VMware Tanzu®

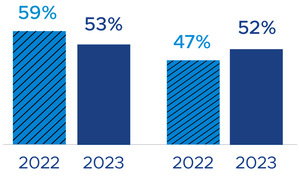
Securing Your Multi-Cloud Infrastructure

If you have security concerns, you're not alone.

97% of State of Kubernetes 2023 respondents reported ongoing security challenges

The focal point is shifting from ensuring security at the time of deployment to maintaining the security of multi-cloud over time. Deploying Kubernetes securely is getting easier, but concerns around maintaining it are growing.

Challenge: Meeting security and compliance requirements

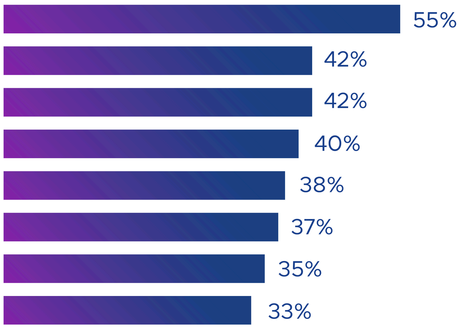


During deployment -6% YOY

Ongoing deployment +5% YOY

As organizations expand into more clouds, the risk of misconfigurations increases

Kubernetes security concerns



What can enterprises do to address security concerns?

Leverage security tools that operate efficiently across multi-cloud environments.

Embrace shift-left security

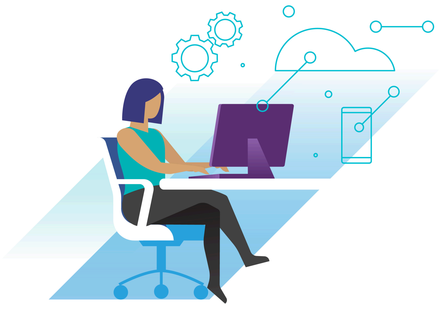
Provide secure software supply chains

Automate patching and container builds

Include a software bill of materials

Include other modern security practices

With cybercrime increasing every year, security teams are taking a more active role in Kubernetes operations—rather than leaving it up to developers and operators.



23% 2023

of respondents stated that security teams are getting involved.

15% 2021

stated that security teams had an active role in Kubernetes operations.

Most valued tools

53%

More than half of survey respondents said data security, protection and encryption is the most useful category of tools for Kubernetes in production.

48%

Nearly half of all stakeholders are willing to invest in paid support or services for security tools.

For more information on these trends and helpful security tools, read the 2023 State of Kubernetes report.