Snyk & Sysdig Integration: eliminate up to 95 percent of vulnerability noise

Complete container security from source to production

The only solution that enables true DevOps security from the time the first line of code is written, through the full lifecycle of the Kubernetes workload. Secure applications from the start, protect them at runtime, and eliminate up to 95 percent of container vulnerability noise.

"Sysdig's deep runtime security visibility and Snyk's developer-first tooling enables developer, DevOps, and security teams to achieve better alignment so they can manage risk without delaying software releases," **~ Suresh Vasudevan, Chief Executive Officer, Sysdig**

"Together with Sysdig, we're now empowering millions more developers worldwide to innovate securely."
~Peter McKay, Chief Executive Officer, Snyk

Why Snyk & Sysdig?

Snyk and Sysdig deliver the broadest security coverage for cloud-native application development and delivery while helping teams reduce noise and risk. The industry-first integration of Sysdig Secure and Snyk Container enables security and development teams to prioritize and address security issues based on their exploitability and business impact.

Build secure from the start

Begin securing containers as early as the Dockerfile is created by automating the selection of up-to-date, secure base images. Identify issues in code and code dependencies even before they hit your pipelines.

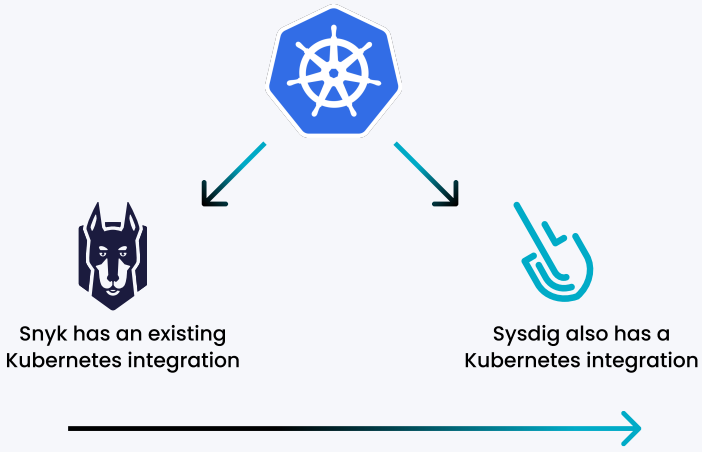
Protect against runtime threats

Detect runtime threats and anomalies across containers, Kubernetes, and cloud, automate alerting and response, and capture detailed activity records for forensics.

Eliminate container vulnerability noise

Cut out up to 95 percent of container vulnerability noise by identifying packages loaded at runtime. Prioritize vulnerabilities to fix first, eliminating the noise of typical container vulnerability scans.

How it Works



01
Snyk exposes information about workload vulnerabilities across CI/CD pipelines, registries, and Kubernetes.

02
Sysdig detects and alerts on container and Kubernetes runtime activity in production environments.

03
Sysdig identifies the container packages that are active in production applications and passes this info to Snyk via API.

04
Snyk filters vulnerabilities using executed package data, significantly reducing the number CVEs of that require developer attention.

Key Use Cases

Container/K8s Security

- Code vulnerability Security/ Scanning
- Image Security
- Automated Base Image Fixes
- Native Git Scanning
- Runtime Security
- Incident Response & Forensics
- Compliance
- Network Security

Cloud Security

- Kubernetes and Cloud Platform Security
- Prioritized Security Alerts
- Cloud Workload Protection

Monitoring

- Security and Monitoring
- Analytics Infrastructure and Application Monitoring
- Ongoing Vulnerability Monitoring

Need more information? Contact jim.armstrong@snyk.io, anthony.seto@snyk.io or wendy.swank@snyk.io or eric.carter@sysdig.com.

sysdig | snyk