QuSecure

Case Study

From Risk to ROI
How A Major EU Telecom Secured Core Router Links with QuProtect R3

November 2025

QuSecure

Executive Summary

A leading European telecommunications provider faced a familiar problem for large, distributed networks: a vast and messy cryptographic estate, and a very real quantum risk horizon.

They knew they couldn't fix everything at once, so they started with a simple question:

> "What's the smartest place to start if we want to take a big bite out of our cryptographic risk quickly, without breaking the network?"

Before engaging any vendors, the provider's network and security teams completed an internal risk review to identify the highest-impact – and highest-risk – links. That led them to router-to-router backbone and aggregation links:

QuProtect R3 Core Security was deployed on the chosen router-to-router footprint and delivered quantum-resilient protection in under one week, with no measurable impact on latency, throughput, or failover behavior and no changes to applications, network topology, or hardware.

A **Quantum Key Distribution** (QKD) proof of concept that required specialized hardware and optical changes

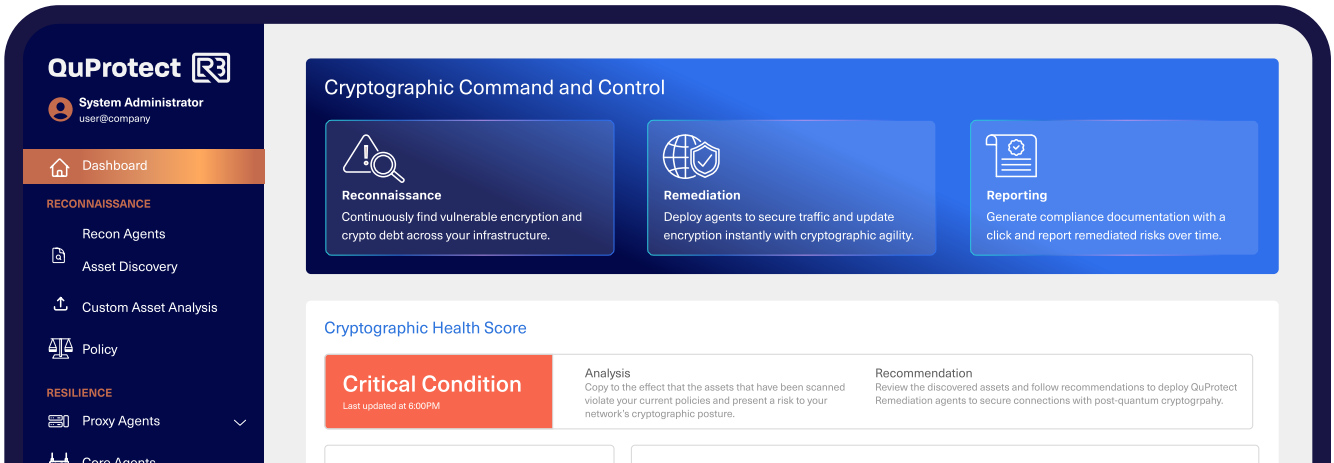
A **discovery-only PQC** assessment solution that could inventory cryptography but not protect live traffic

QuSecure's **QuProtect R3**™ Core Security, a software overlay that uses NIST PQC to harden existing IPsec/MACsec tunnels with post-quantum preshared keys (PPKs) via SKIP – without changing routers or applications

The Bottom Line

QuProtect R3 delivered quantum-resilient protection in under one week—no changes to applications, network topology, or hardware. Where QKD offered theory and discovery tools offered visibility, **QuProtect R3 delivered practical security the network could actually run.** The provider now has a concrete, high-ROI first step on its quantum-safe roadmap—and a path to turn PQC from a cost center into a revenue-enabling capability.

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.



QuSecure

The Strategic Challenge

Shrinking a Huge Risk Surface Without Breaking the Network

Like many large providers, this telecom had:

- Thousands of applications and services
- Multiple generations of cryptography in use
- Tight SLAs and complex topologies spanning backbone and metro networks

They understood the quantum threat: data encrypted today on long-lived links can be captured now and decrypted later once a sufficiently powerful quantum computer exists. At the same time, they faced three practical constraints:

- The cryptographic estate was too large to retrofit every application and service at once.
- Strict backbone and metro SLAs left no room for disruptive changes to routing or encryption.
- Leadership needed visible risk reduction in months, not a three- to five-year transformation program.

> The risk review reframed the problem from "fix everything" to **"fix the highest-impact links first."** Router-to-router backbone and aggregation links emerged as the logical starting point: a small number of tunnels carrying a disproportionate share of critical traffic—and therefore the largest blast radius per tunnel.

By the time they entered the market, the scope was clear: secure existing router-to-router IPsec and MACsec links with quantum-safe protection as quickly and safely as possible.

Why Router-to-Router Delivers Maximum ROI

1. High Leverage from Traffic Aggregation

Each backbone tunnel carries tens of gigabits per second of mixed customer, internal, and control traffic. Securing a small set of tunnels protects hundreds to thousands of downstream applications.

2. Strong Operational Control

Router-to-router paths already sit inside mature operational processes. Latency, packet loss, and failover are continuously monitored—making these links the safest place to introduce a new cryptographic control.

3. Far Fewer Integration Points

Remediating cryptography application by application would mean touching 1,000+ systems. Securing ~20 router-to-router links covers the same traffic—**tens of times fewer integration efforts.**

The conclusion was straightforward: Start where one move protects many things. Router-to-router protection offers a calibrated, high-value first step to remediate cryptographic risk at scale.

QuSecure

What Is QuProtect R3 Core Security

High Level Overview

QuProtect R3 Core Security is a software solution designed to bring quantum-safe security and cryptographic agility to existing IPsec and MACsec deployments—without new hardware or network redesign.

At a high level, Core Security:

- Consists of a cloud-based Orchestrator and distributed Agents
- Requires no new hardware
- Uses ML-KEM (the NIST-standardized KEM) and post-quantum TLS to distribute quantum-safe pre-shared keys (PPKs)
- Hardens existing IKEv2/IPsec and MACsec tunnels rather than replacing them
- Automates key rotation, crypto-agility, and resilience from a central control plane

In this engagement, Core Security was evaluated on one concrete question:

Can it make our existing router-to-router IPsec/MACsec links quantum-safe, without disruption?

The answer was yes.

Deployment Architecture

The deployment centered on QuProtect R3 Core Security with two main components:

QuProtect Core Agents

Deployed as software on Ubuntu VMs within existing hypervisors

Performed post-quantum key establishment

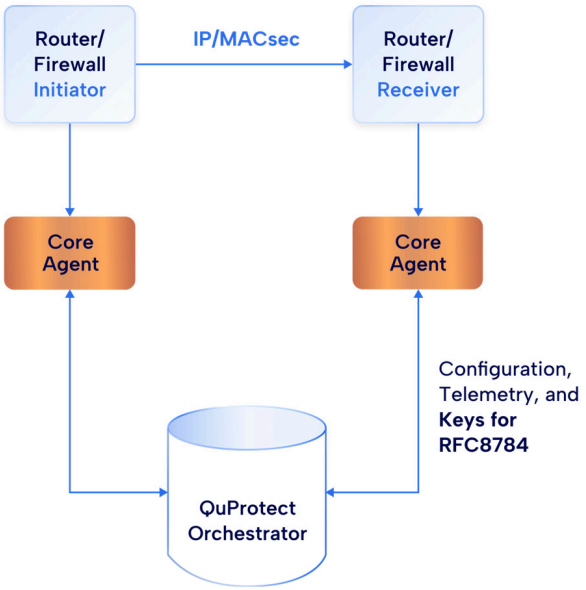
Supplied post-quantum PPKs to IPsec/MACsec endpoints

QuProtect Orchestrator

Operated as a cloud-based management plane

Provided centralized management of cryptographic posture, policy, and key lifecycle

Used post-quantum TLS and ML-KEM to securely distribute quantum-safe PPKs to Agents



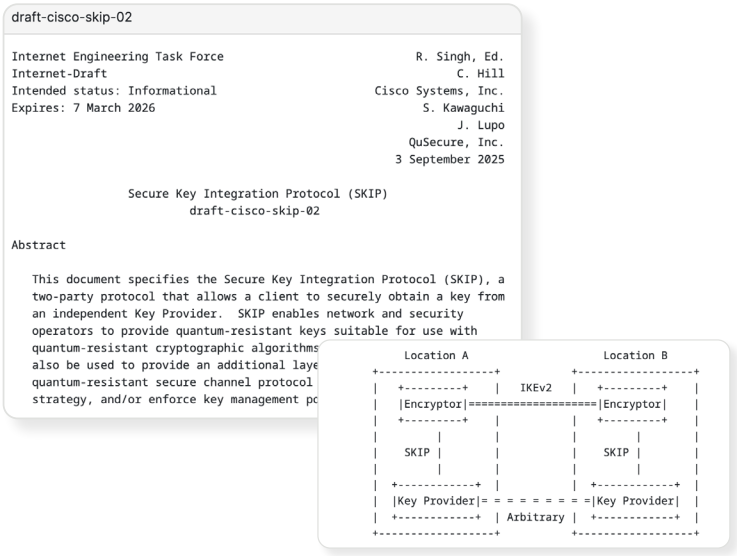
QuSecure

Cisco C8500 Integration

For this engagement, QuProtect integrated with a Cisco C8500-12X router:

- Used RFC 8784 PPK via the SKIP protocol
- Delivered PPKs into existing IKEv2/IPsec and MACsec configurations
- Enhanced the existing crypto posture rather than requiring a new design
- Left routing and traffic engineering unchanged

Routers kept doing exactly what they already do—just with quantum-safe key material mixed in.


draft-cisco-skip-02

Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: 7 March 2026

R. Singh, Ed.
C. Hill
Cisco Systems, Inc.
S. Kawaguchi
J. Lupo
QuSecure, Inc.
3 September 2025

Secure Key Integration Protocol (SKIP)
draft-cisco-skip-02

Abstract

This document specifies the Secure Key Integration Protocol (SKIP), a two-party protocol that allows a client to securely obtain a key from an independent Key Provider. SKIP enables network and security operators to provide quantum-resistant keys suitable for use with quantum-resistant cryptographic algorithms
also be used to provide an additional laye
quantum-resistant secure channel protocol
strategy, and/or enforce key management po

QuSecure architects worked side by side with Cisco architects to shape the QuProtect Core Security product and co-author the Secure Key Integration Protocol (SKIP), an IETF Internet-Draft that advances standards for quantum-resilient key management.

IETF SKIP Draft

Cryptography Stack
(Aligned with NIST PQC Standards)

ML-KEM (Kyber-based KEM)
Used as the post-quantum key-encapsulation mechanism for establishing shared secrets for the tunnels

AES-256-GCM
Used for high-performance symmetric encryption and integrity

Aligns with NIST guidance on symmetric strength in a post-quantum context

Hybrid PQC + Classical Modes
ML-KEM can be combined with classical key exchange (e.g., Diffie–Hellman) where required

Supports a standards-aligned migration posture and interoperability during rollout

Crypto Agility
Policy-driven control over ML-KEM parameters, hybrid policies, and symmetric settings

Allows adjustment as standards and risk tolerance evolve

OPERATOR VIEW
WHAT ACTUALLY CHANGES?

For engineers and operators, the key point was simple:

- The data path looked the same
- The cryptography behind it got much stronger

Existing IPsec/MACsec links stayed in place; QuProtect R3 Core Security quietly upgraded them to quantum-safe, agile cryptography from a centralized control plane.

QuSecure

The Evaluation

The provider evaluated three approaches against the same router-to-router test case: securing existing IPsec between Cisco routers.

NOT SELECTED

Quantum Key Distribution (QKD)

QKD was tested on selected backbone paths. It promised quantum-derived keys, but required:

- Specialized hardware and new optical infrastructure
- Distance and media constraints that didn't work for the full network
- A separate operational model, distinct from existing IP/MPLS stack

Verdict: Too complex and too expensive for wide deployment, especially given existing IPsec/MACsec investments.

NOT SELECTED

Discovery-Only PQC Assessment

A consulting-led solution could scan the estate and produce inventories and reports for planning. But it could not:

- Secure router-to-router IPsec/MACsec tunnels
- Demonstrate quantum-safe security on live traffic
- Prove performance characteristics

Verdict: Answered "Where is our crypto?" but not "How do we fix our highest-value links now?"

✓ SELECTED

QuProtect R3 Core Security

QuProtect R3 was evaluated on whether it could:

- Use NIST-aligned ML-KEM to protect keys for existing IPsec/MACsec tunnels
- Run as software on existing hypervisors and Cisco C8500 routers
- Deliver no measurable performance impact at 10–100 Gbps
- Demonstrate resilience under real-world failure conditions
- Fit into existing change management, NOC, and SOC processes

Result: QuProtect R3 Core Security did exactly that—proving quantum-safe protection could be deployed in production without disruption.

> Considering the PQC product space is pretty new, the QuSecure product quality actually exceeded my expectations... No challenges encountered. The whole experience was very smooth."
>
> Senior Network Architect, CCIE

QuSecure

Technical Implementation With QuProtect R3

Week 1: Establish PQC Control Plane

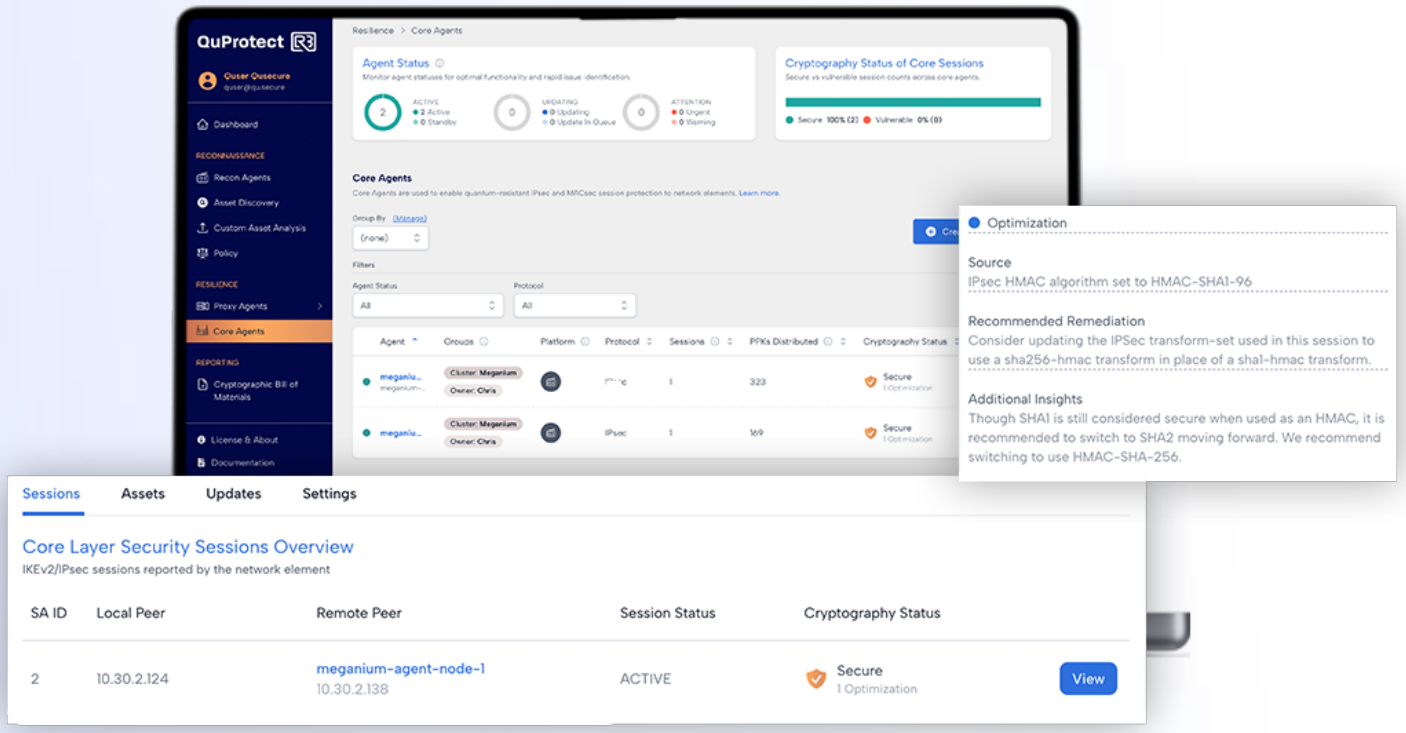
- Deployed QuProtect Core Agents on Ubuntu VMs
- Registered agents to cloud-hosted Orchestrator via existing HTTPS proxies
- Verified PPK synchronization and health checks
- Defined initial ML-KEM and hybrid policies, including key rotation intervals

Week 2: Attach PQC to Tunnels

- Established router-to-agent connectivity for targeted C8500-12X routers
- Configured IPsec tunnels to use RFC 8784 SKIP + PPKs
- Conducted performance tests under realistic load
- Conducted resilience and failover tests

Performance Results

- No measurable increase in latency
- No reduction in throughput
- No adverse impact on packet loss or jitter
- Automatic fallback to classical Diffie–Hellman verified



QuSecure

Key Technical Achievements

Quantum-Safe Protection with Zero Performance Impact

QuProtect R3 Core Security added PPKs to existing IPsec tunnels without changing routing design, adjusting QoS policies, or upsizing router hardware. Latency, throughput, and packet processing metrics remained within normal variance.

Centralized Crypto-Agility

With the Orchestrator, the provider can manage ML-KEM and hybrid crypto policies from a single console—adjusting parameters and rolling out changes across many tunnels without touching each router individually when standards change.

Resilience and Intelligent Fallback

Business continuity remained non-negotiable. QuProtect R3 delivered automatic fallback to classical key exchange when PQC PPK distribution was unavailable, plus continuous tunnel availability during simulated failures. PQC became an additive control, not a new point of fragility.

Automated Key Management

Configurable key rotation (validated at 1-hour intervals), perfect forward secrecy without manual intervention, and alignment with internal and external expectations on key management hygiene.

Business Impact

Coverage and Effort

By focusing on router-to-router links, the provider turned a large problem into a manageable project:

- Multiple IPsec tunnels now protect traffic for **thousands of enterprise customers**
- Multiple MACsec connections protect metro aggregation points
- Versus an application-centric approach that would require touching 1,000+ systems, protecting ~20 strategic network points covers the same traffic

New Revenue and Market Positioning

With quantum-safe router-to-router protection in place, the provider can:

- Offer **quantum-safe connectivity tiers** to high-security customers
- Demonstrate a concrete, operating PQC deployment to regulators and enterprise buyers
- Differentiate from competitors who are still at the planning or lab-only stage

Key outcome: They turned PQC from a pure cost center into a revenue-enabling capability.

QuSecure

Why QuProtect R3 Succeeded Where Others Struggle

Infrastructure-First Design

Augments existing IPsec/MACsec on routers instead of replacing hardware. Aligns with the provider's existing IP/MPLS architecture—no rip-and-replace required.

Resilience by Design

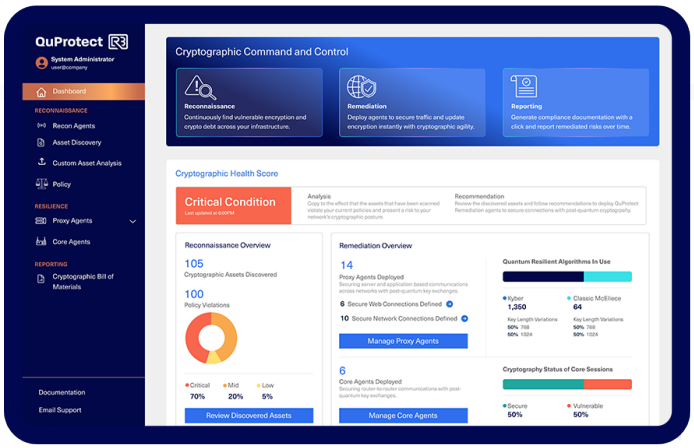
Built-in fallback, automated key rotation, and central policy management. PQC that respects uptime commitments—not just cryptographic theory.

Real-World Proof, Not Just Lab Claims

Deployed under load and failure conditions. Demonstrated non-disruptive behavior in performance and failover tests on production-equivalent infrastructure.

Visibility and Integration

Native integration with existing SOC workflows and CBOM generation for compliance reporting. Fits into how the team already operates.



Looking Ahead

The pilot demonstrated that QuProtect R3 can scale as the footprint grows:

- Sub-second PPK delivery under load
- Agents running across multiple data centers and regions
- Centralized management of cryptographic posture across all protected links

Roadmap

Phase 1

Production deployment across backbone tunnels

Phase 2

Extend MACsec protection across wider aggregation networks

Phase 3

Launch of quantum-safe connectivity services for enterprise customers

Over time, they plan to use more of the QuProtect R3 platform for cryptographic inventory across internal networks and CBOM reporting for continuous compliance.

QuSecure

Key Takeaways for Technical Leadership

If you own backbone, metro, or large enterprise WAN strategy, the core lessons are:

1. Start where one move protects many things

Router-to-router backbone and aggregation links are the highest-leverage place to begin shrinking cryptographic risk. A small number of strategic links can protect traffic for thousands of downstream applications.

2. Preserve proven infrastructure

Enhancing existing IPsec/MACsec on current routers is often faster and safer than rip-and-replace. You've already invested in this infrastructure—extend its value rather than starting over.

3. Design for resilience, not just algorithms

PQC has to coexist with SLAs, change windows, and incident response—not just with standards documents. Automatic fallback and continuous availability are non-negotiable.

4. Use crypto-agility as a system, not a project

A centralized, policy-driven control plane lets you evolve with NIST and your own risk tolerance without repeating the entire rollout every time standards change.

The Bottom Line

You make the biggest dent in quantum risk when you protect the links that carry the most value, with a solution your network can actually run. For this provider, QuProtect R3 Core Security delivered what other approaches could not: **quantum-safe protection deployed in days, not years**, working within existing infrastructure and operational constraints.

+1 (650) 356-8001 info@qusecure.com www.qusecure.com