The Right Way to Secure Open Source Containers

As more government agencies turn to open source containers for application development, they need to adopt measures to ensure the security of those containers. That's not necessarily easy, though. Traditional security management tools, like intrusion detection systems and antivirus software, do not provide visibility into the container and cannot accurately scan containerized applications. Thus, if you're a federal software developer or security manager, you may need to rethink the way you approach container security and adopt a "shift left" mentality, in which security is integrated into the development process from start to finish.

When software development shifts left, security moves from being bolted onto the end of the development process to being proactively implemented from the time the first code is written. Applications are checked for their code quality and vulnerabilities or errors. Adjustments are then made throughout the rest of the software development lifecycle to address any vulnerabilities as they come up. The idea is to identify those vulnerabilities early so the final product is as secure as possible.

Shifting left is a core tenet of DevSecOps, where security managers are integrated into the development process. DevSecOps is closely related to agile development, which containers support. But, how do you secure the containers?

The Right Tools

The open source community is actively working to answer this question. The community has developed technologies designed to increase visibility into the inner workings of containers and support security measures throughout the entire software development lifecycle.

There are a number of open source projects and tools that effectively enhance container security. Some of the more noteworthy ones include Anchore (for scanning and inspection), SonarQube (for code quality), and Open Policy Agent (for policy). The latter is particularly interesting in that it allows for building policies to meet the needs of highly regulated industries, which makes it ideal for government use. With OPA, you can create standardized security policies across a cloud ecosystem, which is particularly great for agencies managing many different clouds.

The Right People

But, tools aren't enough. At the end of the day, good container security comes back to the people involved in the process. Involving security at the outset allows for automated security

checks and compliance, minimizing the chance for unwelcome surprises when an application is finally deployed.

Of course, just because security managers are incorporated into the development process doesn't mean developers themselves shouldn't be cognizant of the security of the applications. It's always good to have another set of eyes to serve as another safety level. And, developers will still be the ones implementing any necessary fixes, so it's beneficial for them to understand the threats. But, a DevSecOps approach provides developers with additional support to ensure the applications they're creating are free of vulnerabilities.

This support is especially important for containerized application development, which has disrupted traditional development practices and created security blind spots. Seeing through those blind spots requires that old adage: the right people, processes, and technologies.