

DATASHEET

Post Quantum Security

Move PQC from a future-threat slide deck to a governed migration program — inventory every cryptographic dependency, run CARAF-aligned assessments, evaluate vendor PQC posture, and track migration to NIST-approved algorithms on one connected platform.



From "we'll deal with quantum later" to a governed PQC operating model

Quantum computing threatens today's cryptography — particularly RSA, ECC, and Diffie-Hellman — and "harvest-now, decrypt-later" exposure has already begun. NIST has finalized the first PQC standards (ML-KEM, ML-DSA, SLH-DSA), and migration windows are measured in years, not quarters. SmartSuite operationalizes how PQC migration actually has to run: every cryptographic element inventoried, every system and vendor evaluated against CARAF criteria, every migration tracked through the Discover → Assess → Prioritize → Migrate → Govern lifecycle. **Every algorithm is inventoried. Every system is evaluated. Every migration is tracked.** The result is a PQC program defensible for regulators, executable for crypto and security teams, and visible for the CISO and board.

Capabilities built for crypto-agile, quantum-resilient governance

Unified cryptographic inventory
Every cryptographic element — algorithms, keys, certificates, protocols, signing mechanisms — lives in one connected inventory linked to the applications, IT assets, vendors, and business processes that depend on it. No more "where is RSA used?" research projects; the inventory answers it.

Vendor PQC readiness assessments
A structured 10-point vendor questionnaire captures PQC Posture, HNDL Exposure, NIST Algorithm Support, Hybrid Mode, PQC Roadmap, Migration Timeline, and Contract Clauses. Quantum Risk Rating per vendor surfaces concentration risk.

CARAF-aligned quantum risk evaluation
Structured, repeatable CARAF evaluations score quantum vulnerability, data lifespan, exposure, and crypto agility — producing defensible CARAF Impact Scores per element. Crypto Evaluation Status moves from Not Started → In Process → Complete with full audit history and evaluator queues.

Migration tracking & executive roll-ups
The PQS Dashboard rolls up PQC Discovery, Evaluation, Readiness, and Migration Progress in real time, with Business Units by PQS Maturity, Crypto Dependency, and PQS Owner. Migration tracks hybrid-mode transitions to ML-KEM, ML-DSA, and SLH-DSA.

PQC readiness at every level

Crypto evaluator & security analyst

Personalized Assess view surfaces only the items they're evaluating — Crypto Apps, IT Assets, Vendors, and Crypto Inventory In Evaluation — with Crypto Inventory by Evaluator showing progress. Drill from a card into the CARAF assessment in two clicks.

PQS program manager & CISO

Full PQS Dashboard with PQC Discovery, Evaluation, Readiness, and Migration Progress against 100%. Cross-portfolio views surface Business Units by PQS Maturity, Crypto Dependency tier, and PQS Owner — what's stale, what's exposed, what needs investment.

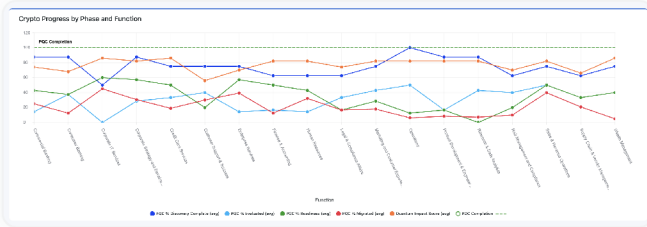
Executive & governance committee

PQC posture rolled up to leadership — readiness percentages, migration progress, business-unit maturity, and crypto dependency levels. Board reports refresh continuously against NIST PQC standards and CARAF; no manual rebuilds before each governance review.

Built differently. SmartSuite is the PQC platform where cryptographic elements, applications, IT assets, vendors, business processes, CARAF assessments, and migration plans live on the same governed graph — so every evaluation reflects current dependencies, every vendor questionnaire ties to the systems that depend on it, and every dashboard reflects real PQC posture, not last quarter's spreadsheet.

Connected to the rest of your GRC program

- **Business Structure & Hierarchy**
Crypto elements link to Applications, IT Assets, and Business Units so PQC exposure aligns to the organization's actual operating model
- **Enterprise Risk Management**
CARAF Impact Scores roll up to the enterprise risk register; quantum risk becomes a tracked, treated risk domain
- **Compliance Assessments & Testing**
NIST PQC alignment, CARAF readiness, and migration evidence feed compliance and audit assessments directly
- **Third-Party Risk Management**
Vendor PQC posture and roadmaps feed third-party risk; contract clauses for PQC requirements track to execution
- **Vulnerability Management**
Quantum-vulnerable algorithms surface alongside conventional vulnerabilities for unified remediation prioritization
- **Issues Management**
Quantum-vulnerable findings and stalled migrations flow to closed-loop remediation with owners and due dates



Crypto Progress by Phase and Function — discovery, evaluation, readiness, and migration tracked across every business function.



Business Unit PQC Review — crypto processes, IT assets, and applications by criticality for any business unit.

Built for everyone with a stake in PQC

Chief Information Security Officer

Oversee enterprise PQC readiness, migration progress, and alignment with regulatory and industry expectations — board-ready in one click.

Crypto Evaluator & Security Analyst

Perform CARAF assessments, evaluate quantum vulnerability and crypto agility, and update Crypto Evaluation Status.

Vendor & Third-Party Risk Manager

Assess vendor PQC readiness, review PQC roadmaps, and ensure contractual alignment with PQC requirements.

PQS Program Manager

Coordinate cryptographic inventory creation, CARAF evaluations, vendor readiness assessments, and migration planning across teams.

Migration & Application/Asset Owners

Execute PQC migration activities, update migration status, and transition systems to hybrid or PQC algorithms.

Executives & Board

Track organizational progress, prioritize investment, and validate strategic alignment with NIST PQC timelines.

Start the PQC migration now — track it like any other program
A complete GRC suite that connects cryptographic risk with vendors, applications, assets, and enterprise risk — on one AI-native Work OS.

NIST PQC
ML-KEM
ML-DSA
SLH-DSA
CARAF

Learn more at <https://www.smartsuite.com/products/post-quantum-security> · Contact your SmartSuite representative to schedule a demo