The Rise of Cloud-Native Apps

Report finds that most organizations are adopting cloud-native apps, Kubernetes and microservices but struggle to secure and operate these complex environments

EXECUTIVE SUMMARY

More and more organizations are adopting cloud-native apps. They provide major benefits, including quicker app development, greater scalability and less vendor lock-in. This survey found that nearly nine in ten respondents are actively using or have started using cloud-native apps today to leverage these benefits. As part of this transition, these organizations are also increasingly leveraging Kubernetes and microservices, which are critical components of highly distributed, cloud-native environments.

However, the growing adoption of cloud-native apps, Kubernetes and microservices has introduced major operational challenges that organizations aren't equipped to solve. Enterprises embracing these three technologies struggle the most with security, putting their businesses at risk. Security challenges are followed closely by networking challenges – namely, connecting distributed clusters and workloads. Both challenges are increasing teams' operational complexity.

Methodology

The survey, conducted by research firm Propeller Insights, polled over 300 IT decision makers across the U.S. Overall, 83% of respondents work at mid-market sized companies that employ between 500–5,000 staff, while the remaining 16.8% work at large enterprises with over 5,000 employees. The vast majority of respondents (89%) work in DevOps, infrastructure and operations or as part of an application team.

Respondents indicate that cloud-native apps and Kubernetes are particularly difficult to secure and connect because of the growing number of APIs and microservices they incorporate, which make apps more distributed and harder to protect.

Key findings include:

- Cloud-native app adoption has become mainstream, with 86% of respondents saying their organization is actively using or have started using cloud-native apps today.
- While over half of organizations are using Kubernetes in some capacity, security and networking challenges are preventing them from using Kubernetes widely across business apps, with only 10% of organizations running half or more of their business apps on it.
- DevOps teams shoulder most of the burden of planning and managing Kubernetes infrastructure and operations: 67% of respondents say DevOps is responsible for choosing networking and security solutions for their Kubernetes environments, while 63% say DevOps is responsible for managing those operations.
- Security and connectivity challenges are also preventing organizations from using microservices for more of their business apps: 57% of respondents say that less than 10% of all their business apps are based on microservices architecture, while 88% say that less than 25% of business apps are based on it.
- Most organizations (58%) say the growing volume of APIs in modern cloud-native apps is causing them problems. Respondents highlighted security as the top challenge resulting from this API sprawl.

CLOUD-NATIVE APP ADOPTION

The overwhelming majority of respondents (86%) say their organization is actively using or have started using cloud native apps today.

Kubernetes is a common component of cloud-native environments, and it brings its own unique operational challenges. In addition, cloud-native apps also rely heavily on microservices architectures and use far more APIs than traditional monolithic apps. The growth of microservices and APIs make cloud-native apps more distributed, complicating their security and networking.

Organizations have to dedicate considerable staff and other resources to manage these complex modern app environments: 68% of respondents say their company uses more than 10 employees to manage Kubernetes environments, app deployments and security policy.

Cloud-native environments are also extremely fast-paced. Over half of these teams (61%) must deliver more than 5 new services per year. These figures are significant given that 83% of respondents work at mid-market sized enterprises.

KUBERNETES ADOPTION

Even though over half of all organizations (56%) currently use Kubernetes in some way, the technology introduces challenges that prevent them from deploying Kubernetes-based apps broadly in production. Only 10% of organizations are running more than half of their business apps on Kubernetes.

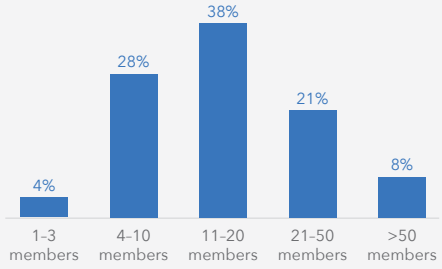
Kubernetes environments are rife with operational hurdles. Over three-quarters of respondents say that they struggle to meet required agility or timelines for activating clusters (76%) and to maintain security within or across clusters (76%). Furthermore, the majority say that maintaining required cluster availability (69%) and achieving required cluster performance (67%) are also key challenges.

These problems are slowing down organizations as they try to roll out new services in Kubernetes environments. Nearly half (43%) of organizations say operational complexity takes up a quarter or more of their time spent delivering a new service in a Kubernetes environment. In addition to slowing the delivery of new services, these challenges are also preventing organizations from deploying Kubernetes apps at high scale. Only 40% of organizations deploy a Kubernetes-based app across 25 or more clusters.

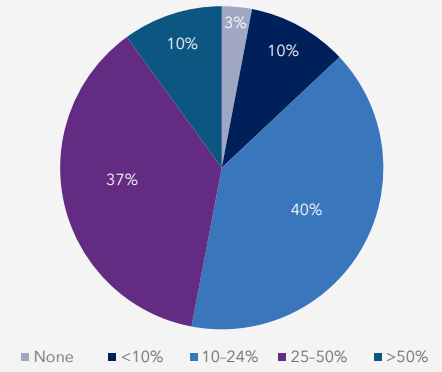
DevOps teams shoulder most of the burden of planning and managing all Kubernetes infrastructure and operations: 67% of respondents say DevOps is responsible for choosing networking and security solutions

86% of respondents leverage cloud-native apps

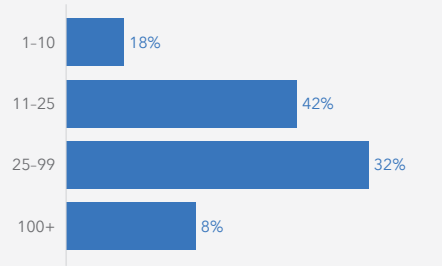
Q: How large is the team managing your Kubernetes environment, app deployments and security policy?



Q: What percent of your business apps are running in a Kubernetes environment?



Q: What is the average number of clusters used for each of your Kubernetes-based apps?



for their Kubernetes environments, while 63% say DevOps is responsible for managing those operations. These responsibilities make it harder for DevOps teams to focus on their primary role -- co-developing, delivering and managing applications to drive greater business value.

API SPRAWL

Due to their intricacy, cloud-native apps feature far more APIs than legacy apps. Many of these APIs are deeply embedded and hidden. Most organizations (58%) say the growing volume of APIs in modern cloud-native apps is causing them problems.

Above all, API sprawl is resulting in major security challenges. Nearly half of respondents (42%) struggle to secure access to their APIs, leaving their cloud-native apps vulnerable. When asked which challenges they face in securing APIs, over half of all respondents cited every one of the following five problems: discovering APIs (57%), learning how each API is used (59%), monitoring API access (57%), generating policies for accessing each API (57%) and securing sensitive information shared via APIs (57%).

In short, organizations struggle to detect, understand and control the APIs in their cloud-native apps. This problem is exasperated by the fact that nearly half of all organizations (42%) have no solution in production today for discovering and securing APIs. Like with Kubernetes, DevOps teams are tasked with addressing these issues. Almost half of respondents (48%) say that DevOps is responsible for all API security, placing further strain on these teams.

MICROSERVICES ADOPTION

Cloud-native apps rely heavily on microservices architectures. Microservices help make these apps more flexible, resilient and easier to deploy. Half of organizations (50%) are using or migrating to microservices for better agility.

However, like increasing APIs, microservices introduce serious security and network challenges. Respondents cited security as the number one challenge (40%) in supporting microservices-based apps, followed by difficulty in connecting microservices and clusters (34%). These issues are preventing organizations from using microservices for more of their business apps: 57% of respondents say that less than 10% of all their business apps are based on microservices architecture, while 88% say that less than 25% of business apps are based on microservices architecture.

Microservices and API growth are directly related, with use of the former driving an increase in the latter. Over half (53%) of organizations say their microservices-based apps use on average more than 25 APIs.

67%

of DevOps teams determine which solutions are selected and

63%

of DevOps teams deploys and operates

48%

have specified the DevOps team (in general) with defining API security policies

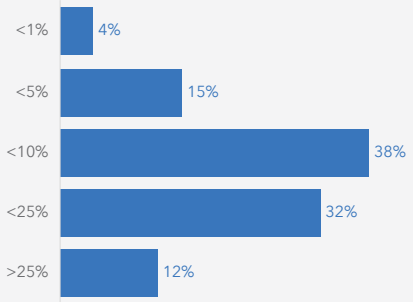
50%

are migrating to microservices because it increases their agility, while

29%

say they are migrating for access to libraries of existing microservices

Q: What percentage of your business applications are based on microservices?



MULTI-CLOUD ADOPTION

In addition to exploring trends and challenges associated with cloud-native apps, Kubernetes and microservices, the survey also looked at multi-cloud adoption. While cloud-native apps are difficult to manage, they're even harder to deploy across multiple clouds.

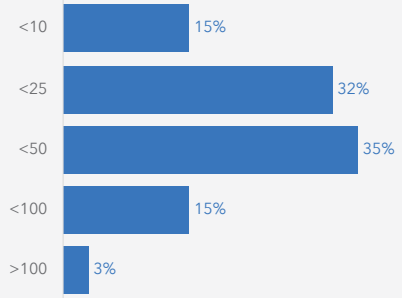
At a high level, the data reveals that multi-cloud momentum is real, with 75% of organizations deploying 20% of their cloud-hosted apps in multiple clouds and 40% deploying 30% or more of their cloud-hosted apps in multiple clouds. Of all organizations deploying apps in multiple clouds, 63% use three or more clouds.

Respondents say that they're mostly deploying databases (92%), analytics (84%) and artificial intelligence and machine learning (75%) workloads across multiple clouds. Broadly speaking, organizations are leveraging multi-cloud environments to maximize availability/reliability (89%), leverage best-of-breed services (79%) and for compliance reasons (75%).

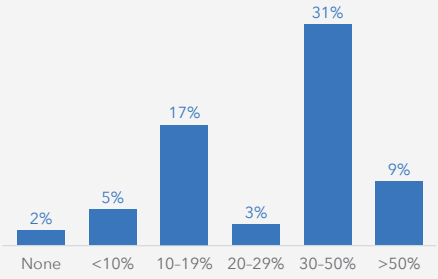
Like with cloud-native apps, Kubernetes and microservices, organizations managing multi-cloud deployments struggle primarily with security and connectivity challenges, as well as general operational challenges. Fifty-nine percent of organizations struggle with either achieving secure and reliable connectivity between providers or managing different platform services. Overall, 56% of respondents find it difficult to manage workloads across different cloud providers.

When connecting cloud providers across a shared workload, over 60% of respondents say that each of these five factors introduce challenges: security (89%), performance (78%), reliability (73%), cost (64%) and lack of managed services (64%).

Q: For the apps you've built using microservices, what is the average number of APIs per app?



Q: What percentage of your cloud-hosted apps (IaaS-based; not SaaS apps) are being deployed across multiple cloud providers?



44% of respondents find it difficult to manage workloads across multiple providers

"Updating all environments to make sure they all stay the same. In addition, the learning curve among cloud providers may cause some trouble."

"It sometimes becomes more complicated when we can't determine where is the problem. It causes delay in the service."

"The biggest challenge is to provide proper security."

"Cross-section of organizations about their adoption of cloud infrastructure."

"Several technical challenges related to the use of workloads across different cloud providers. Exhaustion, data lock in, etc."

"The biggest challenge is to get everyone to synchronize, but once you do, it's very easy to work that way."

"Mainly the challenge in management relationships among vendors and redesigning all cloud patterns."

"The biggest challenges are to manage the whole team."

"Learning how each cloud works since many have differing controls. We also like to see how some clouds perform differently with different info."

Over 70% of respondents say that security problems are exacerbated in multi-cloud environments by the differing security services between providers (77%), the growing number of APIs (75%), and the prevalence of microservices-based apps (72%). As noted earlier, the rise in cloud-native apps has resulted in an increase in the average number of APIs and microservices in each app, making them more difficult to secure.

CONCLUSION

An overwhelming majority of organizations are employing cloud-native apps today, and most of those organizations are using Kubernetes and microservices as part of those cloud-native environments. However, these organizations did not anticipate the operational hurdles -- mainly involving security and networking -- with these environments and are not equipped to fully address them. Put another way, as the app environment has changed, the challenges have changed. Cloud-native apps introduce more APIs and microservices, both of which drive security and networking problems.

A distributed cloud platform provides a new approach for addressing these new challenges. Modern cloud-native apps require equally modern cloud-native infrastructure. While there are a handful of services that address some of these problems, Volterra is the only company that solves all of them through a single, unified SaaS platform. Volterra's distributed cloud platform provides a comprehensive security and networking stack that includes all the tools needed for deploying, connecting, protecting and managing these apps, no matter how highly distributed they are. To learn more, visit Volterra.io.