SOLUTION BRIEF

Secure your Software Supply Chain with Snyk

The greatest risks to your software supply chain come from the pieces out of your control: the ever-increasing usage of third-party, open source libraries, packages, and container base images. Recent high-profile vulnerabilities and malicious packages have accentuated the importance of a secure software supply chain, and government regulations and mandates have put the software bill of materials (SBOM) in the spotlight. SBOMs help with software transparency, but there is more to software supply chain security than SBOMs.

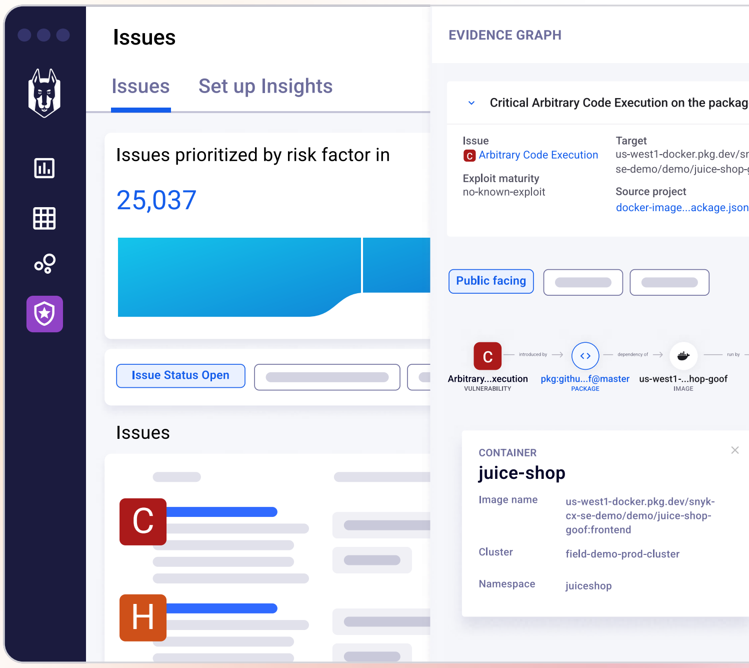
Snyk's Software Supply Chain Security Solution enables AppSec and development teams to reduce their software supply chain risks across the entire SDLC by helping find, prioritize, and fix vulnerabilities in container images, open source libraries, and first-party code. When developers are empowered and enabled to find and eliminate vulnerabilities in third-party dependencies, and AppSec teams can provide guardrails to ensure that security policies are adhered to, so organizations can focus on their products rather than just security.

snyk

Extensive Visibility

Backed by the Snyk Vulnerability Database, Snyk works to identify and fix security vulnerabilities in your projects across the SDLC, protecting:

- **The code you write:** AI-driven, real-time SAST protection helps developers secure code as it's being written, whether you're doing it by hand or leveraging generative AI
- **The open source dependencies you leverage:** Identify vulnerable and malicious packages and eliminate dependency confusion
- **The containers you leverage, build, and deploy:** Find security issues in your base images and the ones you derive from them while being able to determine how, where, and when vulnerabilities were introduced
- **Your deployment manifests:** Identify issues in your Infrastructure as Code to secure misconfigurations and detect drift to stay secure across your public and private cloud infrastructure



Issues

Issues prioritized by risk factor in

25,037

Issues

EVIDENCE GRAPH

Critical Arbitrary Code Execution on the packag

Issue: C Arbitrary Code Execution

Exploit maturity: no-known-exploit

Target: us-west1-docker.pkg.dev/sr se-demo/demo/juice-shop-

Source project: docker-image...ackage.json

CONTAINER

juice-shop

Image name: us-west1-docker.pkg.dev/snyk-cx-se-demo/demo/juice-shop-goof:frontend

Cluster: field-demo-prod-cluster

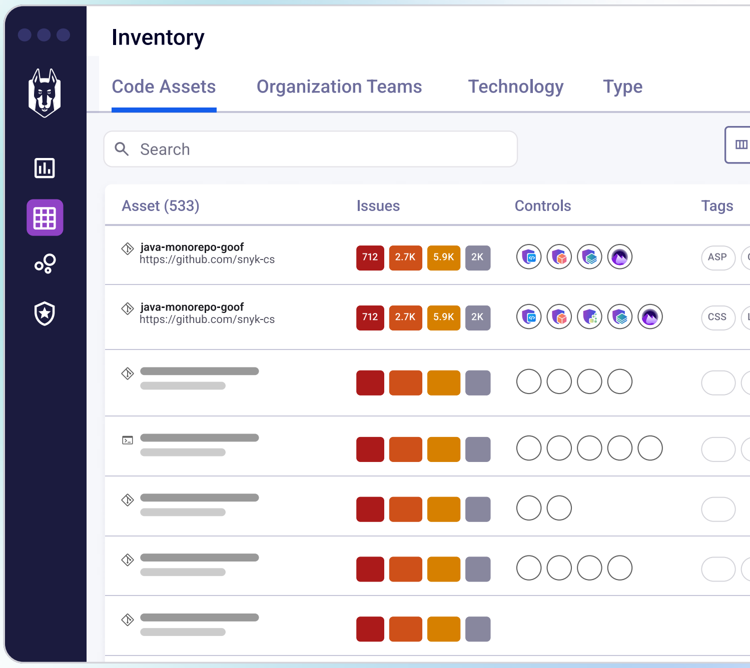
Namespace: juiceshop

All while providing your security team with at-a-glance oversight of your overall security risk posture.

Risk-based prioritization

Determining which vulns to fix first can become daunting when you have hundreds or thousands of vulnerabilities across your application ecosystem. Reachability and vulnerability scores are just two of the risk factors when triaging and prioritizing remediation, but Snyk helps you figure out what to fix first by also considering:

- **Operating system impact:** Some vulns impact various operating systems differently, so the OS you're running on can directly impact the potential risk
- **Runtime risk factors:** Taking into consideration whether or not a vulnerability is in a component that has been deployed allows you to prioritize fixes to mitigate the highest risks first
- **Deployment configuration:** Improperly configured workloads can amplify the potential risk of vulnerabilities: unbounded CPU or memory can lead to DoS, while pods configured with heightened privileges can lead to host compromise
- **Public facing:** A vulnerable component or service that is directly connected to an external, public-facing endpoint poses a greater risk than if it were isolated from direct traffic



Inventory

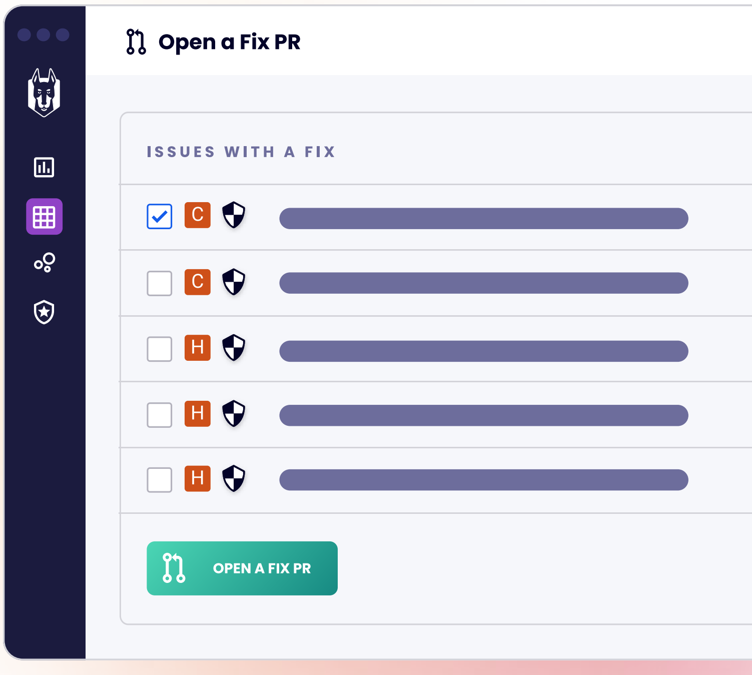
Asset (533)	Issues	Controls	Tags
java-monorepo-goof https://github.com/snyk-cs	712 2.7K 5.9K 2K		ASP
java-monorepo-goof https://github.com/snyk-cs	712 2.7K 5.9K 2K		CSS

These additional signals help Snyk compute a proprietary risk score, which takes into consideration the additional context, enabling you to prioritize, manage, and track security issues and fixes. And, behind the scenes, the world-class security research division at Snyk makes it possible to see risk sooner, enabling you to remove risks faster.

Actionable and automated remediation and prevention

Finding vulnerabilities is great, and fixing them is better. What's even better than that is the ability to fix them automatically in the tools your developers are already using.

- **Fix vulnerabilities in the code you write:** Right in the IDE, with information about why it's vulnerable, with tips and helpers to make your code more secure
- **Customizable one-click fix PRs:** Automatically remediate vulnerabilities in your open source dependencies and reduce third-party risks to your components
- **Wipe out container image vulnerabilities:** Base image recommendation workflows enable you to eliminate multiple vulnerabilities at once rather than one by one, with a single click, allowing your developers to focus on their applications rather than maintaining base images
- **Secure your Infrastructure as Code (IaC):** Empower developers to proactively fix security issues directly in their IDE, CLI, and Git workflows, reducing backlogs and time to fix

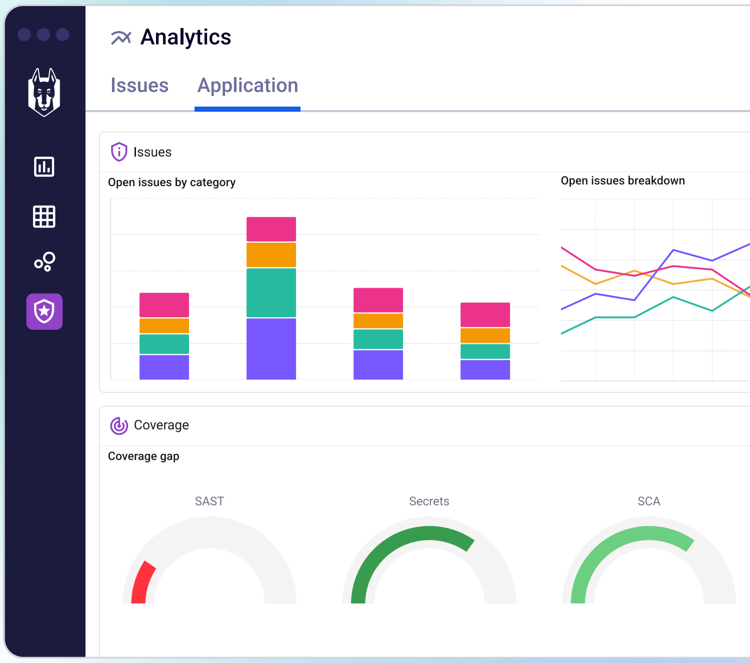


Security works best when it's a habit that happens early and often in the development process and continues throughout delivery. The easiest way to achieve this is to ensure that you provide security tooling that doesn't get in your developers' way but is baked into their workflows and how they work. This shift-left approach, combined with continual monitoring, helps find and fix existing vulnerabilities and provides fast identification and remediation from newly discovered zero-day vulns.

Validate and govern your AppSec program

Security best practices and policies are just guidelines until they're enforced. Snyk allows you to instantiate those guidelines to make sure that they're being adhered to so you can ensure that software that exceeds your risk thresholds doesn't make it into production.

- **Guardrails in CI/CD pipelines:** Enforce security and software license policies with automatic PR checks and security gates in build pipelines to break the build when policies are exceeded
- **Asset discovery:** Comprehensive visibility of the inventory assets involved in building, deploying, and running applications, ensuring they know about every software asset that needs to be protected
- **Identify any gaps in security coverage:** You can't secure what you don't know about, so Snyk helps pinpoint coverage gaps and evaluates the overall performance of your security program
- **Runtime intelligence:** to incorporate runtime risk factors to more effectively prioritize remediation efforts while enhancing application discovery

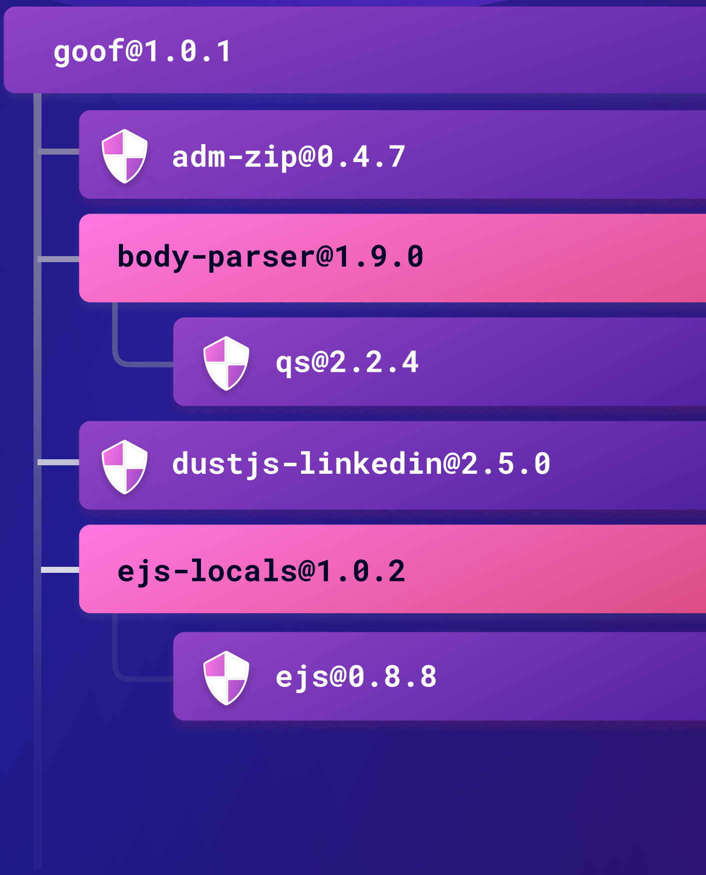


Snyk provides AppSec teams comprehensive visibility into applications across the software development lifecycle (SDLC), from development to runtime, ensuring they know about every software asset that needs to be protected as part of their AppSec program.

Enable software transparency with SBOMs

Whether you're required to share SBOMs for your apps and services or you receive them from your vendors and providers, Snyk helps you translate software transparency into a current risk snapshot.

- **Generate SBOMs:** Snyk can generate CycloneDX and SPDX format SBOMs from your container and open source projects, so you can provide internal teams or external customers a snapshot of your dependencies
- **Test SBOMs:** New vulnerabilities are discovered every day, so it's critical to check the security posture of an SBOMs on a regular basis: the SBOM that seemed secure yesterday might have a zero-day lurking in it today.
- **Enrich SBOMs:** Add vulnerability and license information to provide a point-in-time picture of the related security posture.



Be ready for the next zero-day vulnerability

New vulnerabilities are discovered every day – over 28k were discovered in 2023 alone. Snky helps you identify and mitigate risks posed by zero-day vulns.

- **Find out sooner:** Snyk's vulnerability data goes beyond other sources, and often come out ahead of them for open source vulnerabilities, allowing you to detect vulnerabilities earlier than products using other databases.
- **Identify impacted projects:** Snyk keeps track of what libraries are used by which of your projects, allowing you to quickly identify affected projects and which org owns them
- **Prioritize and fix, fast:** Leverage Snyk's automatic fix tools to quickly fix vulnerabilities in open source dependencies or move you to the stable version of your container base images

Reduce risks in your software supply chain with Snyk. Empower developers to find, prioritize, and fix vulnerabilities in first-party code and third-party packages and container images, and provide your AppSec teams the tools they need to govern your security practice and identify gaps in security coverage, while providing teams visibility of their overall risk.

snyk