From Risk to Resilience: Securing Kubernetes Compliance

Executive Summary

This whitepaper, "From Risk to Resilience: Securing Kubernetes Compliance", explores the evolving landscape of compliance for organizations that use Kubernetes, an open-source platform that automates the deployment, scaling, and management of containerized applications. As the adoption of container technology has risen — and is reported to have 87% of companies running or planning to run containers in production according to Veeam's 2024 Data Protection Trends — the necessity for stringent compliance measures has increased. This is a result of the need to mitigate risks from cyberattacks and protect sensitive data types, including personally identifiable information (PII) and financial records.

This paper highlights international and industry standards such as ISO/IEC 27001, FIPS 140-3, and the NIST Cybersecurity Framework (CSF), that underscore the fact that compliance is essential for safeguarding both individual and organizational information. While addressing the challenges posed by open-source tools like Velero, which often fall short in compliance capabilities and integration support, this white paper explores the benefits of adopting Veeam Kasten *for Kubernetes*, a robust solution that's tailored for Kubernetes environments.

Veeam Kasten, the #1 Kubernetes data protection and mobility solution, provides significant compliance-specific features, including policy automation, granular data recovery, enhanced monitoring, integrated cloud storage, and more. These capabilities not only align with regulatory mandates but also reinforce data security. Ultimately, adopting commercial solutions like Veeam Kasten is framed not just as a compliance mandate but as a strategic necessity, enabling organizations to enhance data governance, operational resilience, and their competitive edge in a complex regulatory landscape.

Introduction

Kubernetes has rapidly emerged as the leading platform for deploying, scaling, and managing containerized applications, virtual machines (VMs), and AI/ML workloads. As a powerful open-source container orchestration solution, Kubernetes was originally developed by Google and released in September 2014. Since then, it has become the industry standard for cloud-native application management, a position highlighted by GigaOm. According to Veeam's 2024 Data Protection Trends Report, 52% of organizations stated they are running containers in production with another 35%+ in the planning/deployment phases, equating to 87%+ each of the three years surveyed. Dynatrace's "Kubernetes in the Wild Report 2025" further underscores Kubernetes' widespread adoption, describing it as the "operating system" of the cloud, based on production data from thousands of organizations globally. As Kubernetes continues to evolve, its enhanced capabilities for managing session-oriented, stateful information highlight the growing importance of compliance with regulatory standards in business operations.

As Kubernetes adoption continues to skyrocket and more critical data is managed within clusters, compliance becomes a critical necessity, especially in regulated environments. This white paper explores the key compliance requirements organizations must keep in mind as Kubernetes adoption accelerates.

First, we will discuss the different types of data managed in corporate applications and align them to protection requirements. We will also cover some of the more prevalent compliance requirements and address guidelines that govern their use. Next, we will discuss the challenges presented when using open-source tools for data protection. Finally, we will demonstrate how Veeam Kasten provides companies with an effective and necessary means to efficiently comply with regulatory oversight and governance.

52%

Percentage of organizations worldwide that had adopted container technology by the end of 2024

90%

Share of the Kubernetes platform deployment market held by commercialized platforms like Red Hat OpenShift.

Identify Application Information that Requires a Safeguard

Regulations are crucial in minimizing the risk to companies facing cyberattacks and ensuring the protection of individual and corporate information from theft. While preventing cyberattacks is a significant focus, regulations address a much wider range of risks, including accidental data exposure, insider threats, privacy concerns, and legal or contractual obligations.

The regulations focused on data protection and information system security play a vital role in addressing these concerns. For this paper, the regulated categories of information include:

- **Personally identifiable information (PII):** These records contain individuals' information such as names, addresses, phone numbers, email addresses, identification numbers, and more. Personnel files are examples of records that contain this sensitive data.
- **Customer data:** Customer records include all types of transaction records and communications that not only protect the relationship between companies and their customers, but also the ability of a company to execute its strategy.
- **Financial records:** Regulations cover sensitive financial data, such as bank account details, credit and debit card information, and financial transactions.
- **Health records:** Regulations also address the protection of medical and medical history records, as well as genetic and biometric data.
- **Government data:** Information generated, processed, or controlled by government agencies—including classified documents, citizen records, national security data, and interagency communications.

Regulations have the primary objective of ensuring the security and safeguard of sensitive information, shielding it from unauthorized access, misuse, or theft. Organizations engaged in business operations, whether at a local or international level, are tasked with the responsibility of adhering to these regulations and meeting the prevailing governing requirements when conducting business.

Framing the Compliance Landscape

Ensuring robust governance for applications deployed with sensitive information requires that those responsible for data protection establish a comprehensive plan that meets regulatory requirements. The evaluation of regulatory requirements should consider industry-specific, regional, and international bodies based on the company's domain. Several key regulatory requirements play significant roles in data protection and compliance activities. Below is a categorized breakdown of key compliance directives:

Sensitive Data Protection

Focuses on safeguarding personal, financial, and health-related information.

- **GDPR (General Data Protection Regulation)**
  Applies to EU citizens' data, even when processed outside the EU. Covers consent, data handling, and breach notification.
- **HIPAA (Health Insurance Portability and Accountability Act)**
  U.S. regulation for protecting personal health information (PHI). Requires privacy policies and safeguards for healthcare data.
- **PCI DSS (Payment Card Industry Data Security Standard)**
  Mandated by the PCI Security Standards Council for organizations handling credit card data. Ensures secure storage, processing, and transmission of cardholder data.
- **DPAs (Data Protection Authorities)**
  National regulators like the UK's ICO enforce GDPR and local data protection laws.

Secure Development & Governance Frameworks

Guides for building secure systems and managing risk.

- **ISO/IEC 27001, 27701, 29100**
  International standards for information security management, privacy frameworks, and privacy-enhancing technologies.
- **NIST Cybersecurity Framework (CSF)**
  U.S.-based framework offering best practices for identifying, protecting, detecting, responding to, and recovering from cybersecurity threats.

Data Protection Authorities (DPAs):

DPAs in each EU country, including the UK's Information Commissioner's Office (ICO), provide guidelines for GDPR compliance, ensuring organizations meet the necessary requirements. It is worth noting that the ICO also sets data protection requirements and guidelines for protecting UK citizens, as the UK is no longer an EU member state.

- **Adversarial Tactics, Techniques, and Common Knowledge (MITRE) ATT&CK**
  Deployed globally, the MITRE ATT&CK matrix helps organizations to map, analyze, and improve threat detection and response. This is an important step used to assess preparedness for event preparedness and response.
- **FINRA (Financial Industry Regulatory Authority)**
  U.S. regulation for securities firms, with indirect implications for international organizations trading with U.S. customers.

Secure Transmission & Cryptographic Standards

Ensures data is securely transmitted and encrypted.

- **FIPS 140-3 (Federal Information Processing Standard)**
  U.S. standard for cryptographic modules used to protect sensitive information during transmission and storage.

Compliance with these regulations is crucial to ensure data protection and cybersecurity in Kubernetes deployments. Adhering to these regulations helps safeguard sensitive data, align with industry standards, and maintain the security and privacy of deployment environments.

The Compliance Gaps of Open-Source Data Protection Tools

While open-source tools are often adopted to reduce costs, they frequently fall short in meeting enterprise compliance requirements. Velero, a Kubernetes-native open-source solution, is widely used by organizations exploring Kubernetes-based application platforms. However, it lacks the robust compliance, automation, and governance features that enterprises demand. Tools like Velero have played a key role in early Kubernetes adoption by offering a flexible entry point for testing and development. Yet, as Kubernetes workloads scale to support global operations and highly regulated environments, these tools often expose limitations in advanced capabilities, ease of use, and the enterprise-grade functionality required for modern data protection and compliance. Here are three critical considerations that you should evaluate when making the decision to include or exclude open-source solutions in your toolkit.

1. **Limited compliance-specific features:** Open-source tools, like Velero for Kubernetes, prioritize community-driven investments that may not keep up with the most urgent compliance requirements. They may lack built-in functionality, such as audit logs, access controls, or reporting capabilities, which are essential for demonstrating compliance.

2. **Lack of official support (including documentation):** Non-commercialized solutions rely on community support, which may not provide the same level of responsiveness as official support teams. Additionally, the absence of controlled release user documentation can make it challenging to find comprehensive and up-to-date guidance, as resources may be scattered across various community forums and Wiki pages.

3. **Integration challenges:** Kubernetes has an extensive ecosystem of applications, distributions, storage, and security services. When using open-source tools, integrations with other components may not be thoroughly tested. This poses a hurdle to seamlessly transitioning to an alternate infrastructure, whether as part of a planned migration or in response to downtime incidents caused by disasters like a cyberattack.

4. **Resource demands for compliance assurance:** To address the limitations of open-source tools in meeting compliance requirements, organizations must invest in comprehensive testing, detailed documentation, and independent verification to ensure these tools align with specific regulatory standards. This often requires additional resources for development, customization, and ongoing support, which can offset the initial cost savings of using open-source solutions.

In today's fiercely competitive market, companies have the option to forgo these challenges altogether. They can opt for a more consistent and proven solution that eliminates the need for such investments.

How Does Veeam Kasten Support Compliance Requirements?

Veeam's leadership is validated by its top ranking in the GigaOm Radar for Kubernetes Data Protection, in which it was recognized both a Leader and Outperformer—a testament to its innovation, enterprise readiness, and operational excellence.

As Kubernetes adoption accelerates—particularly through hybrid compute platforms like Red Hat OpenShift and SUSE Rancher Prime, organizations must align their data protection strategies with evolving compliance mandates. Veeam Kasten is purpose-built to meet these demands, delivering a policy-driven, auditable, and resilient architecture that supports regulatory adherence without compromising agility.

Key compliance features empower Kubernetes platform teams to enhance data protection and management that strengthen their security posture with Veeam Kasten:

- **Data Protection:** Delivers FIPS 140-3–aligned encryption for data in transit and at rest, integrated key management, and immutable, air-gapped storage to meet stringent data confidentiality and integrity requirements.
- **Policy-Based Automation:** Enforces protection policies through Kubernetes-native constructs and Infrastructure as Code, enabling repeatable, auditable workflows that align with frameworks like ISO/IEC 27001 and NIST CSF.
- **Granular Data Recovery:** Supports namespace- and application-level restores with the ability to recreate full environmental states—critical for demonstrating recoverability and resilience under compliance audits.
- **Access Control & RBAC:** Implements fine-grained, namespace-scoped role-based access control (RBAC) to enforce least-privilege principles and support identity governance requirements.
- **Monitoring & Reporting:** Integrates with multiple SIEMs to perform real-time compliance scans and alert them to unauthorized changes, supporting continuous monitoring mandates.
- **Secure Development:** ISO/IEC 27001 compliant and available through Iron Bank, Kasten adheres to secure development lifecycle practices and DoD-grade container hardening standards.

- **Visibility & Retention Oversight:** Provides a centralized UI for managing backup policies, retention schedules, and audit logs—ensuring transparency and traceability for compliance teams.
- **Integrated Secure Cloud Storage:** Ensure your data lands in a secure location with Veeam Data Cloud Vault. This integration provides a fully managed, always immutable, encrypted, and logically air-gapped cloud storage resource, with all-inclusive per-TB pricing.

Veeam Kasten not only meets but exceeds the capabilities of open-source alternatives by offering a comprehensive commercialized Kubernetes backup and restore platform and is equipped with a robust suite of data management tools.

Conclusion

As organizations increasingly rely on Kubernetes for their cloud-native applications, the imperative for robust compliance becomes paramount. This white paper has outlined the critical compliance requirements that govern the handling of sensitive data, ranging from Personally Identifiable Information (PII) to corporate financial records, and examined the unique challenges posed by open-source tools in adhering to these regulations.

In a landscape where cyberattacks are prevalent and regulatory scrutiny is intensifying, leveraging comprehensive solutions like Veeam Kasten enables organizations to effectively manage their data protection strategies while meeting compliance mandates across backups and storage. With a suite of compliance-specific features ranging from automated policy enforcement to advanced monitoring and reporting — Veeam Kasten stands out as a strategic ally for Kubernetes platform teams by facilitating secure, compliant operations across diverse regulatory environments.

Choosing the right tools for data protection is not just a matter of cost-efficiency; it is a strategic decision that influences an organization's resilience and credibility. By adopting Veeam Kasten, companies can confidently navigate the complexities of compliance, safeguard their sensitive information, and maintain operational integrity in an increasingly regulated and competitive landscape. The transition from purely open-source solutions to a hybrid approach with commercial tools represents a commitment to excellence in data governance that organizations cannot afford to overlook. Now that's data resilience.

About Veeam Software

Veeam®, the #1 global market leader in data resilience, believes every business should be able to bounce forward after a disruption with the confidence and control of all their data whenever and wherever they need it. Veeam calls this radical resilience, and we're obsessed with creating innovative ways to help our customers achieve it. Veeam solutions are purpose-built for powering data resilience by providing data backup, data recovery, data portability, data security, and data intelligence. With Veeam, IT and security leaders rest easy knowing that their apps and data are protected and always available across their cloud, virtual, physical, SaaS, and Kubernetes environments. Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 68% of the Global 2000, that trust Veeam to keep their businesses running. Radical resilience starts with Veeam. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

→ Learn more: veeam.com