A Gartner survey shows how security leaders approach securing modern applications that run on containers in a continuous integration/continuous delivery (CI/CD) pipeline. Respondents shared their top three challenges in securing cloud-native applications:

1. Lack of internal/external security awareness
2. Difficulty integrating new tools with legacy ones
3. Unclear boundaries between application and infrastructure

A third of respondents stated that using application security testing tools and conducting security reviews were effective in securing cloud-native applications. However, creating a center of excellence was the No. 1 first choice.

Organizations where the security team is in charge of securing cloud-native applications tend to be less successful in doing so compared to peers that delegate authority.

Respondents then shared which tools they use the most and mature tools came out on top:

- Static Application Security Testing (No. 1 in Development)
- Web Application and API Protection (No. 1 in Production)
- Application Security Monitoring (No. 2 in Production)
- Cloud Workload Protection Platforms and Cloud Security Posture Management
- Infrastructure as Code Scanning

When it comes to streamlining DevSecOps, almost a third of organizations choose to manually integrate their security tools. However, organizations using a more-structured way to integrate tend to have better chances of overall success compared to their peers.

Organizations focus on mature tools, but orchestration is key.

---

**Source:** Gartner's 2021 Enabling Cloud-Native DevSecOps Survey