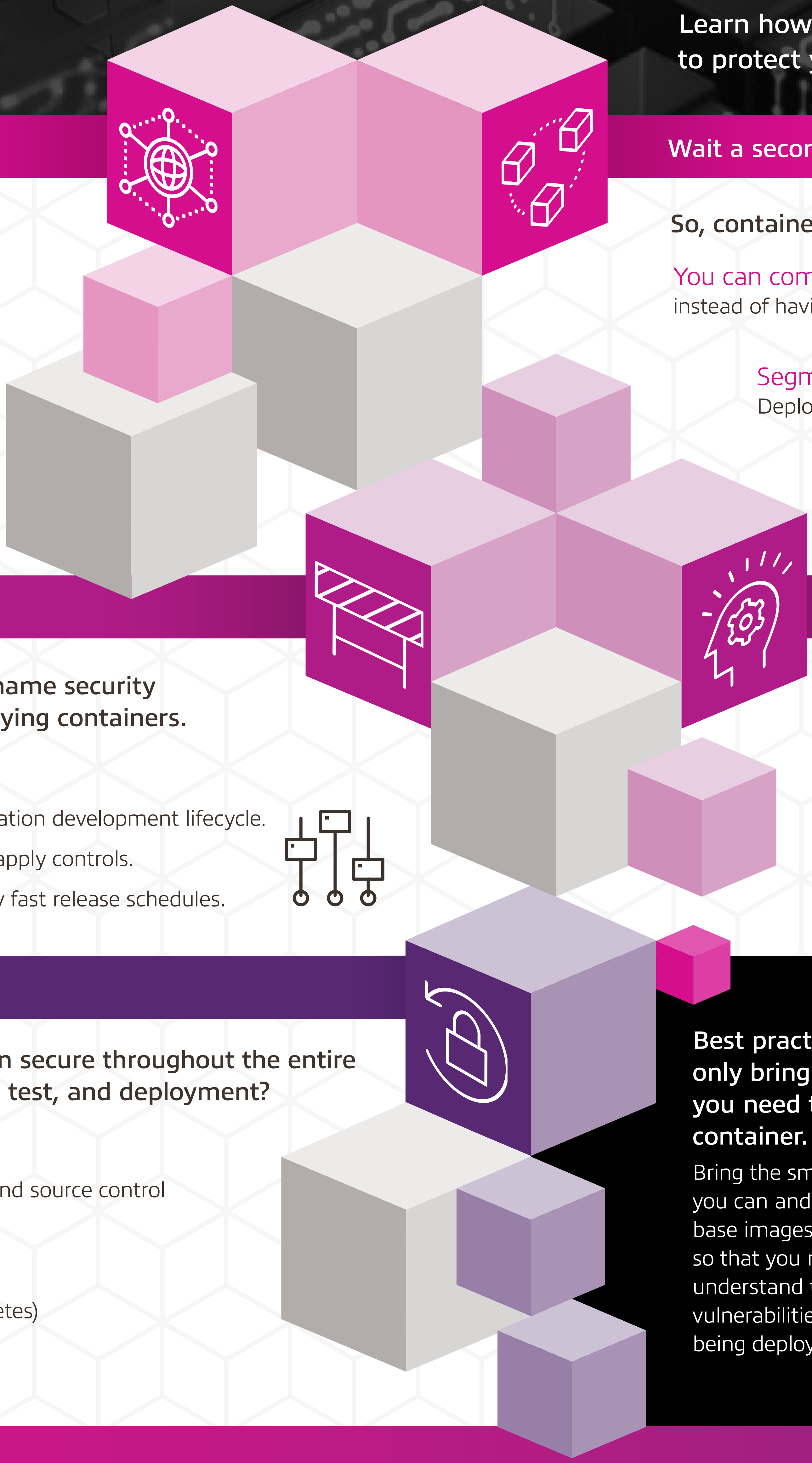
Insight

How to Secure Containers for Kubernetes

As container adoption increases, there is growing concern that security is being left behind. Containers are not inherently secure, and the techniques needed to secure them have some unique aspects compared to traditional approaches.

Learn how to apply controls and manage a new set of attack surfaces to protect your containers, your data, and your business.



A matter of prevalence

92% of organizations use **containers in production.**

83% **use Kubernetes in production.**

23% **are using more than 5,000 containers** across production, Proof of Concept (PoC), test, and development environments.

Wait a second…

So, containers are everywhere? What does this mean?

You can compartmentalize microservices down to a smaller footprint, instead of having monolithic VMs running for numerous services on the same kernel.

Segmentation, portability, and scalability become much easier. Deployment times are shorter, and availability is greater.

Containers are orchestrated by systems like Kubernetes — a layer that needs to be properly managed and secured.

Challenges at hand

Nearly one-third (32%) of IT leaders name security as a top challenge in using and deploying containers.

Why?

Controls must be applied earlier in the application development lifecycle.

The infrastructure itself needs to be used to apply controls.

Security requires keeping up with increasingly fast release schedules.

The experts discuss

Watch as Insight security pros talk through security considerations for containers and Kubernetes in this LinkedIn Live session.

Insight

in Live

Security Considerations for Containerization and Kubernetes

Continuous security

How do you ensure containers remain secure throughout the entire continuous delivery pipeline — build, test, and deployment?

Consider:

- Container compliance, registry, and source control
- Container content
- Network and host security
- Orchestration layer (e.g., Kubernetes) controls and vulnerabilities
- Shadow IT concerns

Best practice is to only bring what you need to the container.

Bring the smallest unit you can and constrain the base images available, so that you really understand the code base, vulnerabilities, and layers being deployed.

Red Hat Advanced Cluster Security for Kubernetes is one solution.

This software protects your vital applications across build, deploy, and runtime, with hundreds of built-in controls to enforce DevOps, industry standards, and configuration management.

Stay up to date on container technologies.

Things are changing rapidly across the container landscape, and it is critical to understand what's available and how to keep driving improvements and security enhancements.

For your journey

Our team is here to support you with container adoption, Kubernetes, and holistic security.
Learn more at **solutions.insight.com/Contact-Us**

Sources:
Cloud Native Computing Foundation (CNCF). (2020). CNCF Cloud Native Survey 2020.
Red Hat. (2021). Red Hat Advanced Cluster Security for Kubernetes.