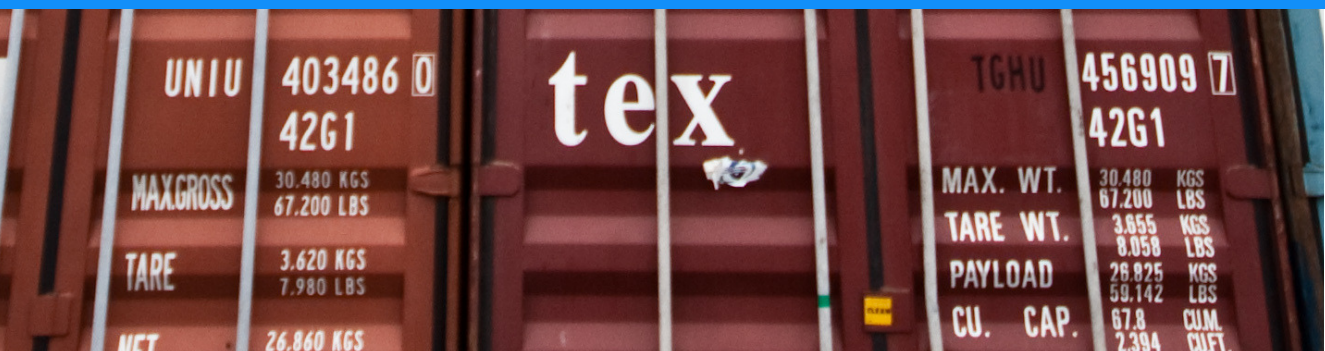




Snapshot of the Container Ecosystem

A survey on the current landscape of the tools and practices being deployed by container users today



APRIL 12, 2017 | ANCHORE.COM

anchore



anchore

We conducted a survey over 60 days that included 242 container users with varying levels of skill and different use cases and toolsets. The report below includes an overview of our findings and an analysis of the data.



anchore.com

Key Findings

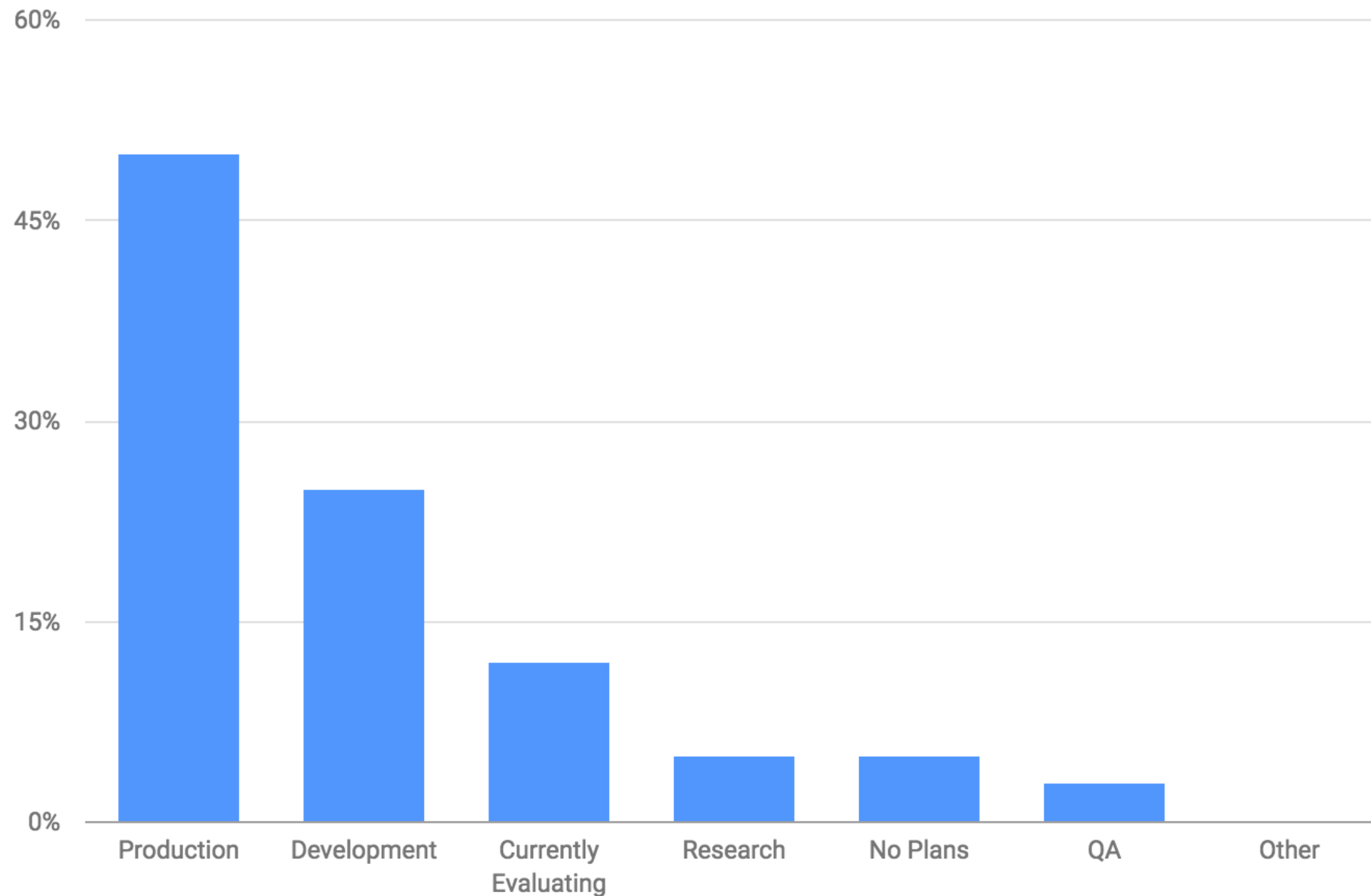
- Production usage of containers is incredibly high for a technology that is still relatively new, being less than 4 years old, with nearly half of respondents running containers in production and 85% actively deploying containers.
- The move from development use cases to production has been rapid and the continued drive towards micro-services and 12-Factor Applications has benefited Docker which offers a simplified approach compared to PaaS platforms.
- Public clouds, especially Amazon Web Services, remains the dominant deployment platform for Docker and Container workloads however we have seen a growth in both on-premises and hybrid deployment models.
- Unsurprisingly Docker Engine remains the most popular runtime platform with the majority of users deploying the Community Edition or Docker Engine provided by their Linux distribution. Monetization of the Container ecosystem remains challenging at the core infrastructure layer with most of the spend occurring higher up the stack at the monitoring, orchestration or security layer.

Key Findings

- Jenkins continues to lead the CI/CD market, once again the community edition far outpaces the commercial Jenkins offering and other paid products. Compared to our last survey Jenkins community edition appears to be gaining share.
- Kubernetes is beginning to take a clear lead in the Orchestration space, adding in the deployments of CoreOS Tectonic and Red Hat OpenShift. Docker Swarm continues to be popular with developers due to its simplicity and the recent inclusion of Swarm within the core Docker Engine has continued that trend.
- Security and governance remain a concern for enterprise users however only half of the respondents have implemented container scanning and of the production deployments only 25% have performed image analysis and inspection.
- Organizations are struggling to apply their existing governance and policies to containers however the majority are looking to address this gap and these organizations are looking for more than just simple CVE based scanning.

How are you using containers today?

ANSWERED: 240



#1

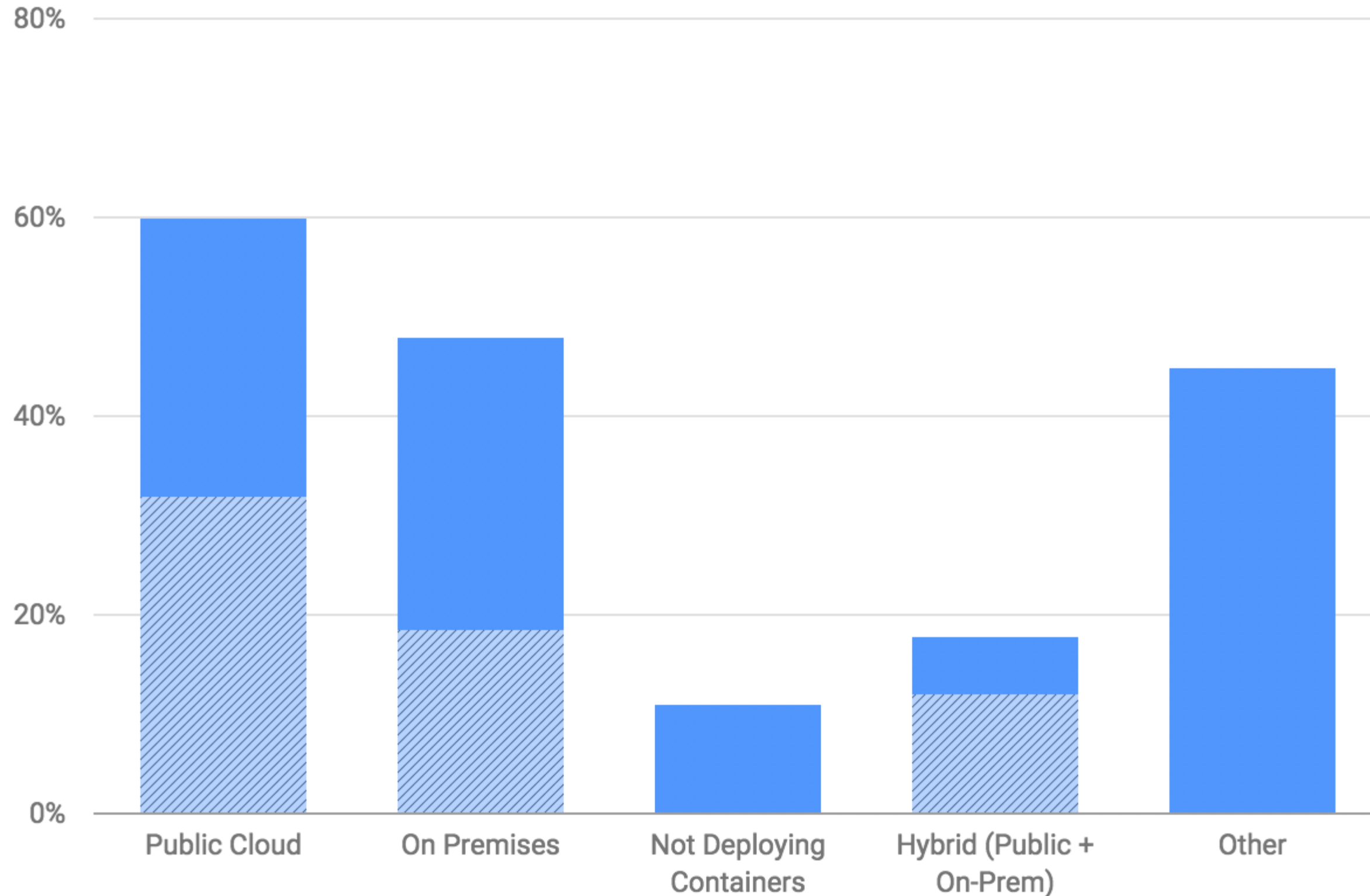
This year Docker celebrated its 4th birthday and with 85% respondents using Docker and over half of our users surveyed running Docker in production there's a lot to celebrate. Very few users today have no plans to run containers and those who are not yet in product are planning to deploy within the coming year.

anchore

Where are you deploying containers?

ANSWERED: 241

 Deploying Containers in Production



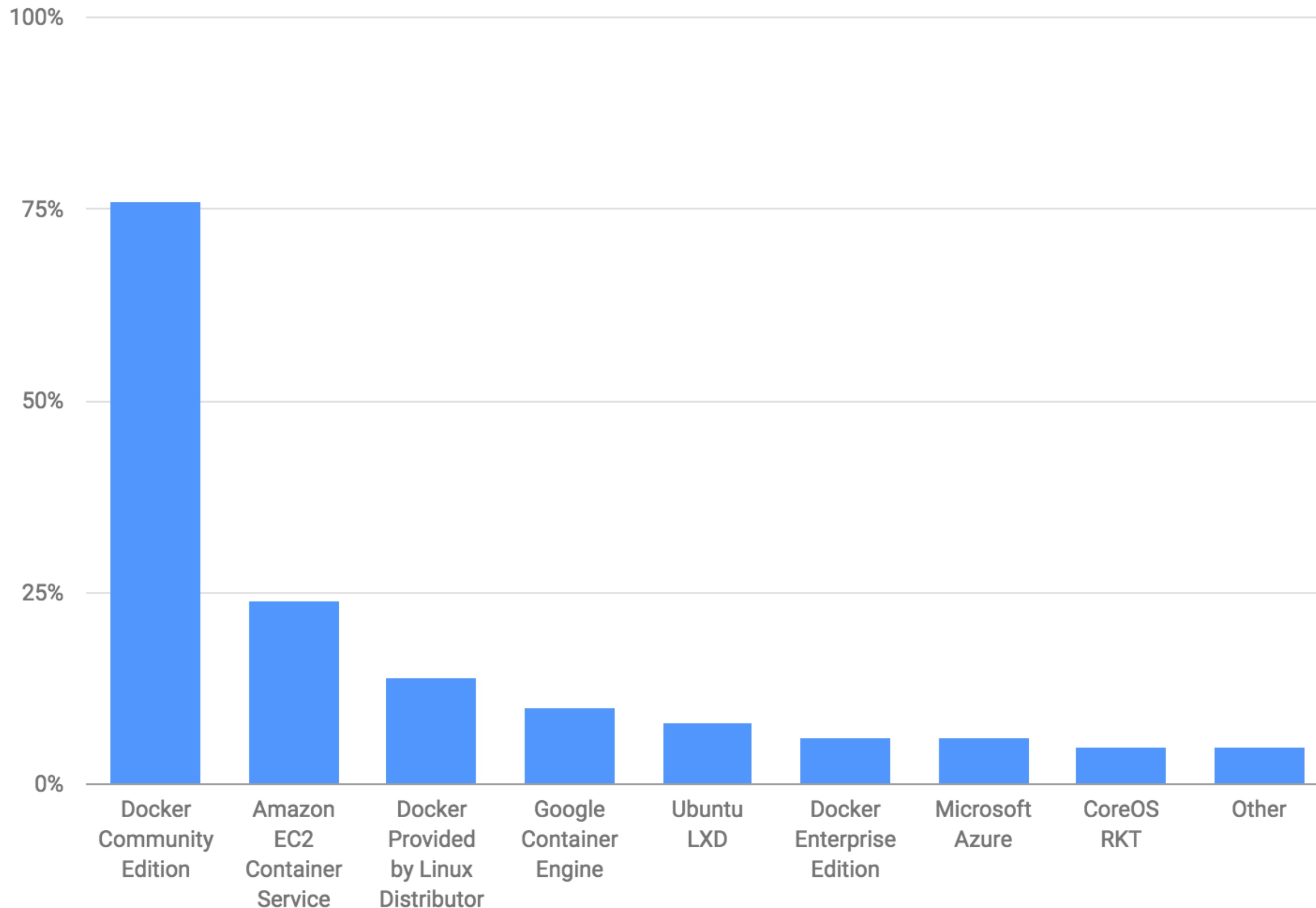
#2

Our previous survey results showed a focus on public cloud based deployments however on-prem and hybrid deployments are increasing as larger organizations are becoming more comfortable with container technologies. Containers continue to simplify deployment of applications and we expect to see the hybrid deployment numbers rise as it becomes easier to move workloads from on-prem to the cloud.

anchore

What container runtime are you using?

ANSWERED: 241



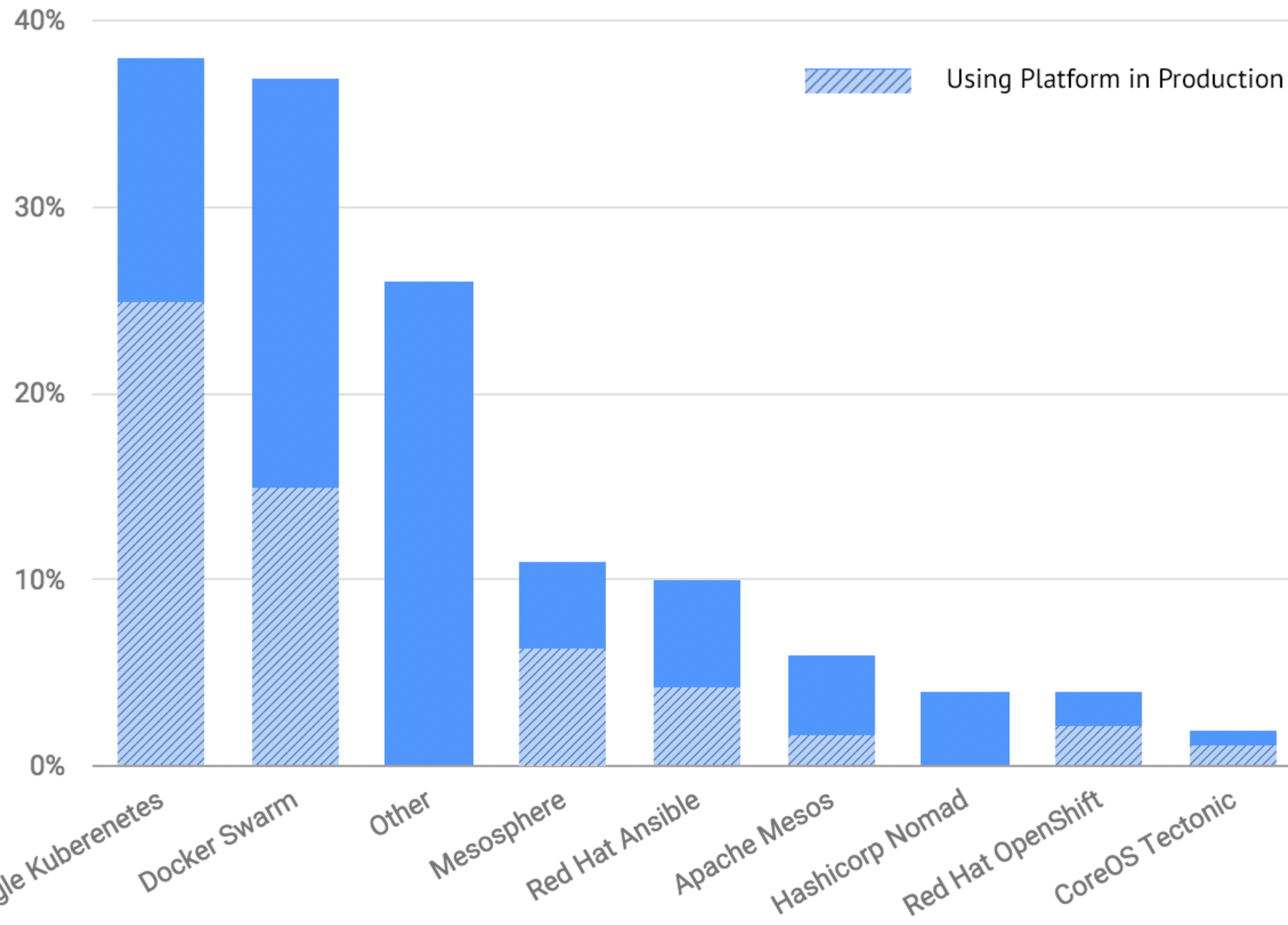
#3

Monetization continues to be a huge challenge for open source vendors especially as organizations become more comfortable with open source. Over half of the the respondents were running without a commercially supported container runtime. It is very common to see free Docker with free Linux on images built by free CI/CD systems. In all but the larger enterprises monetization happens further up the stack in monitoring, orchestration and security products.

anchore

What orchestration platform are you using?

ANSWERED: 241



#4

As the orchestration market matures Docker Swarm & Kubernetes dominate the market with Kubernetes taking the clear lead when you factor in the deployments of vendors such as Red Hat with OpenShift & CoreOS with Tectonic. The majority of Swarm deployments were for use in development, however the race is far from over & Docker's recent move to include Swarm with Docker Engine have helped increase adoption, especially among developers. Native cloud based orchestration including Amazon ECS continue to grow.

anchore

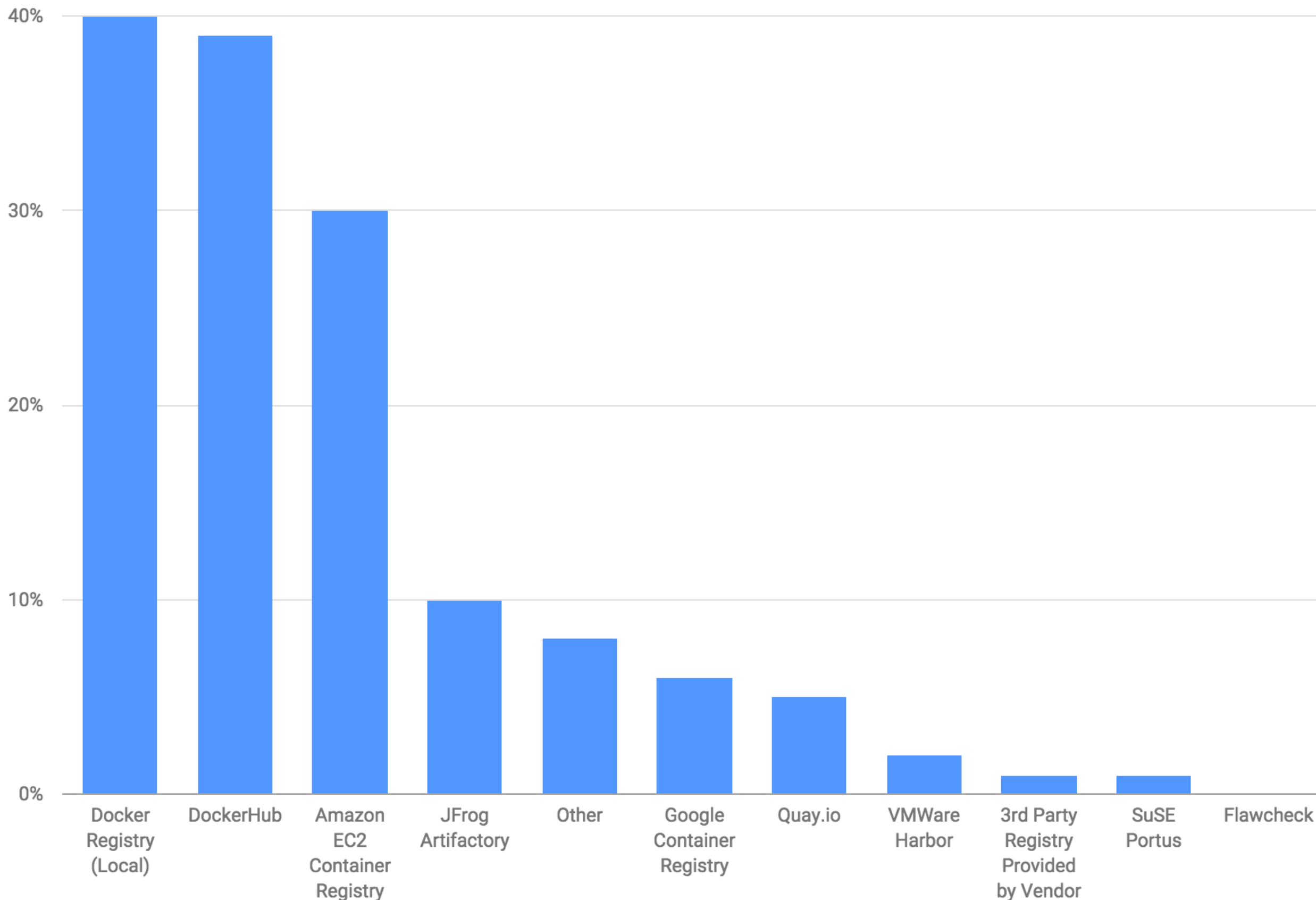
Where are you storing your container images?

ANSWERED: 241

#5

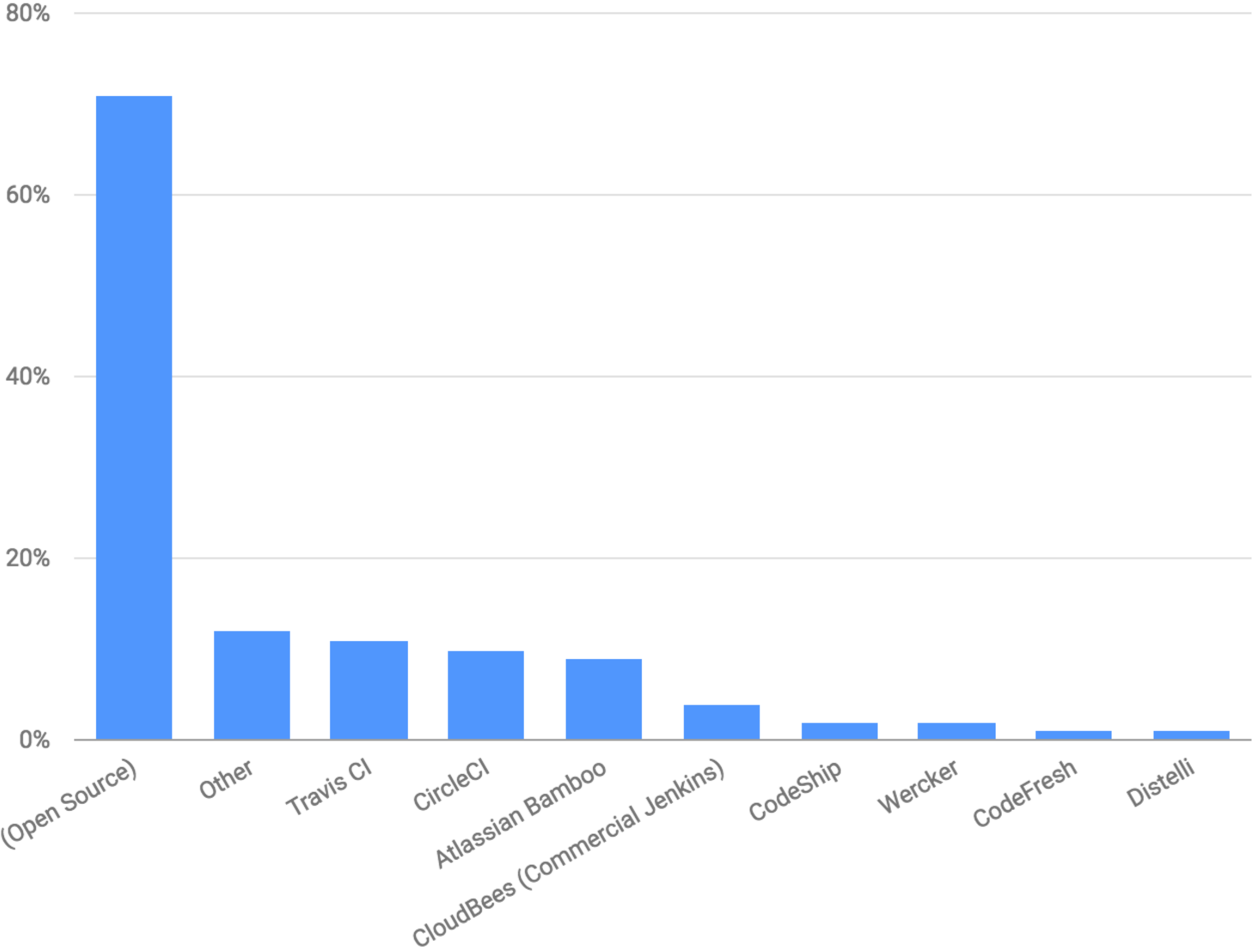
Docker Registry remains the most popular registry for on-premises deployment with Amazon's ECR registry dominating cloud based deployments. In future surveys we will dig into the user of DockerHub to assess DockerHub's usage for private images -vs- public images and official images used by organizations

anchore



What CI/CD platform are you using?

ANSWERED: 241



#6

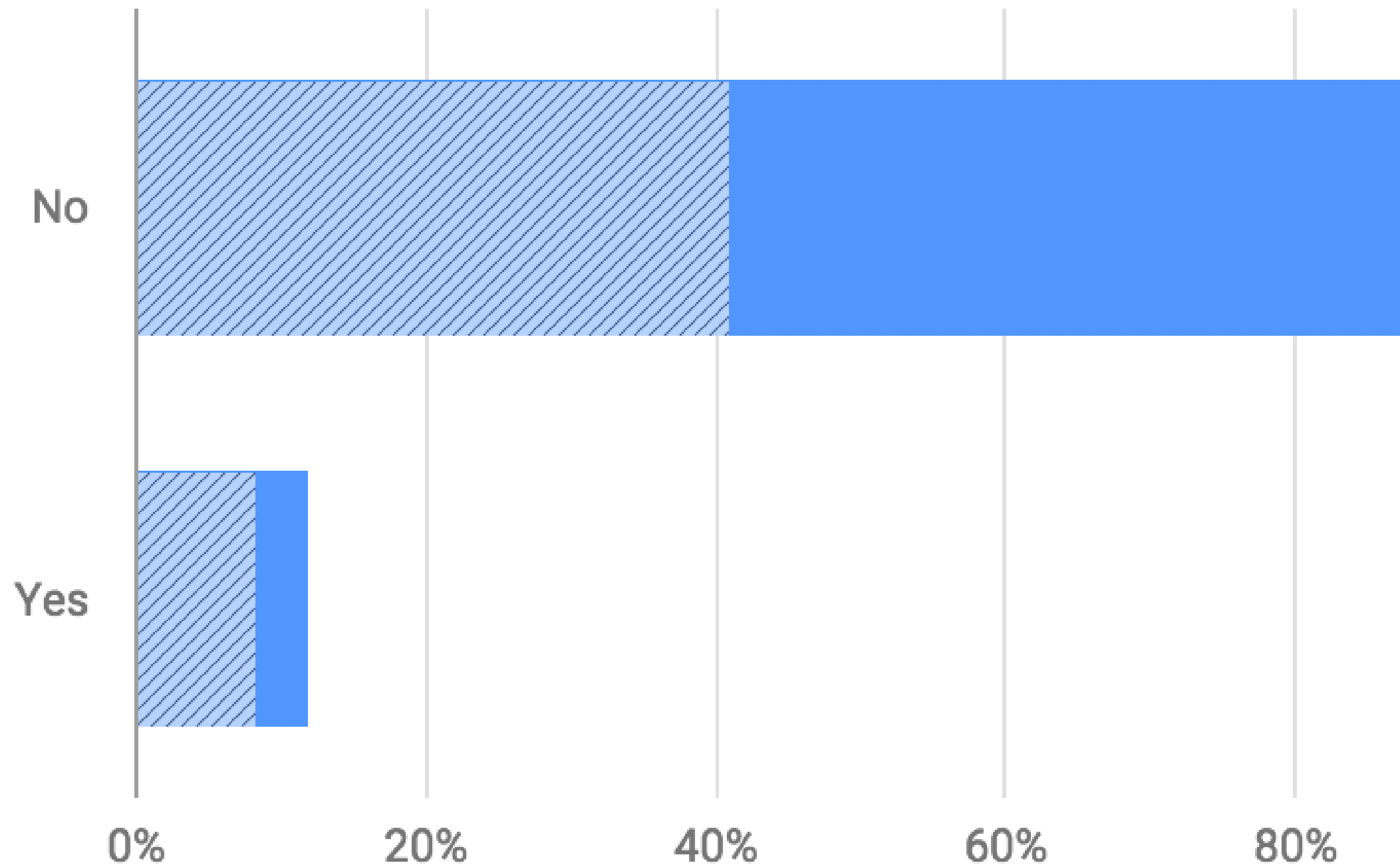
Unsurprisingly the Jenkins platform dominates the CI/CD platform both for on-premises and cloud based deployments. Atlassian Bamboo remains popular within some of the large enterprises surveyed however many organizations surveyed were running multiple CI/CD platforms in addition to Jenkins. Cloud-base CI/CD platforms increased both in terms of vendors offering solutions and in customer usage.

anchore

Do you currently perform any image scanning?

ANSWERED: 241

 Deploying Containers in Production



#7

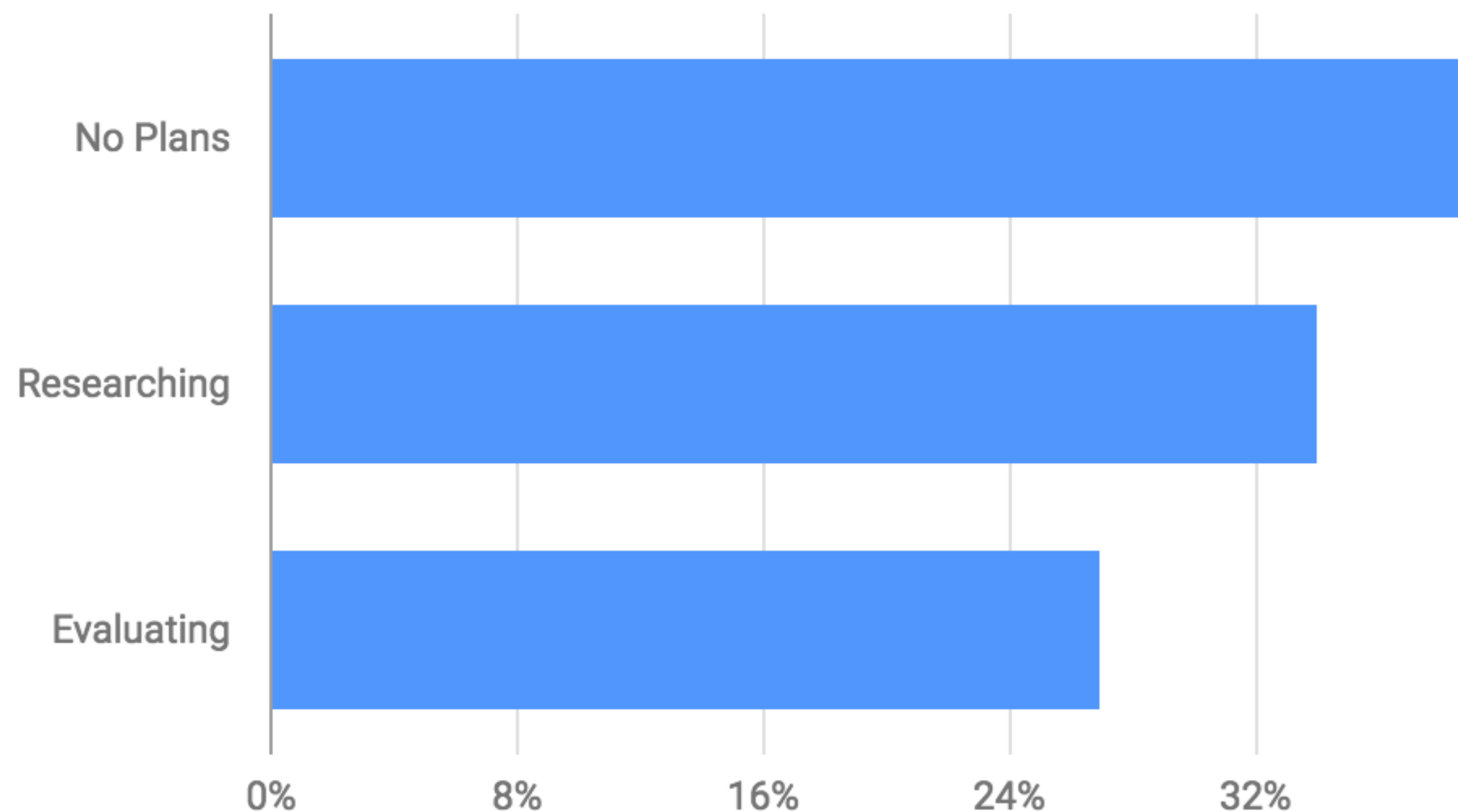
A large number of respondents are not performing any image scanning, with only 18% of product deployments undergoing any form of image scan. Given the recent analysis showing that 80% of Official images on DockerHub container high vulnerabilities* this represents a significant risk for end users.

anchore

*<https://blog.acolyer.org/2017/04/03/a-study-of-security-vulnerabilities-on-docker-hub/>

Do you have any plans to perform image scanning?

ANSWERED: 212



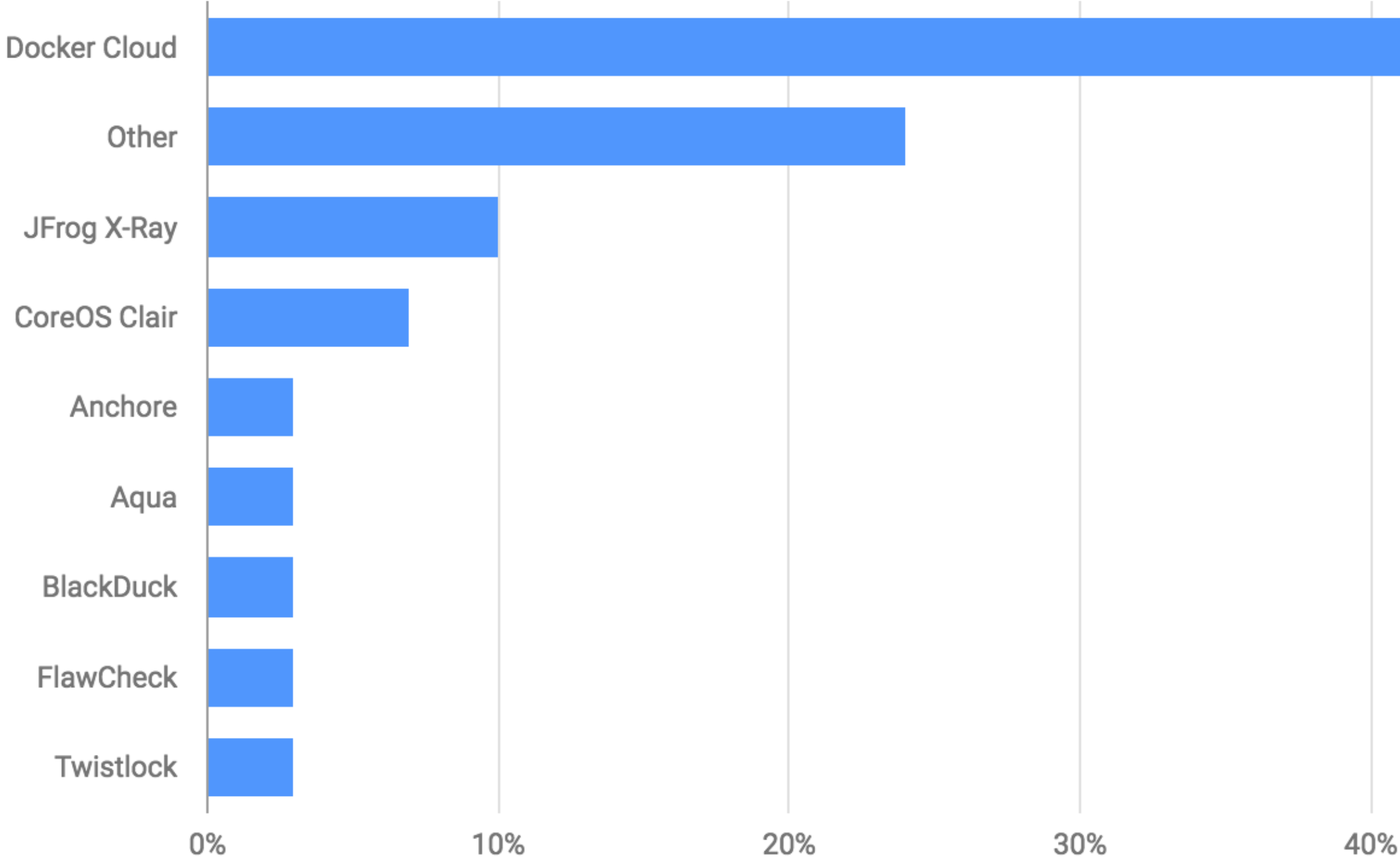
#8

While a large proportion of users identify security as a key concern with container deployments only a little over half of respondents are planning to perform image scans. Surprisingly 25% of these users are running Docker today in production without any image scanning.

anchore

What image scanning tools do you use?

ANSWERED: 29



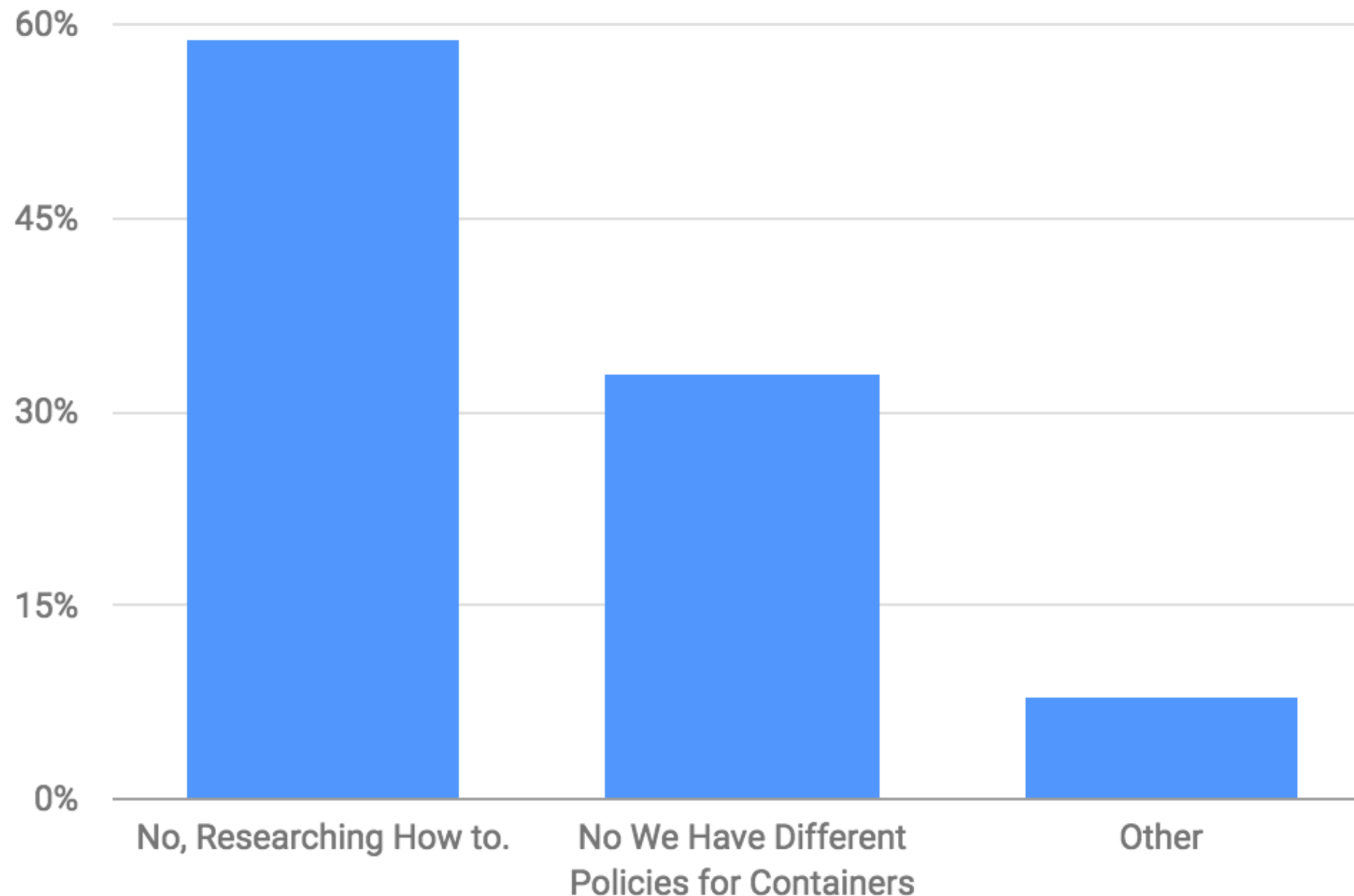
#9

Of the respondents who are currently performing any image scanning, the majority are using the scanning services provided by DockerHub or DockerCloud with scanning focused on official public images rather than user created images.

anchore

Do you apply your current operations & security policies to containers?

ANSWERED: 241



#10

Many organizations continue to struggle to understand how they apply their policies and best practices to their container environments. Only $\frac{1}{3}$ of respondents report that they are establishing new standards for containers - a number that we expect to see increasing in future surveys.

anchore

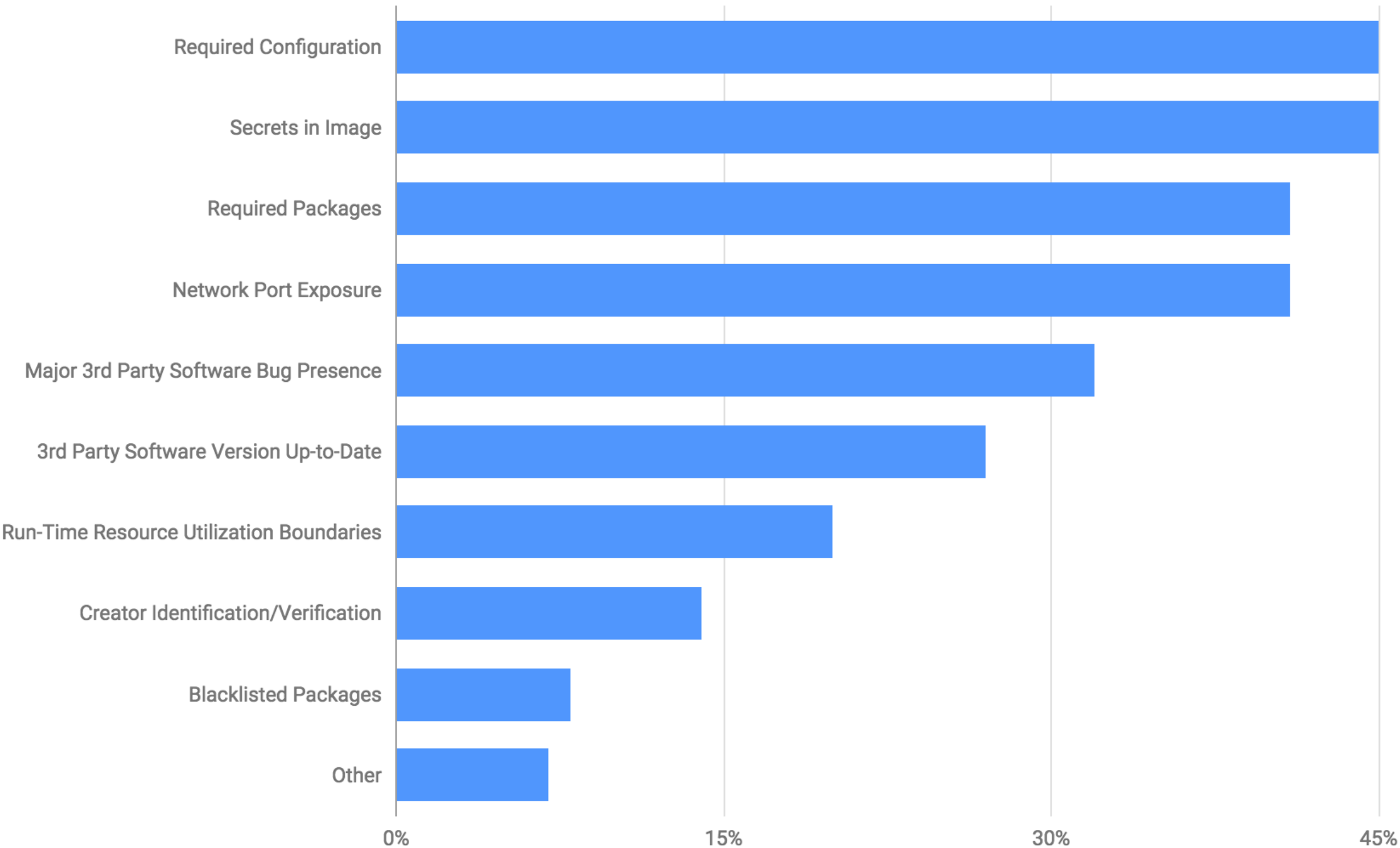
Other than security, what are the other checks that you perform before running application containers?

ANSWERED: 241

#11

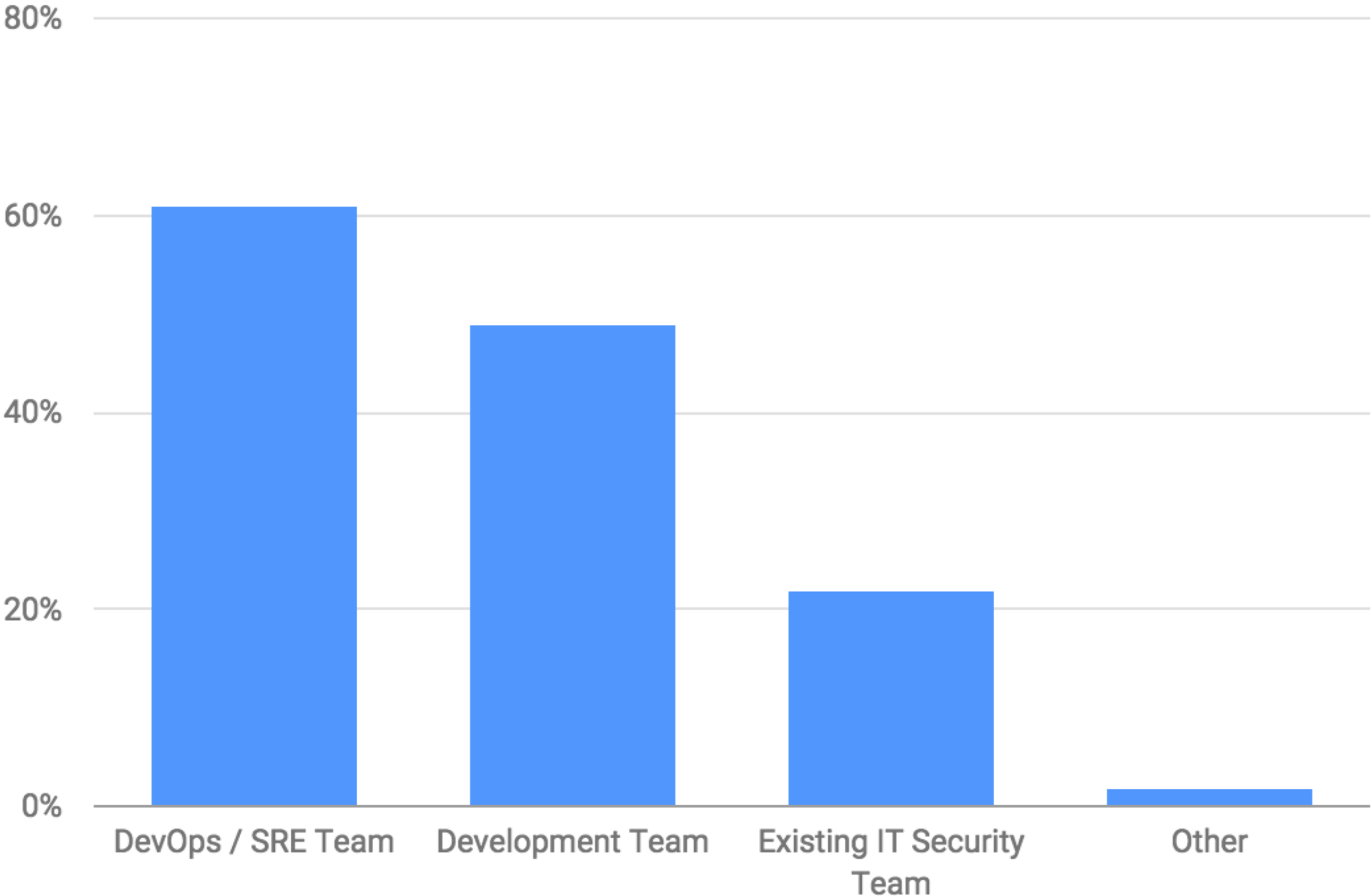
Six months ago our surveys showed that users who considered image security focused on simple CVE scanning on the operating system. In this latest survey we are encouraged to see more focus on the other artifacts within the image, many of which are not covered by traditional scanning solutions.

anchore



Who in your organization is responsible for container security?

ANSWERED: 241



#12

Over the last 6 months we have seen an increased focus on security for container deployments with responsibility transitioning from “unknown” or “no one” to dedicated DevOps or security teams. Collaboration between traditional security teams and DevOps is increasing with many security focused engineers moving into DevOps roles.

anchore



anchore

Learn more and follow us!



@anchore



github.com/anchore



anchore.com



anchore.io

