COHESITY

Solution Brief

# Cohesity Cyber Resilience: Beyond cloud-native backup and recovery

Delivering resilience, security, and simplicity across clouds with lower TCO

## The Cloud Data security challenge

As organizations move to public clouds and SaaS, protecting and securing cloud data has become more complex and frought with risks. While cloud providers secure infrastructure, customers remain responsible for their data, creating shared-responsibility gaps. Fragmented backup tools cause blind spots, inefficiencies, and cyber vulnerabilities while compliance and data-sovereignty demands require tighter control over data location and recovery. Meanwhile, costs rise from redundant storage and replication, and in-cloud backups remain vulnerable to ransomware, insider threats, and outages making resilient data protection essential.

### Cohesity ensures your data is always:

- Securely protected
- Immediately recoverable
- Efficiently managed
- Cost-effective
- Compliant by design

## Why Cohesity beats cloud-native solutions

| Capability | Cohesity Advantage |
|---|---|
| **Unified Protection** | One platform for on-prem, multicloud, and hybrid workloads. |
| **Resilience** | Off-cloud backups ensure recoverability even during cloud outages. |
| **Recovery** | 97% faster restores and large-scale recovery support.<br>Blueprints for orchestrated recovery & rehearsal |
| **Data Security** | Multi-layered zero-trust, immutability, advanced threat detection and isolated vaulting. |
| **Operational Efficiency** | Centralized management and automation across environments. |
| **Cost Optimization** | Deduplication, compression, and policy-based tiering lower TCO. |
| **Compliance** | Built-in governance and audit-ready reporting. |

## Cohesity Case Studies

- 97% faster file restores (<1 minute) and consolidation of Commvault, AWS backup at a leading enterprise software provider
- 2.5 TB Microsoft 365 data restored in 12 hours post-cyberattack – no ransom paid at NASDAQ:
- 24+ hours/month reclaimed via automation; 18-month ROI achieved at a leading Financial Institution

## The limitations of Cloud-native backup

While leading cloud providers have their own cloud-native backup tools that provide basic protection, they lack capabilities to ensure data security and rapid recovery from cyber breaches.

| Challenge | Cloud-Native Backup Limitations |
|---|---|
| **Complex Operations** | Siloed data protection for multiple workloads, each with their own UI leading to operational complexity and management overheads. |
| **Resilience** | Backups stored in the same cloud create a single point of failure during outages or cyberattacks. |
| **Scalability & Coverage** | Limited workload and multi-cloud support; no unified management. |
| **Rising Costs** | Lack of deduplication and compression, and egress charges, managing multiple point solutions drive up costs in the long term. |
| **Security** | Needs manual provisioning of data security features and is prone to human-error or insider threats. |
| **Compliance** | Few tools provide global governance or automated data risk visibility. |

## How Cohesity overcomes these challenges

Cohesity Data Cloud unifies backup, recovery, and cyber resilience across on-premises, hybrid, and multicloud environments—providing one secure, scalable, and multicloud platform for all workloads.

### Comprehensive, unified coverage

- Protects IaaS, PaaS, and SaaS workloads across AWS, Azure, GCP, and Oracle Cloud.
- Extends protection to on-prem data centers, edge locations, and private clouds—capabilities cloud-native tools lack.
- Unified data protection consolidates management, improves visibility, and eliminates silos.

### Cyber resilient by design

- Protecting cloud workloads outside their source cloud enhances resilience against regional outages or cloud-specific cyberattacks.
- Zero-trust data security measures such as immutability, RBAC, Cohesity-managed KMS, and air-gapped cyber vaulting safeguard against both external and insider threats.
- AI-driven anomaly detection and hash-based scanning enables proactive threat mitigation and clean recovery anywhere.

### Efficiency and cost optimization

- 70–90% storage cost reduction via deduplication and compression.
- Automated tiering and archiving optimize spend while maintaining compliance.
- Delivered as SaaS or self-managed—available via major cloud marketplaces, making it easy to offset cloud consumption commits.

### Data sovereignty and compliance

- Sovereign by-design architecture to satisfy regional compliance and privacy requirements
- Unified visibility of where data and metadata are stored, processed, and accessed
- Built-in governance and audit-ready reporting.

## The Bottom Line

Cloud-native backup tools meet basic needs—but Cohesity delivers enterprise-grade cyber resilience with unified protection, stronger security, and superior cost efficiency.

## Real-Life TCO Analysis

### Cost Evaluation of Cohesity data protection vs. AWS Native Backup

As part of a TCO comparison exercise for a Cohesity customer, we conducted a comprehensive analysis of backup cost efficiency across multiple AWS workloads–EC2, MSSQL, and Kubernetes backups utilizing Cohesity BYOL (Bring Your Own License) model and AWS cloud-native backup and storage costs. The results revealed two distinct cost models:

### Cohesity: Higher Start, Dramatically Lower TCO

***"An initial investment that quickly pays for itself."***

Cohesity incurs upfront costs for Amazon EC2 and EBS, but its global, cross-workload deduplication and compression sharply reduces incremental backup data. This results in:

- Up to 93% data reduction (validated by testing and customer deployments)
- Significantly lower S3 storage and data egress costs over time
- Elastic compute optimized to minimize EBS usage
- 40% overall cost optimization compared to cloud-native solutions
- Additional savings due to consolidation of multiple point solutions for backing up variety of workloads

Cohesity delivers exponential savings at scale, making it ideal for diverse enterprise environments, large datasets, and long-term retention.

### AWS Backup: Low Entry Cost, High Long-Term Spend

***"Easy to start, expensive to scale."***

AWS Backup offers simplicity and no license fees, but key limitations drive rising costs:

- No cross-volume or global deduplication
- Every backup stored independently, causing linear cost growth with data volume
- Limited database awareness and scalability for enterprise workloads
- Multiple point tools required across workloads, increasing operational overhead

Over time, storage, replication, and management costs accumulate rapidly.

### Conclusion: Cohesity's Cost Advantage at Scale

While AWS Backup is suitable for small or short-term use cases, enterprises protecting large sets of data or retaining them for extended periods consistently achieve significant lower TCO and higher efficiency with Cohesity. Deduplication-rich platforms like Cohesity Data Cloud and Cohesity NetBackup deliver measurable, sustained cost savings, turning cloud backup from a growing expense into a long-term financial advantage.

**Visit Cohesity for more information**

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

3000185-001-EN 1-2026