



# Build secure containers from the start

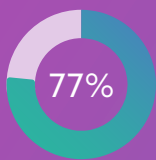
Empower developers to easily find and fix vulnerabilities in containers and Kubernetes applications.

## Containers introduce new risks

Containers are becoming mainstream, but vulnerabilities often go unchecked



75% of global organizations will be running containers in production



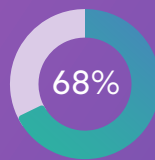
Of the top 1,000 Docker containers, 77% have severe known vulnerabilities

4,500+

Reported operating system vulnerabilities in 5 leading Linux container distributions

## For scalability and speed, container security should be owned by developers

Containers have shifted software packaging to the left and developers now have the responsibility of defining the runtime environment. To support security at scale without slowing down releases, developers need to be enabled to handle container security as well.



68% of developers own the security of container images.

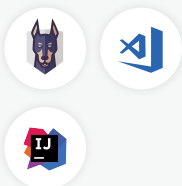
50+

9 of the 10 most popular container images have 50+ vulnerabilities.

## Detect container vulnerabilities throughout the SDLC

### Coding & CLI

Shift security left and test images as they are created



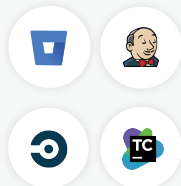
### Code management

Scan Dockerfiles straight from git and fix issues automatically with PRs



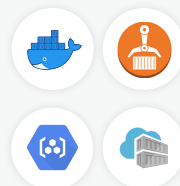
### CI/CD

Integrate security directly into your pipeline. Use policies to break builds based on vulnerability discoveries



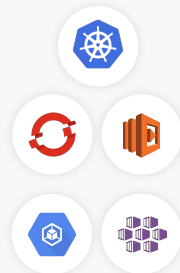
### Registries

Scan images in your registries and continue monitoring for newly disclosed vulnerabilities



### Deployments

Monitor running container workloads and Kubernetes pods



### Reporting

Track trends and exposure close rates across teams and organizations



Powering security across the ecosystem

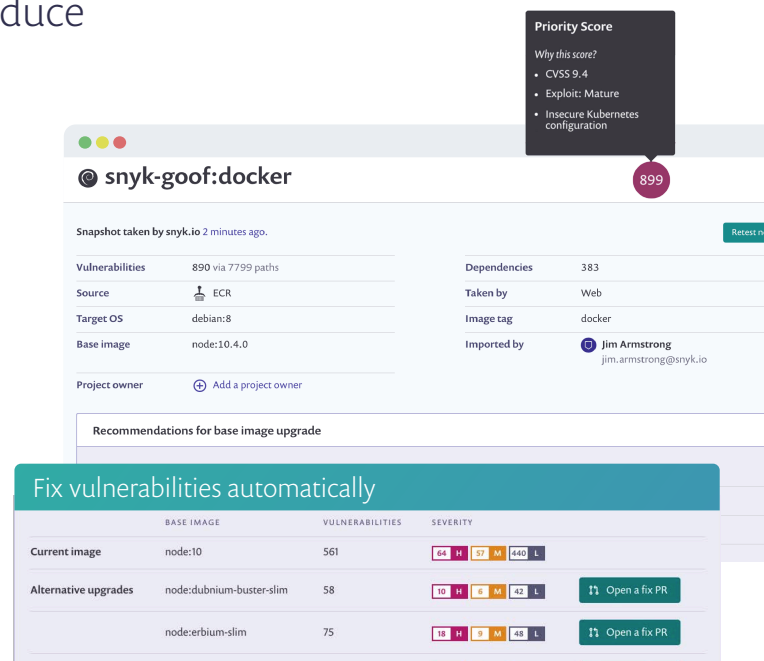
## Light touch and lightweight integration

Snyk enabled us to start following our security processes, looking at vulnerabilities and scanning results, it was a major cultural change for us, and it has resulted in dramatic security improvements.



## Prioritized fix recommendations to reduce time-to-fix and minimize exposure

- ✓ **Automated remediation:** Quickly eliminate vulnerabilities and scale security by upgrading to the most secure base image or by rebuilding the image when outdated.
- ✓ **In-line fixes:** Get straight to the fix, including dependencies and image layers
- ✓ **Prioritize by context:** Focus attention on the highest risk using Snyk's correlation of vulnerabilities across Linux distributions, exploit maturity, and Kubernetes configuration into one priority score.



**Priority Score**  
Why this score?  
• CVSS 9.4  
• Exploit: Mature  
• Insecure Kubernetes configuration

**snyk-goof:docker**  
Snapshot taken by snyk.io 2 minutes ago.

Property	Value
Vulnerabilities	890 via 7799 paths
Source	ECR
Target OS	debian:8
Base image	node:10.4.0
Project owner	Jim Armstrong (jim.armstrong@snyk.io)

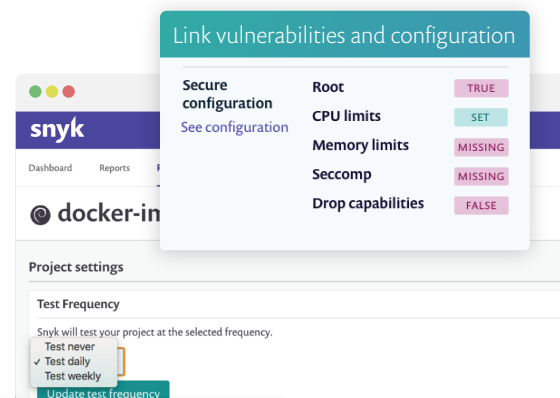
Dependencies: 383  
Taken by: Web  
Image tag: docker  
Imported by: Jim Armstrong

**Recommendations for base image upgrade**

Image	Vulnerabilities	Severity	Action
Current image: node:10	561	64 H, 17 M, 440 L	
Alternative upgrades: node:dubnium-buster-slim	58	10 H, 1 M, 42 L	Open a fix PR
node:erbiun-slim	75	18 H, 17 M, 48 L	Open a fix PR

## Monitor continuously to protect after deployment

- ✓ **Image monitoring:** Monitor your images for newly discovered vulnerabilities and receive alerts via Slack, Jira or email.
- ✓ **Code, containers and Kubernetes:** One tool for security across all aspects of your application, with advanced project management capabilities to help you organize and govern projects as you scale.



**Link vulnerabilities and configuration**

Setting	Value
Secure configuration	See configuration
Root	TRUE
CPU limits	SET
Memory limits	MISSING
Seccomp	MISSING
Drop capabilities	FALSE

**Project settings**

**Test Frequency**  
Snyk will test your project at the selected frequency.  
☐ Test never  
☒ Test daily  
☐ Test weekly  
[Update test frequency](#)



New message from snyk

New vulnerabilities affect 1 of your projects in the Snyk Gitlab Broker organisation.

## Enhance your coverage with Snyk Open Source

Snyk Open Source works together with Snyk Container to provide end-to-end coverage of your applications by adding open source dependency vulnerability detection and fixes. Get automated fixes to the vulnerabilities detected via Snyk's native integrations throughout the development process, all built on top of Snyk's comprehensive database of vulnerabilities in open source.

QUICK START FOR FREE

sales@snyk.io

www.snyk.io