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

Containers simplify deployment but complicate security

Containers have revolutionized application packaging and delivery. They’re lightweight and easy to build, deploy, and manage, and container orchestration platforms, like Red Hat OpenShift, have dramatically simplified the process of deploying and running containers at scale.

But the explosive growth of containers has brought with it image validation and security challenges for operations teams. When a new vulnerability that affects your applications is disclosed, the ability to know precisely which images and containers are impacted is critical, and if your deployment involves hundreds or thousands of containers, individual container scanning won’t scale.

Get automated open source visibility and control

Black Duck OpsSight for Red Hat OpenShift Container Platform provides proactive monitoring of all container images in an OpenShift cluster to give teams visibility into, and control over, the risks associated with open source components in those images.

OpsSight for OpenShift automatically discovers images as they are created or updated by listening for changes within the ImageStream and Kubernetes pod events. 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.
OpsSight continuously monitors the open source found in your containers and alerts you to any vulnerabilities or threats that have been reported since the container was last updated. OpsSight is integrated directly into Red Hat OpenShift Container Platform so operations and infrastructure teams can manage open source security risk efficiently and at scale.

Ensure container image security before, during, and after deployment

The Black Duck OpsSight 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, OpsSight helps teams prevent open source vulnerabilities or components violating policy from being deployed, and alerts them when any new vulnerabilities or policy violations affect containers already in production.

• **Detect.** OpsSight’s automated multifactor open source detection inventories all the open source in container images as they are deployed.

• **Protect.** Black Duck Enhanced Vulnerability Data identifies all known vulnerabilities for the open source in your container images while actionable mitigation and remediation guidance helps minimize exploit risk.

• **Manage.** OpsSight 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.** OpsSight continuously monitors for newly reported open source security vulnerabilities associated with open source in use, providing same-day alerts so teams can understand how newly discovered vulnerabilities affect their containers in production.

For more information, or to request a demo of Black Duck OpsSight for Red Hat OpenShift Container Platform, contact partners@synopsys.com or visit www.synopsys.com/software-integrity/partners/ecosystem/red-hat.

### Resources


---

**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.

**Synopsys, Inc.**
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com