SPOTLIGHT
Sponsored by: Broadcom

Kubernetes is crucial for new AI application delivery; however, security and its complexity limit scalability, driving the need for modern secure private cloud platforms that simplify Kubernetes management for platform engineers while removing developer toil.

Enabling Platform Engineers to Overcome Kubernetes Complexity with a Modern Private Cloud Platform

October 2025

Written by: Jim Mercer, Program Vice President, Software Development, DevOps, and DevSecOps

Introduction

The increasing surge in new application deployments has solidified Kubernetes as the standard for modern software delivery. However, the inherent complexity of managing Kubernetes at scale, from intricate configurations to distributed operations, drives a critical need for modern platform engineering approaches that empower software developers with self-service capabilities while ensuring robust governance, cost control, and security.

AT A GLANCE

KEY TAKEAWAYS

- Kubernetes has become the standard for cloud and AI deployments.
- Platform engineers aim to remove developer toil but need tools for managing Kubernetes complexity.
- Modern private cloud platforms can enable platform engineering teams to manage Kubernetes at scale.
- Improved performance and security are incentivizing organizations to repatriate workloads from public to private clouds.

Tidal Wave of New Applications

By 2028, IDC projects that over 1 billion net-new applications will be created (see *1 Billion New Logical Applications: More Background,* IDC #US51953724, April 2024). The rapid growth of cloud-native applications, driven by DevOps, containers, and microservices, has made container orchestration a critical capability because containers are challenging to manage at scale without an orchestration layer. This trend is driving significant market growth, with IDC forecasting the container infrastructure software market to reach $6.4 billion by 2028. The focus on infrastructure optimization is a key initiative, with 48% of organizations identifying it as a top priority for developing AI applications.

Kubernetes Benefits and Challenges

While containers offer significant benefits, including portability, isolation, and efficiency, managing them at scale without an orchestration layer is impractical. Kubernetes has become the de facto standard, often called the "operating system of the cloud" because it orchestrates containerized applications across a cluster of nodes. The demand for containers and Kubernetes is accelerating, particularly with the rise of generative AI (GenAI) coding assistants, which are speeding up the development and deployment of AI-driven applications. Organizations are increasingly choosing to build their AI applications on Kubernetes while seeking the security of a private cloud to keep AI workloads close to their sensitive corporate data.

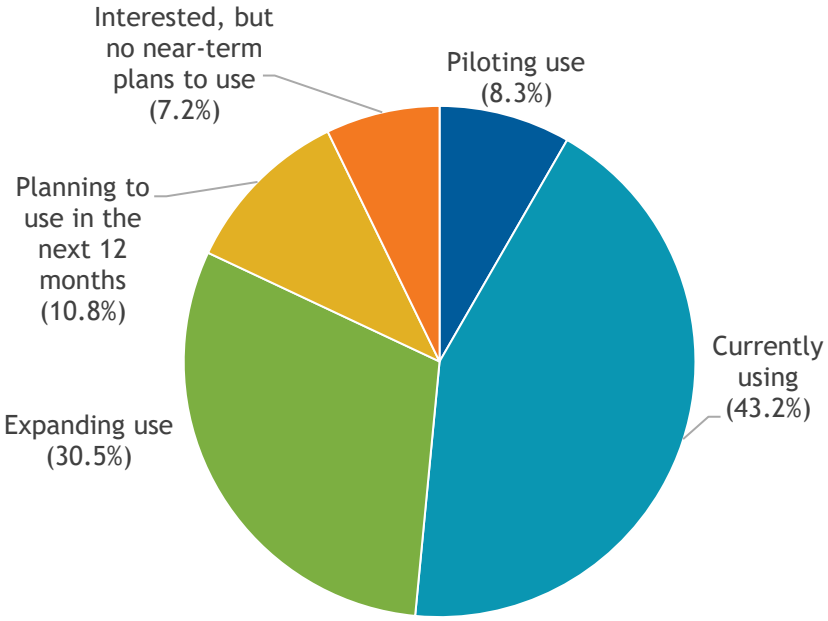
Unfortunately, Kubernetes introduces a significant level of complexity, making it challenging to deploy, configure, and manage, especially at scale. This complexity stems from various abstraction layers and intricate requirements for networking and security. A significant source of this difficulty is its reliance on lengthy and complex YAML configuration files. Maintaining these files is error prone, requiring meticulous attention to detail. Managing all the files, parameters, and settings across different resources becomes a demanding task that can easily overwhelm developers.

Platform Engineering

The widespread adoption of Kubernetes, along with its inherent complexity, is driving the need for sophisticated new approaches in platform engineering. This discipline involves designing and building internal developer platforms (IDPs) that provide software development teams with self-service capabilities. These platforms enable developers to deliver applications more quickly, securely, and with a higher level of quality. The increased adoption of platform engineering has been primarily fueled by the need to manage Kubernetes across the enterprise. Figure 1 shows the growth of platform engineering and demonstrates that the use of IDPs is surging, with 93% of respondents indicating that they are piloting, using, expanding the use of, or planning to use an IDP within the next 12 months.

FIGURE 1: ***Platform Engineering Adoption***

Q *Which of the following best describes your organization's use of an internal developer platform?*



n = 361

Source: IDC's Platform Engineering and DevOps Survey, June 2025

Due to the increasing complexity, cost management, and governance challenges that platform engineers face, there's a growing need for advanced infrastructure automation solutions for Kubernetes. IDC's recent study found that many platform engineering teams have to create custom solutions to add essential security features, such as proper

encryption, data masking, and access control, to their internal developer platforms because native Kubernetes capabilities aren't sufficient (see *IDC PeerScape: Practices to Implement and Scale Platform Engineering,* IDC #US51835124, January 2025). So, for Kubernetes to be scalable across an enterprise, it requires further abstraction and automation.

Benefits

Private Cloud Platform Engineering

Modern private cloud platforms are emerging to help platform engineering teams manage Kubernetes across their entire enterprise application portfolios. These platforms provide key capabilities to enable platform engineers to manage their Kubernetes environments at scale effectively, including:

- Self-service infrastructure access while maintaining governance, balancing developer autonomy with operational control and security requirements, and providing insight into consumption cost to manage resource allocation and prevent cloud spend overruns
- Centralized policy management capabilities for governance, which are crucial for managing complex Kubernetes environments and balancing control with developer freedom and self-service access
- Access to more efficient and secure distroless container images that contain only an application and its essential runtime dependencies
- Life-cycle management that supports end-to-end automated management of the entire cloud infrastructure stack, including compute, storage, network, and software (There is the ability to deal with day 2 operations and runtime complexity, scaling, and multicluster deployments, including versioning that enables organizations to use the latest Kubernetes version or earlier versions if teams are not yet ready to upgrade.)
- Automated multicluster management with the ability to leverage GitOps pipelines for true continuous delivery, ensuring changes are pushed out to Kubernetes environments automatically and that unforeseen configuration drift does not impact production
- Standardization for homogeneous infrastructure across environments, ensuring best practices and compliance with intrinsic security
- A developer experience that reduces toil while maintaining operational excellence but is not so rigid that platform engineers cannot offer Kubernetes YAML manifests that developers can also directly manipulate if necessary

These modern Kubernetes management systems promise to strike a balance between developer autonomy and guardrails and controls, delivering a consistent developer experience. The secret to achieving these capabilities lies in two key areas: implementing frictionless policy as code for automated governance and compliance and a true self-service platform that offers standardized infrastructure components.

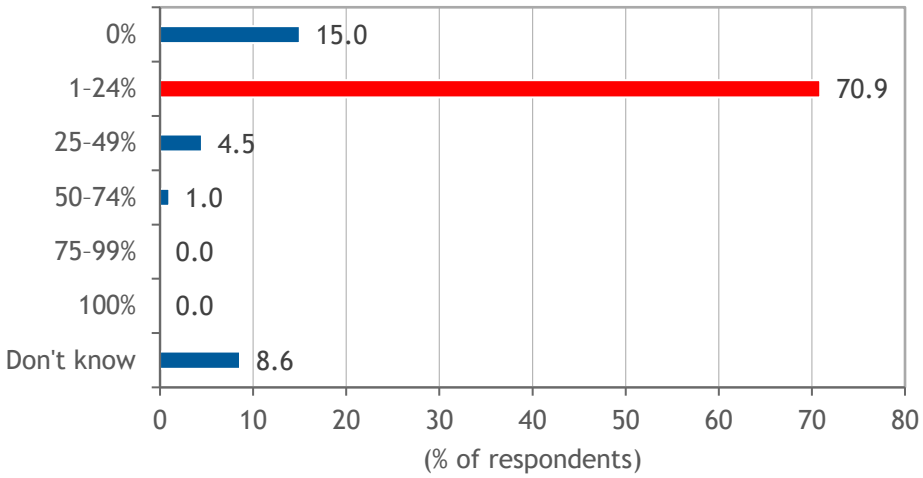
Ultimately, platform engineers require access to a unified platform that enables them to leverage existing skills and tools to manage both VMs and Kubernetes clusters using a standard operational model, thereby minimizing the learning curve and allowing them to quickly become efficient and productive.

Trends

Organizations are increasingly seeking a platform that provides the building blocks for platform engineers to configure and manage Kubernetes. These platforms must enable them to offer self-service access for developers while maintaining crucial governance and control. A growing number of enterprise organizations are discovering the technical and business benefits of using Kubernetes on a full-featured private cloud. Figure 2 shows that there is a wave of repatriation from public clouds to on-premises hosted private clouds.

FIGURE 2: ***The Shift to Private Clouds***

Q What percentage of your organization's application workloads have been repatriated from a public cloud to be deployed on premises over the past 12 months?



n = 313

Source: IDC's PaaS Decision-Maker and Business Value Survey, February 2025

Considering VMware Cloud Foundation from Broadcom

Broadcom developed VMware Cloud Foundation (VCF) to provide an integrated stack of capabilities inside a modern private cloud. It automates deployment, configuration, and life-cycle management in a pre-validated, pre-integrated private cloud platform. It's engineered for scalable and secure multitenancy, enabling platform engineering teams to offer a self-service private cloud for application teams.

Designed with built-in certified Kubernetes runtime and deep integration into the CNCF Kubernetes ecosystem, VCF provides a unified cloud consumption experience through a single interface. Combined, these capabilities allow platform engineering teams to enable developers to seamlessly build, run, and manage all types of applications leveraging AI, with the ability to deploy and run Kubernetes containers and VM-based workloads together on a single platform, with consistent operations. Every cloud provider offers an upstream-conformant Kubernetes distribution (like EKS in AWS), and vSphere Kubernetes Service (VKS) is VCF's distribution.

VCF integrates Kubernetes into its private cloud platform, delivering a unified solution for both VMs and containers. This approach enables simplified management and self-service access. By running containers within VMs on a platform like

VCF, organizations can potentially achieve lower operational expenses and greater flexibility, security, and availability. Furthermore, this can foster better collaboration between platform engineers and cloud administrators.

Key VCF capabilities include:

- Provides operational simplicity and scalability, offering enterprise-grade scaling for production Kubernetes workloads and reduced complexity for platform engineering teams with VKS-enabled deployment and management of Kubernetes clusters, providing developers with a simplified way to provision environments
- Support for private cloud services, including core (e.g., VMs, VKS, networking, volumes, and VM images) and extensible services (e.g., Velero backup and recovery, Cert-Manager certificate management, Harbor image registry, Contour ingress controller, ExternalDNS, Secret Store, Argo CD, Istio Service Mesh, and data services) (Application teams can consume these services using a UI, command-line interface, or declarative Kubernetes-style IaaS API.)
- Offers built-in policy enforcement and compliance automation; also includes IaaS resource policies, based on native Kubernetes Validating Admission and YAML-based policies, as code features to help streamline resource usage by VMs and VKS clusters across tenants and namespaces (Examples of templated out-of-the-box IaaS resource policies include the ability to enforce a single control node Kubernetes cluster, disallow a Kubernetes cluster or VM resource, and label enforcement.)

Purpose Built for Platform Engineering

The VCF platform provides a comprehensive suite of Kubernetes infrastructure management capabilities designed specifically for platform engineers to manage Kubernetes at scale. A consistent stack eliminates the chaos caused by disparate tools and manual integrations, with support for the three latest Kubernetes versions. The platform simplifies complexity with native Kubernetes integration, a unified API, and automated infrastructure provisioning, which streamlines the entire stack's deployment. It also incorporates GitOps management, enabling automatic deployment of infrastructure and applications from a Git repository using Argo CD.

For large-scale environments, VCF enables centralized cluster fleet visibility and Kubernetes workload policy management, which helps platform engineers balance control with developer freedom. Centralization allows platform engineers and security and compliance teams to define and automate governance rules, resource quotas, and security policies that are automatically enforceable when developers provision resources.

VCF also simplifies Kubernetes multicluster life-cycle management, from rapid provisioning to scaling and upgrades. In addition, it includes robust data protection for backing up entire clusters or specific namespaces, enabling recovery in case of failure. By combining VMware's virtualization technology with modern cloud-native capabilities, VCF Automation provides operational consistency, security, and scalability, reducing overhead and ensuring a stable, continuous service.

Broadcom has indicated that the following capabilities will be available in VCF soon:

- VCF Private AI services will enable developers to access a range of capabilities. These include Intelligent Assist for VCF, a GenAI assistant that helps platform engineers configure and maintain VCF and VKS and diagnose and resolve issues faster by accessing Broadcom's knowledge base, reducing downtime. The services also provide OpenAI-

compatible API, multi-accelerator model runtime, multitenant models as a service (MaaS), and Model Context Protocol (MCP) for agentic AI.

- Chiseled Ubuntu containers from Canonical, delivered on the VCF stack, will provide ultrasmall, secure, and efficient container images. These images contain only an application and its essential runtime dependencies, without unnecessary operating system packages, libraries, or tools, reducing resource requirements and the exposed attack surface. Ubuntu images, equipped with precompiled virtualized GPU drivers from Canonical, can streamline deployment and enhance security in air-gapped environments, decreasing reliance on external repositories and internet access. Furthermore, the partnership with Canonical helps streamline support for the Ubuntu OS and containers offered as a part of VCF, with Broadcom serving as the single point of contact.
- Built-in data services will include vSAN Native S3 Object Storage and database as a service (DBaaS) for access to PostgreSQL and MySQL.

Challenges

VMware needs to address the following challenges to compete effectively in the marketplace:

- **Challenge:** Public cloud providers offer their own fully managed Kubernetes services and ecosystems of integrated cloud-native services.
  - **Opportunity:** Broadcom must emphasize the power of providing a truly consistent operational model, highlighting the security and TCO benefits of using VCF at scale as a private cloud that enables effective platform engineering while providing developers with an opinionated path to deployment.
- **Challenge:** Despite its automation capabilities, VCF is an enterprise-grade platform that involves managing multiple sophisticated components, which, on the surface, can lead to a perception of complexity, requiring specialized skills for initial deployment and ongoing management. Organizations might feel overwhelmed by the solution's breadth.
  - **Opportunity:** This objection presents an opportunity for Broadcom to demonstrate how the platform accomplishes a great deal while concealing the complexity of managing Kubernetes from platform engineers and developers. Further, the company should invest in VCF training and certification programs and consider providing out-of-the-box, pre-validated designs and reference architectures.

Conclusion

The proliferation of new applications and the increasing use of GenAI and agentic AI are driving the need for sophisticated platform engineering environments to manage and abstract away the inherent complexity of Kubernetes. Modern private cloud platforms are rising to meet this challenge by providing the crucial capabilities that platform engineers need.

Solutions such as VCF offer a unified and consistent operational model for both traditional VMs and modern containerized applications running on Kubernetes. Organizations adopting and/or needing to scale their platform engineering capabilities and optimize Kubernetes management should consider how VCF can help them mature their platform engineering practices while accelerating application delivery.

About the Analyst

Jim Mercer, *Program Vice President, Software Development, DevOps, and DevSecOps*

Jim Mercer is a program vice president managing multiple programs spanning application life-cycle management (ALM), modern application development and trends, emerging generative AI software development, DevOps, DevSecOps, open source, PaaS for developers, and cloud application platforms. His focus areas are DevOps and DevSecOps solutions research practices. In this role, he is responsible for researching, writing, and advising clients on the fast-evolving DevOps and DevSecOps markets. Mr. Mercer's core research includes topics such as rapid enterprise application development, modern microservice-based packaging, platform engineering, GitOps, application security, software supply chain security, and automated deployment and life cycle/management strategies as applied to a DevOps practice.

MESSAGE FROM THE SPONSOR

Platform engineers are increasingly tasked with supporting a range of Kubernetes clusters while maintaining operational efficiency, security, and policy consistency. VMware Cloud Foundation delivers a unified private cloud platform that automates the provisioning and lifecycle management of Kubernetes infrastructures across multiple clusters and tenants, with consistent policy enforcement and access controls. The platform's self-service capabilities, built-in governance, and declarative APIs empower engineers to streamline operations, manage isolated environments for different developer teams or projects, and reduce manual overhead. For technical guidance on how VMware Cloud Foundation supports platform engineering teams in simplifying Kubernetes infrastructure management, visit vmware.com/VKS.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com