HyperBDR

*Customer Case Study*

# Building Cyber Compliance and Business Resilience via Cross-Cloud DR: How HyperBDR Leads the Way

After ransomware encrypted 90% of one business unit's data — production and backup storage alike — a Bursa Malaysia listed investment holding company rebuilt disaster recovery across two clouds.

Days → minutes recovery | Dual-layer cross-cloud | Cybersecurity Act 2024 compliant

### THE CHALLENGE

Ransomware encrypted both production and backup storage, while the Cybersecurity Act 2024 raised the compliance bar.

### THE SOLUTION

A dual-layer HyperBDR strategy: automated DR in a second Huawei Cloud AZ, plus a third copy held on AWS.

### THE RESULT

Recovery cut from days to minutes, no single point of failure, and an audit-ready compliance position.

| INDUSTRY | SCENARIO | PRODUCT | CLOUDS |
|---|---|---|---|
| **Finance** | **Cross-Cloud DR** | **HyperBDR** | **Huawei Cloud + AWS** |

**Investment Holding Company × OnePro HyperBDR**

ON-PREM → HUAWEI CLOUD + AWS · DUAL-LAYER CROSS-CLOUD DR

OnePro

*Background*

# When the backup storage was encrypted too

The customer is a major investment holding company listed on the Main Market of Bursa Malaysia, operating in a highly regulated environment that requires compliance with a range of cybersecurity regulations — including Malaysia's Cybersecurity Act 2024 (Act 854), which strengthens organizational cybersecurity frameworks and mandates comprehensive measures to safeguard digital assets and maintain investor confidence.

In early 2024, the company was hit by a ransomware attack that encrypted 90% of one business unit's data, causing severe operational disruption and financial loss. Recovery fell back on manual processes that proved slow and inefficient, extending the downtime further. The incident exposed the limits of the company's existing disaster recovery tooling and made the case for a more resilient strategy.

**90%**
Of one business unit's data encrypted

**2**
Storage tiers hit — production and backup

**Days**
Of manual recovery, before HyperBDR

> *"When our security engineer informed me that both production storage and backup storage had been encrypted, I realized traditional disaster recovery strategies were no longer sufficient."*

**Mr. Lim** · Director of IT Infrastructure

*Challenges*

# A new law, and a recovery plan the attack had already beaten

Malaysia's Cybersecurity Act 2024 requires enhanced organizational security frameworks with stringent compliance measures. For a publicly listed company, adherence is critical to both investor trust and regulatory standing. The act mandates:

- Implementation of advanced cybersecurity protocols
- Regular audits ensuring compliance and the effectiveness of security measures
- Establishment of robust incident response plans

## The ransomware incident exposed two critical issues

01

### Inefficient data recovery tools

The tools already in place could not restore critical data within any reasonable timeframe, which is what turned an attack into days of operational downtime.

02

### Encrypted backup storage

Both production and backup storage were compromised in the same attack. Once the backup copy is encrypted too, a traditional disaster recovery design has nothing left to recover from — which is precisely what ransomware is built to achieve.

Both findings pointed the same way: a backup copy that shares its fate with production is not, in practice, a recovery plan.

*Solution*

# A dual-layer, cross-cloud disaster recovery strategy

Working with cybersecurity and cloud infrastructure experts, the company used HyperBDR to build a dual-layer, cross-cloud disaster recovery strategy — automating DR management across multi-cloud environments to maximize both resilience and recovery speed.

01

### Production workloads migrated to the cloud

Production workloads were shifted to Huawei Cloud, reducing dependence on on-premises infrastructure while improving scalability and security — and establishing the foundation the cross-cloud disaster recovery design would sit on.

02

### Automated DR in a second availability zone

A disaster recovery environment was established in a separate Huawei Cloud availability zone. HyperBDR's Boot in Cloud technology creates the cloud storage for backups automatically by invoking cloud APIs, and during recovery restores clean backup data into operational hosts in one click. With automated failover across AZs, downtime fell to minutes.

03

### A third copy stored on AWS

To harden data protection further, a dual-layer cross-cloud backup strategy keeps an additional copy on a separate cloud platform. If the primary backup data on Huawei Cloud were ever compromised or lost, the system fails over to AWS for single-click restoration — protecting against provider-level failure as well as compliance risk.

Two clouds, two layers — so that no single provider, availability zone or attack can reach the last good copy.

*Outcomes and Benefits*

# No single point of failure left

01

### Enhanced business cyber resilience

The dual-layer cross-cloud strategy eliminated single points of failure, significantly strengthening the organization's overall security posture.

02

### Drastically reduced recovery time

With HyperBDR's one-click automated recovery, a process that previously took days was reduced to minutes.

03

### Regulatory compliance achieved

The new DR strategy fully aligns with Malaysia's Cybersecurity Act 2024, meeting audit requirements and raising confidence among regulators and investors.

04

### Strengthened investor confidence

By prioritizing dual-layer cybersecurity and disaster recovery, the company reinforced investor trust and its commitment to protecting stakeholder interests.

The attack showed where traditional DR strategies fall short against modern threats. With a cross-cloud design, the company mitigated its ransomware risk, met its compliance obligations and kept business continuity intact — a framework that matters most for listed companies, where sustained growth and investor trust are the same thing.