COHESITY

Executive summary

Products:
DataProtect, FortKnox

Region:
Americas

Use Case:
Backup and Recovery, Ransomware Recovery

Industry:
Telecommunications

Environments:
Kubernetes, Linux, Microsoft Hyper-V, NetApp, Pure, SAP, VMware, Windows

Benefits

< **90%** Faster recovery

$10M TCO savings over 3 years

67% Lower operational costs

Stronger cyber resilience

SOC 2 compliance

Telecommunications provider hardens security posture while cutting 3-year TCO by $10M

Challenge

As custodians of customer names, addresses, government ID numbers, and payment information, telecommunications providers are growing targets for nation-state actors and other cybercriminals. Regulatory agencies around the world are levying fines of up to tens of millions of dollars on providers whose data breaches are attributable to inadequate cybersecurity. This leading wireless network operator wanted to strengthen its security posture for backups, accelerate recovery after attacks, and simplify operations. The legacy backup and recovery solution lacked modern security protections and had become increasingly expensive to manage.

Why Cohesity

The operator chose Cohesity after a head-to-head comparison against Rubrik during a proof of concept (PoC). Throughout the PoC, the Cohesity sales and technical teams distinguished themselves with rapid response to questions and new feature requests. The operator's IT and security teams liked advanced security protections such as time-bound locks on backups, multifactor authentication, and quorum, a requirement for two or more people to approve any changes. As of 2024, **the Cohesity Data Cloud protects nearly 60 PB of data distributed across multiple data centers and switching sites**. For another layer of resilience, the operator stores a second, virtual air-gapped copy of critical data in Cohesity FortKnox, a Cohesity-managed cyber vault.

Business value

Lower total cost of ownership (TCO)

The operator manages the Cohesity environment with one-third the number of IT staff needed to manage the legacy backup and recovery platform. Three-year TCO (hardware, licensing, operational expense) dropped by $10M.

Stronger cybersecurity practices

The operator now applies security best practices to protect its backups from breaches, including multifactor authentication and requiring two or more people with administrative privileges to approve changes.

Enhanced cyber resilience

By storing a second immutable backup in Cohesity FortKnox, the operator has what it calls a "last line of defense" against ransomware. FortKnox complies with the SOC 2 Type 2 framework for storing customer data in a secure manner, and offers several advantages compared to a homegrown cyber vault system on-premises.

Faster recovery

With instant mass restore, the operator quickly recovers from large-scale outages affecting thousands of virtual machines (VMs) and databases. Compared with the legacy solution, Cohesity recovers data 92% faster—for example, in 2 hours instead of 24. To rapidly identify the most recent backup containing clean data, the operator plans to start using the Cohesity Clean Room solution, an isolated environment with trusted tools for investigating and remediating attacks.

Learn more at www.cohesity.com

COHESITY.com | 1-855-926-4374 | 300 Park Ave., Suite 1700, San Jose, CA 95110

5000153-001-EN 1-2025