Identify vulnerability impact for containers within hours of disclosure, and reduce time to remediation with automated security workflows

Overview

Container orchestration platforms such as Kubernetes dramatically simplify the process of deploying and running containers at scale. Organizations can take advantage of revolutionary container technology, making the build, package, deploy, and manage processes for applications lightweight and easy.

Facilitate deployment, but don’t neglect security

As orchestration advances the explosive growth of containers in mainstream business, security challenges arise for IT operations teams, notably the validation of third-party and internally developed images. New vulnerabilities are disclosed every day, and some of those are likely to affect your organization’s applications. It is critical for you to know precisely which pods and containers are affected. If your deployment involves hundreds or thousands of containers, individual container scanning simply won’t scale.

Get automated open source visibility and control for Kubernetes

To help you get visibility into the open source in your containers, Synopsys offers Black Duck OpsSight for Kubernetes, which provides proactive monitoring of all pods in a Kubernetes cluster to give teams visibility into, and control over, the risks associated with open source components in those images.

Black Duck OpsSight for Kubernetes automatically discovers images as they are used by listening for changes in the pod events stream. It then performs deep container inspection on both operating system and application layers to identify open source security and compliance risks at any phase of container construction. Black Duck continuously monitors the open source found in your containers and alerts you to any vulnerabilities or risks reported since the container was last updated. Black Duck integrates directly into the Kubernetes platform, so operations and infrastructure teams can manage open source security and compliance risk efficiently and at scale.
Ensure container image security before, during, and after deployment

Black Duck OpsSight for Kubernetes open source security and management solution provides visibility into application components as well as dependencies present in base container images. The Black Duck KnowledgeBase™ (KB) is the most comprehensive repository of open source component and vulnerability intelligence available, with information for millions of projects from over 10,000 independent data sources. Using the KnowledgeBase, Black Duck helps teams prevent open source vulnerabilities or components violating policy from being deployed, then alerts them when any new vulnerabilities or policy violations affect containers already in production.

- **Detect.** Black Duck's automated multifactor open source detection inventories all the open source in container images as they are used in the cluster.
- **Protect.** Enhanced Vulnerability Data identifies all known vulnerabilities for the open source in your container images, including actionable mitigation and remediation guidance to help minimize risk of exploit.
- **Manage.** Policy management allows teams to define open source use and security policies, which are evaluated with each scan and documented as metadata on your containers, allowing you to flag images that violate policies and prevent them from deploying to production.
- **Monitor.** Black Duck continuously monitors for newly reported open source security vulnerabilities associated with open source in use, providing same-day alerts so teams can find and fix vulnerabilities before hackers can exploit them.

Be proactive about container security by removing vulnerabilities from container images before they are deployed. For more information contact partners@synopsys.com.

---

**The Synopsys difference**

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to [www.synopsys.com/software](http://www.synopsys.com/software).

---

**Resources**


---

**77% of containers are managed with Kubernetes**

**62% of respondents cite security or compliance as the biggest hurdle to container adoption**

**53% of users report detection of vulnerabilities in container images as a top concern**