

Develop fast. Stay secure.

Key Benefits

- Automate base image upgrades to quickly resolve numerous vulnerabilities
- Continuous monitoring for new exposures
- Match potential threats to Dockerfile commands
- Prioritize fixes based on context and exploitability
- Discover issues in open-source libraries

Product Overview

Snyk Container is a security solution designed to help developers find and fix vulnerabilities in cloud-native applications. Snyk's seamless integration empowers developers to continue to develop fast while ensuring secure code with continuous monitoring of applications in production.

Product features

Continuous monitoring for new vulnerabilities

Import your projects and monitor containers for vulnerabilities. Snyk Container tests your imported projects for known security issues at a frequency you control.

Automated base image remediation

Scale your security capabilities by enabling developers to quickly reduce a multitude of vulnerabilities by upgrading to a more secure base image or rebuilding when the base image is outdated.

Application and container vulnerabilities together

You may not always have access to the original source code that runs in your containers, but vulnerabilities in your code dependencies are still important. Snyk can detect and monitor open-source dependencies for popular languages as part of the container scan.

Prioritize the vulnerabilities posing the highest risk

Ignore or exclude susceptibilities from base images and use risk signals like exploit maturity and insecure workload configuration to help teams cut through the typical noise of container vulnerability reports.

Empower developer teams

Instead of assuming every developer knows the ins and outs of Linux maintenance, Snyk Container gets them straight to the Dockerfile command and dependencies that introduce potential risks.

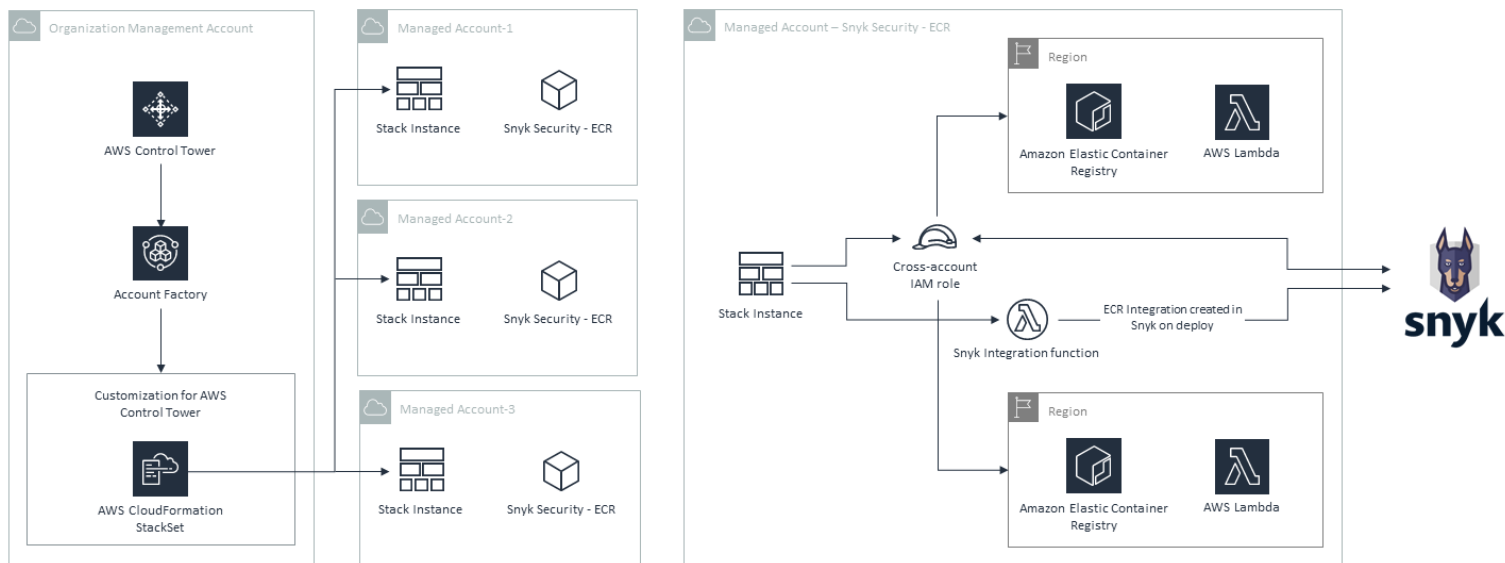


How it works

Snyk Container integrates with Amazon ECR to help you import projects and monitor containers for vulnerabilities. Snyk Container tests your imported projects for known security issues at a frequency that you control. Integration with Amazon Elastic Container Registry (Amazon ECR) is available for all pricing plans.

The Snyk Container integration makes use of AWS CloudFormation to provision an Amazon ECR container registry through AWS Control Tower. When the CloudFormation template is deployed to a region, a single-use AWS Lambda function is deployed which connects to Snyk and establishes the initial integration. A cross-account IAM role is used thereafter to handle access between Snyk and the newly deployed Amazon ECR.

When the AWS CloudFormation stack has been successfully deployed, you're ready to import your projects from the newly launched Amazon ECR registry into your Snyk account.



Differentiators

- Advanced security for all the components of the modern cloud native application in a single platform.
- Security intelligence provides access to our comprehensive vulnerability data to help your own security systems.
- Compliance management offers open-source license usage across your projects.

Data points

1.5+M

Developers build securely with Snyk

8Hrs

Saved per vulnerability through automation

37%

Developers don't implement security automation during CI

2.5X

Increase in open-source vulnerabilities in the last three years