

Quantum readiness made practical

Quantum Central gives teams a practical way to inventory cryptographic assets, prioritize migration, manage change, and prove quantum readiness. Start with the systems that matter most, make measurable progress, and expand the program over time.

Going beyond PKI, it provides visibility across certificates, keys, protocols, libraries, hardware, software, and third-party dependencies. Teams can bring together existing DigiCert Trust Lifecycle Manager data, network scans, and CBOMs and other cryptographic discovery sources to build a unified view of their cryptographic environment and identify quantum-vulnerable assets.

Quantum Central helps teams move from inventory to action. Customizable policies identify weak, deprecated, and quantum-vulnerable cryptography, while readiness scoring and inventory-aware AI help teams prioritize what to address first. Guided remediation workflows turn findings into trackable work, helping teams assign ownership, coordinate remediation, and follow issues through closure.

Dashboards, policy status, remediation tracking, and CBOM exports give teams a measurable record of their progress. Security leaders, auditors, customers, and other stakeholders can see what has been discovered, what remains at risk, and how remediation is progressing.

Key capabilities

Build cryptographic visibility

Combine network scans, data from DigiCert Trust Lifecycle Manager, CBOMs, and other cryptographic discovery sources in a unified view. Track certificates, keys, protocols, algorithms, libraries, hardware, software, and third-party dependencies.

Prioritize migration

Evaluate cryptographic assets against customizable policies to identify quantum-vulnerable, deprecated, or noncompliant cryptography. Use readiness scoring, asset context, and inventory-aware AI to focus remediation on the systems that matter most.

Manage change

Create remediation tasks from policy findings, assign them to asset owners, and track work through resolution. Connect remediation with DigiCert ONE workflows and change management systems to coordinate migration across distributed teams and environments.

Prove quantum readiness

Use dashboards, policy status, remediation history, and CBOM exports to document progress. Give leadership, auditors, customers, and other stakeholders a transparent view of what has been discovered, what remains at risk, and how remediation is progressing.

Benefits



Start without boiling the ocean:

Focus first on priority systems and expand the scope of the program over time. Make meaningful progress without waiting for an exhaustive enterprise-wide inventory.



Turn findings into action:

Add policy, risk, ownership, and remediation context to cryptographic inventory so teams can move beyond identifying problems to resolving them.



Get more value from existing discovery:

Bring together cryptographic discovery data from DigiCert and other sources instead of creating another isolated repository or starting discovery from scratch.



Make readiness measurable:

Track migration progress over time and give leadership, auditors, customers, and internal stakeholders evidence that the organization has a plan and is executing against it.

Data sources and integrations

Bring existing cryptographic data into Quantum Central and add native discovery to build a more complete view of your environment.

Imports

- Network scans
- DigiCert Trust Lifecycle Manager
- Cryptographic Bill of Materials (CBOMs)
- Software Bill of Materials (SBOMs)
- Certificate lifecycle management tools
- Key vaults
- Comma separated values (CSV)

Exports

- CBOM (CycloneDX 1.6+)
- Comma separated values (CSV)

Integrations

- Jira
- REST API
- Others coming soon



Start your quantum migration. Prove every step. [Sign up now.](#)