

Cloud-Native Security and Usage Report 2022

Marcel Claassen
Enterprise Sales Engineer



SYSDIG 2021

Container Security and Usage Report

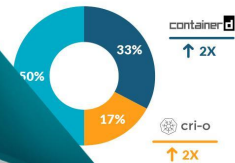
Find out how organizations are using
and securing their Kubernetes environments

What Container Platforms are Being Dep

Container runtimes

We have seen significant growth for both containerd (18% and 4% last year respectively) over Docker (18% and 4% last year respectively) over Docker last year but is down to 50% this year. It is also worth noting that the containerd project announced it will be officially supported by Kubernetes in late 2021. To be fair, it's important to note that Docker has also introduced low-level runtime features. These are being used in a number of projects. Choosing between the two seems a little unclear given the

emergence of several options. Different container runtimes offer different advantages, reduced overhead, stability, extensive compatibility as advantages. Now, however, standards, concerns about making the choice even easier. To make it even easier, project containerd and Kubernetes support using multiple container runtimes. This has typically been designed in a runtime or containerd project. Choosing between the two seems a little unclear given the



What Container Platform

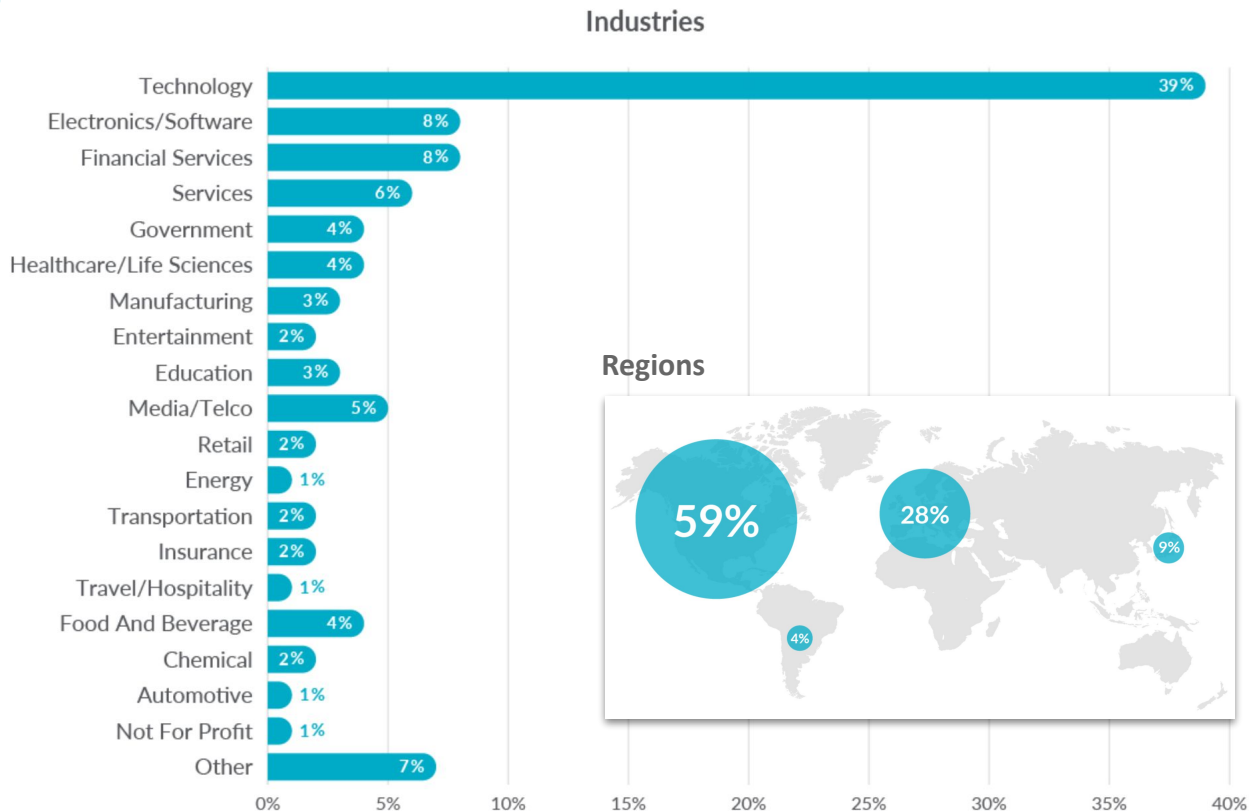
Cloud-Native Security and Usage Report 2022

Key 2022 Themes

1. Container adoption is maturing beyond early adopters
2. Lots of talk, not enough action on shifting security left
3. We're bringing our bad habits with us to the cloud

Data Sources

Real world analysis
of
running containers
and dozens of
industries globally

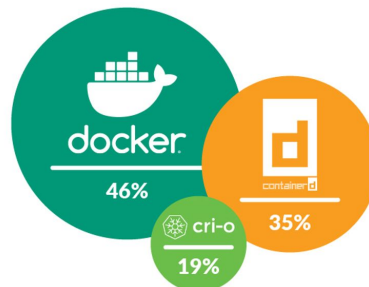


Container statistics

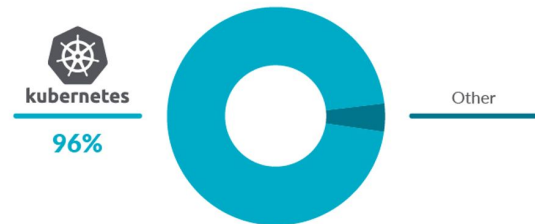
Median containers per host



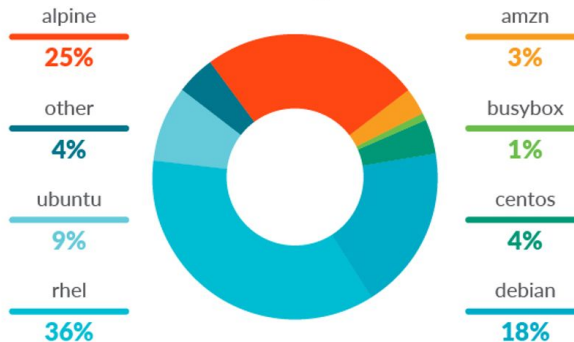
Runtimes



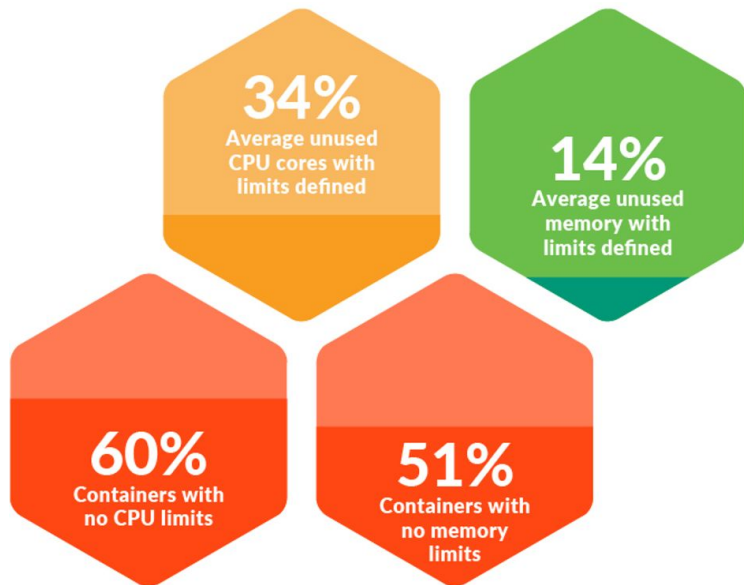
Orchestrations



Base Image OS

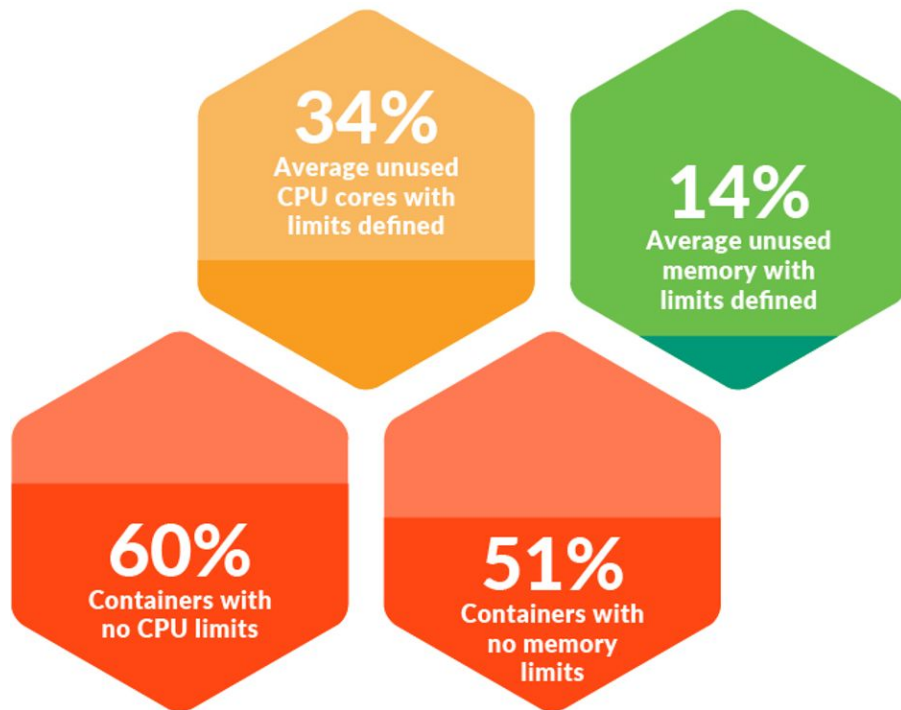


Container statistics



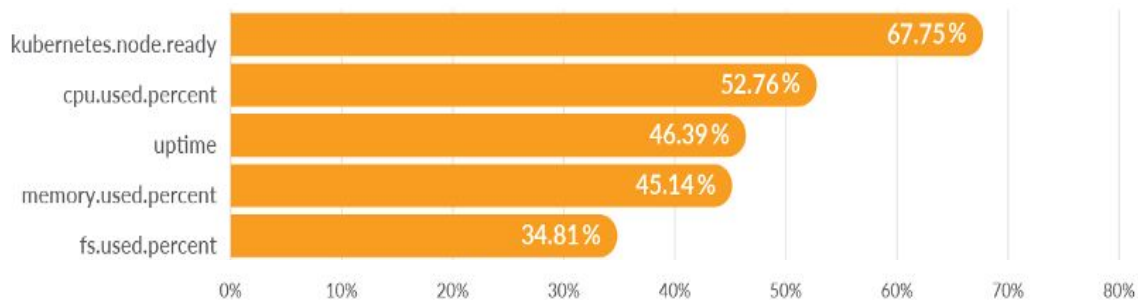
- 50% have no limits defined
- 75% running with high or critical vulnerabilities
- 76% running as root

Capacity planning

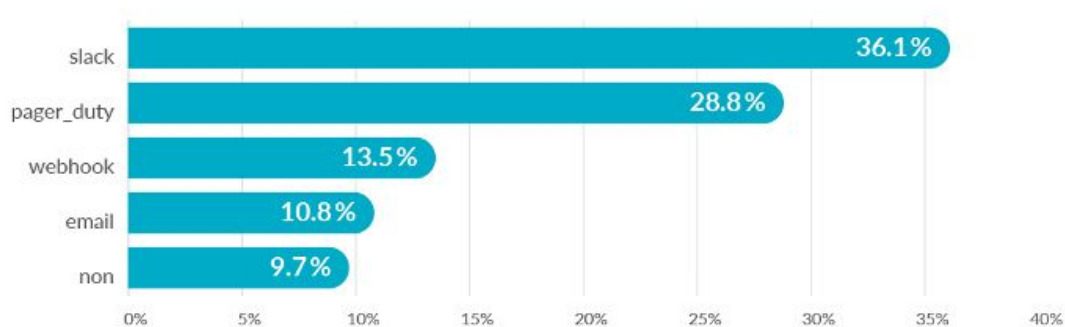


Container alerting

Top 5 Alerts

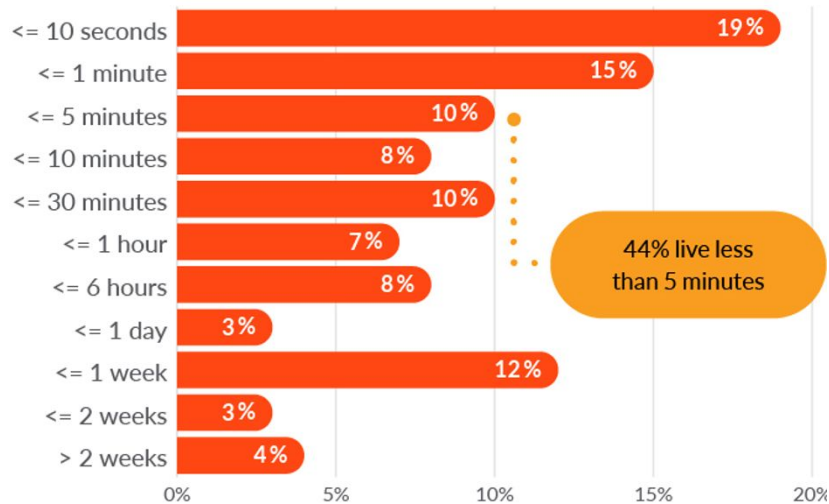


Top 5 Alert Channels

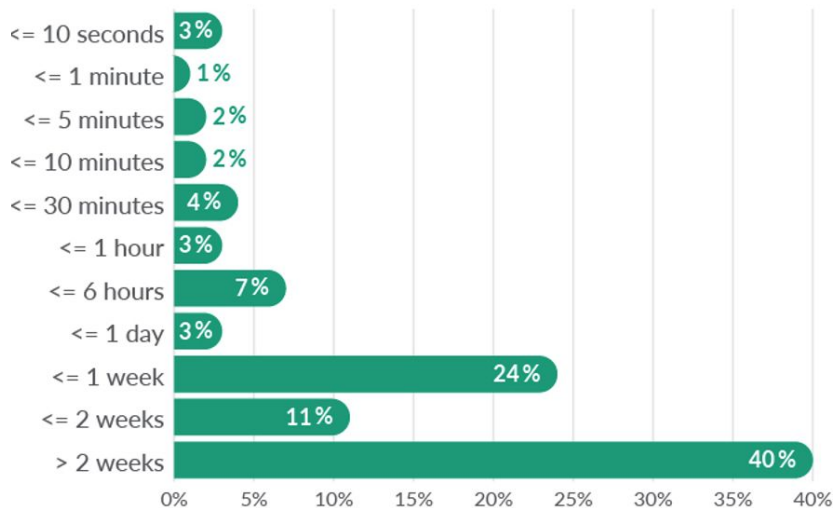


Increasing container lifespan..

Container lifespan



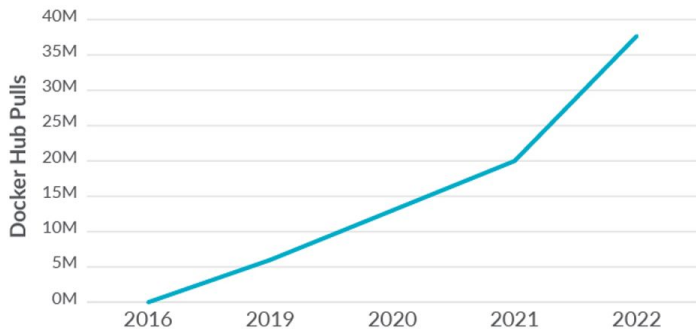
Container image lifespan



...provides more time for attackers to play around

Runtime security

Growth of Falco



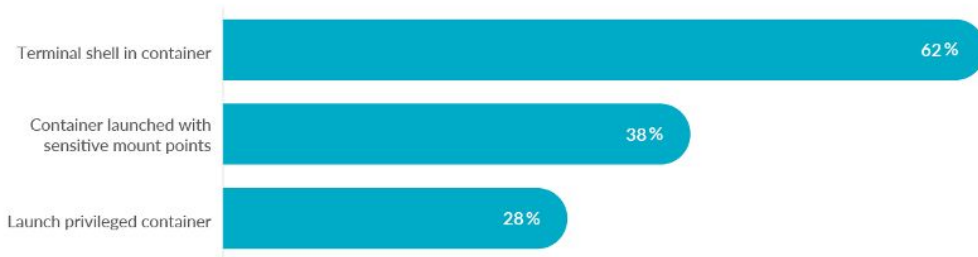
927 contributors

13.132 code commits

4.648 stars

25K contributions

Runtime security alerts



76%
run as root

Image scanning

OS vulnerability by severity



Non-OS vulnerability by severity



Where are images scanned



Patchable vulnerabilities in Runtime



Cloud Security and Identity

Cloud Identity and Access

27%

of customers use the root user account for administrative tasks



48%

of customers don't have MFA enabled on the root user account



Cloud Users and Roles

Human Identities

12%



Non-Human Identities

88%

- 73% contain publicly exposed S3 buckets
- 36% of all S3 buckets is open for public access
- In AWS public access is disabled by default

In summary

- Insecure behaviors like containers running as root and cloud accounts having excessive privileges without MFA.
- Shift left – Start scanning your images early in the pipeline
- Scanning containers is not enough, runtime protection is absolutely required.
- Continued growth of Falco indicates that organizations are leveraging cloud security tools to try to improve their posture.



sysdig

Seeing is **Securing**