Why Zero Trust for Containerized Environments

The disappearing network perimeter

New work paradigms, cloud computing and the adoption of containers accelerate digital transformation, while simultaneously introducing new enterprise security challenges

Containerized environments present unique security challenges

1 Critical vulnerabilities can be introduced in the continuous integration/continuous delivery (CI/CD) pipeline at any stage

2 Misconfiguration errors in registries, Kubernetes, and container hosts

3 New attack surfaces in Kubernetes, Docker, Istio and other tools

4 Inadequate protection in production environments from container exploits and zero-day attacks

Source: Zero Trust Container Security for Dummies

Zero Trust for container environments

What is Zero Trust?

/zirō trəst/

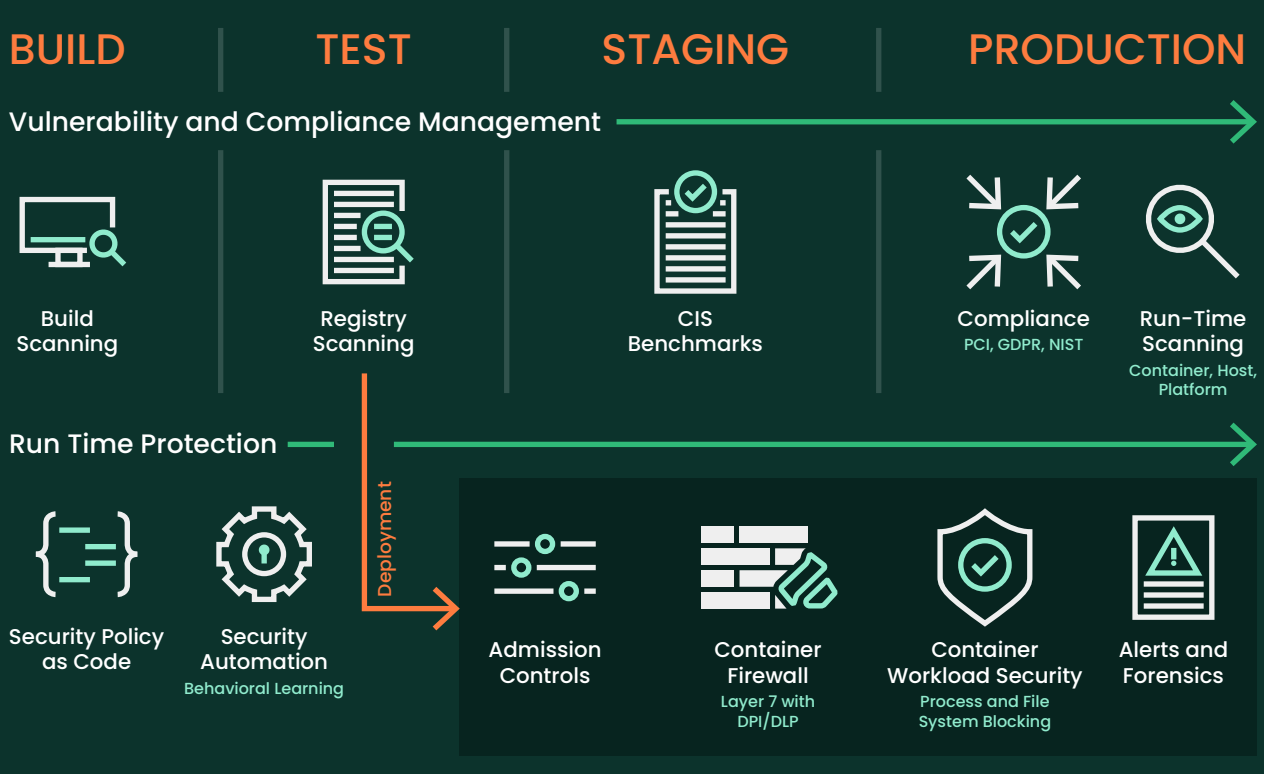
An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. (NIST)

Zero Trust is tailor made for securing containerized environments

Zero Trust replaces implicit mutual trust with authenticated access and centralized network control over a system of edge devices with encrypted connections. This helps address the security challenges of a decentralized IT environment and makes Zero Trust an ideal model for container security in the cloud. (TechTarget)

Activate Zero Trust security from pipeline to production

Full lifecycle security automation is key to a Zero Trust security strategy



Source: Zero Trust Container Security for Dummies

Learn more about Zero Trust for container environments

Download Zero Trust Container Security for Dummies

SUSE