

Sectigo Quantum Ready™

See your cryptographic exposure. Prioritize what matters. Prepare for what comes next.

Sectigo Quantum Ready™ helps organizations build and maintain a Cryptographic Bill of Materials (CBOM) that connects cryptographic assets with the applications, services, data, and infrastructure that depend on them. This system of record helps teams identify quantum exposure, assess readiness, and prioritize post-quantum migration.

Snapshots expire. Change is the only constant.

Cryptography is embedded across applications, infrastructure, certificates, keys, devices, and services. One-time assessments and static inventories provide only a snapshot. Applications change, infrastructure expands, certificates renew, cloud services are introduced, and cryptographic standards continue to mature. Quantum readiness therefore requires an operating picture that stays current as the environment changes.



What cryptography do you depend on?

Algorithms, certificates, keys, protocols, libraries, and services in use across your environment.



Where is quantum exposure concentrated?

Quantum-vulnerable cryptography mapped to the applications, infrastructure, data, and business services it touches.



What should move first?

Prioritized migration paths based on risk, business impact, dependencies, and complexity.



Can you keep PQC readiness current?

A living CBOM with clear accountability and priorities that stays current as applications, infrastructure, certificates, and standards evolve.

Without a baseline, individual teams may develop disconnected inventories, priorities, and migration assumptions. This can make it harder to establish ownership, coordinate testing, plan investments, and respond consistently as standards and technology ecosystems evolve.

Move from readiness goals to action

Introducing Sectigo Quantum Ready™

Sectigo Quantum Ready™ helps organizations turn cryptographic discovery into prioritized PQC migration roadmap.



Discover

Build a CBOM of cryptographic assets across infrastructure, applications, and workloads.

Assess

Evaluate quantum exposure, technical risk, data lifespan, dependencies, and business impact.

Manage

Prioritize findings and build migration plans with owners, milestones, and blockers.

Adapt

Keep the CBOM current as applications, certificates, infrastructure, services, and standards evolve.

It creates a living CBOM at any time, giving teams the visibility and context to prepare for cryptographic change.

Early access for organizations ready to plan

Quantum Ready is intended for organizations that are:

- Building a post quantum or crypto agility program.
- Assessing long term data protection needs.
- Tracking and communicating readiness progres.
- Modernizing PKI and certificate lifecycle management.
- Evaluating PQC migration strategies.
- Creating a cryptographic inventory.
- Coordinating change across teams and environments.

What Quantum Ready™(early access) delivers

Sectigo Quantum Ready™ gives business and technical stakeholders a shared view of their cryptographic landscape:

Cryptographic Bill of Materials

A connected inventory of cryptographic assets and dependencies.

Dependency map

Connections between cryptography, applications, services, data, infrastructure, and owners.

Readiness baseline

A current view of preparedness and visibility gaps.

Prioritized PQC migration roadmap

Ranked activities based on technical and business context.



What teams do with Quantum Ready™(early access)

Quantum Ready™ gives technical and business stakeholders one planning framework. Common use cases for Quantum Ready™ include:



Build a cryptographic discovery plan

Outcome

A current view of the cryptographic estate.



Prepare applications for controlled testing

Outcome

Evidence about technical constraints before you commit to a broader migration plan.



Coordinate vendor and ecosystem readiness

Outcome

The questions, owners, and engagement sequence for evaluating external readiness.



Strengthen crypto-agility

Outcome

A repeatable, visible, governed approach to cryptographic change.

Quantum Ready™ is where Quantum Security Posture Management (QSPM) starts

QSPM is Sectigo's approach to helping organizations achieve and maintain post quantum readiness as cryptography, infrastructure, applications, and standards evolve.

Quantum Ready™ is the first step in that journey, establishing the visibility and context needed to understand cryptographic assets, identify exposure, and prioritize migration efforts with confidence.

What Quantum Ready™ (early access) enables



Understand your quantum risk posture

Build a living inventory of cryptographic assets and identify where quantum-vulnerable algorithms exist. Gain the visibility needed to assess exposure, prioritize action, and plan with confidence.



Maintain trust in long-lived signatures

Software, firmware, documents, records, and device identities may need to verify years from now. That requires knowing where signatures live and how long trust must hold.



Plan for ecosystem dependencies

Migration depends on more than algorithm availability. Applications, libraries, protocols, hardware, platforms, vendors, and relying parties all must support the approach you choose.



Built on Sectigo's certificate and PKI experience

Certificate lifecycle management, PKI, automation, and digital trust expertise applied to the next cryptographic transition. Quantum Ready treats migration as a structured operational program, connecting cryptographic decisions to the visibility, ownership, automation, testing, and governance that enterprise-scale change demands.

Explore Quantum Ready™ early access, complete a readiness assessment, or speak with your Sectigo sales representative.

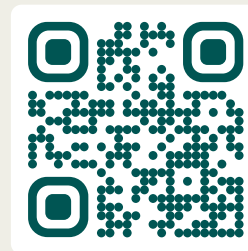
Explore Quantum Ready™ early access

www.sectigo.com/qspm-quantum-ready



Assess your quantum readiness

Qday.net



DISCLAIMER: Quantum Ready™ is early-access offering with limited seats. Features, assessment methods, reports, integrations, supported environments, and availability are subject to change.

About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM), helping organizations secure human and machine identities while reducing the hidden risks of modern digital trust. As certificate volumes grow and lifespans shrink, unmanaged certificates are becoming a source of outages, compliance exposure, and operational disruption. Sectigo uses Orchestrated Automation to deliver Simplicity at Scale through its cloud native CLM platform, bringing visibility, control, and lifecycle management together across complex environments. With more than 700,000 customers, including 65% of the Fortune 500, Sectigo is one of the largest and longest standing certificate authorities, with over 20 years of delivering unparalleled digital trust. For more information, visit www.sectigo.com or follow us on [LinkedIn](#).

