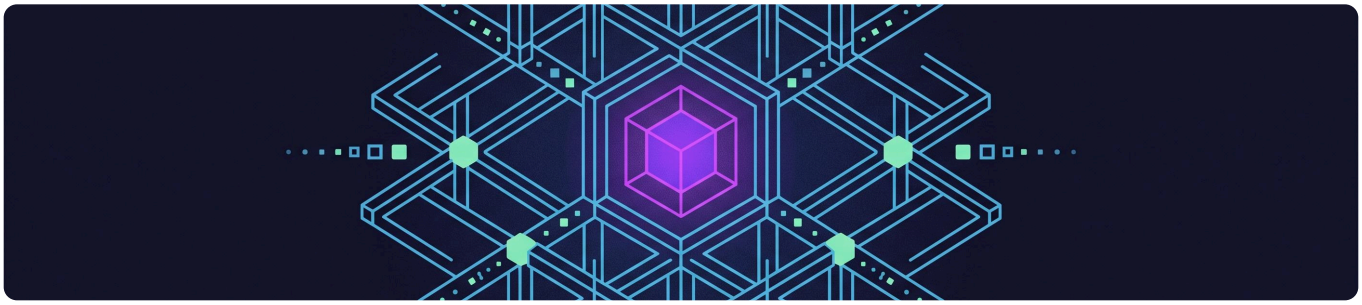
SOLUTION BRIEF - FEDERAL EDITION

Post-Quantum Readiness Through the Enterprise Software Control Plane

Supporting Executive Order 14412 through independent software assessment, migration planning, and continuous post-quantum readiness



The Challenge

The transition to post-quantum cryptography requires organizations to understand, prioritize, and assess software cryptography at enterprise scale. While much of the industry focuses on replacing vulnerable cryptographic algorithms, the broader challenge is managing software risk throughout that transition.

Enterprise software portfolios contain commercial applications, open-source components, internally developed software, AI-generated code, and continuously evolving software updates. Cryptographic implementations are embedded throughout these software assets, making them difficult to identify, evaluate, prioritize, and manage consistently across large enterprise environments.

Discovering vulnerable cryptography is only one part of the problem.
Organizations also require a repeatable process for assessing software, prioritizing migration, and measuring progress as enterprise environments evolve.

Questions Every Organization Should Answer

> **"Which applications in our environment still rely on quantum-vulnerable cryptography?"**

- Which applications contain cryptography requiring review?
- Which cryptographic algorithms and techniques are present?
- Which specific applications demand prioritized migration?
- What concrete evidence supports those decisions?
- How will overall migration progress be measured?
- How will newly introduced software stay assessed?

Clairvoyant Intelligence - PQC Risk Assessment Workflow

1 Enterprise Software Sources

Ingest software from across your environment

Commercial Software
Vendors, ISVs, and COTS apps

Open Source Packages
NPM, PyPI, Maven, and GitHub

Software Updates
Patches, new versions, and fixes

Internal Applications
Proprietary/custom in-house code

AI-Generated Software
Code from AI engines

2 Enterprise Software Control Plane

Independent behavioral assessment and risk evaluation

CLAIRVOYANT

Independent Behavioral Assessment
Deep code analysis in isolated runtime and static environments to uncover latent risks

Post-Quantum Readiness Framework
Evaluates the assessment results for quantum-vulnerable crypotography

Software & Dependenceis | Detect Crytography | Evaluate Risk

3 Governance Evidence

PQC assessment in plain language

Quantum-Vulnerable Algorithms
Weak or deprecated crypto

Affected Applications
Assets with vulnerable crypto

Operational Context
Exposure and risk parameters

Plain-Language Assessment
Clear risks, impacts, and actions

Governance Decision

Approve | Monitor | Migrate | Remediate

Continuous Assessment & Governance

New software, updates, and dependencies monitored constantly to sustain enterprise readiness.

Continuous Monitoring
Ongoing ingesting and assessment of software and updates

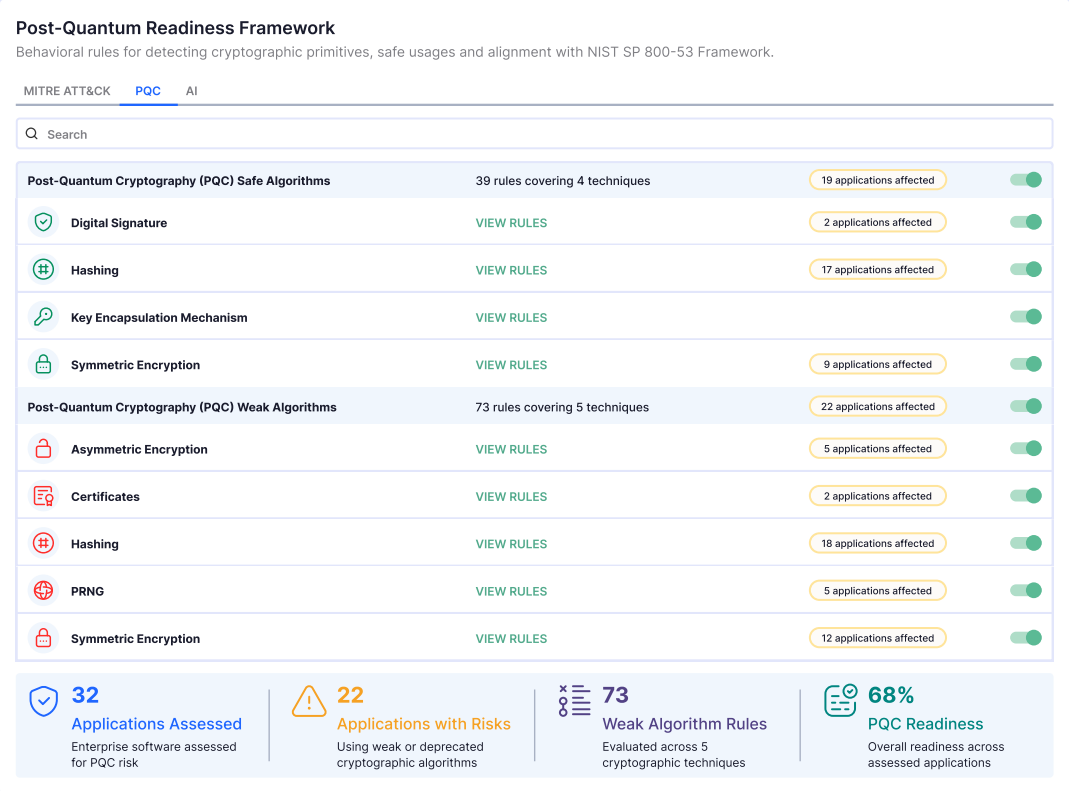
Policy Enforcement
Enterprise PQC policies applied consistently across all software

Metrics & Compliance
Track overall readiness progress and generate audit reports

Post-Quantum Readiness Framework

While cryptographic discovery identifies issues, the Post-Quantum Readiness Framework evaluates software to generate the actionable governance evidence needed to guide and prioritize migration decisions.

- Identify active cryptographic algorithms across software.
- Align cryptographic choices with enterprise policies.
- Pinpoint software packages using vulnerable encryption.
- Prioritize mitigation paths and track overall readiness.
- Track security risks continuously as software evolves.
- Deliver actionable findings to guide migration planning.

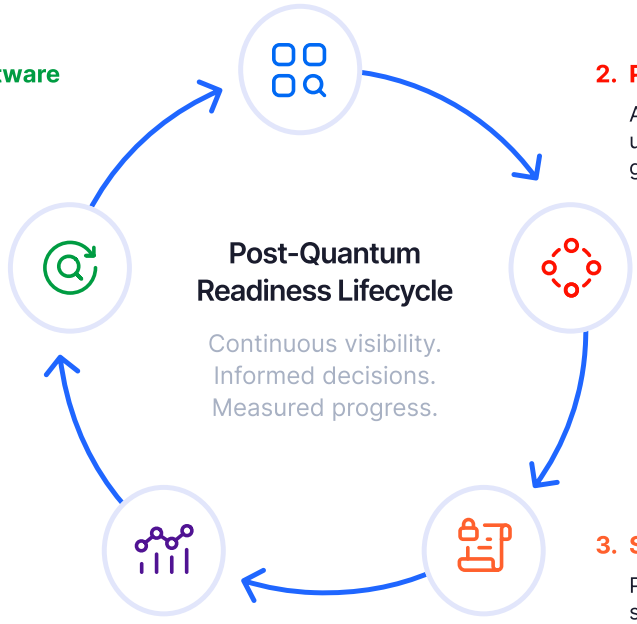


Key Capabilities

1. Evaluate cryptographic algorithms in software.
2. Identify applications with weak security.
3. Measure readiness and support governance.
4. Continuously assess new software updates.
5. Independently evaluate and validate CBOMs.

Figure 2: Post-Quantum Readiness Framework
The framework evaluates software against enterprise policies to identify cryptographic techniques. It highlights affected applications to generate evidence supporting migration and governance.

Assessment to Continual Operations



Outcome

Gain the visibility and evidence needed to reduce quantum risk and make confident software decisions.

Summary

Executive Order 14412 sets clear objectives for transitioning Federal information systems to post-quantum cryptography. Achieving compliance requires a repeatable process to continuously assess software, prioritize migration, and generate the governance evidence needed to guide software decisions.

The Enterprise Software Control Plane provides these risk-informed insights before deployment. Through the Post-Quantum Readiness Framework, it delivers independent software analysis that does not rely on vendor participation or the availability of Cryptography Bills of Materials (CBOMs).