veeam

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 of protecting their Kubernetes applications. To keep business running, robust protection and recovery of the entire application — along with 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 Veeam 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.

Kubernetes deployments are expanding due to their 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 (e.g., in cluster and DBaaS). Lastly, the workloads on Kubernetes, whether newly developed or revamped, exhibit increasing diversity, which highlights the growing importance of virtual machines (VMs) within the Kubernetes ecosystem. These trends emphasize the necessity of not only prioritizing backing up Kubernetes applications and their data, but natively managing the applications themselves among cloud platforms.

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 *for Kubernetes* Use Cases

Backup and Restore

Protect your cloud native Kubernetes and VM applications while preserving 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.

veeam

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 simply, quickly, and reliably, Kasten gives operations and application teams the confidence to withstand the unexpected.

Key capabilities

Data Scaling Enhancements

Protect large-scale application volumes, including millions of files, and optimize backup and restore for more efficient operations.

Google Cloud Storage Immutability

Protect your backups from ransomware attacks with object lock integration with Google Cloud Storage.

Red Hat OpenShift Virtualization

Automatically deploy and protect OpenShift Virtualization virtual machines (VMs) at the edge with validated patterns and production-ready best practices and GitOps.

Granular Data Mover

Dynamically allocate data mover CPU and memory resources on a per-application basis for more efficient resource utilization.

Multi-cluster FIPS Support

Bolster security and adhere to strict benchmarks and best practices fit for governments, now with expanded Kasten multi-cluster management for OpenShift.

SUSE Virtualization

Extend industry-leading, Kubernetes-native resilience to SUSE Virtualization to unify VM and container management.

CBT for Microsoft Azure

Improve export performance and lower resource consumption for Azure Managed Disk volumes with changed block tracking (CBT) integration.

Azure Federated Identity

Eliminate credential risks with our newly supported Azure Identity Federation for OpenShift.

Immutable Restore Point Visibility

Recover applications and data with confidence by easily identifying whether a restore point is immutable or not.

Red Hat OpenShift Dynamic Console

Get critical insights into data protection operations and gain quick access to the Veeam Kasten dashboard directly from OpenShift's console.

OpenShift Security Enhancements

By leveraging new annotations in OpenShift, Veeam Kasten can now ensure precise and secure control over workload permissions.

Kasten DR Enhancements

Enable rapid, in-place recovery of Veeam Kasten itself via next-generation architecture and GitOps-ready configuration.

How Veeam Kasten Works

Discover

Automated discovery of your Kubernetes application.

Protect

Secure your Kubernetes applications and data.

Restore

Quickly and effectively restore your Kubernetes applications and data.

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

Learn More

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