QubitSafe™

Post-Quantum Cryptography Migration Platform

Centralized Platform for Post-Quantum Migration & Risk Management

AccessMatrix Qubit Safe is an end-to-end Post-Quantum Cryptography (PQC) migration platform. Qubit Safe enables organizations to Discover, Assess, Implement, and Monitor their transition to quantum-resistant cryptography. Built on the proven AccessMatrix security foundation, the platform provides a structured, enterprise-ready approach to managing cryptographic posture and risk across the entire PQC lifecycle.

With "Harvest Now, Decrypt Later" (HNDL) attacks already targeting sensitive data, quantum risk is no longer theoretical. Following the finalization of NIST PQC standards in August 2024, regulators across APAC are increasingly requiring organizations to assess quantum exposure and demonstrate readiness.

Qubit Safe supports NIST-approved algorithms including ML-KEM, ML-DSA, and SLH-DSA, and integrates with Open Quantum Safe (liboqs) to enable hybrid cryptographic deployments. Through automated discovery, risk-based assessment, controlled implementation, and continuous monitoring, organizations gain full visibility and control—allowing them to transition to PQC without disrupting existing operations.

Core Modules

Discovery Module
Identify cryptographic assets across environments with comprehensive discovery capabilities

- Git repository and source code scanning
- Binary and compiled code analysis
- Certificate and key discovery
- CyloneDX 1.6 Crypto Bill of Materials (CBOM) export

Assessment Module
Quantify quantum risk and determine migration priorities through intelligent analysis

- Automated cryptographic risk scoring
- Mosca timeline analysis for quantum exposure forecasting
- Migration prioritization based on business impact
- Regulatory framework mapping across applicable standards

Implementation Module
Enable controlled and validated deployment of post-quantum cryptography

- PQC proxy service for seamless integration
- Validation test harness for functional assurance
- Performance benchmarking for algorithm selection
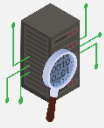- Hybrid cryptographic algorithm support

Monitoring Module
Maintain continuous visibility and governance across cryptographic posture

- Executive-level dashboards and reporting
- Policy violation detection and tracking
- Compliance-ready audit reports
- Real-time alerts for risk and posture changes

Key Capabilities & Benefits

End-to-End Cryptographic Discovery
Automated scanning across source code, binaries, certificates, and keys with CycloneDX CBOM export, delivering rapid visibility and eliminating cryptographic blind spots.

Seamless PQC Implementation
Hybrid-ready PQC proxy, validation testing, and performance benchmarking, allowing quantum-safe adoption with minimal application changes.

Standards-Based Cryptography
Supports NIST-approved post-quantum cryptographic algorithms including ML-KEM (FIPS 203), ML-DSA (FIPS 204), and SLH-DSA (FIPS 205), ensuring long-term cryptographic resilience and global standards alignment.

Intelligent Quantum Risk Assessment
AI-driven risk scoring, Mosca timeline analysis, and regulatory mapping, enabling risk-based migration prioritization and informed decision-making.

Continuous Monitoring & Compliance
Real-time dashboards, policy violation tracking, audit-ready reports, and alerts, maintaining continuous compliance, governance, and executive visibility.

APAC Regulatory Expertise
Pre-built compliance frameworks tailored to key regional regulators including MAS/CSA (Singapore), HKMA (Hong Kong), BOT (Thailand), and BNM (Malaysia), accelerating regulatory readiness across the region.

Scan for more information

🌐 www.i-sprint.com　f iSprintInnov　✗ iSprintInnov　in company/i-sprint-innovations

i-Sprint
Trust without Boundaries