QuSecure

Technical Case Study

Global Telco
TLS Migration & Integrated PQC

MARCH 2026

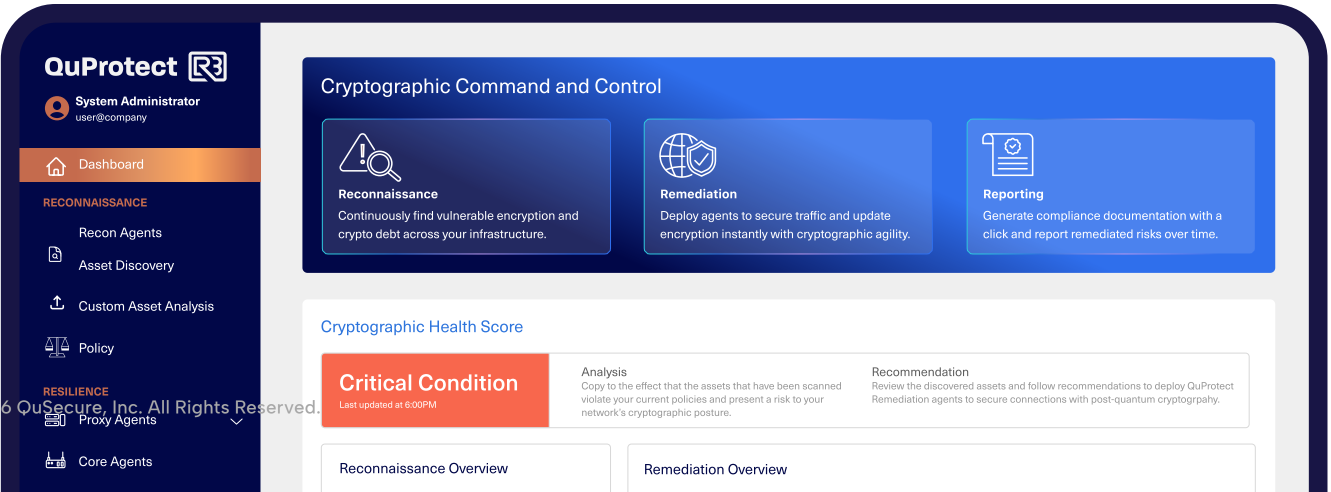
Executive Summary

A global Tier 1 telecommunications provider faced growing cryptographic debt and a near-term compliance clock, running hundreds of legacy and customer-facing services that couldn't tolerate refactors or coordinated change windows. The telco modernized its encryption estate by upgrading from TLS 1.2 to TLS 1.3 and enabling post-quantum-ready key exchange without rewriting legacy applications.

The program was executed end to end on QuSecure's QuProtect R3™ platform: discover critical assets, establish crypto agile policy, deploy at the edge and east west, harden core links, and continuously report a Cryptographic Bill of Materials (CBOM).

At A Glance Proof Panel

Non-Disruptive Rollout	New cryptographic cybersecurity mesh architecture (CSMA) added without impacting other connections; server/client certs can be auto deployed.
Orchestrated Ops	The QuProtect R3™ Orchestrator pushes changes quickly; activity is verifiable via Stats on the connection.
PQ-First By Policy	Enable/disable and drag and drop curve ordering; docs warn that prioritizing pre quantum curves will almost certainly negotiate a pre-quantum session.
QKD Alternative	Network encryption on existing Cisco IPsec and MACsec circuits was strengthened using RFC 8784 out-of-band keys via the Secure Key Integration Protocol (SKIP).
Legacy App Uplift	Front-end proxies terminate TLS 1.3 + hybrid PQ for supported clients and mesh to unchanged back-end apps—even if the app stack only supports TLS 1.2, older protocols, or plaintext.
PQTLS Reality	Post quantum key exchange (e.g., X25519 MLKEM768) runs in TLS 1.3; TLS 1.2 is frozen; ML DSA authentication staged due lack of standardization and larger key/signature sizes.
Scalability	Crypto cybersecurity mesh data plane engineered for tens of thousands of concurrent users with appropriate infra.



Cryptographic Command and Control

Reconnaissance
Continuously find vulnerable encryption and crypto debt across your infrastructure.

Remediation
Deploy agents to secure traffic and update encryption instantly with cryptographic agility.

Reporting
Generate compliance documentation with a click and report remediated risks over time.

Cryptographic Health Score

Critical Condition
Last updated at 6:00PM

Analysis
Copy to the effect that the assets that have been scanned violate your current policies and present a risk to your network's cryptographic posture.

Recommendation
Review the discovered assets and follow recommendations to deploy QuProtect Remediation agents to secure connections with post-quantum cryptogrpahy.

Reconnaissance Overview

Remediation Overview

Why This Mattered

Critical Infrastructure Risk

For the telco, “quantum risk” wasn’t abstract—it meant protecting customer PII and control-plane traffic without adding latency or downtime.

Telco networks carry massive volumes of customer PII and control plane data; TLS is the Internet’s backbone, and the quantum threat hits TLS first because it relies on public key crypto for key exchange and authentication.

Cryptographic Debt

Years of TLS 1.2 and mixed ciphers created operational fragility. Migrating to TLS 1.3 with centralized policy gave the telco a clean, PQ ready control plane and a path to continuous CBOM governance.

In practice, even small crypto changes required coordinating multiple app teams, regression testing, and maintenance windows – turning “routine upgrades” into outage-risk projects.

QuProtect R3™ As The Crypto Agility Control Plane

One orchestrated plane from asset discovery and CBOM to policy, automated certificate lifecycle, security mesh based enforcement, and continuous compliance reporting. Algorithm preferences were centrally governed and pushed fleet wide with no application code changes.

Discover in Order to Prioritize
QuProtect R3™ produced a current CBOM and TLS posture map; internet facing FQDNs and sensitive east west flows were grouped into waves with performance, compatibility, and rollback criteria.

Design for Policy-Based Governance
Crypto Agility Policy
PQ first policy: prefer TLS 1.3 hybrid PQ KEMs (e.g., X25519 MLKEM768); retain pre-quantum only where necessary for client compatibility.

Edge Modernization
Web/Edge Connections
Reverse/gateway proxies in front of web/API workloads. Proxies terminate TLS 1.3, negotiate PQ capable handshakes with supported clients, and cyber mesh to unchanged back end apps, even when those apps only natively support TLS 1.2, older protocols, or even plaintext.

Receipts: Non disruptive listener adds + auto server certs. Stats to verify outcomes.

East-West Modernization
Network Connections
Cryptographic CSMA established TLS 1.3 + PQ ready channels between services; mTLS defaults fit most deployments.

Receipts: Non disruptive listener adds; Orchestrator pushes changes quickly.

Core Transport Hardening - Parallel Track
RFC 8784 Out of Nand Keys on Existing Cisco Links
What we deployed: using QuProtect R3™, the telco enabled out of band keying (RFC 8784) on existing Cisco IPsec/MACsec circuits. R3 orchestrated key delivery/policy via the QuProtect Core interface, upgrading inter site tunnels on current hardware with no router replacement and no application changes.

Why This Path

After two years of QKD experiments, the telco concluded this approach: deploying post-quantum cryptography via orchestrated crypto agility - is currently more scalable, production ready, standards based, and cost effective for global rollout.

Standards QuSecure and Cisco co-authored the IETF SKIP protocol implementing RFC 8784

Interoperability Key source agnostic: R3 can accept keys from PQ ready KMS/HSMs or (where desired) QKD, and enforce uniform policy across mixed brownfield.

QuSecure

How We Rolled Out

Phased Approach

1. **Pilot & Lab Validation**
   One consumer web app and one internal API were front ended; modern clients negotiated PQTLS security mesh while back end stacks remained unchanged.

2. **Core Uplift**
   RFC 8784 OOB keys on targeted IPsec/MACsec paths; ASA enablement blueprint prepared.

3. **Edge Scale Out**
   Gateway placements aggregated many apps behind a high performance tier; DNS/routing steered flows.

4. **Service Tiering**
   Launched a premium “PQC ready encrypted connectivity” option for enterprise customers.

5. **Operate & Report**
   Orchestrated policy updates; continuous CBOM tracking protocols/algorithms/certs and flagging drift.

Architecture Snapshot

```
[Clients/Browsers]
     └ TLS 1.3 (PQ-capable where supported) → [QuProtect cyber mesh]
                                                    └→ [Legacy Apps & APIs]
                                        (no application code changes)

[Site A Network] — IPsec/MACsec + OOB keys (RFC 8784/SKIP) — [Site B
Network]
         ▲                            ▲
         └──── orchestrated by QuProtect R3 (policy, keys, certs, CBOM)
```

Placement Flexibility
Reverse proxy per app, shared gateway per tier, transparent service to service, or site to site.

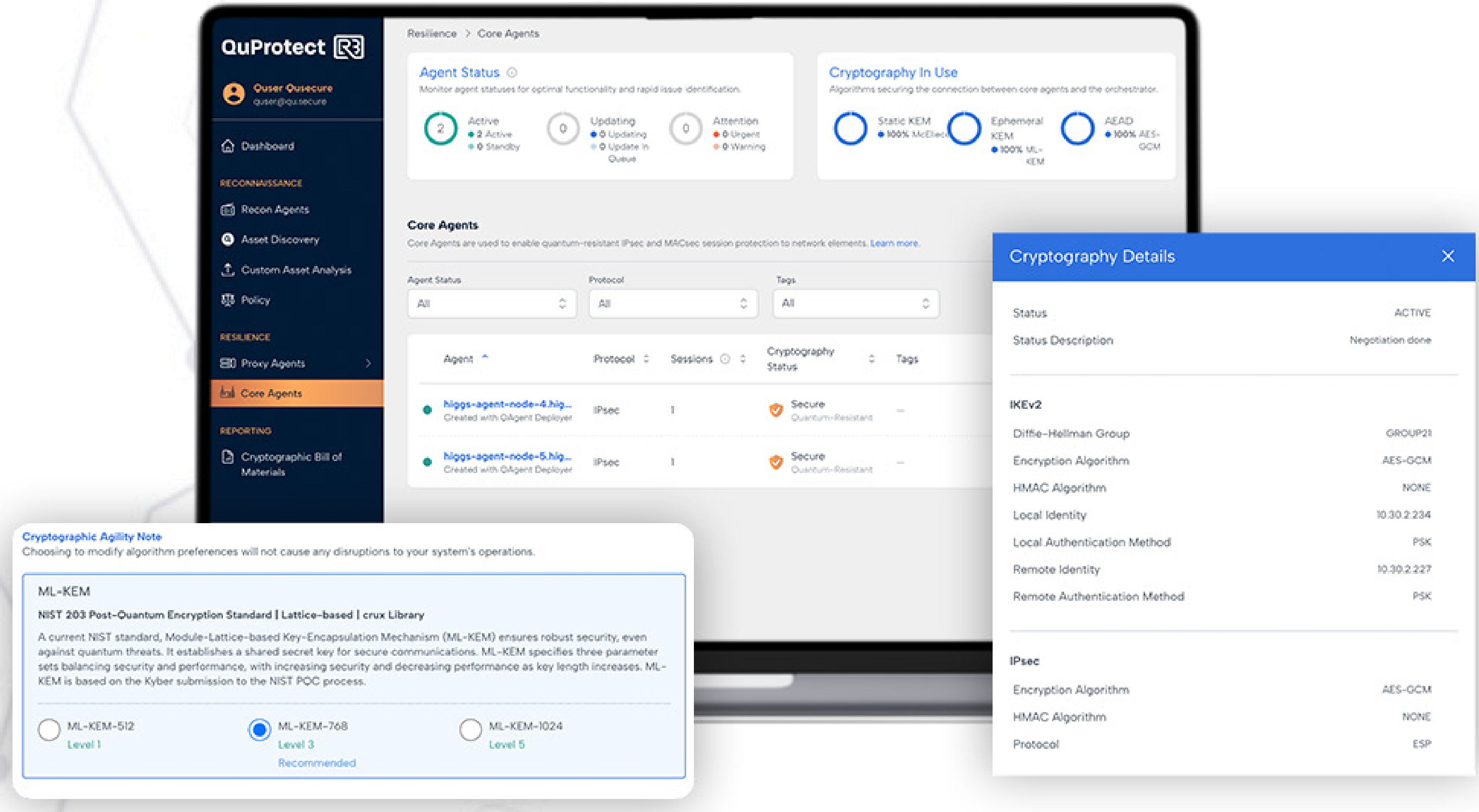
Scale
High performance core, sized to telco-grade concurrency and burst behavior.

Legacy Compatibility Model
Upgrade encryption at the proxy/mesh layer; leave the application untouched.

During the engagement, client » mesh PQTLS required TLS 1.3 + PQ algorithms in the client; some browsers lagged at that time (e.g., Safari). When both ends were proxied service » service, the proxies negotiated TLS 1.3 + PQ regardless of application capability, enabling upgrades even for <=TLS 1.2 and plaintext apps.

QuSecure

QuProtect R3™ Resilience | Core Security
Core Security delivers advanced quantum-resistant IPsec and MACsec protection per RFC 8784. It enables crypto agility, auditability for quantum security at layers 2 and 3, and easily integrates into existing infrastructure.



Agent Status
Monitor agent statuses for optimal functionality and rapid issue identification.

- 2 Active: ● 2 Active, ● 0 Standby
- 0 Updating: ● 0 Updating, ● 0 Update In Queue
- 0 Attention: ● 0 Urgent, ● 0 Warning

Cryptography In Use
Algorithms securing the connection between core agents and the orchestrator.

- Static KEM: ● 100% McEliece
- Ephemeral KEM: ● 100% ML-KEM
- AEAD: ● 100% AES-GCM

Core Agents
Core Agents are used to enable quantum-resistant IPsec and MACsec session protection to network elements. Learn more.

Agent Status: All
Protocol: All
Tags: All

Agent	Protocol	Sessions	Cryptography Status	Tags
higgs-agent-node-4.hig... Created with QAgent Deployer	IPsec	1	Secure Quantum-Resistant	–
higgs-agent-node-5.hig... Created with QAgent Deployer	IPsec	1	Secure Quantum-Resistant	–

Cryptography Details

Status	ACTIVE
Status Description	Negotiation done
IKEv2	
Diffie-Hellman Group	GROUP21
Encryption Algorithm	AES-GCM
HMAC Algorithm	NONE
Local Identity	10.30.2.234
Local Authentication Method	PSK
Remote Identity	10.30.2.227
Remote Authentication Method	PSK
IPsec	
Encryption Algorithm	AES-GCM
HMAC Algorithm	NONE
Protocol	ESP

Cryptographic Agility Note
Choosing to modify algorithm preferences will not cause any disruptions to your system's operations.

ML-KEM
NIST 203 Post-Quantum Encryption Standard | Lattice-based | crux Library
A current NIST standard, Module-Lattice-based Key-Encapsulation Mechanism (ML-KEM) ensures robust security, even against quantum threats. It establishes a shared secret key for secure communications. ML-KEM specifies three parameter sets balancing security and performance, with increasing security and decreasing performance as key length increases. ML-KEM is based on the Kyber submission to the NIST PQC process.

○ ML-KEM-512 Level 1   ● ML-KEM-768 Level 3 Recommended   ○ ML-KEM-1024 Level 5

Program KPIs The Telco Tracked

Coverage
% of priority FQDNs/apps upgraded to TLS 1.3; % of client sessions negotiating hybrid PQ

Performance
P95/P99 handshake deltas; end to end latency under load

Agility
Time to rotate algorithms/certs via policy; number of app team change windows avoided

Core
# of IPsec/MACsec links protected with RFC 8784 OOB keys

Compliance
CBOM completeness and policy drift alerts closed per quarter. This telco counts the US Government as a key customer and had a special eye toward CNSA 2.0 compliance timelines.

QuSecure

Results

Security & Resilience

TLS 1.3 everywhere that mattered; PQ ready where clients support it. Internet facing sessions negotiated PQ capable handshakes without backend changes.

Legacy apps weren't the critical path. TLS 1.2 (and even plaintext) applications were front-ended by the cybersecurity mesh, so app teams avoided code changes and regression cycles.

Hardened core links. Inter site circuits uplifted using RFC 8784 OOB keys on existing Cisco hardware.

QKD Alternative

The telco judged the RFC 8784/SKIP approach a scalable, production ready, standards based, and more cost effective alternative to continuing its QKD pilots—fit for global production.

Operations

Change without disruption. Adding listeners and pushing policy did not interrupt other connections; rollbacks were policy based.

Crypto agility by design. Algorithm ordering and enable/disable controls were centralized—preparing for PQ authentication (ML DSA) when operationally practical.

Continuous CBOM. Executives and audit gained ongoing visibility into protocols, algorithms, and certificates across edge and core (via R3).

Commercial Impact

New premium service tier offering. "PQC ready encrypted connectivity" became a paid option, aligning stronger security with revenue.

Performance, Cost & Time

Primary Customer Concerns

- Handshake latency & P95/P99 response times
- Throughput & cybersecurity mesh footprint at telco grade concurrency
- Cost & timeline vs. rewriting legacy applications

How We Addressed Them

Upfront sizing & tests
We modeled capacity and load tested the cryptographic cybersecurity mesh under realistic traffic; acceptance thresholds aligned to existing SLOs.

Data driven promotion
R3's Stats and external APM corroborated handshake outcomes and latency budgets per wave before promotion.

Avoided rewrites
By terminating TLS at the platform, the telco avoided per app code changes and regression cycles—reducing engineering effort and change window risk.

Exec-Ready Value

Performance Met SLOs at scale; no material impact to customer experience.

Cost/Time Centralized rollout replaced hundreds of application rewrites; fewer change windows, faster coverage.

What Changed

Why Now TLS is the backbone; post quantum algorithms land in TLS 1.3 (TLS 1.2 is frozen).

What Changed A crypto agile control layer now upgrades edge/application traffic to TLS 1.3 with hybrid PQ KEM and hardens core transport via RFC 8784—without refactoring legacy apps.

Scale & Fit Envoy derived reverse/gateway pattern for tens of thousands of concurrent users; deploy per app, shared gateway, transparent service to service, or site to site.

Strategic Result Crypto agility—central algorithm governance and rotation; the next algorithm change is a policy update, not a rewrite.

Next Steps

PQC authentication (ML DSA) pilots with attention to larger key/signature sizes and toolchain readiness.

ASA expansion of RFC 8784 hardening as change windows permit (blueprint complete).

Broaden PQ first policy across additional zones as client support continues to increase.

Closing Thoughts

This was not a narrow protocol tweak. On QuProtect R3™, the telco turned a fragmented TLS 1.2 estate into a TLS 1.3 + PQ ready fabric with crypto agility and CBOM built in:

Discover › Prioritize › Deploy › Operate › Report

and did it without rewriting legacy apps. For a telco carrying the world's PII in transit, that's the difference between falling behind and setting the pace. Others are already moving; if you're not, you're behind.

FAQs

Will this break running apps or force refactors?
No. The cyber mesh terminates TLS on behalf of the app. Adding new listeners happens without disrupting other connections, and certs can be auto deployed.

Is this really TLS 1.3 (not bolt on crypto)?
Yes. PQTLS (hybrid KEMs, ML DSA) is standardized for TLS 1.3. TLS 1.2 is frozen by the IETF TLS WG.

How do we force PQ first safely and keep compatibility?
Use QuProtect R3's enable/disable and drag and drop curve ordering. Docs note that prioritizing a pre quantum curve will almost certainly yield a pre quantum session; leaving PQ curves first enforces PQ first negotiation with compatible clients.

Does it scale to telco workloads?
Yes. The data plane is Envoy derived and engineered for tens of thousands of concurrent users with appropriate infra; this was discussed and validated during the engagement.

Why not continue with QKD for backbone links?
After two years of QKD pilots, the telco concluded RFC 8784/SKIP is the scalable, production ready, standards based, and cost effective path for global deployment on existing hardware. R3 is key source agnostic(KMS/HSM, QKD if desired), so you can still integrate QKD where it makes sense.

What about performance and customer experience?
We sized the cyber mesh up front, load tested under realistic concurrency, and used Stats + APM to verify P95/P99 latency before each wave's promotion. Result: met existing SLOs with no material customer experience impact.

Do clients need PQ support to benefit?
For client to mesh PQTLS, the client must support TLS 1.3 + PQ. At the time, some browsers lagged. For service to service, paired proxies negotiate TLS 1.3 + PQ regardless of app capability, so you can uplift even TLS 1.2/plaintext apps.

How fast can we change algorithms or rotate certificates?
Via R3 policy. Orchestrator pushed updates usually happen quickly, and you can roll out/revert without touching application code.