Container Journal · Security Boulevard · DevOps.com · Techstrong Research · Techstrong tv · Digital CxO

Techstrong Research

PulseMeter

Sponsored by

Orca Security

Study after study confirms Kubernetes is rapidly becoming one of, if not the dominant software platforms for cloud-native container orchestration. The Linux Foundation cites over 3.9 million Kubernetes developers worldwide with large numbers of Kubernetes installments in production.* The accelerated adoption of containers and orchestration technologies aligns with organizations' continued adoption of DevOps processes, workflow pipelines and toolchains, driven by business transformation in search of innovation and market competitiveness.**

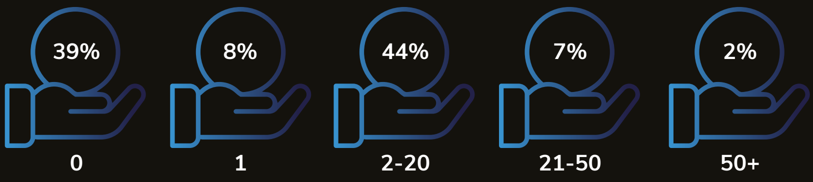
As with most new and rapidly-adopted technologies, security concerns immediately emerge, but do little to deter the accelerating rate of deployments. Kubernetes and containers are no different. Issues ranging from using vulnerable images or components to sidecar injection to orchestration layer privilege escalation make securing Kubernetes challenging. Multiple commercial technologies, as well as open source software solutions, are emerging as contenders to address these container security requirements. Yet these tools must keep up with a dynamic threat environment and protect against both build-time and runtime attacks.

In 2022, Techstrong Research polled our community of DevOps, cloud-native, cybersecurity and digital transformation readers and viewers to take the pulse of their Kubernetes deployments, security concerns and tooling. The Techstrong Research PulseMeter results show concern over container vulnerabilities, security protections in development and production, and a 49/51 percent split as to whether teams have adequate security technologies to secure Kubernetes.

MODEST-SIZED DEPLOYMENTS

At this early stage of the market, most organizations are just getting going with their Kubernetes deployments.

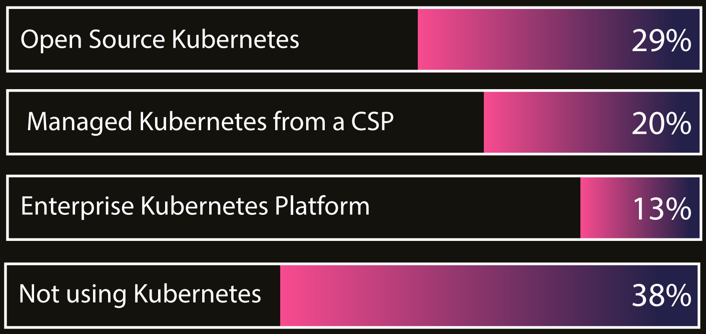
How many clusters do you run on Kubernetes across all phases of development?



MULTIPLE SOURCES OF KUBERNETES

Cloud-native organizations rely on both open source software and commercially-provided solutions.

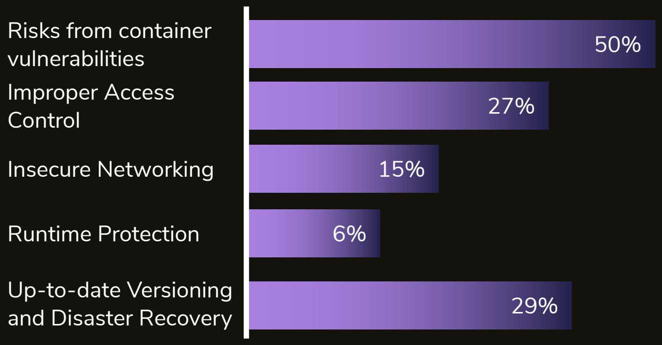
How are you running your Kubernetes-based applications today?



KUBERNETES SECURITY CONCERNS

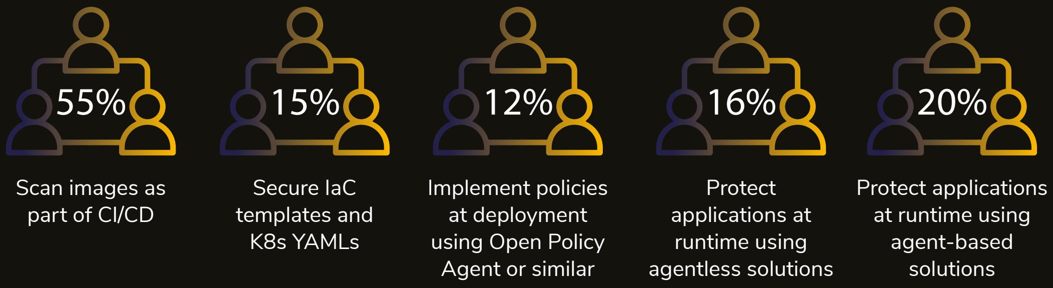
Container software vulnerabilities remain the largest security concern followed closely by improper access control provisioning.

What is your top Kubernetes security concern?

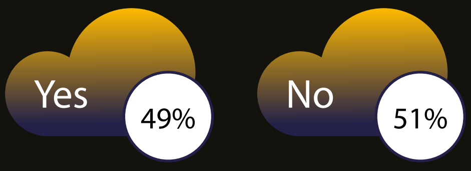


Container and Kubernetes security is concentrated on CI/CD processes and runtime application protection; responses are mixed as to whether organizations have adequate tools and processes to secure Kubernetes.

Have you integrated security controls into the development process?



Does your organization have the right tools and processes for securing Kubernetes?



Techstrong Research Analyst View

Cloud development, test and production environments are increasingly dynamic, driven by automation, infrastructure-as-code (IaC) and declarative GitOps approaches. The plethora of Kubernetes distributions and services from cloud providers bring increased complexity to Kubernetes design, configuration and operations, presenting a daunting security challenge to understaffed organizations working in a dynamic environment. Security and software professionals cannot rely upon a point-in-time security check of the multitude of cloud environments and container configurations. Shifting left to ensure properly configured and secure containers, combined with runtime security monitoring offers the greatest opportunity to reduce and eliminate security vulnerabilities, misconfigurations, and incidents.

*Cloud-Native Computing Foundation Annual Survey 2021, CNCF, https://www.cncf.io/wp-content/uploads/2022/02/CNCF-AR_FINAL-edits-15.2.21.pdf
**The Future of Remote Work and Software Development, Techstrong Research, https://techstrongresearch.com/wp-content/uploads/2021/10/techstrong-research-the-future-of-remote-work.pdf

Sponsored by Orca Security