ENCRYPTION CONSULTING

CASE STUDY

ENTERPRISE ENCRYPTION PLATFORMS

A seamless CipherTrust Manager migration for a 40-year-old telecom

A telecommunications company with around 10,000 employees was running CipherTrust Manager on aging, end-of-life physical hardware. We migrated it to a scalable, high-availability virtual environment, with no data loss and minimal downtime.

SECTOR	SIZE	ENGAGEMENT
Telecommunications	10,000+ employees	CipherTrust migration

40+
Years in business

0
Data lost in migration

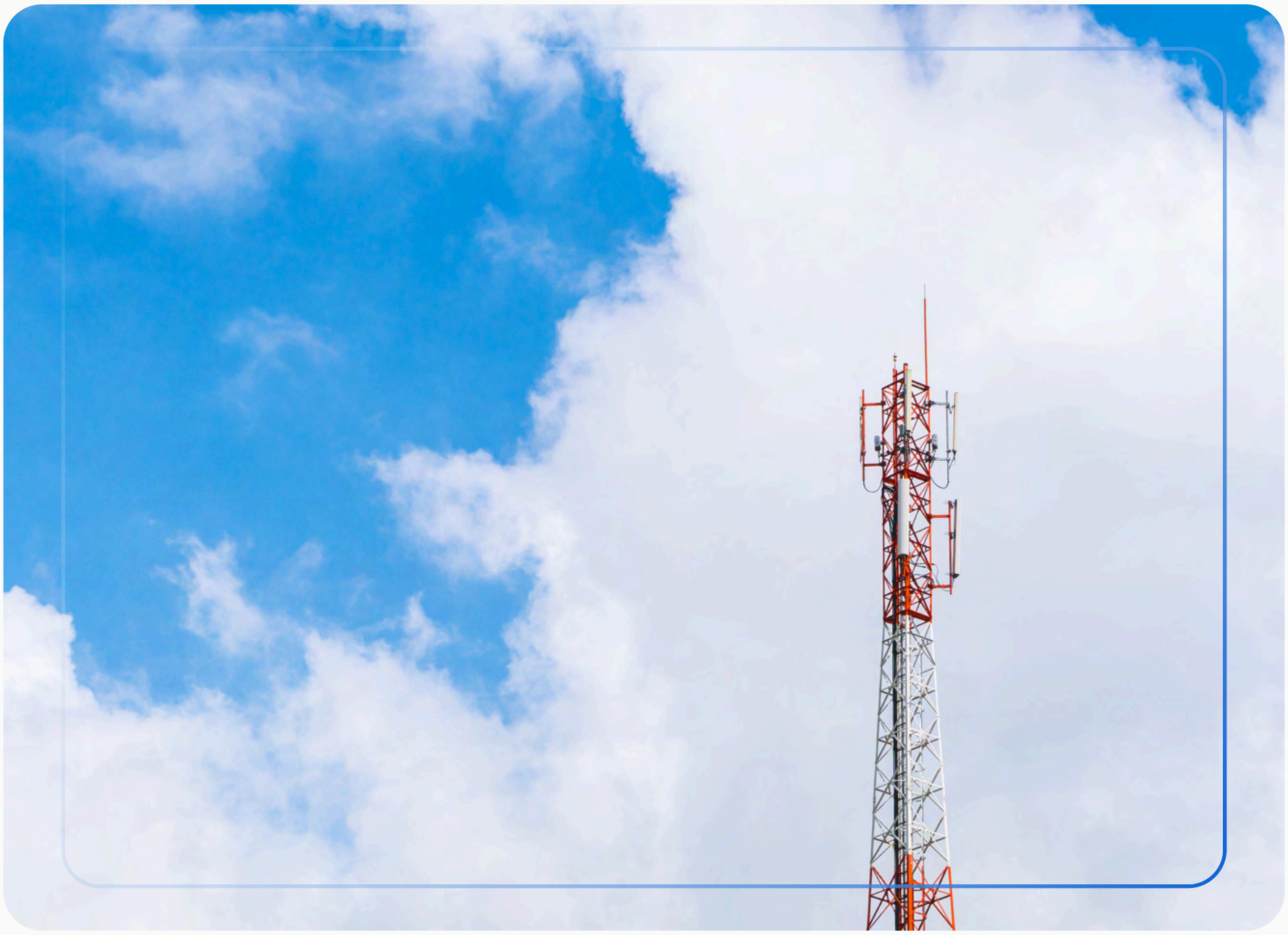
Multi-node
High-availability design

A telecom leader, 40 years in the market

We worked with a telecommunications company that has been in the market for more than 40 years, with around 10,000 employees and billions of dollars in annual revenue. It is recognized for its work across cloud operations, enterprise communication solutions, digital media technologies, and brand telemarketing.

In a fast-moving sector, data security and operational efficiency are non-negotiable, and the company handles millions of pieces of sensitive data every day. Like others in telecom, it is constantly enhancing its infrastructure to meet growing demand, and it had realized that CipherTrust Manager running on physical hardware was no longer enough.

In telecommunications, the key management platform underpins everything. Moving it can't mean downtime, and it certainly can't mean lost data.



An aging platform, at end of life

Migrating the telecom's CipherTrust Manager from physical to virtual surfaced urgent, overlapping risks.

1

Limited scalability

The physical setup couldn't scale with rapidly expanding operations and growing data complexity, and the outdated version simply couldn't keep up.

2

End of life, end of support

The in-house version had reached end of life and vendor support, cutting off critical updates and patches, and clashing with a policy to stay current or N-1.

3

Mounting vulnerabilities

The aging version carried known vulnerabilities that raised the risk of data loss, making the upgrade urgent and the data's safety during it a real concern.

4

Risky key migration

Moving encryption keys, user accounts, and security policies to the new version without losing data was complex, and an in-house attempt had proven too hard.

5

No high availability

The existing system wasn't built for high availability, with multiple points of failure that could cascade into significant downtime and undermine the entire data protection framework.

> With the system at end of life and vulnerabilities mounting, every extra day on the old version raised the data loss risk. The migration had to be precise, low-risk, and complete in one go.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · ENTERPRISE ENCRYPTION PLATFORMS

From physical to high-availability virtual

After analyzing the environment, we built a detailed roadmap, then migrated keys, accounts, and policies with scripts and rollback safeguards into a new, redundant virtual architecture.

Assessment and roadmap

In-depth stakeholder discussions and an infrastructure analysis fed a detailed migration roadmap with secure, high-availability architecture.

Safe migration with rollback

A comprehensive plan with backups, secure snapshots, and a rollback mechanism meant the client's data could always be recovered.

Scripted key migration

We led the migration of keys, accounts, and policies with custom scripts that replicated every configuration accurately and cut human error.

High-availability architecture

A new multi-node design with redundancy and failover ensures that if one component fails, the others keep operations running.

Load balancing and testing

Load balancing spreads workloads across servers, and thorough testing validated configuration, ran vulnerability scans, and watched performance.

Training and CTE agents

Comprehensive training prepared the client's team, and all CipherTrust Encryption agents were migrated and fully operational in the new setup.

04 THE IMPACT

A seamless move, a stronger platform

The migration modernized the telecom's key management without disruption, leaving it scalable, highly available, and back under full vendor support.

0

Data lost, with downtime minimized

Built to scale

The new scalable architecture lets the telecom absorb future growth and new requirements without major additional investment.

Always available

Redundancy and failover minimize downtime, so a single component failure no longer threatens operations.

Faster and current

mproved performance speeds data processing and retrieval, and the supported version now receives every update and patch.

A team in control

Comprehensive training and knowledge transfer left the client's team confident and proactive about managing the new system.

IN SUMMARY

Migrated cleanly, built to grow

By approaching the migration strategically, we moved the telecom's CipherTrust Manager from aging physical hardware to a scalable, high-availability virtual environment, with no data loss and minimal downtime. Scripted migration replicated every key, account, and policy accurately, rollback safeguards protected the data throughout, and a redundant multi-node design with load balancing keeps the platform resilient. Back on a fully supported version and equipped with thorough training, the client now has a modern foundation ready for future growth and evolving data security needs.

GET STARTED

Plan your CipherTrust migration.

Talk to our Platforms team →