Achieving Quantum Resilience with Wiz and PwC

Solution Brief

Strictly private and confidential

Contents

1. Executive Summary

Post-Quantum Cryptography (PQC) is no longer confined to strategy decks, awareness sessions, or planning discussions. Many enterprises are now moving into the early stages of execution by assessing their environments, identifying cryptographic dependencies, and preparing for phased implementation.

That shift is being driven by a practical reality: migrating to quantum-safe cryptography can take years, not months. Recent announcements from Google, U.S. CNSA 2.0 guidance and Canada's Centre for Cyber Security all reinforce the need for organizations to start strengthening their cryptography now, with a risk-based transition to quantum-safe methods targeted for completion between 2029 and 2032. For organizations operating in regulated industries or protecting long-lived sensitive data, preparation is becoming a near-term business priority rather than a future technical consideration.

The urgency is also not limited to the arrival of a Cryptographically Relevant Quantum Computer (CRQC). Organizations should prepare for the possibility that encrypted data captured today could be decrypted in the future, a risk commonly described as "Harvest Now, Decrypt Later" (HNDL). For long-lived sensitive data, delaying action raises exposure and makes transition planning harder.

For many organizations, the real challenge is figuring out where to start. Quantum-vulnerable cryptography is widely scattered across systems, and without clear visibility into exposures and critical assets, creating an effective migration plan can be difficult.

This is where Wiz and PwC come together. Wiz provides holistic visibility into cryptographic assets across modern cloud environments, helping organizations identify exposure across cloud services, public endpoints, secrets, applications, certificates, and code libraries. PwC helps clients turn those findings into action by combining technical expertise, engineering experience, and business context to support PQC readiness and transition planning. That includes helping organizations prioritize risk, establish the governance and program structure needed to manage the transition, and think through practical transition paths for applications, protocols, and trust mechanisms based on current technology availability, compatibility, and long-term crypto-agility needs. Together, Wiz and PwC help organizations move from fragmented discovery to a more structured and actionable path toward quantum readiness.

2. Why Organizations Should Act Now

One of the major reasons organizations are acting now is the risk known as “harvest now, decrypt later” (HNDL). In this scenario, encrypted data captured today by nation-state actors or other espionage-related threat actors may be stored and later decrypted as quantum capabilities mature.

That risk is more acute for long-lived data, including sensitive financial records, intellectual property, regulated data, and other business-critical information that needs to remain protected for years. Organizations should prepare not only for future CRQCs, but also for the present-day risk that sensitive data being transmitted and stored today could be exposed in the future.

The urgency also extends beyond encrypted communications. Quantum risk affects digital signatures, authentication mechanisms, and the broader public key infrastructure (PKI) ecosystem that supports trust across enterprise environments. As a result, PQC preparation is more than a narrow cryptography issue. It is an enterprise-wide planning challenge that begins with understanding where vulnerable cryptography exists, which assets matter, and how to prioritize migration over time.

3. The Challenges: Inventory and Transition Strategy

Moving from PQC awareness to implementation requires more than recognizing the risk. It requires enough visibility to act. Public guidance from NIST, CISA, and NSA consistently points to the same starting point: build a useful cryptographic inventory, understand where quantum-vulnerable cryptography is in use, and use that visibility to prioritize a phased migration plan.

The Inventory Challenge (Visibility)

Visibility is the first challenge. Many of today's organizations lack a holistic Cryptographic Bill of Materials (CBOM) that identifies where cryptography is used, and which algorithms like RSA, ECDH, and ECDSA remain quantum vulnerable.

Scope

While PQC focuses on asymmetric algorithms, inventorying should include both asymmetric and symmetric cryptography across the systems covering public-key algorithms, encryption methods, certificates, protocols, and key management to better understand dependencies and plan migration effectively.

Blind Spots

Without proper inventory tools, outdated or quantum-vulnerable cryptography often hides in third-party SDKs, compiled binaries, container images, API gateways, load balancers, cloud key management services, and vendor-managed platforms. These hidden risks limit understanding of exposure and remediation needs.

The PQC Transition Strategy (Technical Debt and Sequencing)

Once organizations understand where cryptography is deployed, the next challenge is migration. Many of today's enterprises are working through years of technical debt, including legacy protocols, hardcoded dependencies, unsupported platforms, and third-party constraints.

A practical migration strategy usually follows three steps:

1. Identify what should migrate first by using the inventory to locate quantum-vulnerable cryptography, externally exposed systems, and high-value assets.

2. Prioritize communication paths and trust mechanisms that may offer early risk reduction. This often includes upgrading TLS support to 1.3. Wiz's research found that 84% of accessible top domains support TLS 1.3, while only 45% support PQC key exchanges, pointing to a meaningful near-term opportunity to reduce exposure.

3. Plan for the longer-term architectural transition. Some systems will require deeper remediation because cryptography is embedded in application logic, infrastructure, appliances, or vendor-managed services.

In more complex IT and OT environments, this often requires coordinated planning across engineering, architecture, governance, and third-party stakeholders.

4. Wiz: Cloud-Native Cryptographic Visibility for PQC Readiness

Wiz provides the automated technical foundation to help close the visibility gap through the specialized Wiz for Post-Quantum Cryptography Security Framework. Using agentless graph technology, Wiz provides the "Technical Truth" of your environment:

- **Automated Cryptography Discovery and Inventory (ACDI)**
  Wiz generates cloud-native CBOM across the environment using multiple discovery methods.
- **High-Risk Termination Mapping**
  Focuses on urgent priorities such as legacy weaknesses and HNDL-related key exchange exposure.
- **Security Graph Prioritization**
  Correlates cryptographic findings with business criticality, internet exposure, related applications, and data sensitivity.
- **PQC Tester**
  Confirms if web services already support PQC-compliant key exchanges.

5. PwC: Turning Technical Findings into a Practical Transition Strategy

If Wiz helps organizations identify where quantum-vulnerable cryptography exists, PwC helps determine what to do next, in what order, and how you can make the transition practical.

PQC Governance and Program Design

To scale PQC readiness sustainably across the enterprise, organizations should have more than isolated technical fixes. PwC can help organizations formalize how they tackle the challenge by standing up a PQC task force, working group, or Cryptographic Center of Excellence (CCoE) that brings together security, engineering, architecture, infrastructure, procurement, legal, risk, and executive leadership.

Risk Prioritization and Business Context

PwC helps clients put Wiz findings into context so they can decide what matters and should come first. That means looking at cryptographic exposure through the lens of data sensitivity, business criticality, regulatory requirements, operational dependencies, and remediation complexity.

Technical Transition and Crypto Agility

PQC readiness is also an engineering challenge. PwC helps clients assess what can be addressed with current technology, where phased adoption may be needed, and where deeper architectural change is likely required.

This can include:

- Building lab environments
- Assessing near-term transition opportunities
- Evaluating TLS and key exchange transition paths
- Piloting selected applications
- Identifying legacy constraints and dependencies

6. How Wiz and PwC Work Together

Wiz and PwC bring complementary capabilities to PQC readiness.

Discover the cryptographic footprint

Wiz builds visibility across cryptographic assets, services, certificates, and protocols.
PwC helps define the scope of discovery and establish the program structure.

Prioritize what matters

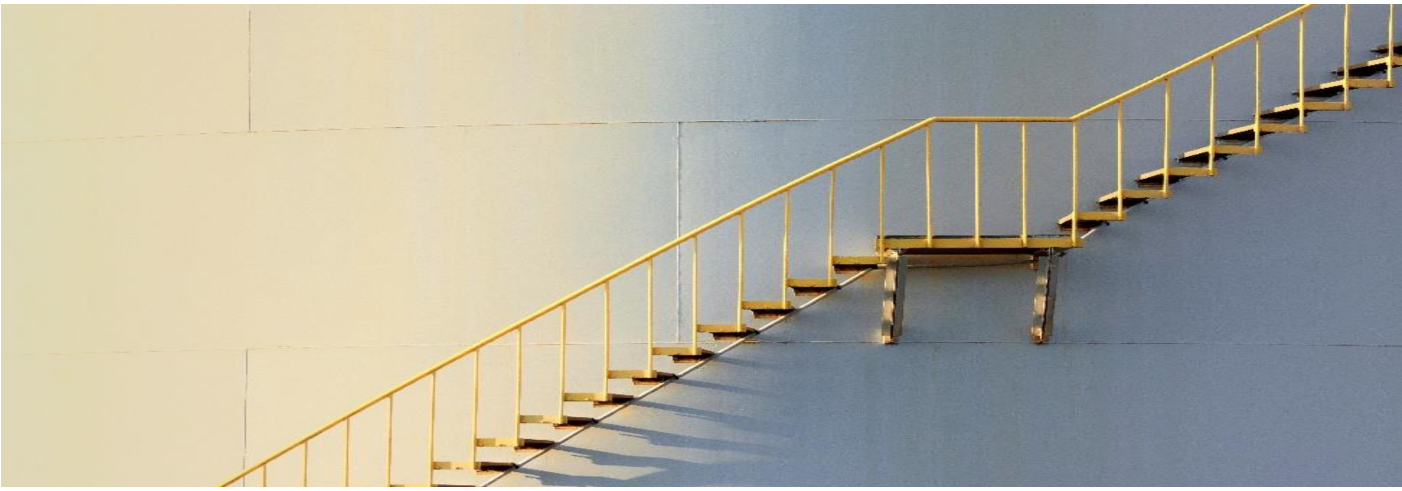
Wiz connects cryptographic findings to technical risk and sensitive data context.
PwC helps interpret findings in the context of business criticality, regulatory requirements, and remediation complexity.

Design the transition path

Wiz helps surface vulnerable algorithms, protocols, and trust paths.
PwC helps shape the transition approach and define practical transition paths across applications, protocols, certificates, and trust mechanisms.

Sustain readiness over time

Wiz supports ongoing visibility as environments change.
PwC helps establish the governance, third-party risk updates, and enterprise processes needed to manage cryptographic change over time.



7. Next Steps

Don’t wait for “Q-Day.” Contact your **Wiz GSI lead** or Nidhu Nalin (Cyber, Data and Tech Risk Principal, PwC US) or Jason Hall (Cybersecurity Principal, PwC Canada) today to start your **Post-Quantum Readiness journey**.

pwc.com