creates major challenges for telecom network operators and service providers by sharply reducing network layer visibility and breaking traditional middlebox-based monitoring and lawful intercept workflows. Decrypting and inspecting TLS 1.3 traffic is also resource intensive, often requiring costly hardware upgrades to avoid bottlenecks.

Mitigation strategies include:

- **Endpoint-level security:** Shifting monitoring and enforcement from the network to the endpoint.
- **Session key intercept (SKI):** Extracting session keys for legal/authorized monitoring.
- **Behavioral analysis:** Using AI/ML to analyze packet behavior and traffic patterns rather than relying on payload inspection.

To move beyond reactive security, telecom operators should implement industry best practices, including:

- **Implementing adaptive security frameworks:** Shift from static controls to dynamic, risk-based models that adjust to threat intelligence.
- **Integrating artificial intelligence (AI) for proactive threat detection:** AI-driven analytics can identify anomalies and predict attacks before they escalate.
- **Strengthening supply chain security:** Enforce vendor risk management and continuous monitoring to mitigate third-party vulnerabilities.
- **Adopting Zero Trust at scale:** Extend Zero Trust principles across information technology (IT), OT, and cloud environments for holistic protection.
- **Regular cryptographic audits:** Take inventory and validate cryptographic assets to prepare for PQC migration.

PQC Readiness: The Time to Act

Quantum computing is no longer a distant concept; it is a looming reality that will fundamentally disrupt today's cryptographic foundations. Traditional cryptographic algorithms like RSA and Elliptic Curve Cryptography (ECC), the bedrock of secure communications today, will be broken with ease once large-scale cryptographically relevant quantum computers (CRQCs) emerge. And experts believe that this may happen as early as 2030.

The need to transition to post-quantum cryptography (PQC) is fueled by three key interconnected factors:

- **Harvest now, decrypt later (HNDL):** Threat actors are already exfiltrating massive amounts of sensitive data today, intending to decrypt it once quantum capabilities mature. Quantum cloning and quantum collision attacks are a few other potential post-quantum threats telecom operators need to prepare for.
- **Implementation complexity:** Migrating to PQC is not a quick patch; it requires a fundamental redesign of cryptographic systems, protocols, and applications across the entire ecosystem. Telecom networks rely on deeply embedded cryptography in operating systems, PKIs, IoT devices, and HSM roots of trust. Introducing PQC means re-engineering these layers without disrupting service continuity.
- **Time-intensive transition:** The migration to PQC spans years because telecom environments are vast and heterogeneous. NIST standardized the first three PQC algorithms in August 2024. Moreover, the organization plans to deprecate ECDSA and RSA algorithms by 2030 and officially disallow their use by 2035, giving organizations less than five years to migrate to PQC. Operators must synchronize upgrades across thousands of endpoints, legacy systems, and third-party vendor products. A phased roadmap is essential, but even with aggressive timelines full migration may take years, making early action critical to avoid interim vulnerabilities. Delaying action risks exposure during the transition.

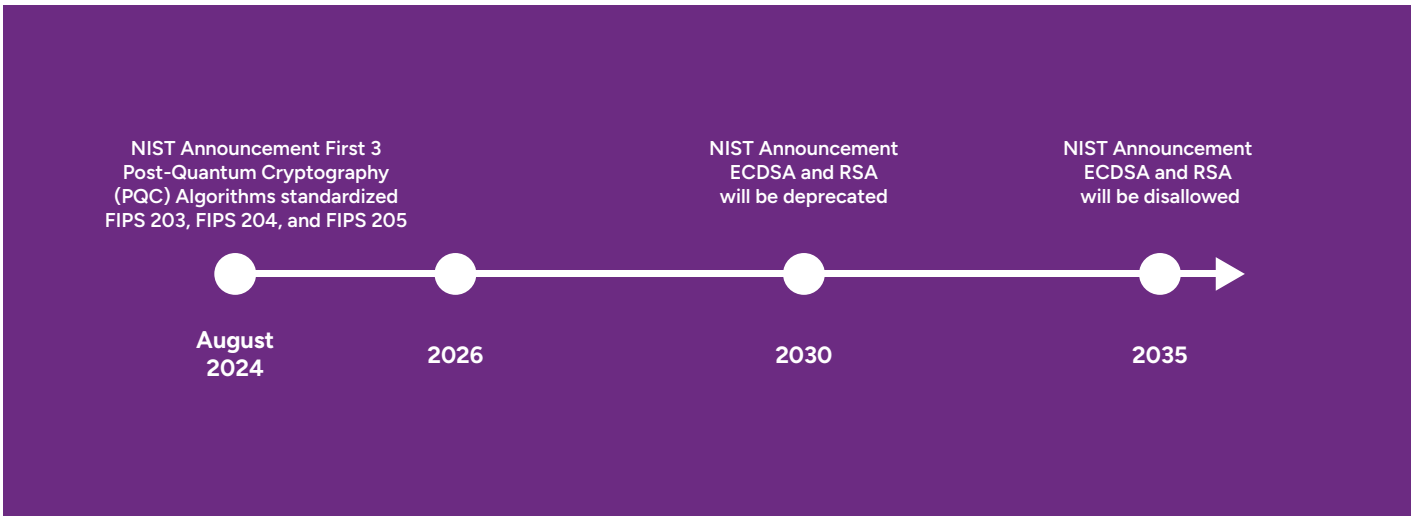


Figure 2: PQC – NIST timelines

While there is an urgent need to migrate to PQC, challenges abound:

- **Synchronizing upgrades across heterogeneous networks:** Public-key cryptography is woven into every layer of telecom infrastructure, from operating systems and applications to HSMs, embedded devices, and PKI root authorities. Public-key cryptography is deeply embedded everywhere – operating systems, applications, HSMs, embedded devices, and PKI roots. Coordinating the simultaneous upgrade of a massive number of dependent systems across disparate networks, often involving legacy or vendor-locked equipment, is a monumental task. The migration must avoid introducing chaos or downtime.

> "Telecom networks are vast and heterogeneous, spanning legacy systems, cloud-native platforms, and critical network functions. Migrating cryptographic algorithms across such diverse environments without service disruption is a major operational hurdle." Telecom infrastructure expert

- **Performance trade-offs:** The new PQC algorithms, while quantum-resistant, often have larger key sizes, larger ciphertexts, and sometimes slower performance compared to their asymmetric counterparts. This impacts network bandwidth, data storage needs, and the latency of cryptographic operations, particularly on low-power devices like IoT sensors. Benchmarking these performance trade-offs against operational requirements is essential.
- **Interim vulnerabilities and hybrid schemes:** There is no single perfect PQC algorithm, and cryptographers are still verifying their long-term security. Hence, a hybrid cryptography approach should be carefully evaluated and considered as essential during the transition. It maintains existing security against classical attacks while adding a layer of quantum resistance. However, implementing and managing these dual-algorithm schemes introduces new complexity and potential interim vulnerabilities if not executed precisely.

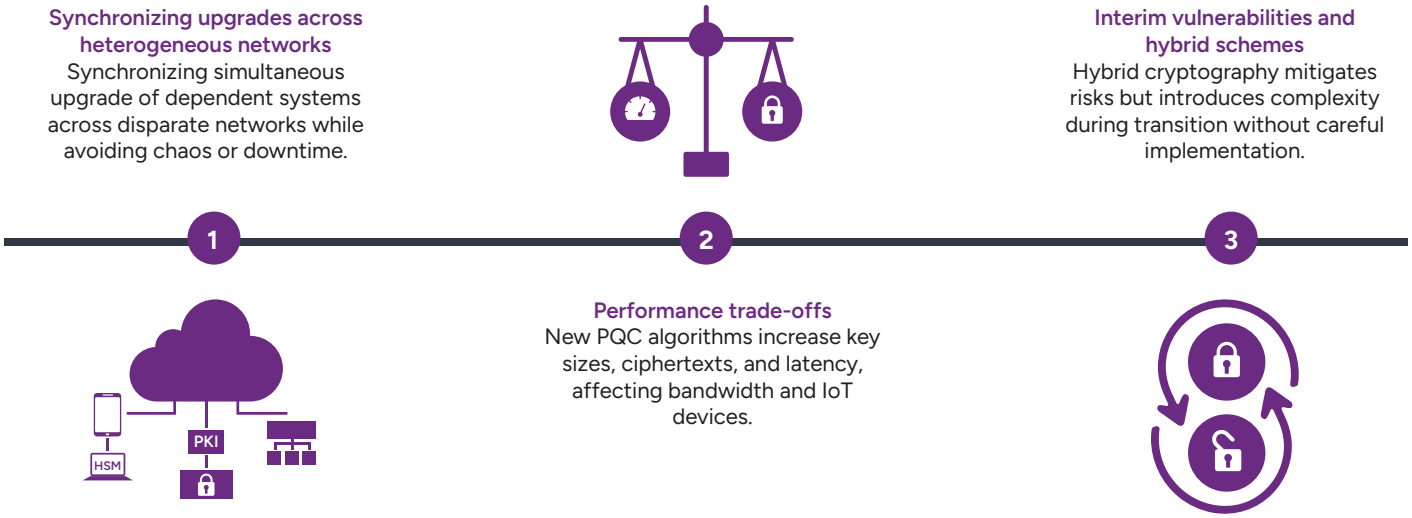


Figure 3: PQC Migration Challenges

Achieving PQC readiness requires a structured, multi-phase roadmap. The following steps, derived by NIST, CISA, and NSA, are critical for PQC readiness:

Steps	Description
1. Develop a quantum-readiness roadmap	Establish an orchestrated, organization-wide transition plan. This roadmap should include a timeline for phasing out existing encryption methods and integrating new PQC standards, with a goal for full transition by around 2035. The CISA website provides a joint fact sheet with more details.
2. Conduct a comprehensive cryptographic inventory	Identify all systems, applications, and assets that use quantum-vulnerable cryptography. This includes keys, certificates, cipher suites, and protocols. Automating this discovery process can be helpful.
3. Prioritize by risk and lifespan	Not all data is equal. Prioritize migration efforts for systems that protect high-value or long-life data (e.g., health records, trade secrets) that need to remain confidential for decades. This "harvest now, decrypt later" threat is a primary driver for immediate action.
4. Ensure cryptographic agility	Design and implement systems with cryptographic agility, which is the ability to quickly and flexibly update or switch between cryptographic algorithms. This is crucial as PQC standards may continue to evolve.
5. Engage vendors and partners	Collaborate with commercial-off-the-shelf (COTS) and cloud-based product vendors to understand their PQC migration roadmaps. Ensure that future contracts require vendors to provide PQC-enabled products.
6. Implement PQC standards as they are finalized	NIST has standardized the first set of PQC algorithms, which include ML-KEM and ML-DSA. Organizations should begin integrating these into their systems and products immediately.
7. Apply a risk management framework	Integrate quantum risk into your organization's enterprise risk assessments and leverage the NIST Cybersecurity Framework (CSF) or Risk Management Framework (RMF) for a structured approach.

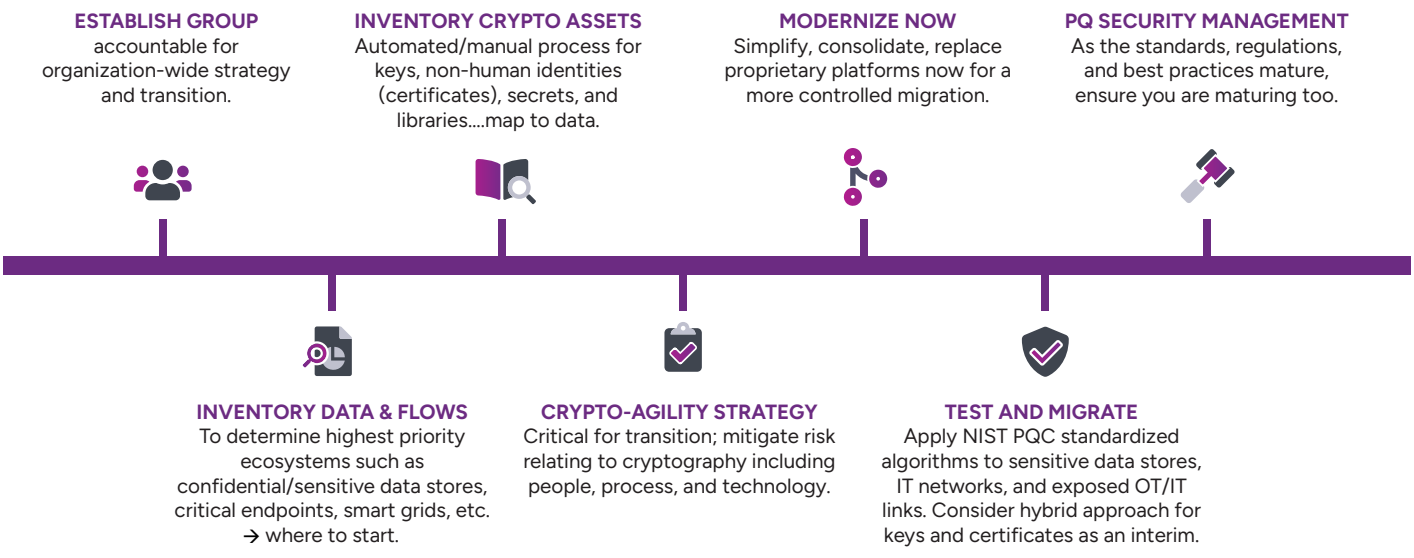
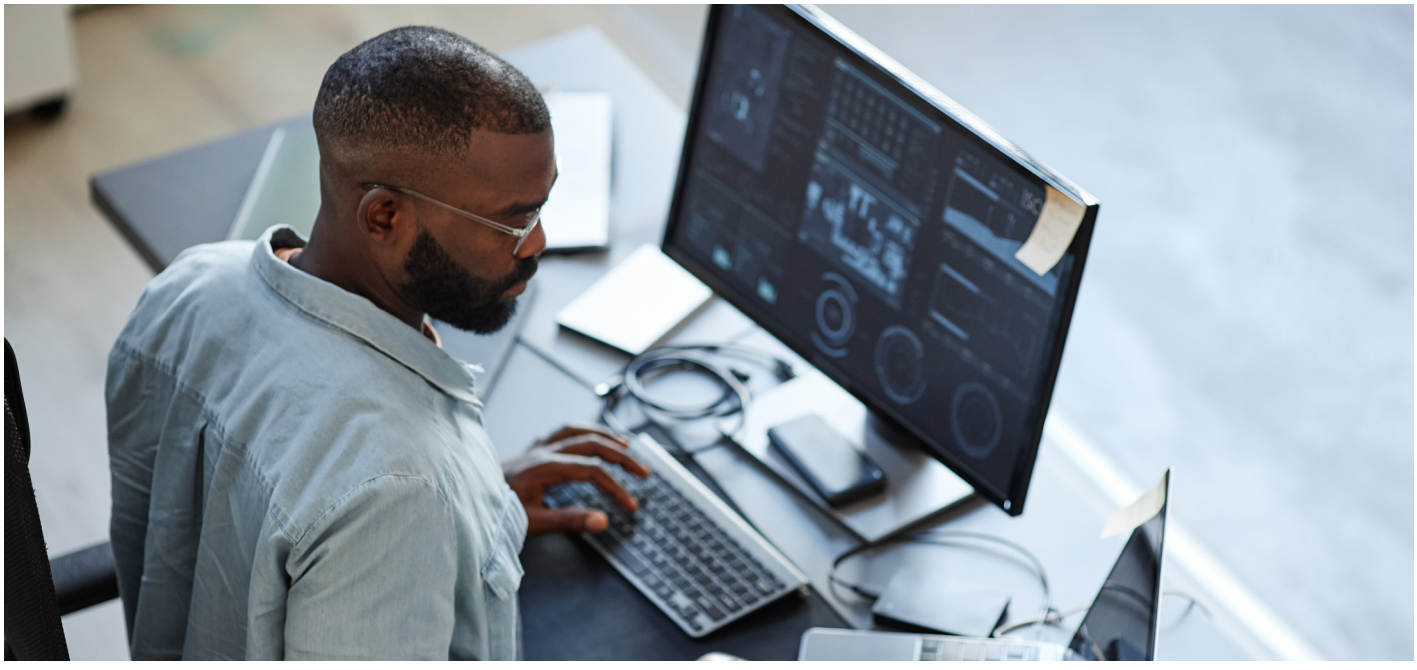


Figure 4: Preparing for post-quantum in the telecom sector

Strategic Roadmap for Telecom Operators

Telecom operators face intense pressure from rapidly evolving threats, complex global regulations, and the need for business model reinvention. The following strategic roadmap outlines the necessary steps for telecom operators to build operational resilience, achieve post-quantum readiness, and maintain stringent global compliance over the next decade.

Timeline	Cyber Resilience	PQC Readiness	Compliance
Immediate (0–12 Months)	• Inventory cryptographic assets and IAM gaps • Work toward implementing Zero Trust • Strengthen supply chain security	• Conduct quantum risk assessment • Engage vendors on PQC support	• Map posture against FCC, NIS2/DORA, UK Telecoms Security Act, and other important regulations • Set up incident reporting workflows
Medium-Term (12–36 Months)	• Deploy adaptive security frameworks • Completely implement Zero Trust • Integrate AI-driven threat detection • Expand MFA and PAM coverage	• Launch PQC pilot projects • Develop migration roadmap aligned with NIST and regional mandates	• Harmonize compliance programs • Automate audit and reporting processes
Long-Term (36+ Months)	• Achieve resilience maturity with predictive analytics • Embed resilience in business continuity planning	• Complete full migration to quantum-safe algorithms • Establish crypto-agility frameworks	• Maintain continuous compliance posture • Position as industry leader in secure, quantum-ready services



Entrust's Post-Quantum Portfolio in the Telecom Sector

As the telecom sector braces for the quantum era, Entrust is well-positioned with a comprehensive post-quantum (PQ) security portfolio, delivering quantum-resilient solutions with real-world applications. With quantum computing threatening to render traditional encryption obsolete, Entrust empowers energy providers to future-proof their infrastructure now.

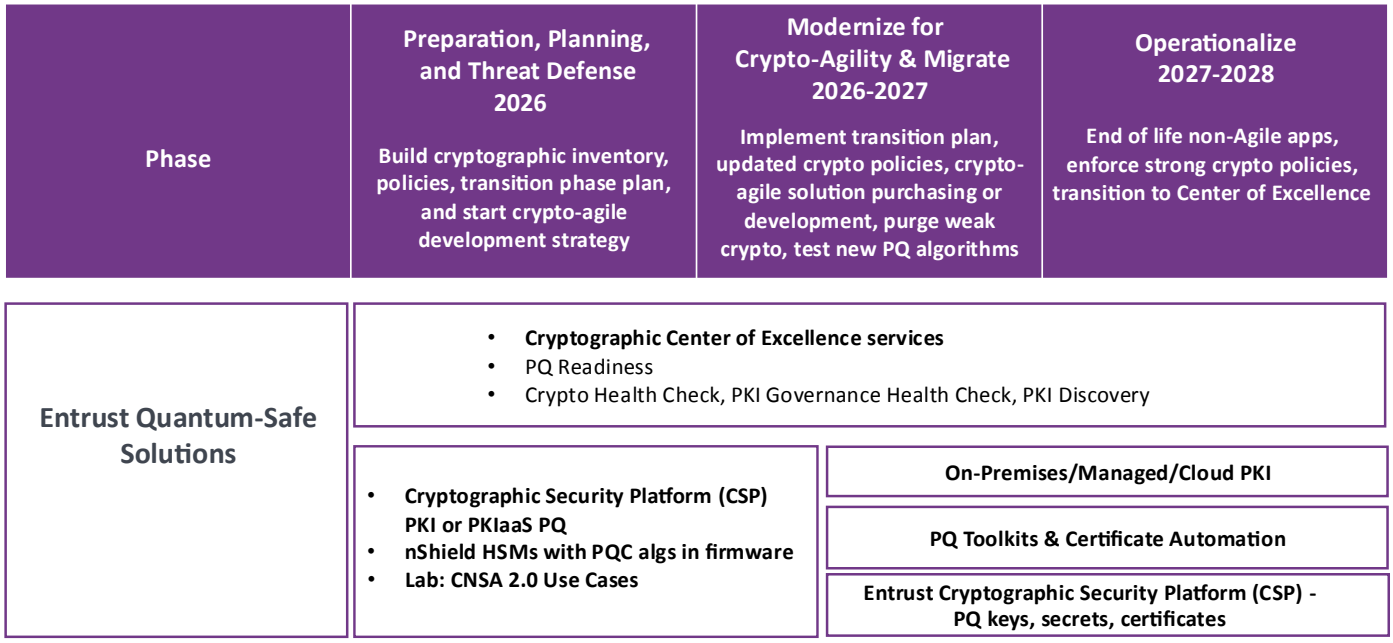


Figure 5: Entrust PQ-ready solutions mapped to post-quantum timeline

Cryptographic Security Platform

Entrust's Cryptographic Security Platform provides end-to-end, enterprise-wide cryptographic security management for machine identities and data security across IT and OT systems. It supports post-quantum cryptography, helps meet compliance with regulations by alerting on prohibited key usage (or when cryptography is misused, weak, or non-standard), and enables centralized visibility and crypto-agility of keys, secrets, and certificates.

PKI as a Service for PQC

Entrust's PKI as a Service for PQC (PKIaaS PQ) is a cloud-based solution that supports hybrid and composite certificates, blending classical and PQC algorithms, such as ML-DSA, ML-KEM, and SLH-DSA, while aligning with NIST's post-quantum drafts. It enables scalable issuance of quantum-safe digital identities, making it ideal for telecom IoT networks and remote grid management. By facilitating secure authentication and continuous verification, this service supports Zero Trust architectures, ensuring telecom utilities can maintain operational integrity and protect against quantum-enabled attacks.

PQC readiness assessment

The Entrust Cryptographic Center of Excellence (CryptoCoE) offers the PQC Readiness Assessment, which evaluates an organization's cryptographic maturity by inventorying assets, identifying risks, and providing a tailored migration roadmap with remediation recommendations. The service prioritizes the protection of long-term data, which is critical for telecom operators managing SCADA systems and IoT devices. By helping to ensure compliance with regulatory standards and enhancing resilience against quantum threats, this assessment helps telecom companies prepare for a secure transition to post-quantum environments.

nShield Hardware Security Modules (HSMs)

Entrust nShield 5 HSMs are PQ-ready, supporting the NIST standardized PQC algorithms ML-DSA, ML-KEM, and SLH-DSA in firmware, while serving as a high-assurance root of trust for protecting an organization's cryptographic keys. Their FPGA-based architecture delivers out-of-the-box crypto-agility, enabling new or emerging algorithms, including performance-accelerated PQC, to be introduced via firmware updates after deployment.

Building on this foundation, Entrust nShield HSMs also provide a FIPS-certified boundary for 3GPP authentication workflows, securely generating and safeguarding long-term subscriber keys and supporting MILENAGE, TUAK, and other 3GPP algorithms at high throughput. With deterministic hardware-backed key control and scalable deployment models, they function as the trust anchor for secure 4G/5G core authentication, UDM/AuC, AUSF, SEPP, and SIM provisioning systems, ensuring both future-proof cryptography and robust mobile-network identity protection.

Securing Telecom for the Quantum Future

As quantum computing accelerates toward reality, telecom operators must act decisively to strengthen cyber resilience, initiate post-quantum migration, and align with global compliance mandates. Proactive transformation today will safeguard critical infrastructure, ensure regulatory readiness, and position operators as leaders in a secure, quantum-resilient future.

By combining Entrust's leadership in PQC, crypto-agile HSMs, and future-ready key management with the telecom industry's advancements in 5G and 6G technologies and QKD-enabled networks, operators gain a comprehensive roadmap for securing identities, authentication, and communications, both today and in the quantum era.

Contact Entrust to discuss how we can help you find a clear path forward, enabling you to secure your infrastructure, help meet compliance mandates, and lead the transition to a quantum-resilient future.

ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.

entrust.com Toll-Free: 888.690.2424 | International: +1.952.933.1223 | sales@entrust.com

ENTRUST
SECURING A WORLD IN MOTION