BLESSING PHIRI | TECHNICAL SOLUTIONS ENGINEER

Technical Comparison Brief

Protecting Kubernetes: Veeam Kasten vs NetBackup for Kubernetes

For: Platform and backup teams choosing a container data protection strategy

Reference	**SAMPLE-BKP-001**
Date	**2026 (sample)**
Status	**Final**
Prepared by	**Blessing Phiri**

Portfolio sample

A vendor-neutral brief written for customer conversations. Product capabilities change often, so confirm details against current vendor documentation before making a decision.

1. The core difference

Both products protect Kubernetes workloads, but they start from opposite ends.

	NetBackup (Cohesity)	Veeam Kasten
Starting point	An enterprise backup platform extended to Kubernetes	A data protection platform built for Kubernetes
Mental model	Containers are one more workload alongside VMs, databases and files	Applications are Kubernetes objects and their relationships
Who it suits	Central backup teams running one platform for everything	Platform engineering and DevOps teams

NetBackup brings Kubernetes into a familiar, centrally governed backup estate with global deduplication and long-term retention. Kasten runs inside the cluster, discovers applications automatically and treats each one, including its configuration and data, as the unit of backup and restore.

The real question is not which product is better, but who owns Kubernetes data protection in your organisation: the central backup team or the platform team.

2. Architecture

Category	NetBackup (Cohesity)	Veeam Kasten
Deployment	Kubernetes protection configured from the NetBackup primary server, with a data mover in the cluster	Runs entirely inside the cluster as Kubernetes services and custom resources
Management	NetBackup web UI, alongside all other workloads	Kasten dashboard, kubectl and GitOps
Discovery	Automatic discovery of namespaces, PVs and PVCs	Automatic discovery of applications and their resources
Protection unit	Namespaces and persistent volumes	Applications: workloads, config, secrets and volumes together
Policy model	Central protection plans across clusters	Label and namespace-based policies inside Kubernetes

3. Backup and recovery

Category	NetBackup (Cohesity)	Veeam Kasten
Backup method	CSI snapshots, with backup from snapshot to NetBackup storage	CSI snapshots, exported to object or other storage
Storage	NetBackup storage targets with global deduplication	Object storage natively; more targets through Veeam Backup & Replication
Application consistency	Through hooks and orchestration	Kubernetes-aware hooks and blueprints
Restore scope	Namespaces and persistent volumes, to alternate locations	Whole application or individual objects
Cross-cluster restore	Supported, including to a different Kubernetes distribution	Native application mobility and DR between clusters
Recovery model	Data and namespace restore; app config may need validating	Application config and data restored together

4. Ecosystem and integration

Category	NetBackup (Cohesity)	Veeam Kasten
Strategy	One platform for VMs, databases, files and containers	Kubernetes-native, with optional enterprise integration
Enterprise backup link	Native: Kubernetes sits inside NetBackup	Integrates with Veeam Backup & Replication
Deduplication	Global deduplication engine	Through Veeam Backup & Replication
Long-term retention	Native archive and tiering	Object storage; tape and capacity tier via Veeam Backup & Replication
Workload coverage	Broad, legacy and modern	Focused on Kubernetes

5. Security and ransomware resilience

Category	NetBackup (Cohesity)	Veeam Kasten
Immutability	Immutable and WORM storage options	S3 Object Lock and immutable repositories
Isolated recovery	Isolated recovery environment options	Hardened repositories via Veeam Backup & Replication
Threat detection	Malware scanning and anomaly detection	Expanded when integrated with the wider Veeam platform
Maturity	Long-established enterprise security model	Strong, particularly as part of the Veeam stack

6. Which fits your organisation

Organisation profile	Better fit	Why
Central backup team owns all data protection	NetBackup (Cohesity)	Keeps governance, reporting and one control plane
Kubernetes-first or cloud-native	Veeam Kasten	Native integration and application-level recovery
Self-service DevOps model	Veeam Kasten	Label-based policies teams can manage themselves
Strict governance, mixed estate	NetBackup (Cohesity)	Centralised audit and compliance across all workloads
Hybrid estate with VMs, Kubernetes and DR	Veeam Kasten with Veeam Backup & Replication	Native Kubernetes protection plus enterprise retention

7. Summary

Dimension	Stronger option
Kubernetes-native design and DevOps fit	Veeam Kasten
Application-aware restore	Veeam Kasten
Centralised governance across all workloads	NetBackup (Cohesity)
Breadth of enterprise backup ecosystem	NetBackup (Cohesity)
Ransomware resilience	Comparable; depends on the architecture deployed

8. Questions to ask before choosing

- Who will own Kubernetes backup day to day: the backup team or the platform team?
- Is there already a NetBackup or Veeam estate that the choice should fit into?
- Do you need to restore whole applications, or mainly data volumes?
- What are your RPO and RTO targets per application tier?
- Do you need to move workloads between clusters or distributions for DR?
- What retention, immutability and audit evidence does your regulator require?

About this sample. A vendor-neutral comparison prepared for customer conversations. It reflects publicly documented capabilities at the time of writing; both products evolve quickly, so validate details with each vendor. Prepared by Blessing Phiri as a portfolio sample.