Checklist: Container Security from Code to Runtime

Building applications using DevOps practices with containers, Kubernetes, and cloud, helps you rapidly meet business needs. In fast-moving cloud-native environments, security requires a different approach. From development through production, teams must stay vigilant against cyberattacks and tackle the unique security risks of modern applications. Using the tools and practices outlined in this checklist, your organization can successfully navigate the challenges of container security following three key principles:

- Build secure from the start.
- Protect against runtime threats.
- Prioritize security alerts that matter.

Code Security

With containers, application security begins with your code. Code security tools for software composition analysis (SCA) and static application security testing (SAST) will help you analyze your code and dependencies to spot issues early in development.

Open Source Security

Development teams need to find, prioritize, and fix security vulnerabilities and license issues in the open-source components they are using in their applications. Software composition analysis (SCA) tools for open source help you scan for open source dependencies and flag vulnerable packages.

Image Security

Selecting the right base image and automating image scanning policies will help you ensure the security of your container images. New vulnerabilities are disclosed continuously. Choosing a container security solution that alerts you to new vulnerabilities, including those running in production, is key to effective image security.

sysdig snyk

Infrastructure as Code Security

In modern cloud-native environments, infrastructure-as-code (IaC) templates, such as YAML, Terraform, and Helm, enable you to deploy consistent and repeatable configurations. Policy-based IaC security tools strengthen security and compliance by auto-detecting and auto-remediating IaC misconfigurations and drift.

Runtime Security

Runtime security lets you detect and respond to threats to your running containers. To spotting abnormal behavior, even during the short run of container tasks, requires the equivalent of a real-time security camera that detects activity and captures incidents while alerting you to events.

Vulnerability Prioritization

Faced with hundreds of vulnerabilities, developers often don't know where to focus remediation efforts, or what order to do them in. Using runtime insights to identify software packages executing in running containers can help you prioritize what to fix first to address real risks, while eliminate noise.

Network Security

DevOps teams are often blind to how containers are communicating, making it difficult to create effective network security policies. Deep visibility into how containers are connected and what's needed to function properly is essential. Tools like network topology maps together with Kubernetes network policies empower you effectively address container network security.

Kubernetes and Cloud Platform Security

Improperly configured hosts, container runtimes, clusters, or cloud resources can leave doors open to attacks. Automating checks like CIS benchmarks and compliance measurements will help you spot and remediate Kubernetes and cloud platform misconfigurations to reduce risk.

Incident Response and Forensics

The ephemeral nature of containers complicates incident response. Lack of digital evidence surrounding a security breach can leave you blind. The ability to record activity surrounding a container event will ensure you can investigate and respond quickly even after a container is no longer alive.

Container Security from Code to Runtime with Snyk and Sysdig

Snyk and Sysdig bring together developer security and runtime security tools to bridge developer, DevOps, and SecOps silos. Pairing early detection and vulnerability management with accurate runtime threat protection, Sysdig and Snyk help teams ensure container protection from code to runtime.

Learn more

Want to dive deeper? Access the extended Container Security from Code to Runtime Checklist guide for even more insight into container security best practices.

Download Guide