

CUSTOMER SUCCESS STORY

The copy the attacker could not reach.

A European bank discovered during a tabletop exercise that a compromised domain admin could delete every backup it held. **UPC Cyber vault** put one copy beyond that reach — and beyond its own administrators.

One credential

The exercise found a **single point of failure nobody had drawn**. Backups authenticated against the same directory as production, so the credential that would encrypt the estate was also the credential that could destroy the means of recovering it.

THE SITUATION

Protected by backups that shared an identity

The bank's backup estate was modern, tested, and well-run. It was also reachable:

- **Shared directory authentication.** Backup repositories trusted the same Active Directory as production, so stolen domain-admin credentials reached both.
- **Policy-based retention.** Immutability was enforced by the backup application, which meant an administrator could change it.
- **Network-reachable repositories.** Every backup target was addressable from the production network on a standing path.
- **Restore assumed, not proven.** Recovery testing covered individual systems, never a full clean restore under incident conditions.

THE DECISION

Put the last copy in a different domain

Rather than harden the existing repositories further, the bank added a vault with its own identity, its own storage rules, and no standing route from production — with AI validating every copy it received.

“We had spent years making backups faster. The exercise showed we had never made them unreachable. Those are different problems, and only one of them matters once someone is inside.”

— CHIEF INFORMATION SECURITY OFFICER

DEPLOYMENT SNAPSHOT

SECTOR

European banking group

PROTECTED

Core banking · Payments · Customer records

STORAGE

WORM object storage with retention lock

IDENTITY

Dedicated vault credentials and RBAC

ISOLATION

Logically air-gapped, transfer windows only

VALIDATION

AI-tested restorability and malware scanning

ALIGNMENT

DORA and PCI-DSS obligations

EVIDENCE

Tamper-evident audit trail

WHAT WAS DEPLOYED

Immutability

WORM-enabled object storage with retention locks enforced at the storage layer, so protected copies cannot be modified or deleted while locked.

Identity

Dedicated vault credentials and separate RBAC, isolated from the production directory — a compromised domain admin has no path into the vault.

Isolation

Logically segmented recovery domain with **no standing network path**; connectivity exists only during deliberate, time-limited transfer windows.

Validation

AI-driven validation testing restorability and scanning for malicious code, so an infected or corrupt copy is identified before it is needed.

WHAT CHANGED

BEFORE UPC CYBER VAULT

- Backups authenticating against the **production directory**
- Retention enforced by application policy, not storage
- Every repository reachable on a standing network path
- Restore proven per system, never as a clean full recovery
- A single compromised credential able to destroy recovery

WITH UPC CYBER VAULT

- A vault with its **own identity** and access controls
- **Storage-layer WORM** that no account can override
- Air-gapped, with connectivity only during transfer windows
- Every copy **AI-validated** and malware-scanned
- Tested recoverability evidenced for supervisors

WHERE THE CHANGE CAME FROM

Identity isolation was the fix

Separating vault credentials from the production directory removed the single failure mode the exercise exposed, which hardening the existing repositories could not address.

Immutability moved down a layer

Enforcing retention at the storage layer rather than in the backup application meant the control no longer depended on who held administrative rights.

Validation replaced assumption

AI-tested restorability converted 'the backups should work' into a verified property of each copy.

WHY THIS MATTERS IN FINANCIAL SERVICES

Capabilities doing the work in this deployment:

Storage-layer WORM

Dedicated vault credentials

Air-gapped isolation

AI-driven validation

Malware scanning

Tamper-evident audit

DORA alignment

PCI-DSS alignment

BOTTOM LINE

UPC Cyber vault gave a bank one copy that a compromised administrator — theirs or an attacker's — simply cannot reach.

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](tel:+1-888-853-7733)



X

x.com/unitedlayer



LINKEDIN

linkedin.com/company/unitedlayer