SYNOPSYS® + Red Hat

# Application and Container Security Integrated Seamlessly With Your Red Hat Products

## The challenge

Modern organizations depend on software, and many are scrambling to develop and deploy applications quickly enough to keep pace with demand. Attackers are also aware of this problem, forcing a shift in security risk from the network to the application layer, where 84% of all cyber attacks occur.

Organizations of all sizes face similar challenges when it comes to application and container development and deployment:

- Deploying containers with vulnerabilities puts users and their data at risk.
- Developing secure software adds process complexity that could slow productivity and delay availability.
- Rushing the build or test exposes you to risk and may lead to a security breach or production outage.

It's difficult to know what open source code is in your applications, especially after adding them to containers. While you can manage some container images through CI/CD, many can originate outside your sphere of control. Synopsys' Black Duck for OpenShift secures all container images regardless of registry source.

## The solution

The partnership between Synopsys and Red Hat helps organizations build secure, high-quality code—minimizing risks while maximizing speed and productivity. Red Hat OpenShift is a hybrid cloud, enterprise Kubernetes application platform that allows you to build, deploy, and manage your container-based applications consistently across cloud and on-premises infrastructure.

Black Duck automatically scans, identifies, and monitors third-party open source in container images deployed in OpenShift:

- **Black Duck OpenShift Connector.** Deployed as an OpenShift project, the OpenShift connector is integrated into both OpenShift and Black Duck APIs for seamless analysis.
- **Image scanning.** A Black Duck container image scan is triggered during pod creation and image events in supported container registries such as OpenShift Integrated and Quay.
- **Image monitoring.** Black Duck continuously monitors the open source identified in container image scans and annotates and labels pods and images when new vulnerabilities or policy violations occur.

## Solutions

RED HAT® OPENSHIFT

Red Hat Quay

Black Duck Software Composition Analysis + Black Duck Connector for OpenShift

## Benefits

- Automated container image scanning
- Identify security vulnerabilities
- Manage risk from open source components
- Continuously monitor container images for vulnerabilities

Red Hat

Technology Partner

OpenShift Certified Operator

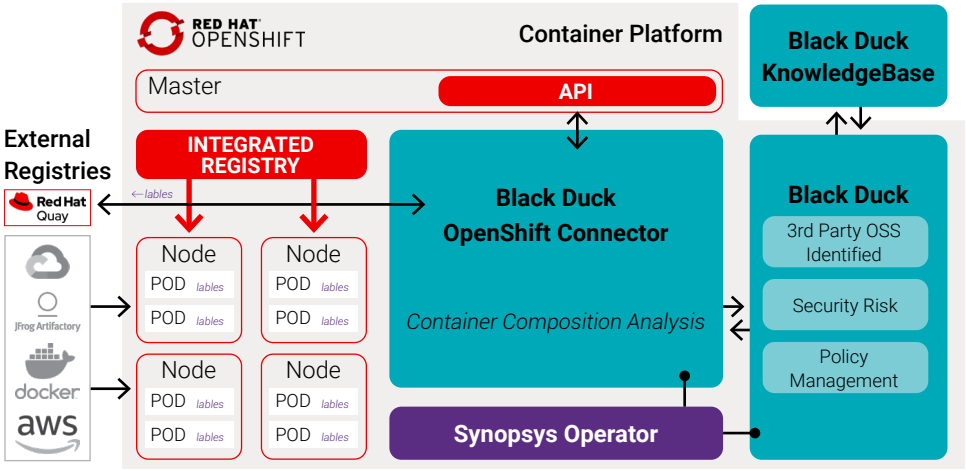
## About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers integrate new and existing IT applications, develop cloud-native applications, standardize on our industry-leading operating system, and automate, secure, and manage complex environments. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500. As a strategic partner to cloud providers, system integrators, application vendors, customers, and open source communities, Red Hat can help organizations prepare for the digital future.

Learn how Synopsys and Red Hat together help customers build secure, high-quality software faster at synopsys.com/RedHat.

## Synopsys and Red Hat Integration Architecture

Organizations must be able to streamline and accelerate development within Red Hat products without sacrificing security. Synopsys' Black Duck for OpenShift is certified as a Red Hat Operator within OpenShift's Operator Hub. It integrates seamlessly with the OpenShift Pod API and Quay webhooks to analyze the composition of container images and identify security, license, and operational issues that must be addressed.




## The benefits

- **Comprehensive container analysis.** Black Duck analyzes everything in a container, including the application layer, using KnowledgeBase™, the most comprehensive repository of open source component and vulnerability intelligence available, with information from over 19,000 data sources.
- **Vulnerability remediation time reduction.** The Synopsys Cybersecurity Research Center provides Black Duck Security Advisories within 24–48 hours of a published vulnerability, helping you make intelligent remediation decisions.
- **Fewer false positives.** Black Duck understands open source forks and Linux backports and marks vulnerabilities as patched when appropriate, significantly reducing the number of vulnerabilities you need to investigate.

Synopsys and Red Hat work together to help customers manage their open source components and associated risks inside container images. Black Duck for OpenShift automatically discovers images as they are created or updated by listening for changes within the image stream and Kubernetes pod events. It 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.

## 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.

For more information about the Synopsys Software Integrity Group, visit us online at 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