PartnerOneIT

Post-Quantum Cryptography Readiness Assessment

Prepare Today. Transition Tomorrow.

Post-Quantum Cryptography Readiness Assessment

50%+ computers capable of breaking current encryption will emerge within 15 years.

Quantum computing isn't science fiction anymore—it's a timing problem. Organizations still relying on traditional cryptography face a quiet but growing risk: encrypted data being harvested today and cracked tomorrow. When the switch flips, unprepared environments won't fail gracefully. They'll fail loudly. This assessment ensures that doesn't happen to you.

Why This Matters

Quantum computers will eventually break the cryptographic systems protecting your data, communications, and digital trust infrastructure. The threat isn't theoretical—adversaries are already collecting encrypted data with plans to decrypt it once quantum capabilities mature. This "harvest now, decrypt later" strategy means the clock is already ticking.

Government mandates are accelerating the timeline. NIST will deprecate quantum-vulnerable algorithms by 2035, with high-risk systems transitioning much earlier. Organizations that wait will face rushed migrations under pressure. Those that prepare now will make the transition a non-event.

What This Service Does

Our Post-Quantum Cryptography (PQC) Readiness Assessment evaluates your current cryptographic and PKI environment through the lens of crypto agility—not just compliance. Using the Crypto Agility Maturity Model (CAMM), we identify where quantum-vulnerable algorithms exist, how certificates and keys are managed, and how quickly your organization can adapt when post-quantum standards become mandatory.

Rather than recommending disruptive rip-and-replace fixes, we deliver a phased, practical roadmap that prepares your systems to transition smoothly—much like the organizations that quietly succeeded during Y2K.

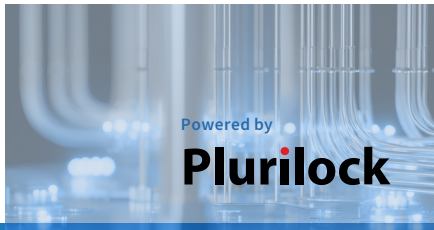
How We're Different

- **Crypto Agility Over Compliance** We treat cryptography as an adaptive capability, not a static control. The goal isn't just meeting mandates—it's building an environment that can evolve as standards change
- **Operational Resilience First** We focus on practical transitions that preserve business continuity, not theoretical risk scenarios that create panic. Your operations continue while your cryptography modernizes
- **Hybrid Cryptography Strategy** We prepare you for the reality of running both classical and post-quantum cryptography side-by-side during the transition, ensuring compatibility and security through the change
- **Unified Roadmap** Security, engineering, and governance often operate in silos. We align all three into one coherent transition plan so everyone moves forward together

This is preparation, not panic.

What You Walk Away With

- **Clear Risk Visibility**: Comprehensive view of where quantum-vulnerable cryptography exists across your environment—from PKI and certificates to application-level encryption and key management
- **CAMM Maturity Benchmark:** Baseline assessment using the Crypto Agility Maturity Model that you can track over time as you improve your ability to adapt cryptographic systems
- **Phased Transition Roadmap**: Prioritized, practical plan aligned to real operational constraints—not a theoretical timeline that ignores how your organization actually works
- **Executive-Ready Insights**: Technical findings translated into business impact so leadership understands the risk, the timeline, and the investment required
- **Actionable Guidance**: Practical next steps that enable crypto agility without disruption—what to do first, what can wait, and how to build momentum



 Contact: 1-480-500-6076 | info@partneroneit.com

Business Outcomes

- **Avoid Rushed Migrations** Organizations that start now control the timeline. Those that wait will scramble under regulatory pressure and operational urgency.
- **Protect Long-Term Data** If your data must remain confidential for years or decades, waiting until quantum computers arrive means that data is already at risk today.
- **Reduce Technical Debt** PQC readiness forces you to inventory and modernize cryptographic systems that often go untouched for years—turning mandatory compliance into strategic modernization.
- **Build Adaptive Security**: Crypto agility isn't just about quantum. It's about building infrastructure that can adapt as threats, standards, and technologies evolve.

Who This Is For

- Security and infrastructure leaders responsible for PKI, identity, and digital trust
- Organizations with long data retention requirements or highly sensitive information
- Regulated environments preparing for future compliance mandates
- Enterprises that want quantum readiness without operational shock
- Teams seeking to turn a compliance mandate into strategic infrastructure improvement

The Timeline Is Real

- **2030**: NIST deprecates 112-bit security algorithms
- **2035**: Full transition to quantum-resistant systems mandated for federal agencies
- **15 years**: Estimated window before quantum computers may break RSA-2048

The organizations that start now will make the transition a non-event. The rest will scramble under pressure. This service ensures you're in the first group.

Contact us today to assess your quantum readiness.

info@partneroneit.com

Powered by Plurilock

Post-Quantum Cryptography

Deliverables

- Comprehensive Gap Analysis Report- includes PKI and Crypto Agility Posture
- PQC Readiness Roadmap- includes Detailed Recommendations Prioritized by Impact and Effort
- Executive Summary- includes Visual Charts, CAMM Scorecards, and a Summary of Key Findings
- Technical Guidelines & Checklists

Sample Scope

- Coverage of 5,000 user/service identities
- Coverage of 50-150 systems/ applications
- Coverage of 10,000 endpoints

Level of Effort

- Architect, PKI SME, PM
- 4-week engagement

**Pricing is for illustration purposes only, actual cost may vary as a result of multiple engagement-specific factors.*

Sample Price

$52k-70k

Assessment Tooling and Platforms

- **PKI Tools** *(Included)*
- **NIST Guidelines** *(Included)*

Services Powered by Plurilock

Data Protection Services

IAM, DLP, DSPM, Firewall, Switching, and Network/ Wi-fi Modernization ▪ Data Security Posture Assessment ▪ Post-Quantum Readiness ▪ Zero Trust Implementation

Cyber Adversary Simulation & Response

Penetration testing ▪ Red and purple teaming; Tabletop exercises ▪ Social Engineering, Deepfake, and AI Prompt Injection Vulnerability Testing ▪ App, API, and ICS/SCADA Testing ▪ Software Development Lifecycle and Code Testing ▪ Digital Forensics and Incident Response

Cloud Security Services

Cloud Visibility and Assurance Assessments ▪ Cloud Access Security Broker Implementation and Modernization ▪ Cloud Governance ▪ Multi-Cloud Hardening ▪ Cloud Guardrails

Beyond Governance, Risk, & Compliance

Vulnerability Management ▪ Third-party Risk and C-SCRM ▪ Asset Management ▪ Audit Readiness ▪ Automated Compliance Monitoring ▪ Cyber Risk Quantification ▪ CISO 360 Baseline Assessment

IT Service Delivery

IT Service Management (ITSM), CMDB, ITIL ▪ EDR/XDR ▪ Project and Portfolio Management ▪ Security Tool Integration

Secure Operations

24x7 MDR ▪ Staff Augmentation ▪ Threat Hunting Programs

Selection of current and past customers that can be publicly represented

Plurilock CRITICAL SERVICES