Protecting Legacy Applications in the Quantum Era

Why Certes DPRM Matters Right Now

For years, boards and executives have invested heavily in digital transformation, yet the backbone of many enterprises still depends on legacy applications. ERP platforms, financial systems, healthcare databases, and industrial control software were never designed with modern cyber threats in mind, let alone the disruptive reality of quantum computing.

That gap presents a serious business risk. Attackers are not waiting for organizations to finish multi-year modernization projects. They are harvesting sensitive data now, with the expectation of decrypting it later once quantum computing achieves full strength. For enterprises operating under strict regulatory regimes such as GDPR, DORA, NIS2, and sector-specific mandates like CJIS, leaving these applications exposed carries financial, legal, and reputational consequences.

> ***"Legacy applications hold the crown jewels of the enterprise. Rewriting or replacing them takes years, but attackers only need seconds once quantum computers reach scale."***
>
> *Simon Pamplin – CTO, Certes*

The Quantum Threat to Legacy Systems

Quantum computers will eventually have the power to break widely used cryptographic standards like RSA and ECC through Shor's algorithm. This is not a distant or theoretical scenario. The "harvest now, decrypt later" threat means adversaries can collect encrypted data today and unlock it once quantum capabilities mature.

Legacy applications are especially vulnerable because:

They weren't designed for rapid cryptographic agility.
Updating them to support post-quantum cryptography (PQC) often requires deep code changes, if not complete redesigns.

They form part of complex, interconnected ecosystems.
Even if one system is updated, its connections to others remain weak points.

They handle high-value data.
Whether intellectual property, patient records, or financial transactions, legacy apps often carry exactly the kind of information adversaries are targeting.

In short, the systems enterprises rely on most are the least prepared for quantum-era risks.

Why Traditional Approaches Fall Short

Enterprises know they need to act, but typical strategies—modernization, patching, or bolting on additional security tools—have major flaws:

- Application rewrites are slow and expensive, often leaving exposure for years.
- Security overlays meet audit requirements but fail to deliver true resilience.
- Uncertainty in PQC standardization creates the risk of investing in the wrong upgrade path.

> **"Businesses can't afford to gamble on what might become the right PQC standard years from now. They need a solution that delivers immediate protection, aligns with NIST-approved approaches, and adapts as the standards evolve. That is exactly what DPRM provides."**
>
> *Paul German – CEO, Certes*

CERTES

Certes DPRM:
Post-Quantum Protection Without Rewriting Legacy

Certes’ Data Protection & Risk Mitigation (DPRM) solution solves this challenge. It delivers rapid deployment of post-quantum-ready protection without requiring changes to applications themselves.

With Certes DPRM, organizations can:

- Add PQC-compliant protection transparently, securing data in motion regardless of the application’s native capabilities.
- Accelerate quantum readiness and achieve compliance today instead of years from now.
- Simplify deployment across cloud, hybrid, and on-prem environments.
- Stay aligned with PQC standards as they mature, without disruptive reengineering.

The Path Forward

Quantum computing will redefine cybersecurity, but the biggest risk for enterprises is inaction. Legacy applications cannot be left unprotected while modernization projects unfold.

Certes DPRM gives organizations the bridge they need: quantum-safe protection that can be deployed immediately, allowing them to safeguard sensitive data today while planning tomorrow’s upgrades on their own schedule.

The choice is clear. You can preserve the value of legacy systems and achieve quantum resilience at the same time—with DPRM making both possible.

Contact Certes

300 Corporate Center Drive,
Suite 140 Pittsburgh, PA 15108

1 (888) 833-1142
sales@certes.ai

CERTES