sonatype

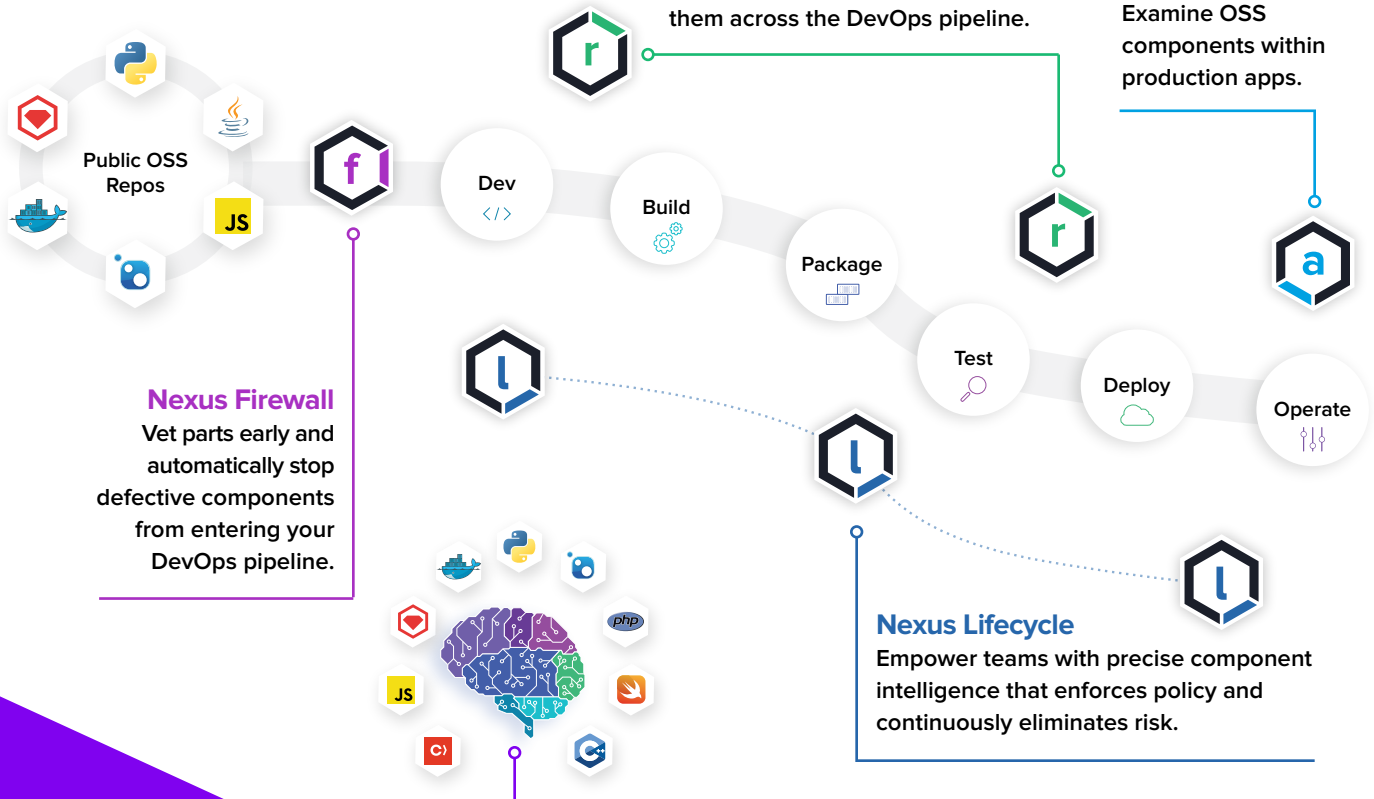
RED HAT® OPENSHIFT Container Platform

Deliver Secure Applications at Scale with Sonatype and Red Hat

Enterprises are increasingly moving toward cloud infrastructures and containers to increase application velocity. While containers make it easier for developers to innovate faster, it does not remove the inherent risk of open source components used to build modern applications. With nearly 90% of an application made up of open source components, it's now more important than ever to automatically enforce open source policy and control risk across every phase of your SDLC.

Containers moving through a DevOps pipeline must be continuously scanned and monitored for security vulnerabilities and license risk. Running an untrusted container can lead to numerous attacks so it's important to validate containers across the entire SDLC and prior to any runtime execution.

The Nexus Platform Automates Open Source Governance at Scale



Nexus Repository Pro

Manage libraries and store parts in a universal repository and share them across the DevOps pipeline.

Nexus Auditor

Examine OSS components within production apps.

Nexus Firewall

Vet parts early and automatically stop defective components from entering your DevOps pipeline.

Nexus Lifecycle

Empower teams with precise component intelligence that enforces policy and continuously eliminates risk.

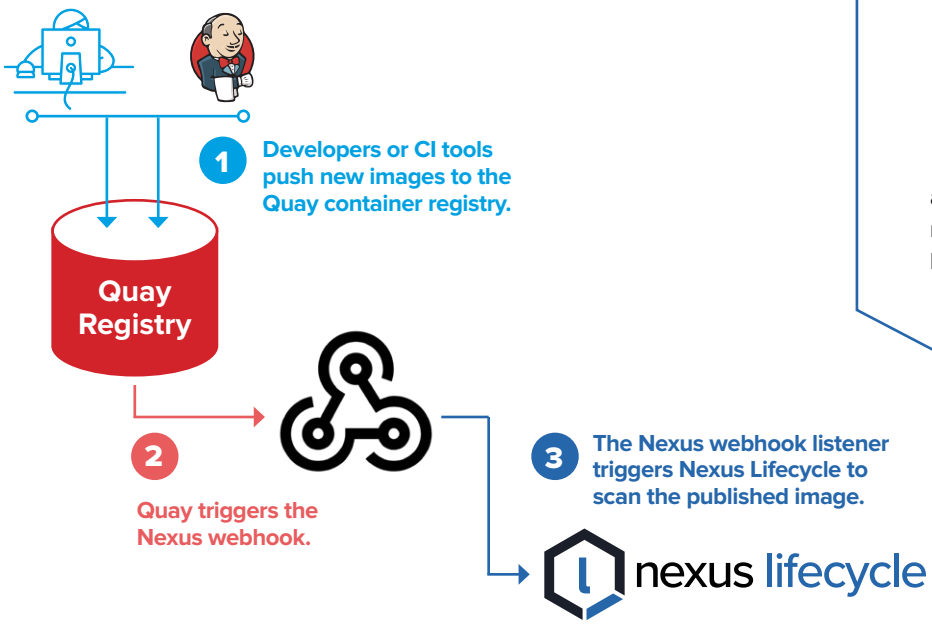
Nexus Intellegence

Superior open source data service continuously refined by AI, machine learning, and 65 world class researchers powers our products.

Nexus Lifecycle and Quay Integration

The container lifecycle lives in parallel to the modern SDLC. Containers are built, stored, and orchestrated using separate solutions than traditional application deployment and management models. Nexus Lifecycle integrates directly with RedHat Openshift and Quay container lifecycle management to automate and enforce open source governance policies in the containerized applications used every day.

Virtually all Docker repositories support webhooks to detect when a container is published to a staging registry and then trigger security scans like Sonatype's Nexus Lifecycle and Docker CIS Benchmarks.



nexus lifecycle

Nexus Lifecycle automatically creates a software bill of materials and identifies any security and license risk found within the containerized application.

Nexus Lifecycle enforces open source policies by sending warning alerts or failing builds as it moves through the container lifecycle.

With an Integrated Nexus Lifecycle and OpenShift Quay Solution:

- Developers continue to adopt containers to speed time to innovation without adding additional risk to their projects.
- Security teams rest assured knowing that applications are continuously monitored for open source vulnerabilities across the SDLC, including production applications.
- Operations teams welcome the continued use of containers to reduce the time and complexity involved in delivering and maintaining production applications.