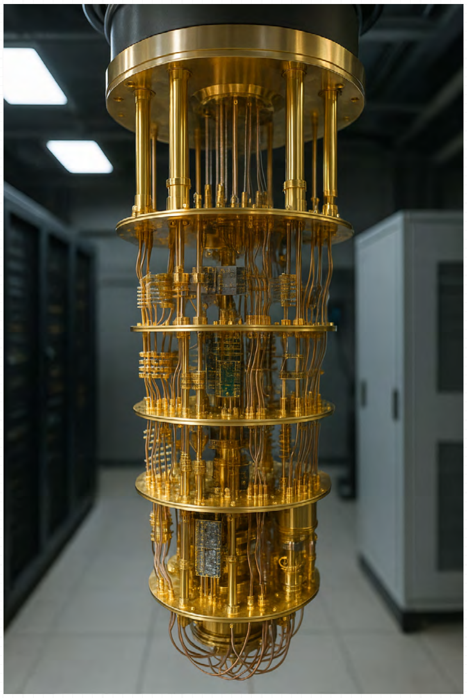
binarly.io

Future-Proofing Cryptography: Binarly's Post-Quantum Migration Solution

The Quantum Threat

Quantum computing isn't a far-off fantasy. It's a fast-approaching reality that attackers could soon decrypt historical data once secured by today's quantum-weak algorithms. Government agencies, critical infrastructure, telecoms, and financial institutions are especially at risk. With NIST forecasting the disallowance of certain algorithms by 2035 (and regions like Australia eyeing as early as 2030) the migration to post-quantum algorithms is not just a technical upgrade; it's an urgent imperative.



Binarly's PQC Migration Solution

The Binarly Transparency Platform includes a solution for Post Quantum Computing (PQC) discovery and asset management to help enterprises understand and mitigate their cryptographic risk. By analyzing binaries for quantum-weak algorithms, the platform delivers actionable insights on cryptographic materials, ensuring you know exactly how and where to start your PQC migration plan.

The solution focuses on determining the cryptographic stance of your binary packages by:

- **Deep Binary Analysis:** Pinpoints all cryptographic materials in use, including hidden or undocumented dependencies in both first- and third-party components. Unlike vendors that focus on cryptographic agility or network-wide controls, our platform zeroes in on identifying the cryptographic stance within specific binaries.
- **Actionable Insights:** Provides a comprehensive view of which algorithms are susceptible to quantum attacks. A dedicated Cryptographic Materials tab offers enhanced, actionable information to drive informed decision-making. By cataloging cryptographic assets, our tool enables organizations to assess the readiness of their devices and systems — from computers to IoT devices — and to plan their migration to quantum-safe algorithms.
- **Risk Identification:** Enables you to gauge the PQC readiness of your products and devices — helping you prioritize upgrades and secure the most at-risk areas before quantum threats become a reality. Our capabilities have been integrated with partners like SandboxAQ and QuSecure to provide an end-to-end solution, bridging gaps in endpoint and network perspectives while ensuring complete cryptographic risk management.

Digging Deeper

The Binarly Transparency Platform, available in SaaS form or on-prem, has been fitted with patented technologies to handle discovery, inventorying, and assessment of cryptographic assets:

- **Cryptographic Keys:** Ownership, algorithm identifier, format, and status (active or deprecated) accurately documented.
- **Certificates:** Validity period, ownership, and algorithm used, captured and displayed in streamlined reports.
- **Algorithms:** Accurate tracking and identification of algorithms in use, and assessment of their ability to resist quantum attacks.
- **Protocols:** Inventory that includes version and implementation details to track any dependencies.

Binarly's integration with SandboxAQ delivers a unified, powerful solution for companies seeking to facilitate and accelerate their cryptographic modernization journey, including their post-quantum readiness. These capabilities include:

- **Cryptographic Reachability:** Identify which cryptographic algorithms in a binary are actively used, so you can prioritize changes that truly matter.
- **New Standards Compliance:** Track NIST-approved post-quantum algorithms, pinpoint outdated cryptography, and plan targeted updates for quantum-safe security.
- **Enhanced cryptographic bill of materials (CBOM) and reporting:** Build a robust inventory of certificates, keys, and algorithms while generating streamlined reports for cross-team collaboration.

About Binarly:

Binarly is a U.S.-based firmware and software supply chain security company founded in 2021. The flagship Binarly Transparency Platform helps device manufacturers, OEMs, and enterprise product security teams detect vulnerabilities, misconfigurations, secrets, and malicious code in devices and software supply chains. Leveraging decades of research and program analysis expertise, we secure businesses, critical infrastructure, and consumers while assisting organizations in transitioning to a post-quantum cryptography (PQC) environment. For more information, visit **https://binarly.io**.

Binarly's award-winning research team is known for technical excellence:

750+ CVEs

Most assigned a high or critical impact score.