



# Kubernetes and Cloud Database Backup as a Service

## Introducing CloudCasa

CloudCasa is a powerful and easy to use Kubernetes backup service for DevOps and IT Ops teams, that is fully integrated with Azure Kubernetes Service (AKS) and Amazon EKS, well as supporting all other major distributions and managed services. CloudCasa pushes the boundaries of traditional data protection by also offering Kubernetes and cloud security scanning.

With CloudCasa, you don't need to be a storage or data protection expert to backup and restore your Kubernetes clusters. Just install the CloudCasa agent and let it do all the hard work of protecting cluster resources and persistent data from human error, security breaches, and service failures, providing business continuity and compliance that your business requires. It's easy for a single cluster, and just as easy for a large multi-cluster, multi-cloud, and hybrid cloud environments.

In addition to being application aware, CloudCasa is also cloud platform aware. CloudCasa integrates with your Azure and AWS accounts to auto-discover your AKS and Amazon EKS clusters and allows users to set global backup policies across a multi-cluster, multi-account environment. CloudCasa also allows protection of common adjacent workloads such as Amazon RDS. CloudCasa is one of a kind proactive data protection service that also detects and alerts vulnerabilities in Kubernetes clusters and Cloud accounts to improve overall security posture.

## Solution Highlights

As a SaaS offering, CloudCasa offers many benefits vs. do-it-yourself backups such as Kasten and Velero, including:

- CloudCasa is a cyber-resilient backup service delivering tamper-proof recovery points, encryption in transit and at rest, in a virtual air-gapped domain.
- CloudCasa allows customers the flexibility to backup to their own S3 storage.
- CloudCasa performs proactive security posture reviews to identify misconfiguration and compliance risks in Kubernetes Clusters (Container, Config, Network and Benchmark Scans) and cloud accounts.

- CloudCasa is now available in several marketplaces/catalogs: SUSE Rancher catalog, the Digital Ocean Marketplace, the Red Hat catalog, AWS Partner Catalog etc.
- CloudCasa was ranked as a Fast Mover and the best rated SaaS offering in its very first year in the 2021 GigaOm Radar report for Kubernetes Data Protection.

## Built for the Cloud

**Cloud Native:** Built with Kubernetes in public cloud, leveraging Kubernetes APIs and the CSI framework to deliver a highly available backup service.

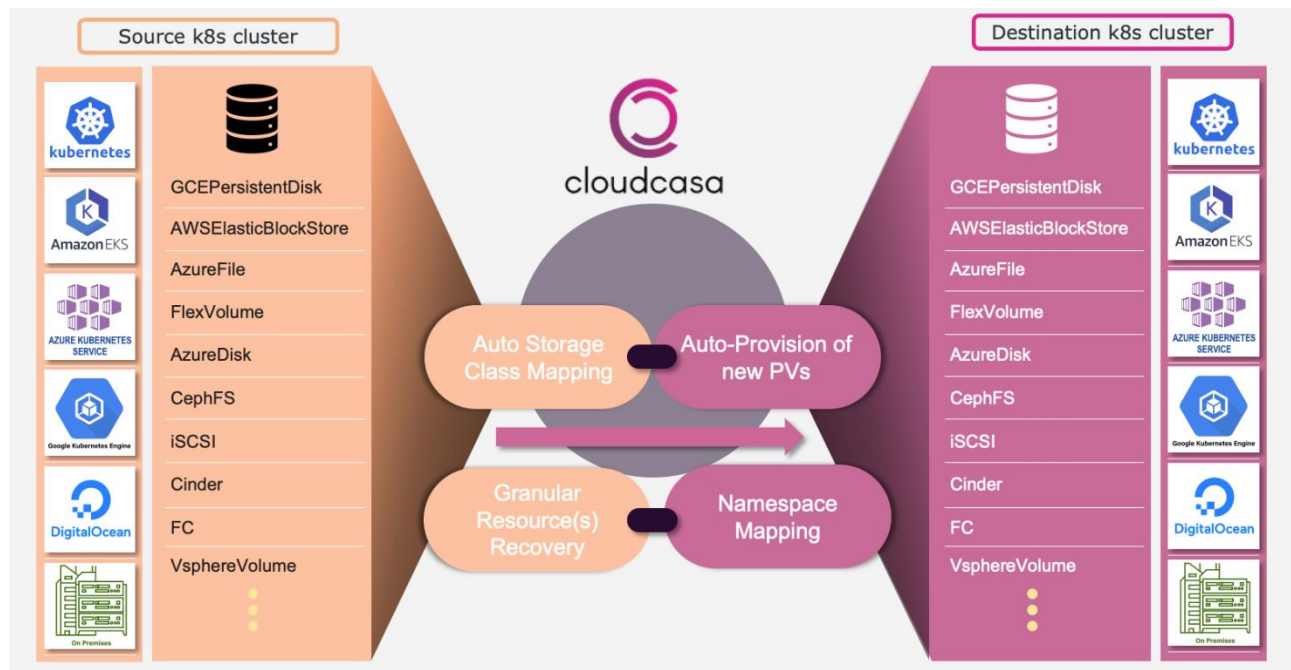
**Cloud Scale:** Backup service auto-scales to adapt to bursts and growth. Service can also backup to CloudCasa managed storage that never runs out.

**Cloud Aware:** Integrates with Azure and AWS accounts to auto-discover and auto-protect AKS clusters, Amazon EKS clusters and Amazon RDS databases.

**Cloud Secure:** Robust protection against fraudulent system access; enables tamper-proof backups and performs proactive vulnerability assessments.

**Cloud Mobile:** Migrates data across multi-cloud and multi-cluster environments with mapping of storage classes, namespaces, IAMs, and security groups.

**Cloud Smart:** Built in customizable Application Templates for popular databases such as MySQL, Mongo, and PostgreSQL.

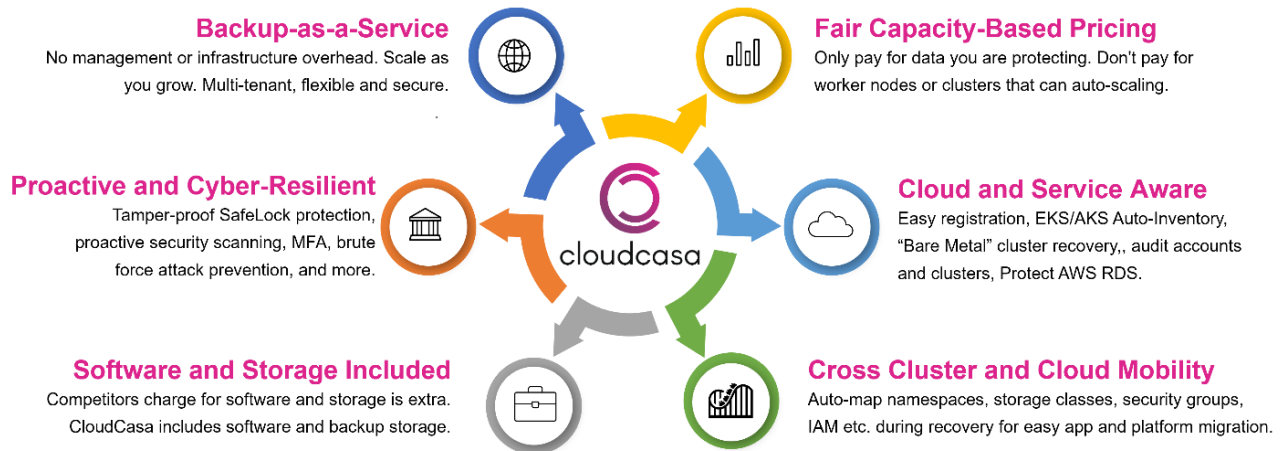


## Why CloudCasa vs Alternatives?

Kubernetes developers and platform teams have several options to choose from. Velero is a powerful open-source framework to protect Kubernetes data one cluster at a time, which relies on the ecosystem partners to fill gaps for multi-cluster, multi-cloud environments. Kasten by Veeam offers many of the same benefits, however it is

architected as a traditional standalone application that is deployed and maintained by the users themselves.

The following are some key considerations to choose CloudCasa over alternatives.



## "Bare Metal" Cluster Restore for Disaster Recovery

As user adoption of Kubernetes continues to rise, more stateful workloads are running on Kubernetes resources. If a local outage occurs and you lose a cluster or if an entire site is destroyed, the application and data need to be quickly recovered for business continuity. For AKS or EKS users to successfully recover missing or corrupted data, there must be a destination for the cluster to restore to. That is why most AKS and EKS customers utilize stand-by clusters to act as the destination for recovery in these scenarios. The problem with stand-by clusters is that they need to be setup before the need for recovery and they consume resources while they sit idle waiting to be used.

With CloudCasa, due to its cloud integration, a backup takes a snapshot of the cloud account configurations in addition to the Kubernetes resources and data. This provides CloudCasa with the ability to spin up a brand new AKS or EKS cluster, using the cloud configuration information, in real-time during a restore. This is called Bare-Metal Cluster Recovery, and it eliminates the need for stand-by clusters.

## Cross-Cluster and Cross-Cloud Data Migration

Data recovery is not only used for disaster recovery but many other use cases as well. Data migration via recovery of data can also be used in the context of application transformation, application migration, and even separating staging from production in different cloud accounts. Each of these scenarios require data to move from one Kubernetes cluster, or one cloud account, to another. CloudCasa's cross-cluster and cross-cloud restores allow users to more effectively utilize the data that they have protected. Users have the ability to backup Kubernetes data hosted on one platform, on one cloud account, or cloud entirely, to another.

## Backup-as-a-Service vs Self-Managed Backups

Updating and patching a backup application are tasks that the teams do not have to be doing. Sizing, scaling, monitoring catalog space usage etc. are additional complex

tasks that are tapping into the same resource-constrained teams running your critical business applications. CloudCasa takes all of this burden away from your teams by delivering Backup as a Service.

## Virtual Air Gap vs Same Failure Domain

A standalone backup application is typically installed on one of your Kubernetes clusters being protected and if that cluster were to experience a failure, your entire backup infrastructure is down. CloudCasa runs on a highly available and well-maintained public cloud infrastructure that guarantees a 99.95% SLA. Since the chances of the service provider and customer environments are attacked at the same time is minimal, it presents customers with a virtual air gap domain.

## Proactive Protection vs Last Line of Defense

All Kubernetes solutions support backup and recovery of Kubernetes workloads to S3 Storage. Most support immutability or tamper-proof capability that acts as a last line of defense. CloudCasa also has the ability to do proactive vulnerability assessments on your Kubernetes Clusters and alert you to address problems before they are exploited.

## Utility Pricing vs Unpredictable Pricing

Most Kubernetes backup products charge based on worker nodes because storage allocated per worker node is still low. Worker nodes are also the primary variable in auto-scaling configurations, thereby introducing unpredictability in pricing. CloudCasa supports your long term growth of Kubernetes by employing utility-based pricing based on capacity protected. You can use unlimited worker nodes, clusters, distributions and cloud providers as long as you are under the capacity licensed.

## Cloud Integrated vs Cloud Compatible

Most Kubernetes backup solutions can protect AKS and EKS Clusters and use Azure or Amazon S3 as backup destinations. CloudCasa is deeply integrated with these cloud providers - unlike alternatives - so an Azure or Amazon user can scan in their cloud accounts and auto-discover all clusters for centralized data management.

CloudCasa can perform continuous vulnerability assessments on your Azure and Amazon accounts covering over 20 popular cloud services similar to the assessments done on Kubernetes clusters. CloudCasa collects AKS and EKS metadata during cluster backup and auto-creates a new cluster based on these settings during recovery, removing the need for expensive stand-by clusters for recovery.

## Your Next Step

Start with Free Service plan of CloudCasa, which allows you to back up your cluster resource data and protect your persistent volumes with local snapshots. No payment information is required, no limits are placed on the number of managed snapshots, worker nodes, or clusters, and retention times of up to 30 days are allowed.

CloudCasa is backed by [Catalogic Software](#), a proven data protection company with over 20 years of experience safeguarding enterprise data.