

# QuSecure

Case Study

## Protecting What You Can't Replace Crypto Agility For Oil & Gas Critical Infrastructure

2026

## Executive Summary

A multi-national oil company with 50,000+ employees successfully piloted post-quantum cryptography, validating quantum-resistant encryption for exploration data in a production-equivalent environment, a chance to address a massive set of risks head-on.

**The threat is already here.** Adversaries are collecting encrypted data today with the expectation of decrypting it when quantum computing matures. For geological surveys and reservoir models that remain commercially sensitive for 20+ years, the protection window is closing... not when quantum computers arrive, but now, while that data is being harvested.

**The alternative is both impractical and more costly.** Application-level cryptographic migration would require coordinating hundreds of development teams across 5-7 years, with extensive application code changes, and still leave SCADA and industrial control systems unprotected. For many legacy systems, there is no migration path at all. QuProtect R3 excels at enabling PQC migration for precisely these legacy environments.

**This infrastructure will operate through the 2040s.** The data it carries will be valuable even longer. Neither can be replaced on normal enterprise timescales – but the cryptography protecting both can be modernized now, without operational disruption.

<p><b>Network Integration</b></p> <p>Network-level quantum-safe gateways integrated with existing security infrastructure and support segmented systems without changing applications or workflows. QuSecure adapted to customer needs with quick response times throughout the integration process.</p>	<p><b>Crypto Agility</b></p> <p>Crypto agility could be operated in practice via QuProtect R3™, with algorithms rotated centrally and propagated to gateways without touching endpoints. The migration caused no disruption to performance.</p>	<p><b>Long Lasting Data Secured</b></p> <p>The organization could secure data that will be valuable for 20+ years on infrastructure that will operate for 30+ years and cannot be replaced on normal IT timescales.</p>
--	---	---

**The pilot provided enough operational proof for production deployment approval and a multi-year budget for phased enterprise rollout. It turned PQC and cryptographic agility from an abstract future concern into concrete capabilities.**

*This case study is based on a real engagement with a national oil company. All identifying details have been anonymized; the technical and operational themes are preserved.*

The screenshot displays the QuProtect R3 dashboard interface. On the left is a navigation sidebar with sections for RECONNAISSANCE (Recon Agents, Asset Discovery, Custom Asset Analysis, Policy), RESILIENCE (Proxy Agents, Core Agents), and REPORTING (Cryptographic Bill of Materials). The main content area is titled 'Cryptographic Command and Control' and features three primary actions: Reconnaissance (Continuously find vulnerable encryption and crypto debt), Remediation (Deploy agents to secure traffic and update encryption), and Reporting (Generate compliance documentation). Below this is the 'Cryptographic Health Score' section, which shows a 'Critical Condition' (last updated at 6:00PM) and provides analysis and recommendations. The bottom of the dashboard includes overview cards for Reconnaissance (105 Cryptographic Assets Discovered), Remediation (14 Proxy Agents Deployed), and Quantum Resilient Algorithms In Use (represented by a progress bar).

## The Challenge

### Oil & Gas Technology Landscape

The oil and gas sector operates with a diverse technological landscape: modern enterprise applications alongside constrained devices and decades-old legacy systems. Creating a disparate web of pain for network owners attempting comprehensive security updates. SCADA systems, proprietary industrial protocols, embedded controls with limited processing power, and applications running on outdated platforms all coexist within the same infrastructure, each presenting unique PQC migration challenges.

### Data Outlives Infrastructure

Geological survey data informs drilling decisions for more than 20 years. Reservoir models remain commercially sensitive for decades. The data's value curve is long.

The infrastructure carrying that data is also long-lived, but rigid. SCADA systems, legacy applications, industrial controls, and proprietary protocols will operate into the 2040s. They cannot be replaced without massive capital expenditure, re-certification, and years of planning.

“ U.S. critical infrastructure assets are often designed to operate for decades.

[Sandia National Laboratories](#)  
[2021 Critical Infrastructure Decision-Making Study](#)

Cryptography operates on a very different timeline. Current encryption standards protecting this data are already vulnerable or will be deprecated as standards evolve. Adversaries harvesting encrypted data today will exploit it as vulnerabilities emerge and computational capabilities advance.

#### STRUCTURAL MISMATCH

- ◆ Data with decades-long value
- ◆ Infrastructure with decades-long lifecycles that cannot be easily replaced
- ◆ Cryptographic standards change every few years

### The Disparate Web of Pain: Application-Level Migration Is Impractical

In organizations with decades of accumulated technology—whether enterprises with 50,000+ employees or mid-sized operations with complex legacy infrastructure—application-level migration means updating hundreds of applications: custom-built systems from the 1990s, third-party software with vendors long gone, embedded systems with no development environment.

Each app would need its own development work, testing, and deployment window.

Development teams already prioritize business features over cryptographic updates. Many developers do not have specialized knowledge of how to best deploy cryptography. Additionally, accurate testing requires recreating production scenarios that often do not exist outside of live environments. Coordinating PQC changes across hundreds of applications becomes a multi-year program.

For 20–30-year-old SCADA systems, proprietary industrial protocols, and embedded controls, coordinated application-level updates are effectively impossible. There are no vendors to support changes, no test harnesses that reflect real-world behavior, and change control is constrained by safety and certification requirements. The cost and complexity of application code changes alone would be prohibitive—making network-level protection both the easier and more cost-effective solution.

The organization needed proof that it could protect its highest-value data without:

Disrupting operations

Replacing infrastructure

Or spending years in application-level migration

## Why Network-Level Protection

QuProtect R3™ deploys at network gateways, providing an optimal approach to solving the cryptographic migration challenge. By separating security from application logic, organizations gain long-lasting cryptographic management without being locked into the lifecycle constraints of their applications.

Applications, endpoints, and legacy infrastructure do not change. Data flows through quantum-safe tunnels transparently. This separation is beneficial because it allows security to evolve independently—when cryptographic standards change, only the gateway layer needs updating, not the thousands of applications and endpoints behind it.

In this pilot, gateways were deployed at strategic network points to protect exploration data flows. No applications were modified. No workflows changed. The entire effort (from planning,

to deployment, to validation) completed in three months in a production-equivalent environment.

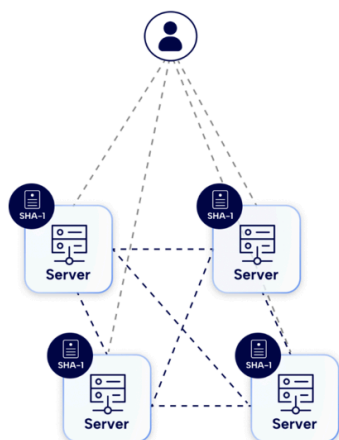
At enterprise scale, this shifts the migration approach from impractical to achievable.

At enterprise scale, this shifts the migration unit:

- Network and security teams deploy gateways at defined points.
- A single team manages a single technology, on a coordinated schedule.
- Timelines are measured in months, not years.

For infrastructure that cannot be modified the protection happens at the network layer. Those systems continue to operate as they always have. The encryption protecting their communications evolves at the gateway.

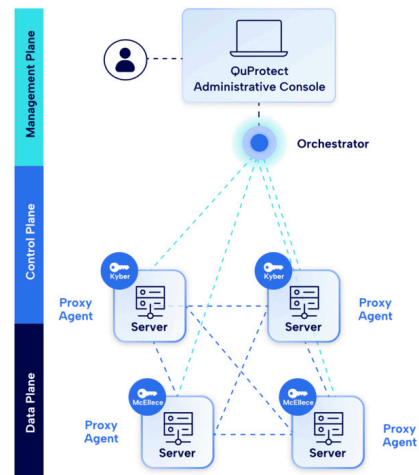
### Application-Level Cryptography Management



Impossible for many legacy and OT systems. Each application needs its own development work, testing, and deployment window.

Requires extensive application code changes across hundreds of systems.

### Network-Level Cryptography Management



Single team manages single technology with timelines measured in months.

Legacy systems protected without modification. Network-level protection is the easier and more cost-effective solution compared to alternative approaches like application code changes.

## The Pilot

### Scope

QuProtect R3 agents were deployed in a production-equivalent test environment that mirrored actual field operations. Exploration data flows from multiple operating regions were routed through quantum-safe tunnels and validated.

The full effort, from initial planning through deployment and validation, took approximately three months.

### Organizational Challenges

#### Ownership

At the outset, application development teams assumed they would need to update their code. Each team began assessing backlog impact and estimating months of development work to integrate PQC.

Security architecture and network teams argued for a network-level approach to avoid this coordination nightmare. The debate quickly became less about cryptography and more about ownership:

- Who owns PQC migration?
- How should priorities be set across business units and regions?

The pilot resolved this at a practical level. In the test environment, network-level protection was demonstrated end-to-end. Application teams watched their systems operate unchanged through quantum-safe gateways. Once they saw their workloads function normally without code changes, the conversation shifted from: “how do we update our applications?” to “how quickly can we deploy this approach?”

#### Prioritization & Phased approach

Even with a network-centric design, classic enterprise scaling challenges remained:

- ◆ **Prioritization conflicts:** Security wanted to start with the highest-value data. Network operations wanted to begin where deployment was simplest and lowest risk. Each business unit believed its use case should be first in line.
- ◆ **Resource allocation:** There were practical questions about who would fund the gateways, how network engineering time would be allocated, and how to sequence PQC alongside other infrastructure projects.
- ◆ **Multi-region complexity:** Different regions had different IT maturity levels, change control processes, and regulatory requirements. What worked in one geography could not be assumed to work in another.

The pilot created a reusable model for these decisions. By focusing on exploration data—high business value, well-defined flows, and clear executive sponsorship—the organization established a prioritization pattern: start with use cases that combine strong business value with deployment feasibility, then leverage success to drive further rollout.

## Integration Work and Real Challenges

Network-level architecture simplified application coordination, but it did not eliminate integration work. The pilot made clear where the real effort would be in a full rollout.

### What Worked Smoothly

QuProtect R3's network-layer architecture meant exploration applications did not change. Field teams continued using existing workflows. Data moved through quantum-safe tunnels without any user-facing differences. From the perspective of the business, nothing "looked" different.

## QuSecure's Adaptive Integration Approach

Throughout the pilot, QuSecure demonstrated adaptive responsiveness to customer needs with quick turnaround times on integration requirements. When challenges emerged – from SIEM formatting to certificate management workflows—the QuSecure team worked collaboratively to develop solutions tailored to the organization's specific environment.

### What Required Focused Work

**SIEM Integration:** SIEM integration revealed the gap between vendor defaults and enterprise reality. QuProtect R3's log formatting did not match existing Splunk correlation patterns the SOC relied on. The security team spent two weeks building custom correlation rules and working with QuSecure support to adjust log structure. That effort produced reusable templates so subsequent deployments would not repeat it.

**Certificate Management:** The organization's enterprise PKI and approval processes were designed for traditional server certificates, not gateway deployments at this scale. Initial certificate provisioning ran into delays because workflows did not match the gateway-centric model. Security and PKI teams collaborated to create a governance model that fit existing processes while supporting QuProtect's architecture.

**Network Monitoring and Baselines:** Existing performance monitoring tools were not designed for encrypted tunnels through gateways. Network operations needed to establish new baselines for protected data paths, then tune alert thresholds based on observed patterns. SOC analysts had to learn what "normal" looked like in a quantum-safe gateway environment.

**Change Control Documentation:** Enterprise change management required extensive documentation and testing plans. Building that documentation extended the initial approval cycle but resulted in a comprehensive package that now serves as the template for production deployments.

The pilot demonstrated that network-level deployment removes the need to coordinate hundreds of application teams, but enterprise integration still requires targeted work. It identified where that work resides and turned it into reusable patterns.

## Performance Validation

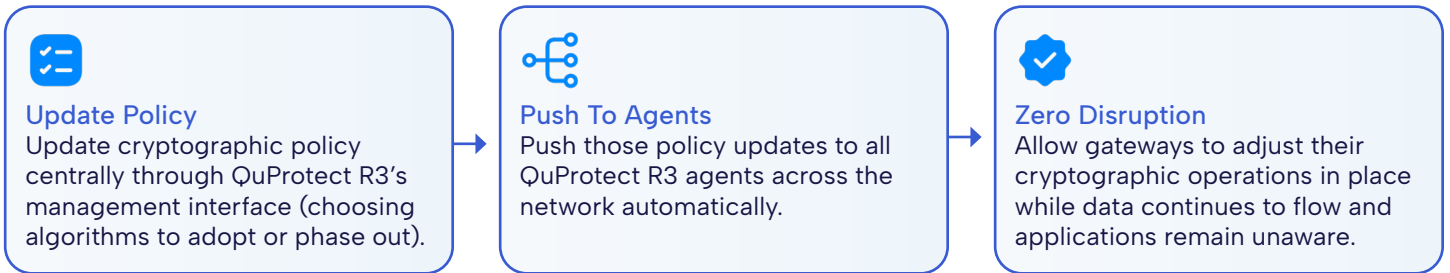
Testing with production-like traffic patterns validated that the migration caused no disruption to performance – latency impact was negligible and within acceptable parameters for field-to-datacenter communications.

While QuProtect R3 provides performance testing capabilities through its product tooling, the organization chose to leverage their own established testing tools to validate results within their existing operational frameworks.

## KEY CAPABILITY VALIDATED

# Demonstrable Crypto Agility

The pilot validated QuProtect R3's crypto agility controls in operation—not just in design. When standards change, the organization can adapt in minutes, not years.



## What The Pilot Proved

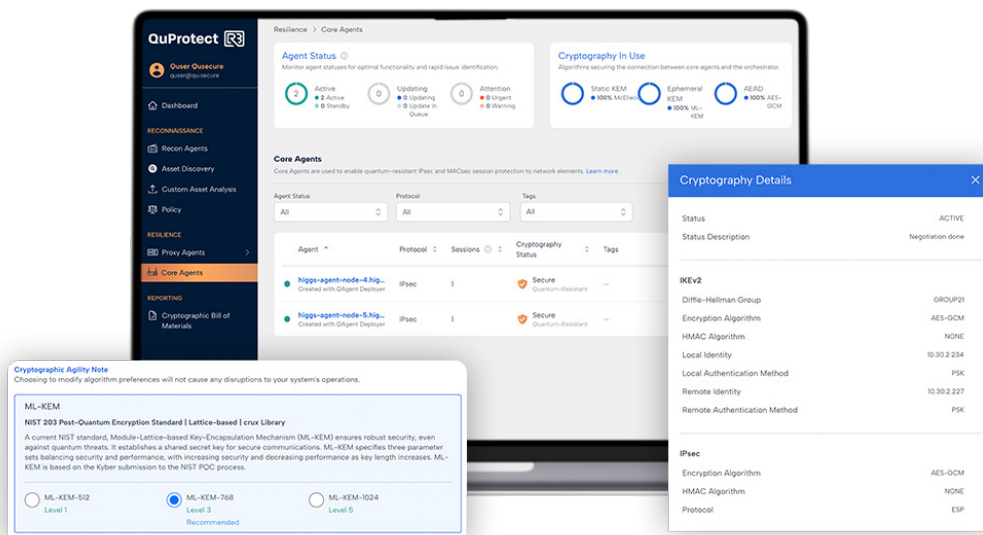
The organization tested algorithm rotation during the pilot, updating gateways from one PQC algorithm configuration to another through policy changes. This validated that:

- Policies could be updated centrally.
- Gateways would adapt automatically.
- Data flows would continue without disruption.
- Applications and endpoints did not need to be modified.

## Why This Matters

For infrastructure that cannot adapt, such as 30-year-old SCADA systems, the gateway becomes the point of agility. The SCADA system does not "know" encryption changed. The gateway protecting it has updated based on centralized policy. As standards evolve over the remaining 15–20 years of the infrastructure's life, the organization can keep pace without ever touching the systems themselves.

This capability directly addresses a fundamental problem in the energy sector: infrastructure lifecycles measured in decades, cryptographic lifecycles measured in years, and no practical way to update many of the systems in between.



## Results

<b>Phased Production Deployment Greenlit</b>	Operational validation in a production-equivalent environment provided the proof executive leadership needed. The exploration business unit served as an executive sponsor for production rollout.
<b>Crypto Agility Demonstrated</b>	Centralized policy updates and algorithm rotation were proven operationally. The organization established a way to adapt as cryptographic standards evolve without touching applications, redeploying infrastructure, or coordinating hundreds of development teams.
<b>Integration Framework Established</b>	The org achieved successful migration for legacy systems that would have otherwise been unmigratable through application-level approaches. SIEM correlation rules documented for reuse. Certificate management workflows adapted to gateway model to support segmented systems. Network monitoring baselines established. SOC procedures updated. Change-control templates created and approved. No parallel infrastructure required.
<b>Deployment Approach Validated</b>	Gateway placement strategy, performance benchmarks, and testing procedures were defined and proven in practice. Production deployment can proceed with confidence.
<b>Legacy System Protection Achieved</b>	The network-level approach enabled quantum-safe protection for decades-old SCADA systems, proprietary industrial protocols, and embedded controls—systems with no viable application-level migration path. These previously unmigratable systems are now protected against quantum threats without modification, operational disruption, or performance degradation.
<b>Industry Positioning Strengthened</b>	The organization moved from PQC in planning to PQC in operation, with a clear path to production scale and a foundation for future regulatory and competitive requirements.

### Program KPIs Tracked

#### Coverage

% of exploration data flows protected; # of field regions routed through quantum-safe tunnels

#### Performance

End-to-end latency impact on field-to-datacenter communications; throughput under production-equivalent load

#### Agility

Time to rotate algorithms/certs via policy; # of application team change windows avoided

#### OT Readiness

# of legacy/SCADA systems protected without endpoint modification; OT-to-IT boundary coverage

#### Integration

SIEM correlation rule reusability; certificate provisioning cycle time; change control template adoption

#### Compliance

CBOM completeness; policy drift alerts closed; alignment to anticipated CNSA 2.0 requirements

## Next Steps

### Phased Enterprise Expansion

The successful pilot has established the foundation for a larger-scale rollout across additional business units and regions, with the validated integration framework enabling accelerated deployment time-lines. Production deployment begins with the exploration data flows validated in the pilot, with plans for broader enterprise rollout building on this proven foundation.

- **External-facing applications:** High-visibility services benefit first, building confidence with customers and stakeholders, while posing lower internal coordination complexity than cross-business-unit internal systems.
- **Internal high-value flows:** Inter-facility communications, business-critical applications, and financial systems follow, using the same network-centric approach but with deeper business unit coordination.
- **Multi-region coordination:** The framework established during the pilot is adapted to different regional regulatory requirements, IT maturity, and change-control processes.
- **Resource model:** Funding is shared between central security and business unit IT budgets. Network operations teams are staffed to handle PQC deployment alongside other projects. Reusable change-control templates shorten approval cycles.

The pilot transformed PQC from an abstract concept into a defined program with a validated approach, known integration work, and an agreed scaling model.

### Identified Use Case: Operational Technology

The exploration data pilot validated network-level protection in an IT-like environment. Operational technology represents the next frontier. For energy companies, OT is the challenge that ultimately determines whether cryptographic migration is achievable at scale.

OT infrastructure in energy operations has constraints that make traditional security approaches impractical:

- Refineries operate continuously with control systems managing safety-critical processes.
- Pipeline SCADA systems coordinate operations across large geographic areas with deterministic timing requirements.
- Offshore platforms run extraction equipment in remote locations where unplanned downtime creates immediate safety risks and large revenue impacts.

These systems were installed 20–30 years ago and will remain operational through the 2040s. Many run proprietary software from vendors no longer in business. Safety certifications took years to obtain and cannot be easily revalidated. Change control reflects hard-learned lessons about the consequences of modifying infrastructure. Application-level updates are often impossible. Endpoint modifications risk voiding safety certifications. System replacement is not economically viable and in many cases not technically feasible within operational constraints.

At the same time, this infrastructure carries data adversaries value most: real-time operational parameters, control system communications, and operational intelligence with decades-long relevance. The encryption protecting this data today will be deprecated well before the infrastructure can be replaced, but the infrastructure itself cannot be updated to keep pace with cryptographic change.

For energy-sector security organizations, OT cryptographic protection is not just another use case. It is the test case that determines whether the overall PQC migration approach is viable. The organization that proves quantum-safe protection for OT infrastructure solves the constraint that defines the industry's cryptographic challenge. Everything else becomes a variation on that solution.

## About QuProtect R3™

QuProtect R3 is a post-quantum cryptography platform that enables organizations to discover cryptographic assets, remediate vulnerabilities, execute cryptographic agility, and report on cryptographic posture across IT and OT environments.

The platform uses a network-layer architecture, deploying agents at gateways to create quantum-safe encrypted tunnels without requiring endpoint modifications. This makes quantum-safe cryptography viable in environments where application-level remediation is impractical, particularly in energy infrastructure, legacy systems, and operational technology with decades-long lifecycles.

QuProtect R3's crypto agility allows algorithm updates through centralized policy changes rather than system-by-system modifications, enabling adaptation as standards evolve. The platform integrates with existing enterprise security infrastructure and security operations, enabling organizations to adopt quantum-safe protection while building on what they already have.

**35 Policy Violations**

Severity	Count
Critical	0%
High	31%
Medium	0%
Low	69%

**Secure Quantum-Resistant**

## Appendix How QuProtect R3™ Addresses OT



QuProtect R3 applies the same core principles used in the exploration data pilot to OT:

### Network-layer protection without touching endpoints:

Gateways sit between OT networks and IT systems, creating quantum-safe tunnels for OT-to-IT flows, inter-facility communications, and remote operations. SCADA systems, PLCs, and industrial protocols are not modified. The 30-year-old control system never knows encryption changed.

### Crypto-agility for infrastructure that cannot adapt:

As PQC standards evolve, vulnerabilities are discovered, or new threats emerge, encryption can be updated through centralized policy changes via the QuProtect R3 orchestrator. Over the remaining 15–20 years of an OT system's life, cryptographic standards may change multiple times. QuProtect allows organizations to keep pace without ever touching the underlying OT systems.

### Performance designed for industrial requirements:

Gateway deployment can be designed to maintain the deterministic timing that industrial protocols require. Latency is kept within acceptable parameters for non-safety-critical OT communications, and safety-instrumented systems remain isolated from any performance impact.

**Integration with existing OT security:** QuProtect R3 is designed to complement existing OT security investments (segmentation, OT monitoring, and industrial security tooling) by adding quantum-safe protection at the network layer rather than replacing existing controls.

**Phased deployment:** Rollout begins at OT-to-IT boundaries and lower-risk communications, validated first in non-production environments, then gradually expanded to more critical control systems. This approach respects OT safety culture and local change-control requirements.

### Priority OT Use Cases

Remote operations communications · Inter-facility SCADA · Vendor remote access · OT-to-IT analytics flows · Backup and disaster recovery paths for OT systems

Organizations that validate quantum-safe OT protection now will have operational experience and proven patterns when regulations and mandates arrive.