

CUSTOMER SUCCESS STORY

The model weights nobody could rebuild.

An enterprise AI team realised its most valuable asset — months of fine-tuned model artefacts — sat outside every backup policy it had. **UPC Cyber vault** brought the AI estate under the same protection as the applications using it.

Months to rebuild

AI artefacts are high-value and hard to reconstruct. Fine-tuned weights represent accumulated compute, curated data, and experimental iteration; losing them is not a restore problem but a re-run of work measured in months and GPU-hours.

THE SITUATION

The most valuable assets were the least protected

A protection review of the AI platform produced an uncomfortable inventory:

- **Model registries were treated as build output.** Nobody had classified fine-tuned weights as production state requiring recovery.
- **Vector indexes were assumed rebuildable.** The rebuild time had never been measured, and the source data had since changed.
- **Training datasets carried curation effort** that no raw source could reproduce.
- **Attackers increasingly target AI assets**, which are valuable both to destroy and to steal.

THE DECISION

Treat AI artefacts as production state

The team extended Cyber vault to cover model registries, curated datasets, and vector indexes, with immutable retention and AI validation applied to the artefacts as well as the applications.

“We had disaster recovery for the application and nothing for the model it depends on. Restoring one without the other gives you a service that starts and then does not work.”

— HEAD OF AI PLATFORM

DEPLOYMENT SNAPSHOT

SECTOR

Enterprise AI platform team

PROTECTED

Model registry · Curated datasets · Vector indexes

STORAGE

Immutable WORM object storage

ISOLATION

Air-gapped from the training environment

VALIDATION

AI restorability testing on artefacts

VERSIONING

Retention across model versions

RECOVERY

Coordinated with application recovery

SCOPE

Aligned to the applications' tiering

WHAT WAS DEPLOYED

Model artefacts

Model registries and fine-tuned weights held as immutable copies, versioned so a specific known-good model can be recovered rather than only the latest.

Data

Curated training datasets protected with the same retention rules as the records they derive from, preserving the curation effort they represent.

Retrieval

Vector indexes protected rather than assumed rebuildable, with restore time measured instead of estimated.

Coordination

Recovery of AI artefacts **orchestrated alongside the applications** that bind to them, so a restored service comes back functional.

WHAT CHANGED

BEFORE UPC CYBER VAULT

- Model registries treated as **build output**, not state
- Vector index rebuild time never measured
- Curated datasets unprotected despite their cost
- Application recovery would restore a non-functional service
- AI assets outside every retention policy

WITH UPC CYBER VAULT

- Model artefacts held as **immutable, versioned copies**
- Vector indexes protected with measured restore times
- Curated datasets under the same retention as their sources
- AI and application recovery **coordinated**
- The AI estate inside the protection scope

WHERE THE CHANGE CAME FROM

Artefacts reclassified as state

Recognising fine-tuned weights as production state rather than build output is what brought them into scope — a classification decision, not a technical one.

Rebuildable was measured, not assumed

Timing an index rebuild turned a comfortable assumption into a number, and the number justified protecting them.

Recovery became functional

Coordinating artefact and application recovery meant a restored service actually worked rather than merely starting.

WHY THIS MATTERS FOR AI TEAMS

Capabilities doing the work in this deployment:

Model registry protection

Versioned artefact retention

Curated dataset protection

Vector index recovery

Immutable WORM storage

Air-gapped isolation

AI validation

Coordinated recovery

BOTTOM LINE

UPC Cyber vault brought model weights, curated data, and vector indexes under the same protection as the applications that depend on them.

Ready to test your last clean copy?

Book a Cyber vault architecture review, or run a ransomware recovery simulation.

UPC Cyber vault

UNITEDLAYER.COM



EMAIL

contact@unitedlayer.com



PHONE

+1-888-853-7733



X

x.com/unitedlayer



LINKEDIN

linkedin.com/company/unitedlayer