Product overview

#1 Kubernetes Data Protection and Mobility

Veeam Kasten *for Kubernetes*

Cloud Native Security and Enterprise Scale

As Kubernetes adoption accelerates in the cloud-native era, organizations need to address the critical requirement for protecting their Kubernetes applications. To keep business running, robust protection and recovery of the entire application along with the data services — must be addressed to overcome misconfiguration, outage, and security threats that compromise availability.

Containers play a pivotal role in the development of cloud native applications. According to an ESG survey conducted for Kasten in 2022, 83% of enterprises are projected to adopt containers by 2024. Additionally, Kubernetes has emerged as the go-to container orchestration platform, with 66% of organizations currently using it in production. Notably, a Cloud Native Computing Foundation February 2024 blog post, "The 2024 Trends on Cloud Computing", by Kelsey Hightower and Alex Saroyan, emphasizes that effective workload management, regardless of hosting location, will be the primary focus of cloud strategy in 2024.

Why legacy backup fails Kubernetes workloads

- Volume backup does not fully protect cloud native applications and data
- Protecting cloud native workloads with traditional backup solutions increases management cost
- Traditional software tools lack visibility into Kubernetes applications and data
- Legacy backup solutions do not scale with your enterprise Kubernetes workloads
- Standard backup does not protect your Kubernetes applications / workloads against ransomware attacks

The deployment of Kubernetes is expanding due to its ability to support distributed locations, cluster groupings, and the rising popularity of edge traffic. Furthermore, databases and other stateful applications are becoming more diverse in terms of capabilities and deployment patterns (such as in-cluster and DBaaS). Lastly, the workloads on Kubernetes, whether newly developed or revamped, exhibit increasing diversity, highlighting the growing importance of virtual machines (VMs) within the Kubernetes ecosystem. These trends emphasize the necessity of not only prioritizing the backup of Kubernetes applications and their data, but also of managing the applications themselves among cloud platforms.

Veeam Kasten *for Kubernetes* Use Cases

Backup & Restore

Protect your cloud native Kubernetes and VM applications, while preserving your business-critical data

Disaster Recovery

Manage how backups are replicated off-site to meet business and regulatory requirements

Application Mobility

Move applications between clouds and on-premises for test/dev, load balancing, data management and upgrades

Ransomware Protection

Protect your Kubernetes platform during cyberattacks to preserve business continuity

Product overview

Why Veeam Kasten *for Kubernetes*

Veeam Kasten delivers secure, **Kubernetes native data protection and application mobility**, at scale, and across a wide range of distributions and platforms. Proven to recover entire applications quickly and reliably, coupledwith its core tenet, simplicity, Veeam Kasten gives operations and application teams confidence to withstand the unexpected.

Key Capabilities

Designed for FIPS 140-3

Enable compliance with the latest Federal Information Processing Standard (FIPS) using OpenShift.

Immutability With Azure Blob

Expands existing support for immutable S3 backups to Azure, ensuring backup data cannot be deleted or maliciously encrypted.

Block Mode Volume Immutability

Extends immutability support to block mode Kubernetes volumes to enhance ransomware protection

Immutable RestorePoint Visibility

Easily identify which backups are protected by immutable storage in the UI.

Azure Sentinel SIEM Integration

Provides early warnings to block malicious actors from compromising enterprise data.

Secure Deployment Enhancements

New configuration options for Kasten authentication to enable integration with Kubernetes Secret management solutions

OpenShift Advanced Cluster Management Policies

Enable secure and consistent deployment of Kasten across all ACM-managed clusters.

OpenShift ImageStream Image Protection

Natively backup and restore local registry container images managed by ImageStreams to ensure reliable recovery.

Efficient OpenShift Virtualization VM Backups

Direct CephRBD integration to provide enhanced performance and capabilities for block mode backups.

Kasten Self-DR Improvements

Improved performance for exporting Kasten RestorePoint catalog, protecting Kasten multi-cluster configuration, and new UI for restoring Kasten.

VBR Instant Recovery Improvements

Added automated migration to primary storage and ability to monitor migration progress directly from Kasten UI.

Azure Container Marketplace Availability

Consolidates subscription & payment management by leveraging existing Azure contracts and credits.

How Veeam Kasten works

Discover

Automated discovery of your Kubernetes application

Protect

Secure your Kubernetes application and data

Restore

Quickly and effectively restore your Kubernetes application and data

> Quick to deploy and easy to use via a state-of-the-art management interface or a cloud native API. Enables DevOps team agility to identify and protect system applications.

Learn More

For more information, visit Veeam.com or follow @Veeam on X.