HyperBDR

Customer Case Study

From Crisis to Innovation: HyperBDR Powers Future-Ready Transformation for a National Social Security Agency

After a day-long outage took its systems offline, a national social security agency moved disaster recovery from its private cloud to Huawei public cloud — 1,000+ VMs, a 30-minute RTO, and 80% less deployment labour.

1,000+ VMs protected | 30-minute RTO | 5-minute RPO | 80% labour saved

THE CHALLENGE

Strict RPO and RTO compliance over 1,000+ VMs spanning 7 Windows and 11 Linux versions, on a single, inflexible architecture.

THE SOLUTION

HyperBDR tiered incremental synchronization, Boot in Cloud recovery and automated agent deployment onto Huawei public cloud.

THE RESULT

30-minute RTO with a 5-minute RPO on core systems, 80% less labour cost and 70% lower DR storage cost.

INDUSTRY	SCENARIO	PRODUCT	TARGET CLOUD
Government	**Private to Public Cloud DR**	**HyperBDR**	**Huawei Cloud**

National Social Security Agency × OnePro HyperBDR

HUAWEI CLOUD STACK → HUAWEI PUBLIC CLOUD · 1,000+ VMs

OnePro

Background

A day offline, and millions of citizens affected

In August 2023, a sudden power outage at the data center of a national social security agency brought its business systems to a halt for nearly a day. Hospitals and medical institutions were affected, and the health and social security services of millions of citizens were put at risk.

As one of the largest social security agencies in its region, it serves millions of people with medical, social security and health management services. The outage exposed the limits of its local IDC disaster recovery solution in both recovery speed and capacity.

To minimize disruption and stay compliant, the agency moved its disaster recovery environment from the on-premises Huawei Cloud Stack (HCS) private cloud to Huawei public cloud.

Challenges

Compliance, scale and an architecture that could not keep up

01

Compliance pressure demanded a cloud DR transformation

The agency must meet strict RPO and RTO compliance requirements: the medical system has to keep Electronic Health Records secure against loss, and for critical social infrastructure, recovery time is what protects public trust.

02

High DR cost in a large-scale, complex environment

The plan covers at least 1,000+ virtual machines spanning seven versions of Windows hosts and eleven versions of Linux. That scale drives up the cost and complexity of traditional DR, so automated deployment and operations management were needed.

03

A single architecture struggling with new demands

As digital transformation and public service innovation continue, the agency's requirements keep changing. The private cloud platform is slow to adapt — it cannot absorb sudden surges in load or answer new cyber threats — which limits agility.

Solution

Protection tiered to what each system actually needs

The agency's business systems span a wide range of domains with very different data consistency requirements, so the OnePro team built a differentiated incremental synchronization strategy in HyperBDR rather than applying one policy to everything.

SYSTEM TIER	EXAMPLE SYSTEMS	SYNCHRONIZATION
High business continuity	Cancer patient management applications, financial systems	**5 min · RPO 5 min**
High data consistency	Digital health certificate systems	**1 hour · RPO 1 h**
Medium priority	Monitoring and alert systems	**12 hours · RPO 12 h**
Non-critical / non-real-time	Public works tracking systems	**24 h, or weekly / monthly full**

02

Boot in Cloud: one-click activation

Integrated with Huawei Cloud APIs, systems launch in the cloud from predefined strategies and automated instructions. Multiple business hosts reach the OS login page in 10–15 minutes, meeting the agency's 30-minute RTO.

03

Concurrent transfer and automated deployment

The initial full sync of 1,000+ VMs ran in parallel at 40–50 machines per day. Automated agent installation covered 500 Windows machines in 2.5 hours; 700 Linux systems took slightly longer but were deployed within 2 working days.

04

Cloud-native integration for cross-cloud resilience

Deep cloud-native integration enables dynamic resource scheduling and orchestration across cloud environments, so the agency can absorb surges in public service load, emerging cyber threats and regulatory change — under one visual management console.

Benefits

Resilient in 30 minutes, at 80% less effort

1,000+
Virtual machines protected

30min
Recovery time objective

80%
Labour cost saved

70%
Lower DR storage cost

01

30-minute resilience, and compliance with it

The agency achieved a 30-minute RTO and a 5-minute RPO against its SLA: core systems recover with minimal data loss, and every other system is restored to its latest valid state within minutes.

02

Deployment from 15 days down to 2

Automated agent installation removed the need to deploy backup manually on each virtual machine, cutting the DR deployment cycle from 15 days to 2 and saving over 80% in labour cost — with storage cost down more than 70% against traditional solutions.

03

A foundation for future-ready innovation

Resources can now be scaled on demand from the public cloud when public service demand rises, and backup data can be managed and analysed — bringing AI and deep learning to risk forecasting and healthcare and social security trend analysis.

> *"HyperBDR has exceeded our expectations by meeting both our current compliance and recovery needs, while also aligning with our strategy of deepening technological integration and continuous innovation."*

J.M. · Director of Business Continuity and Disaster Recovery Management, The National Social Security Agency

Ready to build DR in the cloud?

Talk to OnePro about protecting your workloads with HyperBDR.
oneprocloud.com · enquiry@oneprocloud.com

OnePro

Free Trial