A CTO's Guide to Navigating the Cloud-Native Container Ecosystem

Published 31 March 2023 - ID G00785512 - 15 min read

By Analyst(s): Arun Chandrasekaran, Wataru Katsurashima

Initiatives: Digital Products and Services

The cloud-native ecosystem is evolving to encompass a broad set of technologies, projects and vendors. CTOs can use this research to assess this ecosystem's technologies and vendors, and create robust strategies to accelerate their product delivery.

Overview

Impacts

- Container platform technologies are rapidly proliferating, creating an ecosystem of new open-source projects, products and vendors that technology innovation leaders find difficult to navigate.
- Kubernetes platform vendors are broadening their portfolios, but making diverse bets across the technology stack and use cases, which complicates platform selection decisions.

Recommendations

CTOs driving business transformation through technology innovation should:

- Create a weighted decision matrix for selecting a container platform by considering the factors outlined in Table 2 of this research, along with other key criteria to ensure that objective decisions are made.
- Adopt a platform engineering approach, to the extent possible across use cases to enhance architectural consistency, homogenize operational know-how, simplify developer workflow and provide sourcing advantages.
- Map your functional requirements to the container management platforms and identify any gaps that can be potentially filled by open-source projects and products.

- Reduce the risks of working with startups through constant communication and feedback on product quality, support issues and functionalities desired.

Strategic Planning Assumptions

By 2028, more than 95% of global organizations will be running containerized applications in production, which is a significant increase from fewer than 50% in 2023.

By 2028, 25% of all enterprise applications will run in containers, which is an increase from fewer than 15% in 2023.

By 2028, more than 70% of commercial OSS vendors in the container ecosystem will offer their software as SaaS.

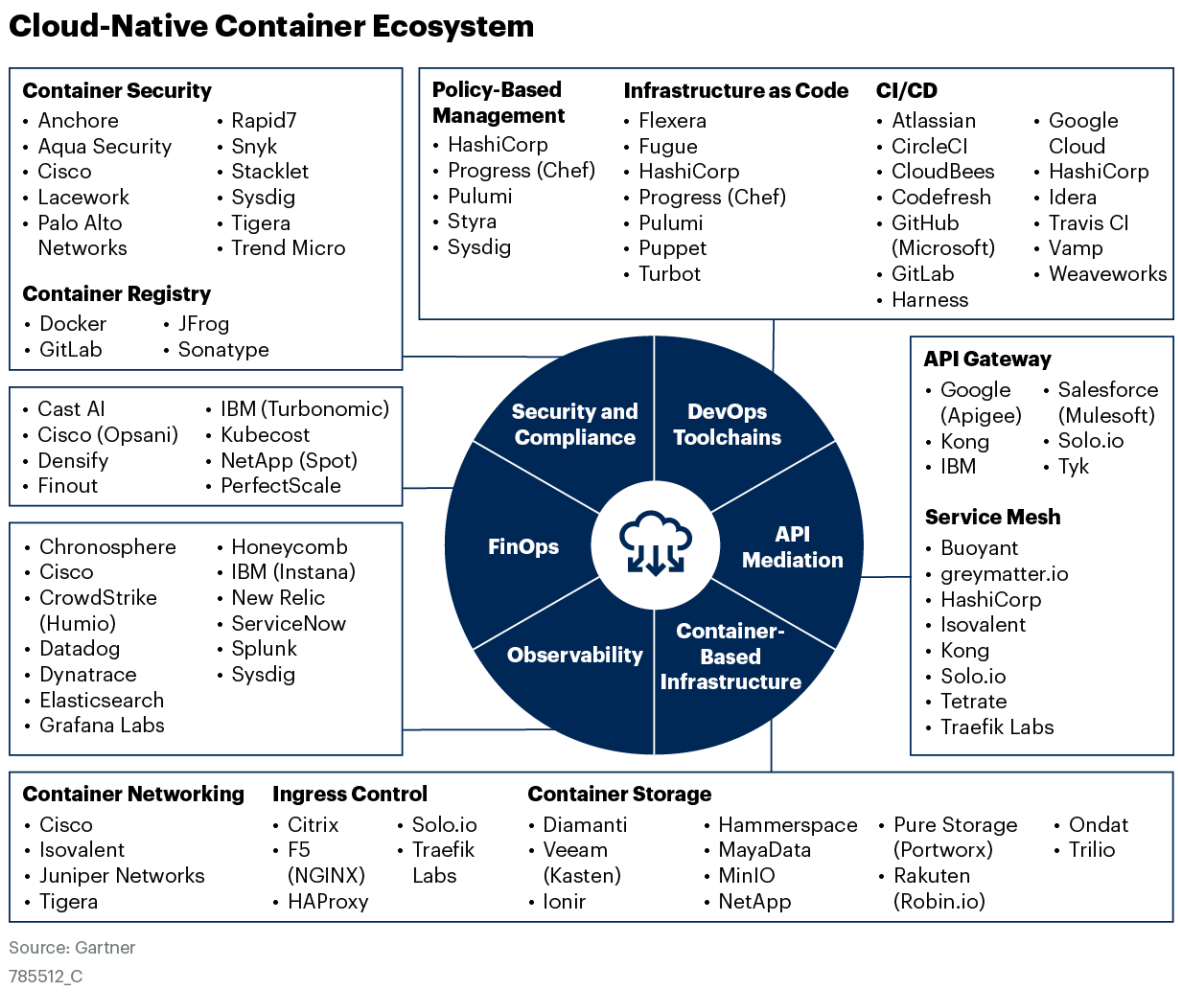
Introduction

This document was republished 9 May 2023. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

Cloud computing technologies are becoming the foundation of digital business platform strategies. Innovation leaders, such as enterprise architecture (EA) leaders and CTOs, are being measured on their ability to modernize application environments, enhance software velocity and nurture a collaborative culture that emphasizes innovation and agility. Containers and Kubernetes are becoming popular technologies for cloud-native applications and have significantly grown in adoption during the past five years. Gartner estimates that close to 50% of enterprises are running containerized workloads in production and nearly 15% of total workloads run on containers today.

Despite the apparent progress and the continued industry consolidation, the container ecosystem continues to be fragmented and fast paced. This makes it difficult for EAs and CTOs to build robust cloud-native architectures and institute operational governance. Containers are not a monolithic technology; however, the ecosystem is a hodge podge of several components vital for production readiness. The key technology categories of a container ecosystem are summarized in Figure 1.

Figure 1: Cloud-Native Container Ecosystem



Source: Gartner
785512_C

Gartner

Impacts and Recommendations

Proliferating Container Platform Technologies Have Created an Ecosystem of Open-Source Projects, Products and Vendors

The containerized platform architecture has several components. At its foundation is a container runtime that enables developers to deploy applications, configurations and other dependencies in a container image. The most common container engines are containerd (originated from Docker) and CRI-O. There are upcoming technologies such as WebAssembly runtime (Wasm) that can augment or even replace container runtime for specific use cases such as edge deployments.

Container orchestrators include capabilities for policy-based deployment, managing application configuration, ensuring highly available cluster resources and integrated containers with the rest of IT infrastructure tools. The most common orchestrators are Kubernetes (which is the most widely deployed and supported) and Amazon Elastic Container Service (Amazon ECS), while HashiCorp's Nomad has limited traction in the enterprise.

Container management platform vendors such as Amazon Web Services (AWS), Microsoft, Google, Red Hat, SUSE, (Rancher) and VMware take this to the next level. They provide management console, automation features, and operational, security and developer tools (and most of the technologies listed in Table 1). They integrate many components vital for running containerized workloads in production.

The Cloud Native Computing Foundation (CNCF) is the governance body that hosts several of the open-source projects in this space. Table 1 summarizes the key architectural components of platform engineering tools for Kubernetes (beyond container runtime and orchestrators), so that EAs and CTOs are aware of the choices for making informed decisions. The table includes open-source projects and pure-play vendors only. More detailed comparison of container management platform vendors are provided in the subsequent section.

Table 1: Container Management Platform Components

(Enlarged table in Appendix)

Container Technology/ Market Category	What It Is	Key OSS Projects	Key Pure-Play Vendors and Startups
Networking	Software that manages communication inside the container pod, between container clusters, and from the outside world. Incumbent network vendors and cloud service providers (CSPs) offer CNI plug-ins that integrate with their cloud platform and networking products and offer capabilities such as policy management and multitenancy.	Antrea, Project Calico, CNCF (Container Network Interface [CNI]), Cilium, Open vSwitch	Cisco, Juniper Networks, Tigera, Isovalent
Storage	Container native storage products deliver granular data services, high availability and performance for stateful applications with deep integration with the container management systems.	Container Storage Interface (CSI), Longhorn, OpenEBS, Rook, Velero	Datacore (MayaData), Diamanti, Hammerspace, ionir, MinIO, NetApp, Nutanix, Ondat, Pure Storage (Portworx), Rakuten Symphony (Robin.io), Trilio, Veeam (Kasten)
Ingress control	This component functions as the network communications gatekeeper of a container orchestration cluster. All inbound traffic to services running inside the cluster must pass through the ingress gateway.	Envoy, Contour, Traefik Labs	Citrix, F5 (NGINX), HAProxy, Traefik Labs, Solo.io
Observability	Observability tools enable a skilled observer — a software developer or site reliability engineer (SRE) — to effectively explain unexpected system behavior.	Elastic (Elastic Stack), Fluentd, Grafana, Jaeger, Kiali, OpenTelemetry, OpenTracing, Prometheus, Zipkin	Chronosphere; Cisco, Datadog, Dynatrace, Elastic (Elasticsearch), Grafana Labs, Honeycomb, CrowdStrike (Humio), Instana, Lightstep, New Relic, Splunk, Sysdig
FinOps	FinOps tools enable adequate financial governance, cost anomaly detection, budgeting and cost-optimization to cloud-native environments.	OpenCost	Cast AI, Cisco (Opsani), Densify, Finout, IBM (Turbonomic), Kubecost, NetApp (Spot), PerfectScale
Security and Compliance	Container security starts in development with an assessment of the risk/trust of the content of the container, secrets management and Kubernetes configuration assessment. It also extends into production with runtime container threat protection and access control.	Clair, Cloud Custodian, Falco, Kyverno, Notary, Vault, Aqua Trivy, Secure Production Identity Framework for Everyone (SPIFFE), SPIFFE Runtime Environment (SPIRE)	Anchore, Aqua Security, Cisco (Portshift), Lacework, Nirmata, Palo Alto Networks, Rapid7, Snyk, Stackrox, Sysdig, Tigera, Trend Micro
Policy-Based Management	Policy-based management tools allow IT organizations to express IT requirements programmatically, which is critical for ephemeral, container-based environments. The automation toolchain can then enforce these policies automatically.	Open Policy Agent (OPA), Gatekeeper	HashiCorp, Progress (Chef), Pulumi, Styra, Sysdig
Registry	Container images and associated deployment manifests need to be managed and version-controlled. Registry services offered by public cloud providers are fully managed, while private registries incur greater management overhead, but they can reside in a private network, typically resulting in better performance than you would expect from a remote registry.	Harbor, Project Quay	Docker, GitLab, JFrog, Sonatype
Infrastructure as Code (IaC)	IaC is the creation, provisioning and configuration of compute, network and storage infrastructure as source code. IaC is a foundational requirement to scale infrastructure automation in containerized environments.	Ansible, Chef, Crossplane, Puppet, SaltStack, Terraform	HashiCorp, Progress (Chef), Pulumi, Puppet, Turbot, Upbound
Continuous Integration/Continuous Delivery (CI/CD)	The CI/CD approach enables DevOps teams to create an automated pipeline for producing software in short cycles.	Argo, Concourse, Flux, Jenkins, Jenkins X, Tekton, Spinnaker	Akuity, Atlassian, CircleCI, CloudBees, Codefresh, GitHub, GitLab, Harness, HashiCorp, Idera, Travis CI, CircleCI (Vamp), Weaveworks
API Gateway	API gateways enforce policies around operational management, security, format translation and analytics for the collection of business and technical metrics associated with API use.	Ambassador, Gloo Edge, WSO2	Google (Apigee API Management), Kong, Salesforce (MuleSoft), Solo.io, Tyk
Service Mesh	Service mesh is a distributed computing middleware that optimizes communications among application services, especially in microservices architecture. Microservices require a distributed middleware that optimizes service-to-service communications (e.g., dynamic discovery and self-healing connections) in a secure, dynamic and reliable fashion, which is what service mesh enables.	Istio, Linkerd, Open Service Mesh, Zuul, Service Mesh Interface, Kuma, HashiCorp Consul	Buoyant, F5, greymatter.io, HashiCorp, Isovalent, Kong, Solo.io, Tetrate, Traefik Labs.

Source: Gartner (March 2023)

Recommendations:

- Map your functional requirements to the container management platforms and identify any gaps that can be potentially filled by open-source projects and commercial products outlined in this research for effective deployments.
- Choose open-source projects carefully, based on software release history, permissiveness of software licensing terms, and vibrancy of community, characterized by a broad ecosystem of vendors that provide commercial maintenance and support.

- Reduce the risks of working with startups by evaluating their viability and through constant communications and feedback to them on product quality, support issues and functionalities desired. Startups can deliver innovation in advance of established vendors, but carry risks.

With Broadened Portfolios, Kubernetes Platform Vendors Are Making Diverse Bets Across the Technology Stack and Use Cases

Several components make up a container platform. Large vendors integrate these components as a cohesive unit. There are two main types of container platform vendors:

- Hyperscale cloud providers offer integrated cloud infrastructure and platform services (CIPS) capabilities that allow users to develop and operate cloud-native applications with a unified environment. Almost all of these providers can deliver an effective experience within their platforms, including some use cases of hybrid cloud and edge. They also offer multicloud solutions to cater to growing customer needs beyond a single provider environment. Key cloud providers include Alibaba Cloud, AWS, Google Cloud, Microsoft Azure, Oracle Cloud, IBM Cloud and Tencent.
- Software vendors offer platform software that can be used to deploy a private IT or public cloud service. Vendors in this category offer on-premises, edge solutions and may offer either marketplace or managed services offerings in multiple public cloud environments. Key software vendors include Red Hat, VMware, SUSE (Rancher), D2iQ, Mirantis, HashiCorp (Nomad), Hewlett Packard Enterprise (HPE), Kubermatic and Spectro Cloud. There are managed service provider-style offerings here from vendors such as Giant Swarm, Platform9 and Rafay Systems.

The following factors are becoming critical determinants in choosing the right platform provider:

- Automated, secure and distributed operations
    - Hybrid and multicloud
    - Edge optimization
    - Support for bare metal
    - Serverless containers
    - Security and compliance

- Application modernization
  - Developer inner and outer loop tools
  - Service mesh support
- Open-source commitment
- Pricing

The container platform vendors outlined in Table 2 are the most commonly referenced ones in Gartner client inquiries. Hence, we provide a more detailed comparison.

Table 2: Container Platform Vendors

(Enlarged table in Appendix)

Selection Factor	AWS	Google Cloud	Microsoft Azure	Red Hat (IBM)	SUSE (Rancher)	VMware
On-Premises	Amazon ECS Anywhere, Amazon Elastic Kubernetes Service (Amazon EKS) Anywhere, Amazon EKS Distro (self-supported), Amazon ECS/ Amazon EKS on AWS Outposts	Anthos, Google Distributed Cloud Hosted	Azure Kubernetes Service (AKS) on Azure Stack Hub and AKS on Azure Stack HCI	OpenShift subscriptions — Red Hat OpenShift Kubernetes Engine, OCP and Red Hat OpenShift Platform Plus; Red Hat OpenShift on IBM Cloud Satellite	Rancher Kubernetes Engine (RKE)	VMware Tanzu for Kubernetes Operations; VMware Tanzu Application Platform
Multicluster Management for Hybrid Cloud	Amazon ECS Anywhere; Amazon EKS Anywhere	Anthos Fleet multicluster management, Anthos Config Management	Azure Arc	Red Hat Advanced Cluster Management for Kubernetes	Rancher	Tanzu Mission Control
Multicloud	Amazon EKS Distro (self-supported)	Multicloud support for Anthos on AWS, Anthos on Azure, Anthos on VMware and bare-metal. In addition, management support for EKS, AKS clusters	Azure Arc-enabled Kubernetes supports conformant Kubernetes clusters, including managed services running in other clouds (Amazon EKS and GKE) Certified support for Kubernetes distributions from Canonical, Kublr, Mirantis, Nutanix, SUSE Rancher, Red Hat, VMware, and Wind River	OpenShift Dedicated on AWS and Google Cloud Platform (GCP); native managed service on AWS and Azure (ROSA and ARO); Red Hat Advanced Cluster Management for Kubernetes supports EKS, IBM Cloud Kubernetes Service (IKS), AKS, and GKE as well as OpenShift-based managed services	Cluster life cycle management for RKE, EKS, AKS, GKE, Alibaba Cloud Container Service for Kubernetes (ACK), Tencent Kubernetes Engine (TKE), and Huawei Cloud Container Engine (CCE) clusters	Support for both own and conformant Kubernetes clusters including EKS, AKS, GKE and OpenShift clusters
Managed Cloud Services	Amazon ECS; Amazon EKS; Red Hat OpenShift Service on AWS (ROSA)	Google Kubernetes Engine (GKE)	AKS; Azure Red Hat OpenShift (ARO)	ARO, ROSA; Red Hat OpenShift on IBM Cloud; OpenShift Dedicated on AWS and GCP	Hosted Rancher provides managed Rancher Management Server	VMware Cloud with Tanzu services
Edge	AWS IoT Greengrass; Amazon ECS/ Amazon EKS on AWS Wavelength; Amazon ECS/ Amazon EKS Anywhere; Amazon EKS Anywhere on Snow	Anthos at Edge; Anthos on Google Distributed Cloud Edge	Azure IoT Edge	OpenShift — single node, three-node, remote worker node configuration; MicroShift (preview)	K3s (lightweight distribution for edge)	Tanzu for Kubernetes Operations can be deployed on edge
Bare-Metal Support	Yes	Anthos clusters on bare metal	Yes on Azure Arc	Yes	Yes	No Kubernetes runtime provided, but bare-metal management on Tanzu Mission Control (TMC)
Serverless Containers	AWS Fargate	Cloud Run; GKE Autopilot	Azure Container Instances (ACI), Azure Container Apps	Red Hat OpenShift Serverless	N/A	Cloud Native Runtimes for Tanzu
Security and Compliance	Security in Amazon EKS; security in Amazon ECS; Center for Internet Security (CIS) Amazon EKS Benchmark	GKE security overview, securing Cloud Run, GKE Sandbox, CIS GKE Benchmark	Azure security baseline for Azure Kubernetes Service; CIS AKS Benchmark	OpenShift Container Platform security and compliance; Red Hat Advanced Cluster Security for Kubernetes; CIS Benchmark for OpenShift Container Platform	Rancher security, SUSE NeuVector, CIS Benchmark Rancher	VMware Tanzu Kubernetes Grid security overview; vSphere with Tanzu Security; Security Measures in VMware Tanzu Mission Control; Compliance Scanner for VMware Tanzu
Dev Tools	AWS Marketplace, AWS CodeBuild, AWS CodeCommit, AWS CodePipeline, AWS Copilot, AWS CodeDeploy	Cloud Marketplace, Cloud Build, Cloud Code (IDE for K8S Apps), and Google Cloud Deploy	Marketplace, Azure DevOps, GitHub Actions for AKS, support for major IDE engines	Developer console, CodeReady Workspaces (IDE), Red Hat Runtimes, Red Hat Marketplace, OpenShift Pipelines and OpenShift GitOps	App catalog, Fleet (GitOps CD)	VMware Marketplace, Tanzu Build Service, Tanzu Data Services, Spring Cloud Services
Service Mesh	AWS App Mesh — Envoy based; Hosted control plane (proprietary)	Anthos Service Mesh (Envoy and Istio based) — available on Anthos and GCP	Open Service Mesh AKS add-on	OpenShift Service Mesh (Istio and Envoy-based)	Istio	Tanzu Service Mesh (Envoy and Istio-based)
Open Source	Amazon ECS is proprietary, Amazon EKS is CNCF conformant. Amazon EKS Distro is an OSS distribution but AWS doesn't provide direct support	CNCF conformant distribution	CNCF conformant distribution	CNCF conformant and upstream release is OKD available under Apache License 2.0.	CNCF conformant and fully open source under Apache License 2.0	CNCF conformant distribution
Pricing	10 cents per hour per cluster (Amazon EKS);Free (Amazon ECS)	10 cents per hour per cluster (GKE)	Free, or 10 cents per hour per cluster with uptime SLA option (AKS)	Tiered, per core, per year (per month also available for public cloud use)	Per node, per year	Per core or CPU, per year

Source: Gartner (March 2023)

Recommendations:

- Strive to standardize on a consistent platform, to the extent possible across use cases, to enhance architectural consistency, democratize operational know-how, simplify developer workflow and provide sourcing advantages.
- Create a weighted decision matrix by considering the factors outlined above to ensure an objective decision is made.
- Prioritize developers' needs and their inherent expectations of operational simplicity, because any decision that fails to prioritize the needs of developers is bound to fail.

Evidence

[1] Detailed briefings were conducted with most vendors represented in this research. In addition, the co-authors handled more than 1,000 client inquiries and other interactions on this topic during the past 12 months.

Document Revision History

The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem - 18 August 2021

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

CTOs' Guide to Containers and Kubernetes — Answering the Top 10 FAQs

How to Run Containers and Kubernetes in Production

Market Guide for Container Management

How to Scale DevOps Workflows in Multicluster Kubernetes Environments

Quick Answer: Cloud, Kubernetes, SaaS — What's the Best Security Posture Management for Your Cloud?

A CTO's Guide to Serverless Computing

Table 1: Container Management Platform Components

Container Technology/Market Category	What It Is	Key OSS Projects	Key Pure-Play Vendors and Startups
Networking	Software that manages communication inside the container pod, between container clusters, and from the outside world. Incumbent network vendors and cloud service providers (CSPs) offer CNI plug-ins that integrate with their cloud platform and networking products and offer capabilities such as policy management and multitenancy.	Antrea, Project Calico, CNCF (Container Network Interface [CNI]), Cilium, Open vSwitch	Cisco, Juniper Networks, Tigera, Isovalent
Storage	Container native storage products deliver granular data services, high availability and performance for stateful applications with deep integration with the container management systems.	Container Storage Interface (CSI), Longhorn, OpenEBS, Rook, Velero	Datacore (MayaData), Diamanti, Hammerspace, ionir, MinIO, NetApp, Nutanix, Ondat, Pure Storage (Portworx), Rakuten Symphony (Robin.io), Trilio, Veeam (Kasten)
Ingress control	This component functions as the network communications gatekeeper of a container orchestration cluster. All inbound traffic to services running	Envoy, Contour, Traefik Labs	Citrix, F5 (NGINX), HAProxy, Traefik Labs, Solo.io

	inside the cluster must pass through the ingress gateway.		
Observability	Observability tools enable a skilled observer — a software developer or site reliability engineer (SRE) — to effectively explain unexpected system behavior.	Elastic (Elastic Stack), Fluentd, Grafana, Jaeger, Kiali, OpenTelemetry, OpenTracing, Prometheus, Zipkin	Chronosphere, Cisco, Datadog, Dynatrace, Elastic (Elasticsearch), Grafana Labs, Honeycomb, CrowdStrike (Humio), Instana, Lightstep, New Relic, Splunk, Sysdig
FinOps	FinOps tools enable adequate financial governance, cost anomaly detection, budgeting and cost-optimization to cloud-native environments.	OpenCost	Cast AI, Cisco (Opsani), Densify, Finout, IBM (Turbonomic), Kubecost, NetApp (Spot), PerfectScale
Security and Compliance	Container security starts in development with an assessment of the risk/trust of the content of the container, secrets management and Kubernetes configuration assessment. It also extends into production with runtime container threat protection and access control.	Clair, Cloud Custodian, Falco, Kyverno, Notary, Vault, Aqua Trivy, Secure Production Identity Framework for Everyone (SPIFFE), SPIFFE Runtime Environment (SPIRE)	Anchore, Aqua Security, Cisco (Portshift), Lacework, Nirmata, Palo Alto Networks, Rapid7, Snyk, Stacklet, Sysdig, Tigera, Trend Micro
Policy-Based Management	Policy-based management tools allow IT organizations to express IT requirements programmatically, which is critical for ephemeral, container-based environments. The	Open Policy Agent (OPA), Gatekeeper	HashiCorp, Progress (Chef), Pulumi, Styra, Sysdig

	automation toolchain can then enforce these policies automatically.		
Registry	Container images and associated deployment manifests need to be managed and version-controlled. Registry services offered by public cloud providers are fully managed, while private registries incur greater management overhead, but they can reside in a private network, typically resulting in better performance than you would expect from a remote registry.	Harbor, Project Quay	Docker, GitLab, JFrog, Sonatype
Infrastructure as Code (IaC)	IaC is the creation, provisioning and configuration of compute, network and storage infrastructure as source code. IaC is a foundational requirement to scale infrastructure automation in containerized environments.	Ansible, Chef, Crossplane, Puppet, SaltStack, Terraform	HashiCorp, Progress (Chef), Pulumi, Puppet, Turbot, Upbound
Continuous Integration/Continuous Delivery (CI/CD)	The CI/CD approach enables DevOps teams to create an automated pipeline for producing software in short cycles.	Argo, Concourse, Flux, Jenkins, Jenkins X, Tekton, Spinnaker	Akuity, Atlassian, CircleCI, CloudBees, Codefresh, GitHub, GitLab, Harness, HashiCorp, Idera, Travis CI, CircleCI (Vamp), Weaveworks
API Gateway	API gateways enforce policies around operational management, security,	Ambassador, Gloo Edge, WSO2	Google (Apigee API Management), Kong, Salesforce (MuleSoft), Solo.io,

	format translation and analytics for the collection of business and technical metrics associated with API use.		Tyk
Service Mesh	Service mesh is a distributed computing middleware that optimizes communications among application services, especially in microservices architecture. Microservices require a distributed middleware that optimizes service-to-service communications (e.g., dynamic discovery and self-healing connections) in a secure, dynamic and reliable fashion, which is what service mesh enables.	Istio, Linkerd, Open Service Mesh, Zuul, Service Mesh Interface, Kuma, HashiCorp Consul	Buoyant, F5, greymatter.io, HashiCorp, Isovalent, Kong, Solo.io, Tetrate, Traefik Labs.

Source: Gartner (March 2023)

Table 2: Container Platform Vendors

Selection Factor	AWS	Google Cloud	Microsoft Azure	Red Hat (IBM)	SUSE (Rancher)	VMware
On-Premises	Amazon ECS Anywhere; Amazon Elastic Kubernetes Service (Amazon EKS) Anywhere; Amazon EKS Distro (self-supported); Amazon ECS/Amazon EKS on AWS Outposts	Anthos; Google Distributed Cloud Hosted	Azure Kubernetes Service (AKS) on Azure Stack Hub and AKS on Azure Stack HCI	OpenShift subscriptions — Red Hat OpenShift Kubernetes Engine, OCP and Red Hat OpenShift Platform Plus; Red Hat OpenShift on IBM Cloud Satellite	Rancher Kubernetes Engine (RKE)	VMware Tanzu for Kubernetes Operations; VMware Tanzu Application Platform
Multicluster Management for Hybrid Cloud	Amazon ECS Anywhere; Amazon EKS Anywhere	Anthos Fleet multicluster management, Anthos Config Management	Azure Arc	Red Hat Advanced Cluster Management for Kubernetes	Rancher	Tanzu Mission Control
Multicloud	Amazon EKS Distro (self-supported)	Multicloud support for Anthos on AWS, Anthos on Azure, Anthos on VMware and bare-metal. In addition, management	Azure Arc-enabled Kubernetes supports conformant Kubernetes clusters, including managed services running in other clouds	OpenShift Dedicated on AWS and Google Cloud Platform (GCP); native managed service on AWS and Azure (ROSA and ARO);	Cluster life cycle management for RKE, EKS, AKS, GKE, Alibaba Cloud Container Service for Kubernetes (ACK), Tencent Kubernetes	Support for both own and conformant Kubernetes clusters including EKS, AKS, GKE and OpenShift clusters

		support for EKS, AKS clusters	(Amazon EKS and GKE). Certified support for Kubernetes distributions from Canonical, Kublr, Mirantis, Nutanix, SUSE Rancher, Red Hat, VMware, and Wind River	Red Hat Advanced Cluster Management for Kubernetes supports EKS, IBM Cloud Kubernetes Service (IKS), AKS, and GKE as well as OpenShift-based managed services	Engine (TKE), and Huawei Cloud Container Engine (CCE) clusters	
Managed Cloud Services	Amazon ECS; Amazon EKS; Red Hat OpenShift Service on AWS (ROSA)	Google Kubernetes Engine (GKE)	AKS; Azure Red Hat OpenShift (ARO)	ARO; ROSA; Red Hat OpenShift on IBM Cloud; OpenShift Dedicated on AWS and GCP	Hosted Rancher provides managed Rancher Management Server	VMware Cloud with Tanzu services
Edge	AWS IoT Greengrass; Amazon ECS/Amazon EKS on AWS Wavelength; Amazon ECS/Amazon EKS Anywhere; Amazon EKS Anywhere on Snow	Anthos at Edge; Anthos on Google Distributed Cloud Edge	Azure IoT Edge	OpenShift — single node, three-node, remote worker node configuration; MicroShift (preview)	K3s (lightweight distribution for edge)	Tanzu for Kubernetes Operations can be deployed on edge
Bare-Metal Support	Yes	Anthos clusters on	Yes on Azure Arc	Yes	Yes	No Kubernetes

		bare metal				runtime provided, but bare-metal management on Tanzu Mission Control (TMC).
Serverless Containers	AWS Fargate	Cloud Run; GKE Autopilot	Azure Container Instances (ACI), Azure Container Apps	Red Hat OpenShift Serverless	N/A	Cloud Native Runtimes for Tanzu
Security and Compliance	Security in Amazon EKS; security in Amazon ECS; Center for Internet Security (CIS) Amazon EKS Benchmark	GKE security overview; securing Cloud Run; GKE Sandbox; CIS GKE Benchmark	Azure security baseline for Azure Kubernetes Service; CIS AKS Benchmark	OpenShift Container Platform security and compliance; Red Hat Advanced Cluster Security for Kubernetes; CIS Benchmark for OpenShift Container Platform	Rancher security; SUSE NeuVector; CIS Benchmark Rancher	VMware Tanzu Kubernetes Grid security overview; vSphere with Tanzu Security; Security Measures in VMware Tanzu Mission Control; Compliance Scanner for VMware Tanzu
Dev Tools	AWS Marketplace, AWS CodeBuild, AWS CodeCommit, AWS CodePipeline, AWS Copilot, AWS CodeDeploy	Cloud Marketplace, Cloud Build, Cloud Code (IDE for K8S Apps), and Google Cloud Deploy	Marketplace, Azure DevOps, GitHub Actions for AKS, support for major IDE engines	Developer console, CodeReady Workspaces (IDE), Red Hat Runtimes, Red Hat Marketplace, OpenShift Pipelines	App catalog, Fleet (GitOps CD)	VMware Marketplace, Tanzu Build Service, Tanzu Data Services, Spring Cloud Services

				and OpenShift GitOps		
Service Mesh	AWS App Mesh — Envoy based; Hosted control plane (proprietary)	Anthos Service Mesh (Envoy and Istio based) — available on Anthos and GCP	Open Service Mesh AKS add-on	OpenShift Service Mesh (Istio and Envoy-based)	Istio	Tanzu Service Mesh (Envoy and Istio-based)
Open Source	Amazon ECS is proprietary; Amazon EKS is CNCF conformant. Amazon EKS Distro is an OSS distribution but AWS doesn't provide direct support	CNCF conformant distribution	CNCF conformant distribution	CNCF conformant and upstream release is OKD available under Apache License 2.0.	CNCF conformant and fully open source under Apache License 2.0	CNCF conformant distribution
Pricing	10 cents per hour per cluster (Amazon EKS)/Free (Amazon ECS)	10 cents per hour per cluster (GKE)	Free, or 10 cents per hour per cluster with uptime SLA option (AKS)	Tiered, per core, per year (per month also available for public cloud use)	Per node, per year	Per core or CPU, per year

Source: Gartner (March 2023)