sysdig

2019 Container Usage Snapshot

Five-minute container life highlights the need for specific security controls

Enterprises are adapting to cloud-native architectures. As a result, usage patterns, processes, and organizational structures are changing.

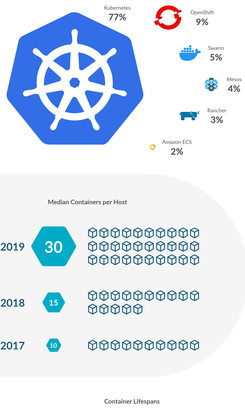
We've collected insights from real-time, real-world usage of over 2 million running containers to shed light on the current state of infrastructure, applications, security, and compliance practices.

Orchestration

Kubernetes Dominates

Kubernetes takes a whopping 77% share of orchestrators in-use. That number expands to 89% when you add in Red Hat OpenShift and Rancher – both built with Kubernetes.

The results change significantly when looking at on-prem deployments. Read the full report to see how.



Container Density

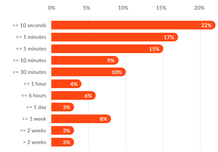
Containers-Per-Host Density Increases 100%

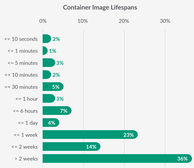
The median number of containers per host doubled to 30 in the past year. More apps and more compute power = more containers.

Lifespan

The Short Life of Containers

Yes, containers are ephemeral. Surprisingly, over half of containers are alive for less than five minutes. The number of containers alive for 10 seconds or less has doubled since 2018 to 22%. The growth of batch processing and serverless frameworks or Kubernetes is likely responsible for the shift.





Lifespan

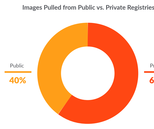
Container Image Churn

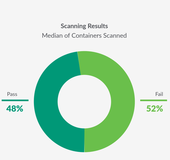
Over half of container images are replaced – aka churn – in a week or less. The use of CI/CD pipelines that help developer teams deliver code faster, and turn great ideas into reality faster, results in more new images, more often.

Security

Public vs. Private Images

With more containers and more churn, new security tools and processes are needed to keep up. We found that 40% 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 3 million hosted images.





Security

Image Scanning

To prevent 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.

> "We need to check configurations and validate that our images are free of vulnerabilities before pushing to production."
>
> - Global Travel Company

Security

Top Runtime Threats

Runtime security detects anomalous behavior in production as a last layer of defense. Falco, the CNCF open source project contributed by Sysdig, enables runtime policies that detect security violations and generate alerts. Using Sysdig Secure, which automates runtime security with Falco policies, we found that the top security risks encountered include containers that:

> With security events, the frontline is our developer team. They know what their applications should and should not be doing."
>
> - Director of Engineering at a Global Travel Company

> "Troubleshooting, forensics, and audit can be handled at scale when you have a single source of truth across the teams."
>
> - VP of Engineering at a Top 5 Investment Bank

Compliance

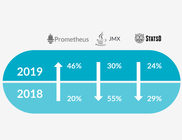
Container Compliance Issues

To reduce risk and meet compliance standards including PCI-DSS, HIPAA, and GDPR, organizations should regularly check hosts and containers against a set of best practices. Audits performed using the CIS benchmark for Docker reveal room for improvement. For example, we found that on the median, container hosts have 21 containers that run as root and 4 containers that run in privileged mode.

Services

Top 10 Open Source Containers

Open source powers innovation across infrastructure and applications. Here are the top 10 open source technologies deployed.



Custom metrics

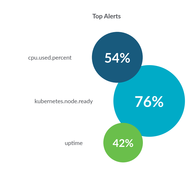
Prometheus Rises

Custom metrics solutions are a popular way to monitor applications in production clouds. Prometheus metric use increased 130% y/y – up from 20%. Alternatives like JMX metrics (for Java apps) and StatsD are diminishing, down 45% and 17% respectively.

Alerts

Top Alert Conditions

Alerts showcase what users see as most disruptive. The most commonly used alert conditions have shifted in favor of Kubernetes infrastructure while continuing to focus on resource utilization and uptime. Of more than 800 unique alert conditions used across Sysdig customers, here are the top 3:



Learn even more about the dynamics of container usage, security, and compliance in the Sysdig 2019 Container Usage Report.

GET IT NOW

sysdig