2021 Container Security and Usage Snapshot

Shifting left is not enough! Doors are still being left open.

In 2020, we saw an acceleration of cloud adoption that led to an increase in container usage. This increase, combined with the fact that half of containers live less than five minutes, reinforces the need to manage container-specific security risks. A majority of our customers scan images during the build stages, but we still see risky configurations. To run container applications with confidence, it's important to address configuration risk, detect runtime threats, and ensure that a detailed recording of container activity is available for incident response and forensics. As we have done the past four years, we are sharing critical annual insights from real-time, real-world usage of nearly 1 billion unique containers that our customers have been running in our environment over the past year. Our goal is to shed light on the current state of container infrastructure, applications, security, and compliance practices.

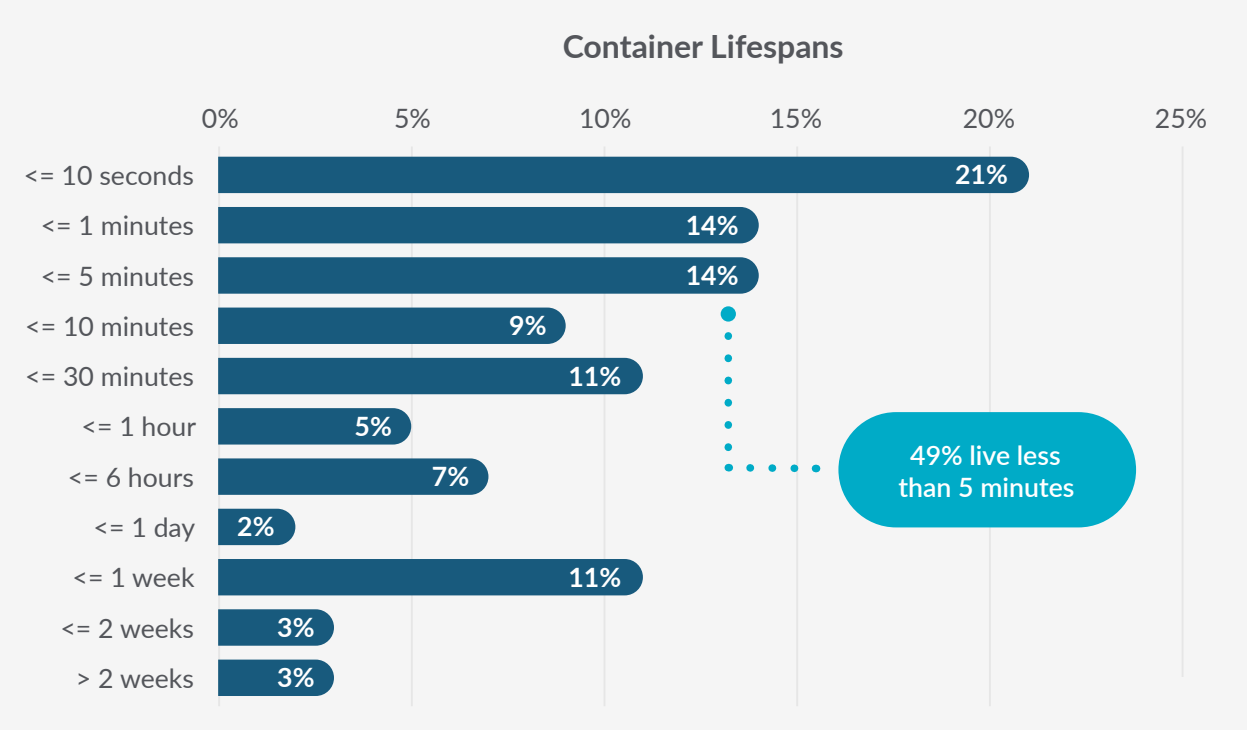
Key 2021 Trends

Security	Open Source	Container Usage
74% of customers are scanning images during the CI/CD build stage	3x increase in Falco adoption	4x increase in containerd and CRI-O
58% of containers run as root	35% growth of Prometheus metric use	33% growth in container density
49% of containers live less than 5 minutes	4.7x increase in usage of Go	60% increase in Quay.io usage

Container Security

Why Shift Left: The Short Life of Containers

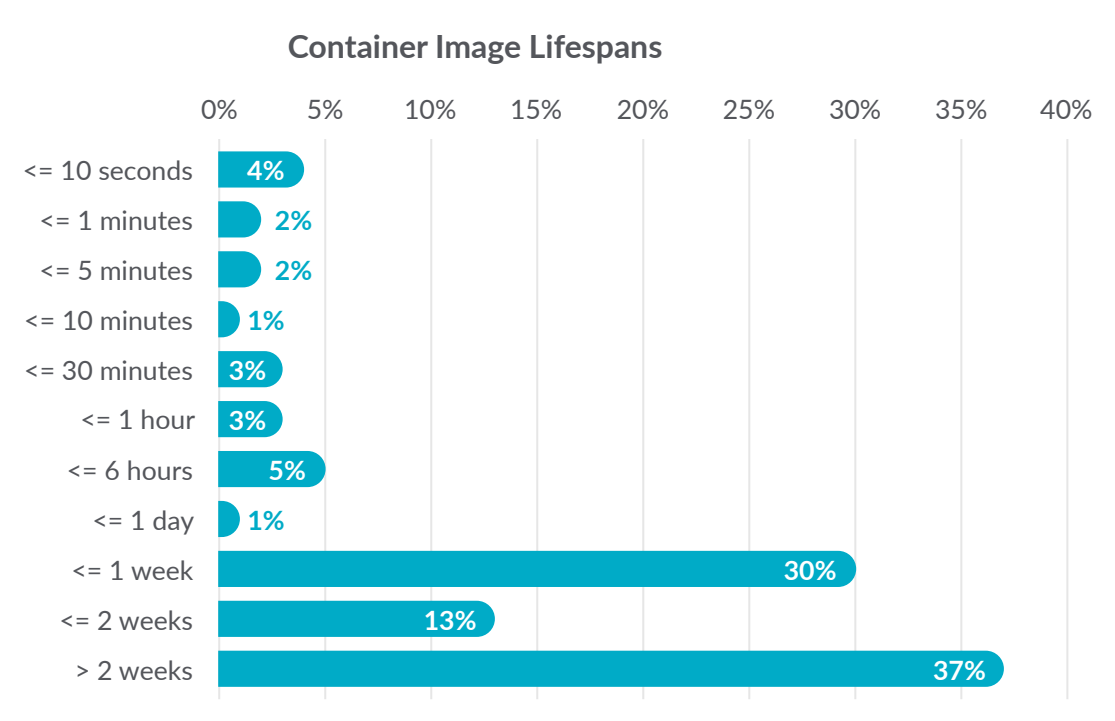
Containers have a short-life and need specific security implications. 49% of containers continue to be alive for less than five minutes. The ephemeral nature of containers remains one of the technology's unique advantages, but presents new issues to consider for security and compliance.

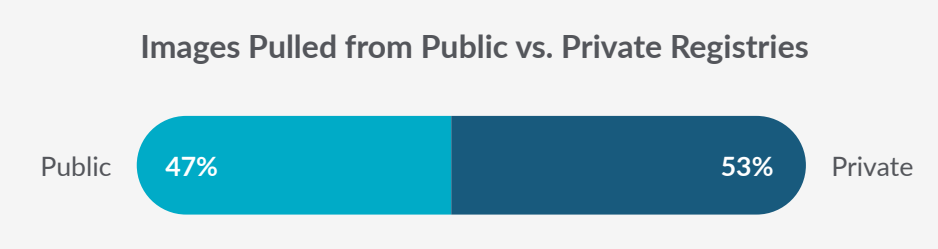


Container Security

Container Image Churn

Half of the container images are replaced – also known as churn – in a week or less. Automating scanning in CI/CD pipelines and registries can help developers deliver code faster, turning great ideas into reality faster, with more new images, more often, while managing the security risk.





Container Security

Public vs. Private Images

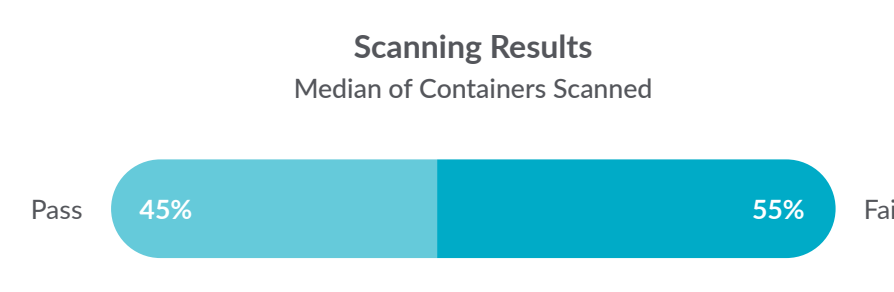
With more containers and more churn, new security tools and processes are needed to keep up. We found that 47% of images are pulled from public sources. The risk? Few are checked for security vulnerabilities. Docker Hub, for example, certifies less than 1% of its nearly three million hosted images.

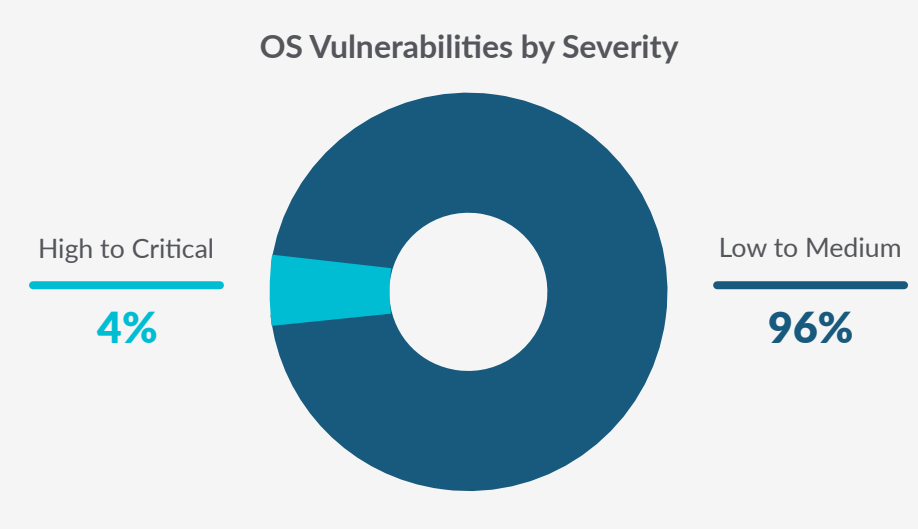
> "A manual image scan could take 10 minutes per check-in. With Sysdig, all of that just becomes automatic as part of the pipelines as the team is doing their deployments. Today, we handle thousands of merges per day. If you consider each could take 10 minutes on average and multiply that by thousands a day, we wouldn't be able to operate close to the same speed without Sysdig."
>
> \- SAP Concur

Container Security

Image Scanning

Preventing vulnerabilities in production requires image scanning. Pass and fail rates for images scanned over a five-day period reveal that over half of images have known vulnerabilities with a severity of high or greater.





Container Security

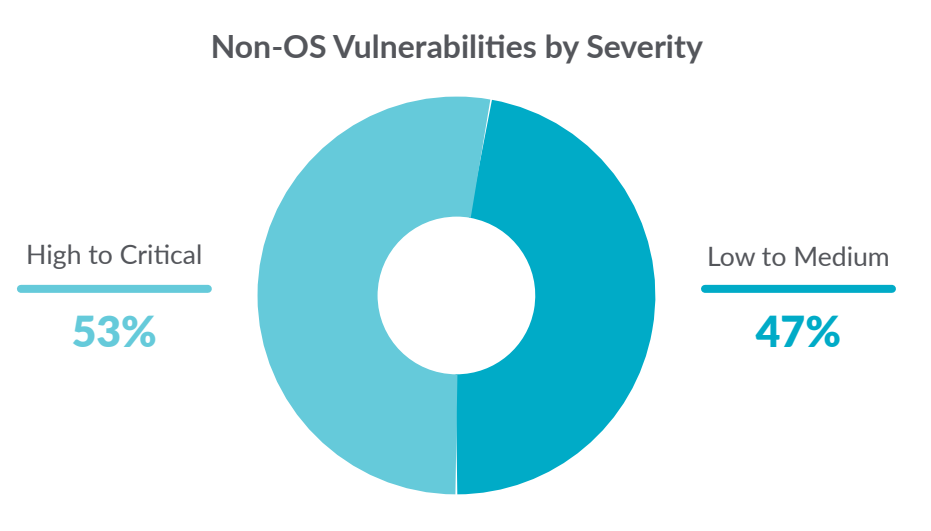
OS Vulnerability Snapshot

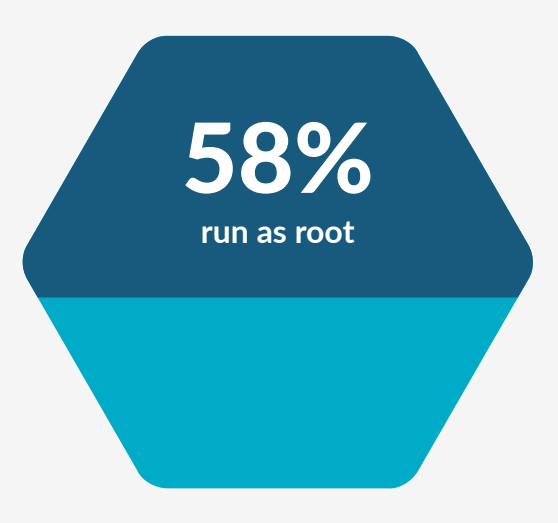
We noticed that four percent of OS vulnerabilities are high or critical. Although this may seem low, if an OS vulnerability is exploited, it can compromise your entire image and bring down your applications.

Container Security

Non-OS Vulnerability Snapshot

Non-OS vulnerability snapshot: Many teams don't check for vulnerabilities in third-party libraries. We found that 53% of non-OS packages have high or critical vulnerabilities. Developers might be unknowingly pulling in vulnerabilities from non-OS open source packages, like Python PIP, Ruby Gem, etc., and introducing security risk.





Container Security

How Common Are Risky Configurations?

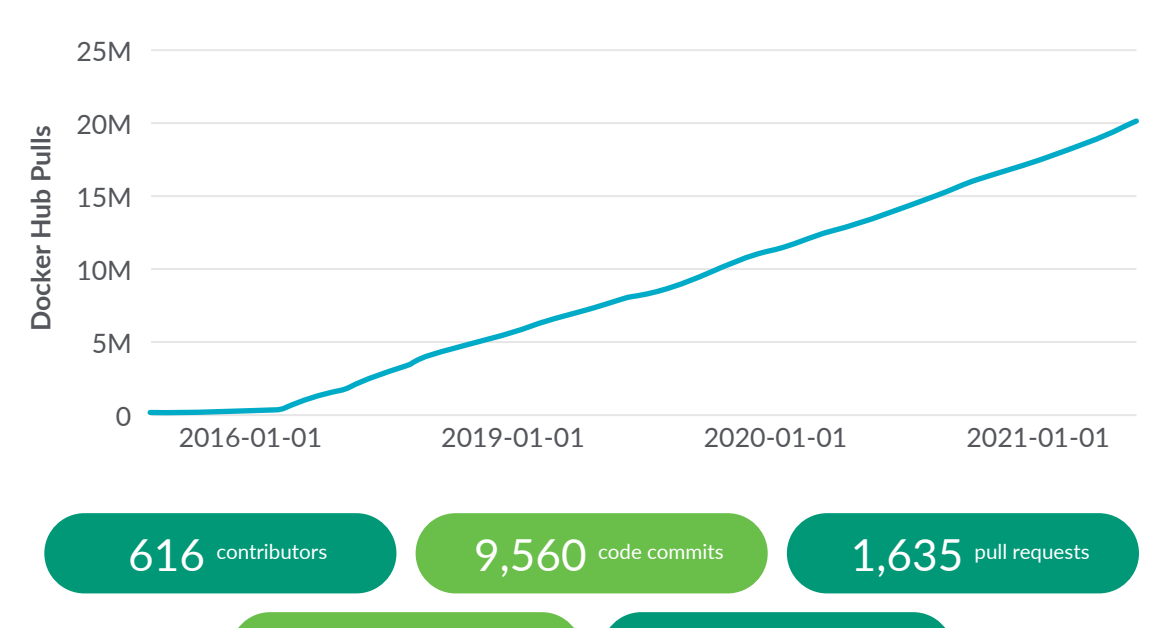
While teams understand the need to scan for vulnerabilities, they may not be scanning for common configuration mistakes. What we see is that 58% of images are running as root, leaving an opening for an attacker to execute malicious processes inside the container.

From talking to our customers, in practice, even if risky configurations are detected at build time, teams don't stop containers from moving to production. Instead, they allow a grace period to fix the issue and continuously monitor for suspicious behavior, in order to continue deploying quickly.

Open Source Software Gains Momentum

Falco Adoption Grows Over 3X

Runtime security detects anomalous behavior in production as a last layer of defense. Falco, the CNCF open-source project contributed by Sysdig, creates runtime policies, detects security violations and generates alerts. Falco is quickly gaining momentum, with adoption increasing by 300 percent over last year.



	Prometheus	StatsD	JMX
2020	62%	20%	19%
2019	46%	24%	30%
2018	20%	29%	55%

Metric types in use on average

Open Source Software Gains Momentum

Prometheus Gains Dominance

Custom metric solutions give developers and DevOps teams a way to instrument code to collect unique metrics. Of the three mainstay solutions, JMX, StatsD, and Prometheus, Prometheus metric use increased 35% YoY across our customers — with over 60% of our customers using it.

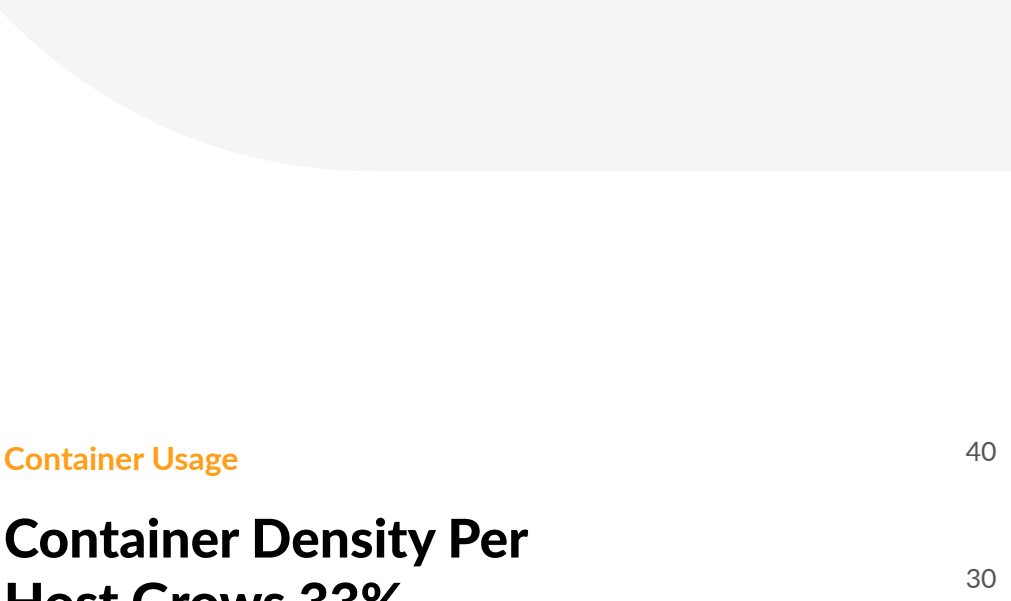
Open Source Software Gains Momentum

Top 3 Open Source Technologies Deployed by Sysdig Customers

Go is going places!

NGINX	GO	PostgreSQL
66%	↑ 66% ↑	24%

> "We can tell our developers to emit metrics with Prometheus. You won't have to think about it. They'll just show up in Sysdig."
>
> \- COTA Healthcare



Container Usage

Container Runtimes: Containerd and CRI-O Usage Grows 4x

Over the past year, we have seen significant growth for both containerd and Red Hat created CRI-O, both of which were recently adopted by the CNCF in 2019. To be fair, it's important to note that containerd is used by Docker.

Container Usage

Container Density Per Host Grows 33%

This year, container density grew 33% year-over-year compared with the 100% increase from last year. While the primary goal of containers is to speed development and deployment, many organizations are benefiting from increased utilization of hardware resources due to container efficiencies.

A majority of our customers are scanning images during the build stages, but still see risky configurations. This validates the need to continuously scan images in the registries and at runtime to protect against vulnerabilities. Addressing runtime security, mitigating configuration risks, and capturing container activity for incident response and forensics is essential for securely operating container applications with confidence.

Open source is growing as a core component in Kubernetes environments. The growth of Falco, Prometheus, and Go demonstrate the need for open source solutions to solve the critical problems of securing and monitoring containers.

> "With the audit log inside our S3 buckets, we can just go back and see what happened in the event of an attacker coming into the platform. We can also see if they took anything or how they gained access. Having this information saves so much time, because without the audit trails, how do you know what happened? Other solutions do not offer this. Beyond that, Sysdig will help identify who needs to be notified and with lessons learned from the configurations."
>
> \- Worldpay

Learn even more about the dynamics of container usage, security, and compliance in the Sysdig 2021 Container Security and Usage Report.

GET THE FULL REPORT NOW

sysdig