Product use case

Veeam Kasten Use Case

Ransomware Protection with Veeam Kasten

Emerging Menace: The Alarming Concern of Ransomware Attacks

Ransomware attacks have emerged as one of the most significant concerns for enterprises. According to the Veeam Ransomware Trends Report 2024, 75% of organizations get hit by cyberattacks, and most report getting hit more than once. While historical instances of ransomware attacks haven't targeted Kubernetes deployments directly, concerns about Kubernetes vulnerabilty have risen. In fact, Red Hat's "State of Kubernetes Security Report 2023" revealed that 67% of organizations surveyed postponed their Kubernetes deployments due to security concerns. Notably, among their respondents, a substantial 90% experienced a cybersecurity incident in the past 12 months.

Why is Kubernetes Vulnerable to a Ransomware Attack?

Kubernetes stands out as a robust orchestration platform that offers numerous advantages for overseeing and expanding containerized applications. Nevertheless, like any other complex system, Kubernetes is not impervious to vulnerabilities that malevolent actors can exploit. These vulnerabilities include inadequate access controls, exposed API servers, reliance on default configurations and the utilization of outdated Kubernetes versions (or associated backup software). While these vulnerabilities warrant caution as you push forward with container deployments, they are not insurmountable. Armed with the appropriate tools and processes, you can mitigate them effectively.

New Tools for New Computing Infrastructures

Introduced as Kasten K10 in 2016, Veeam Kasten tackles the industry's apprehensions regarding Kubernetes data protection and enables organizations to harness the myriad advantages of orchestrated Kubernetes container ecosystems. Veeam Kasten continues to evolve to meet customers' changing needs with updates that ensure adherence to best practices, business continuity, and reliable data protection against a spectrum of potential threats.

Key Veeam Kasten Ransomware Capabilities

Consistency Guardrails Protect Kubernetes Mobility and Restore Capabilities

Veeam Kasten empowers DevOps and data management professionals to apply consistent rules to all roles and layers in a Kubernetes production environment. This inhibits cybercriminals from establishing a foothold in critical systems.

Ransomware Monitoring Detects When Malware is Present in Secured Copies

Veeam Kasten is designed to make it easy to view the security status of your entire deployed Kubernetes data protection platform. This proactive approach effectively nullifies any potential leverage that ransomware attackers might seek to gain over Kubernetes operations.

Clean and Clear Backup Management Protects Service Continuity and Restoration

Veeam Kasten empowers both DevOps and deployment teams, regardless of whether they operate on-premises, in public or private clouds, or in hybrid deployments with comprehensive control over secured backups and information. This allows for effortless re-deployment onto a secured platform or seamless migration to alternate environments.

Product use case

Combating Ransomware

While Veeam Kasten cannot directly intercept a cyberattack, it can be deployed as part of a data protection strategy to minimize the impact of a ransomware attack.

Data Protection

Veeam Kasten empowers users by facilitating the seamless creation and scheduling of routine application backups and their associated persistent volumes. Backups are insulated from primary storage and can be used to restore operations in the case of inadvertent or deliberate data loss or file corruption.

Isolation from Ransomware

Veeam Kasten isolates production and backup environments from production to ensure operations can be restored from a clean and reliable backup in the event of an incident. Key information such as configuration data and credentialled information can be secured on-premises, offsite, online or within immutable storage options to address a specific scenario.

Point-in-Time Recovery

Veeam Kasten allows users to recover their data from specific points in time, which can be helpful when rolling back to a known state of operation is necessary. Point-in-time recovery is particularly important for restoring services in a disaster recovery (DR) scenario, such as a ransomware attack.

Application Mobility

Veeam Kasten's capabilities extend to application mobility enable graceful application and data migration across Kubernetes clusters, including to separate production resources. If a previously live platform is compromised, teams can swiftly restore the most recent and secured backup of their choice.

Adhering to Kubernetes' best practices like creating and maintaining backups on a regular basis strengthens your ability to safeguard your digital assets. By integrating Veeam Kasten into your data protection workflow, you'll be able to effortlessly reinstate your applications and data to earlier states should any malicious incidents occur.

Veeam Kasten Ransomware Protection Features

Early Threat Detection

Raise an early flag on potentially malicious activity or imminent attacks.

Encrypted and Immutable Backups

Always have a safe and consistent copy of your applications and data.

Accelerated Recovery

Quickly and effectively restore your Kubernetes application and data

as quick and secure restores minimize business downtime due to attacks.

*Ponemon Institute, (August 2022), Cost of a Data Breach Report 2022. IBM Security, https://www.ibm.com/reports/data-breach veeam

Product use case

Feature Summary

Veeam Kasten Ransomware Protection Features	
Encryption	• Provides end-to-end encryption of application/configuration data and associated metadata artifacts both in flight and at rest.
Enterprise ransomware	• Enables scaling cloud-native data and application protection efficiently while preserving a security profile against ransomware attacks.
IAM and Kubernetes-native RBAC	• Identity Access Management (IAM) establishes a binding to Role Based Access Control (RBAC) permissions to regulate computer and network resources available in the GUI.
Immutable backups	• Backup data immutability and restore point visibility keep the recovery path tamper-proof and open to thwart ransomware and enhance workflows.
Kubernetes Audit	• Veeam Kasten events can now be natively logged into Kubernetes Audit and analyzed to raise an early flag on potentially malicious activity.
Kyverno	• Kyverno enables the production team to avoid deviation from mandated data protection objectives and consistently matches the legal requirements of data security fiats.
OPA	• Open Policy Agent (OPA) and OPA Gatekeeper enable policy enforcement guardrails that are accessable through REST APIs and used to enable backup and recovery processes.
Rootless	• Veeam Kasten temporary and permanent pods do not require root access and support GKE Autopilot with rootless permissions. Kasten also aligns to Pod Security Policy or Security Context Constraints on OpenShift platform environments.
SBOM	• Software Bill of Materials (SBOM) guarantees a software release supply chain origin and chain of custody.

Integrated Veeam Kasten Partner Ransomware Capabilities	
Amazon GuardDuty	• Amazon GuardDuty detects and escalates malicious IP attempts to thwart Veeam Kasten resources, or when anonymous access is suspiciously via AWS S3 attack detection.
Azure Blob	• Ideal for AKS and ARO backups, you can configure retention directly through Kasten's UI
AWS KMS	• Supports AWS KMS secrets manager, making it easier to implement a hardened, secure DR workflow.
Iron Bank	• Hosted on the DoD Platform One, source for hardened and approved containers that meet DevSecOps Reference Design.
Red Hat Advanced Cluster Security	• Red Hat Advanced Cluster Security layers pre-configured security compliance scans of Veeam Kasten's namespace and can escalate when certain modifications are attempted on resources.
SIEM integration	• Security Information and Event Management (SIEM) data integration for security event correlation and analysis by third party solutions, including Azure Sentinel and DataDog.
Hashi Corp Vault	• HashiCorp Vault encrypts a Veeam Kasten master key that's useful when protecting cross-cloud snapshot migration.

Product use case

Veeam Kasten *for Kubernetes* Data Protection Platform

Veeam Kasten is a Kubernetes-native data protection platform that provides enterprise operations teams with an easy to use, scalable, and secure system for backup and restore, disaster recovery (DR), and application mobility of Kubernetes applications. With Veeam, teams achieve Kubernetes-native resilience against ransomware attacks. Kasten offers an application-centric approach and deep integrations with relational and NoSQL databases, Kubernetes distributions and APIs, and cloud platforms. This provides teams with the freedom to choose any infrastructure they want while achieving maximum operational simplicity. Policy-driven and extensible, Kasten also includes features such as full-spectrum consistency, database integrations, automatic application discovery, multi-cloud mobility, and a powerful web-based user interface.

> “Throughout our evaluation, Enterprise Strategy Group determined that Kasten can deliver the data protection and recovery capabilities required by Kubernetes applications. We examined this by comparing how traditional solutions and Kasten address four major use cases: Backup and restore, DR, application mobility, and ransomware protection.”

Dispelling the Myths of Kubernetes Data Protection
ESG 04 2024

Kubernetes Data Protection Use Cases: Summary

Veeam deeply understands Kubernetes and it’s unique challenges with regard to backup, restore, DR, application mobility, and ransomware protection. Veeam Kasten helps enterprises successfully run applications on Kubernetes with confidence.

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.

→ For more information, visit [Veeam.com]() or follow [@Veeam]() on X.