You Want Secure Containers? Start With Secure Container Contents

Bill Weinberg | Senior Director and Analyst, Open Source Strategy | The Linux Foundation | October 22, 2015

Containerization is hot. This form of lightweight virtualization lets more applications run on a single server or cloud instance and lets IT organizations create and deploy those applications faster and more reliably.

Enterprise containerization meets several enterprise IT goals simultaneously:

- Containers provide a convenient, self-contained development and deployment vessel that simplifies integration, aggregation and management of diverse application components
- Containerization encourages developers to rethink application architecture and scope into "micro-services", boasting "just enough" capabilities to meet technical and business requirements, in line with agile development practices
- Using containers accelerates time-to-deployment and minimizes time to re-deployment for patching, updates and new releases

Despite containers' fostering a minimalist, incremental approach to the software life-cycle, container contents can be anything but "micro". Popular container images (on Docker Hub and elsewhere) can contain hundreds or even thousands of open source packages, comprising libraries, application frameworks and other utilities and middleware.

The open source software components contained in off-the-shelf container images, as well as in fully custom containers, provide developers with a foundational "leg up", freeing them to concentrate on value-added and differentiating functionality in their applications. But those same open source components can expose applications to myriad vulnerabilities. According to a 2015 study by BanyanOpps, more than 30 percent of popular images in the Docker Hub contain high priority security vulnerabilities.

The key, then, to container security starts with the contents! This may seem axiomatic, but in providing manageable, easily deployable units, containers also hide a multitude of detail, including vulnerabilities. To address the container security challenge, Black Duck is partnering with Red Hat, integrating Black Duck scanning and open source security vulnerability-mapping – the Black Duck Hub – with Red Hat OpenShift, a Platform-as-a-Service (PaaS) that features rapid container-based application deployment.

The collaboration will ensure that containers in the OpenShift registry are free of known vulnerabilities. Ultimately, both COTS and custom containers deployed on OpenShift will be able to deploy with greater confidence. By leveraging the Black Duck Knowledge base of over 1.1 million projects and over 100,000 known vulnerabilities, developers and IT organizations will be able to create and deploy more secure container-based apps across the entire software development life cycle.

OPENSHIFT