

POST-QUANTUM CRYPTOGRAPHY (PQC) WITH ORCA

Find quantum-vulnerable algorithms across your cloud, see which assets depend on them, and build a migration plan aligned to post-quantum standards.

THE CHALLENGE:

Quantum Risk Is a Present-Day Problem

Quantum computers will eventually break the RSA and ECC algorithms that secure most encrypted connections and digital signatures in the cloud. Adversaries aren't waiting. They are harvesting encrypted data today to decrypt later, which makes PQC readiness a present-day problem. NIST finalized its first PQC standards in August 2024, and regulators are now setting migration deadlines, including targets starting in 2030 for US federal agencies.

Yet most organizations still can't answer the first question to get started. Where is quantum-vulnerable cryptography running in our cloud today? Years of set-and-forget cryptography have left weak algorithms buried in managed services, certificates, public endpoints, container images, and code. Point-in-time audits go stale in a cloud that changes continuously, and they can't tie an algorithm to the asset and risk behind it.

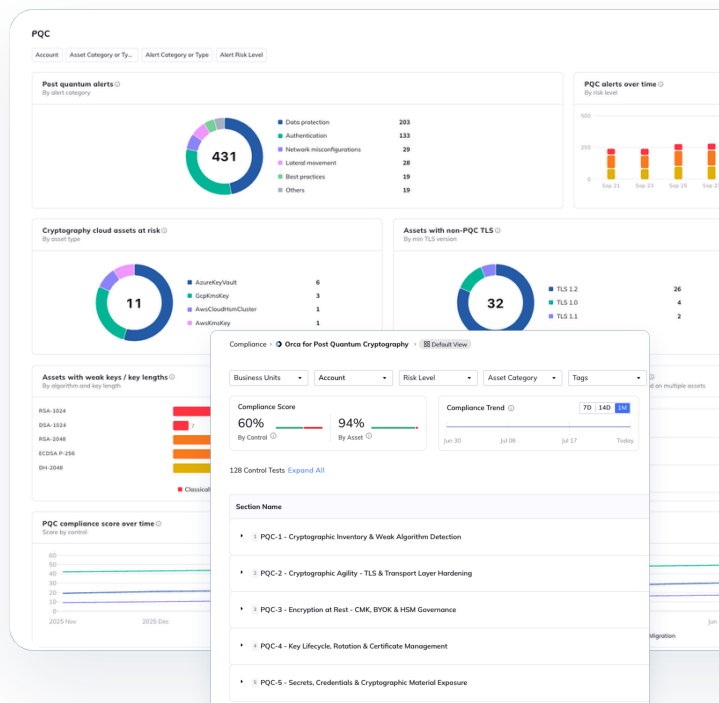
THE SOLUTION:

Know Where Your Quantum Risk Lives Before You Migrate

Orca turns PQC readiness from an extensive research project into a prioritized, trackable program. Orca uses its patented agentless SideScanning™ technology and Unified Data Model to provide complete visibility throughout your entire cloud and AI estate. The Orca Platform identifies where quantum-vulnerable algorithms, specifically RSA and ECC, are in use, builds a Cryptographic Bill of Materials (CBOM), and ties each finding to the asset that relies on it.

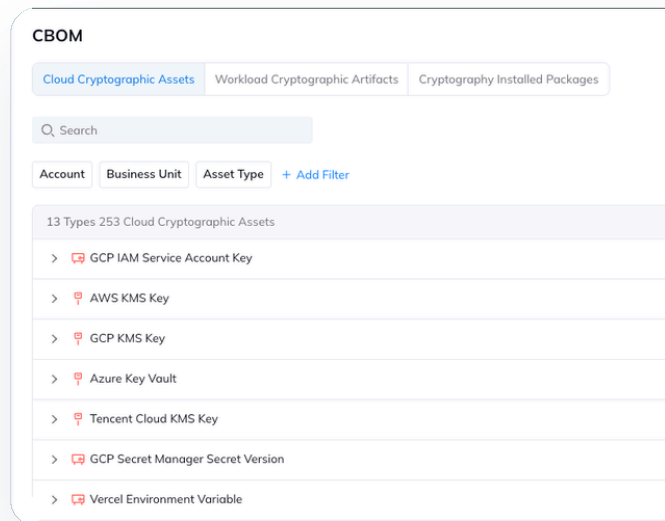
Those findings roll up into a dedicated Post-Quantum Cryptography Compliance Framework aligned to NIST's finalized PQC standards. Instead of a raw list of cryptographic findings, teams get a priority-ordered view that separates what is vulnerable to attacks today, what is exposed to "Harvest Now, Decrypt Later," and what belongs in longer-term migration planning.

Because Orca already understands your cloud context, including internet exposure, sensitive data, identities, and attack paths, teams can focus first on the cryptographic weaknesses that protect the most valuable and most exposed assets.



01 See It

- **Continuous, agentless visibility.** Orca SideScanning™ keeps the inventory current as the environment changes, with no agents to deploy and no fresh audit required.
- **Coverage across cloud, code, AI, and runtime.** Cryptographic risk detection spans CSPM, AppSec, and runtime through the Orca Sensor, so weak crypto is found whether it lives in a cloud service, a repository, or a running workload.
- **Cryptography Bill of Materials (CBOM).** A dedicated inventory of your cloud cryptography assets and artifacts, including algorithms, keys, certificates, and cryptography packages. Available in the platform and through exports in the CycloneDX standard.



02 Prioritize It

- **PQC Alerts View.** A dedicated view of every PQC finding, tied to the affected asset and enriched with Orca's cloud context so teams fix the riskiest crypto first.
- **Post-Quantum Cryptography Compliance Frameworks.** A dedicated PQC framework organizes findings by urgency and automatically maps them to NIST and the EU Cyber Resilience Act. It sits alongside Orca's library of 200+ pre-built and customizable frameworks, with one-click reporting.
- **PQC Dashboard.** Use Orca's pre-built PQC Dashboard to visualize and track PQC posture and migration progress over time, so security leaders can track the metrics that matter most and report readiness to stakeholders.
- **Attack path analysis and risk prioritization.** Orca's attack path analysis and dynamic risk scoring show which assets are exposed to the internet, reachable through risky identities, or connected to sensitive data. Applying that context to PQC findings helps teams separate vulnerable cryptography on high-risk assets from the cryptography that can wait.

03 Act On It

- **Orca MCP Server.** Connect Orca to the AI assistants your team already uses through the Orca MCP Server. Teams can investigate cryptographic exposure, understand PQC findings, and plan migration steps in natural language with the same context that powers the Orca Platform.
- **Workflows and integrations.** PQC migration is a multi-year program, not a one-time fix. Orca routes findings to the tools teams already use, such as Jira, ServiceNow, and Slack, with clear ownership so remediation moves efficiently at scale.

About Orca

Orca Security delivers security for the companies that build. As cloud, applications, AI and app generation expand the attack surface, Orca transforms security risk into the context teams need to act. The Orca Platform provides complete visibility across cloud, AI, and application environments, correlates risk across every layer, and prioritizes the exposures that matter most so organizations can remediate faster and innovate with confidence. Trusted by hundreds of organizations, including SAP, Autodesk, Gannett, Lemonade, and Digital Turbine, Orca is backed by leading investors including Temasek, CapitalG, ICONIQ Capital, and Redpoint Ventures. Learn more at orca.security. Connect your first account in minutes at orca.security or book a personalized demo.



Ready to try it out?

Sign up for a demo. Visit orca.security/demo

