Product overview

#1 Kubernetes Data Protection and Mobility

Veeam Kasten *for Kubernetes* V7.0

Cyber Resilience and Enterprise Solutions

Veeam Kasten release V7.0 delivers cyber resilience and enterprise focused innovations. It provides customers with a rigorous, standards compliant security environment, enhances ransomware protection and broadens enterprise integrations with support for large-scale Kubernetes environments. This release of the leading Kubernetes data protection platform addresses the increased demand for robust container security that is accompanying expanded Kubernetes deployments.

Increasingly, enterprises are implementing cloud native architectural principles to construct, deploy, and manage applications. By utilizing DevOps methodologies, cloud native architectures enable companies to innovate at a faster pace, enhance reliability and scalability and reduce costs. As Kubernetes becomes increasingly prevalent, we can expect a parallel evolution in tools and support systems to accomodate this growth.

Containers play a pivotal role in the development of cloud native applications. According to an ESG survey conducted for Kasten, 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

Veeam Kasten 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, coupled with its core tenet, simplicity, 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.

Product overview

Spotlight: New in Veeam Kasten *for Kubernetes* V7

Veeam Kasten V7.0 helps customers protect and secure their applications and data, and scale their cloud-native data protection efficiently, offering feature updates that leverage cloud native integrations. New features include:

Cyber Resilience

FIPS compliance: FIPs 140-3 compliant security for federal sector environments.

Ransomware Protection: Expanded data protection options with Azure Blob immutability and GUI visibility of immutable RestorePoints.

Observability: Additional SIEM integration with Azure Sentinel.

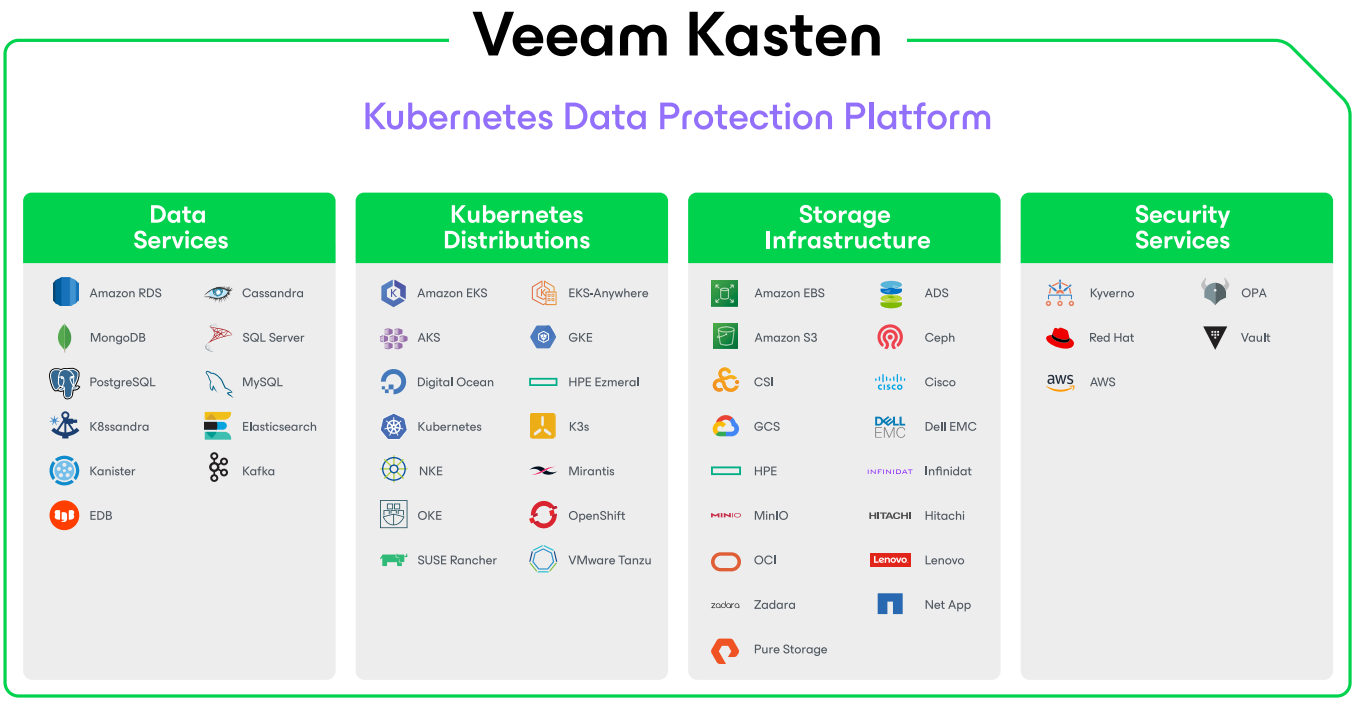
Authentication: Secure authentication using HashiCorp Vault as a backend.

Enterprise Solutions

VM and cloud-native advances: OpenShift Advanced Cluster Management integration, ImageStream support and efficient VM backups.

Recovery features: DR performance enhancements, VBR Instant Recovery Migrate and Stop, and In-place volume cloning.

Cloud transactability: support for Azure Container Marketplace.



Product overview

Veeam Kasten *for Kubernetes* Top Features and Benefits

Category	Features	Benefits
Recover Entire Applications Rapidly recover entire applications – including underlying data and configuration – with confidence and ease.	Policy Automation	• Efficiently manage data protection operations and ensure business continuity at enterprise scale.
	Application Centric	• Ensure reliable backup and recovery with flexible framework that is application aware and consistent.
	Automated DR	• Automate application restores to alternate clusters and locations for reliable Disaster Recovery (DR).
Ensure Security and Resilience Securely operate with built-in protection against cyberthreats with immutable, encrypted backups, and self-service restores.	Immutable and Encrypted	• Safeguard data against ransomware and other threats by placing backups in an encrypted and WORM state.
	Air-Gapped and Secure Self-Service	• Secure operations with least required privileges settings on a per-app level and Kubernetes native RBAC.
	Security Certified and Integrated	• Provides security teams early warning and remediation capabilities, even in sensitive public sector environments.
Application Mobility Across Platforms Easily enable hybrid- and multi-cloud with seamless application mobility across different infrastructure, and distributions	Cross Cloud Portability	• Move applications across namespaces, clusters, or clouds for DR, or clone them for test & development.
	Transforms Across Distributions	• Easily modify the contents of K8s resources when restoring or migrating across deployment environments.
	VMs on Kubernetes	• Migrate, modernize and manage VMs on Kubernetes without refactoring the entire application

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.