

Confidence Before Cutover

A DR-first VMware soft landing — how a Hong Kong financial institution replaced VMware without gambling on a single, high-stakes weekend.

Industry	Financial services, Hong Kong
Scale	Approximately 30 VMware virtual machines, 40 TB of business-critical data
Challenge	Replacing VMware without risking business continuity
Approach	Disaster recovery first; migration validated through repeated drills before cutover
Platform used	HyperBDR
Outcome	Production cutover with zero surprises, followed by continuous protection on the new platform

~30 VMware virtual machines migrated	40 TB business-critical data protected	2 months of repeated, end-to-end drills	Zero surprises at production cutover
--	--	---	--



The question behind the migration

At the end of 2025, a Hong Kong financial institution began reassessing its VMware environment. The reason was straightforward: changes to VMware's commercial model had introduced uncertainty around future infrastructure costs, making long-term planning harder to pin down.

For a financial institution, though, moving away from VMware was never going to be a simple lift-and-shift. The production environment carried around 30 virtual machines and 40 TB of business-critical data, supporting a web of interconnected services. A failed cutover would not stay contained; it would ripple straight into business continuity.

So the question the institution faced was not **whether** to move. It was **how** to move without gambling on a single, high-stakes weekend.



The soft landing journey

1

NOVEMBER 2025 · DISASTER RECOVERY FIRST

Protect production where it already lives

Rather than starting with a migration plan, the institution began with HyperBDR, establishing continuous disaster recovery from its existing VMware environment to a newly deployed private cloud. Production stayed exactly where it was, running on VMware, while HyperBDR quietly and continuously replicated protected data to the target platform.



What this really was — on paper it looked like a disaster recovery project. In practice, it was the first stage of the migration, built without anyone having to say so out loud.

2

DECEMBER 2025 – JANUARY 2026 · RECOVERY VALIDATION

Turning a recovery target into a production candidate

This two-month stretch turned out to be the heart of the whole project. Multiple recovery drills were run against the private cloud, and each one tested far more than whether data had copied across successfully.

Every drill checked virtual machine start-up, application availability, network connectivity, database services, user access and full business workflows, end to end. Each success chipped away at migration risk. Each issue was caught, fixed and verified again before it ever had the chance to matter in production.



The turning point — over time, the recovery environment stopped being just a disaster recovery platform. It became a fully validated production candidate.



3

LATE JANUARY 2026 · PRODUCTION CUTOVER

An anticlimax, in the best possible way

By the time cutover arrived, it was almost an anticlimax, in the best possible way. Production workloads moved from VMware to the private cloud using the same HyperBDR recovery workflow that had already been proven, repeatedly, over the previous two months.

No second platform was brought in for the migration itself. No separate cutover procedure had to be designed from scratch. For a process that so often keeps IT teams up at night, cutover here was simply the final, well-rehearsed execution of a plan that had already succeeded many times before.

4

AFTER CUTOVER · CONTINUOUS PROTECTION

The journey did not end at go-live

Once the new environment had been running stably for a while, the institution turned to the next stage of its resilience strategy: extending disaster recovery, on the same HyperBDR platform, to a second private cloud cluster.



One continuous thread — VMware disaster recovery, then VMware replacement, then disaster recovery for the new production platform. Throughout, the underlying platform never changed.



What made this different

Most organisations planning a VMware replacement treat disaster recovery and migration as two separate projects, run by different teams, on different timelines, sometimes with different tools. This case took a different path: the same journey, in stages, on one platform.

Area	Traditional migration	DR-first soft landing
First time on new platform	Production cutover	Early recovery drill, weeks in advance
Validation	Limited, often theoretical	Repeated, end-to-end, on real data
Tooling across stages	Different tools for DR, migration and protection	One platform throughout
Risk at cutover	Highest point of the whole project	Lowest, because the outcome is already proven
Confidence source	Planning documents and assumptions	Evidence from drills that already succeeded



Why it worked

Strip away the technology and the story is fairly simple. The institution built disaster recovery first. It validated the target platform repeatedly, not once. Only after confidence had been earned, through evidence rather than assumption, did it move production. And afterwards, the same platform carried on protecting what it had helped build.

Recovery environments became production validation environments. Recovery drills became migration rehearsals. Production cutover became the final, low-drama step of a process that had already been tested to destruction, safely, in a sandbox that looked exactly like production.

HyperBDR supported the entire arc: continuous data protection, automated recovery orchestration, repeatable validation, production cutover and ongoing disaster recovery, all on a single platform, without the coordination overhead of stitching separate tools together at each stage.

Continuous data protection

Automated recovery orchestration

Repeatable validation

Production cutover

Ongoing disaster recovery



A different way to think about VMware replacement

For organisations weighing up their own VMware exit, the lesson from this project is less about a specific tool and more about sequencing. Disaster recovery does not have to be the last box ticked after a migration. It can be the first step that makes everything after it safer.

Don't migrate first. Build confidence first.



ABOUT US

OnePro Cloud

OnePro Cloud helps enterprises transform trusted data into intelligent, AI-powered operations. By combining expertise in data resilience, hybrid cloud, and AI infrastructure, we enable organisations to protect, govern, and activate enterprise data for AI. From data protection to AI-ready data and intelligent applications, we help businesses turn data into knowledge, knowledge into intelligence, and intelligence into operational AI.

OnePro

