ENCRYPTION CONSULTING

CASE STUDY

ENTERPRISE ENCRYPTION PLATFORMS

Unifying multi-cloud key management for a US telecom with a CipherTrust Manager upgrade

A US telecommunications leader with a market cap over $200 billion was running key management across clouds with no consistent standard, on an end-of-life CipherTrust Manager. We upgraded it to unify encryption across AWS, Azure, and Google Cloud.

SECTOR	SIZE	ENGAGEMENT
Telecommunications	Multi-cloud + hybrid	CipherTrust upgrade

2.10
CipherTrust version reached

Multi-cloud
Key management unified

PQC
Algorithm support added

A US telecom leader, built on 5G speed

Our client is a United States telecommunications firm with a market capitalization of over $200 billion in 2024, consistently outpacing major global rivals by pushing the boundaries of technology and security. With more than 1,000 network specialists, it delivers some of the fastest 5G network services available.

Whether customers are on the road, in the air, or looking for high-speed home internet with unlimited plans and the latest devices, the firm's reputation rests on performance and reliability. Behind that, a sprawling multi-cloud environment needed key management it could actually depend on.

When encryption is scattered across clouds with no common standard, scale becomes the enemy. Unifying it was the foundation for everything else.

A legacy platform, stretched past its limits

Across a sprawling multi-cloud estate, an aging CipherTrust Manager left key management inconsistent and exposed.

1

Fragmented key management

Each cloud handled keys differently, AWS KMS one way, a third-party tool another, with mismatched rotation, so the team couldn't track policies consistently.

2

Overlapping scan failures

On the legacy 2.0 version, starting a second scan on a data store still being scanned made the first fail repeatedly, disrupting workflows and forcing re-runs.

3

No standardization, high latency

Applications used different crypto standards, AES-256 here, AES-128 there, and inefficient key management introduced latency and performance bottlenecks.

4

No key-export logging

The old version didn't record key-export requests made soon after a prior export, leaving no audit trail for security monitoring or compliance.

5

Insecure protocols, downtime, and end of life

CipherTrust Manager still ran TLS 1.0, widening the attack surface to APTs, suffered downtime during routine maintenance, and had reached end of life with no further patches or vendor support.

> “The existing CipherTrust Manager version could no longer support the organization's multi-cloud scale. Upgrading wasn't optional; it was the foundation for everything else.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · ENTERPRISE ENCRYPTION PLATFORMS

From legacy 2.0 to a unified platform

We assessed the environment, then guided a staged upgrade from 2.0 to 2.10, moving keys and policies with zero downtime and unifying encryption across every cloud.

Assessment and scoping

We assessed crypto configuration, network, and protocols across their on-prem, cloud, and hybrid setup, and sized the node count to scope the upgrade.

Guided upgrade path to 2.10

We selected the right version and guided the full path from 2.0 to 2.10, whose high-availability and multi-region support suited their many nodes.

Zero-downtime migration

PowerShell scripts moved keys and policies into the cloud platforms and databases with no downtime, while an agentless module inventoried keys across the estate.

Unified multi-cloud keys

With BYOK and HYOK across AWS, Azure, and Google Cloud, the organization's encryption practices finally became consistent everywhere.

Modern protocols and microservices

The upgrade dropped TLS 1.0 for a TLS 1.2 minimum and added full encryption support for microservices architecture.

Higher performance and tokenization

Stronger cryptographic performance protects data in transit in real time, and high-speed tokenization handles key operations at scale.

Unified, compliant, quantum-ready

The upgrade transformed the telecom's security operations, unifying key management across clouds, aligning with major standards, and readying it for what's next.

3

Major compliance standards aligned

BEFORE — audit gaps

AFTER — aligned

Unified across every cloud

Encryption and key management are now consistent across multi-cloud and hybrid systems, with secure inter-service communication for microservices.

Compliance, aligned

Encryption now meets NIST SP 800-57, PCI DSS 4.0, and CMMC 2.0, closing the gaps that had caused audit failures.

Lower latency, lower cost

Reduced latency and automated key rotation cut manual work and operational costs, while limiting the risk of human error.

Resilient and quantum-ready

Back under full vendor support and patched, with post-quantum algorithm support readying the firm for quantum-era threats.

IN SUMMARY

A foundation built to scale securely

Facing outdated encryption and a multi-cloud estate it could no longer manage consistently, the telecom upgraded CipherTrust Manager from 2.0 to 2.10 with zero downtime. The new platform unifies key management across AWS, Azure, and Google Cloud with BYOK and HYOK, replaces TLS 1.0 with modern protocols, and adds high-speed tokenization and microservices encryption. It now aligns with NIST SP 800-57, PCI DSS 4.0, and CMMC 2.0, runs under full vendor support, and supports post-quantum algorithms, turning an aging system into a resilient, scalable foundation for the future.

GET STARTED

Modernize your CipherTrust platform.

Talk to our Platforms team →