

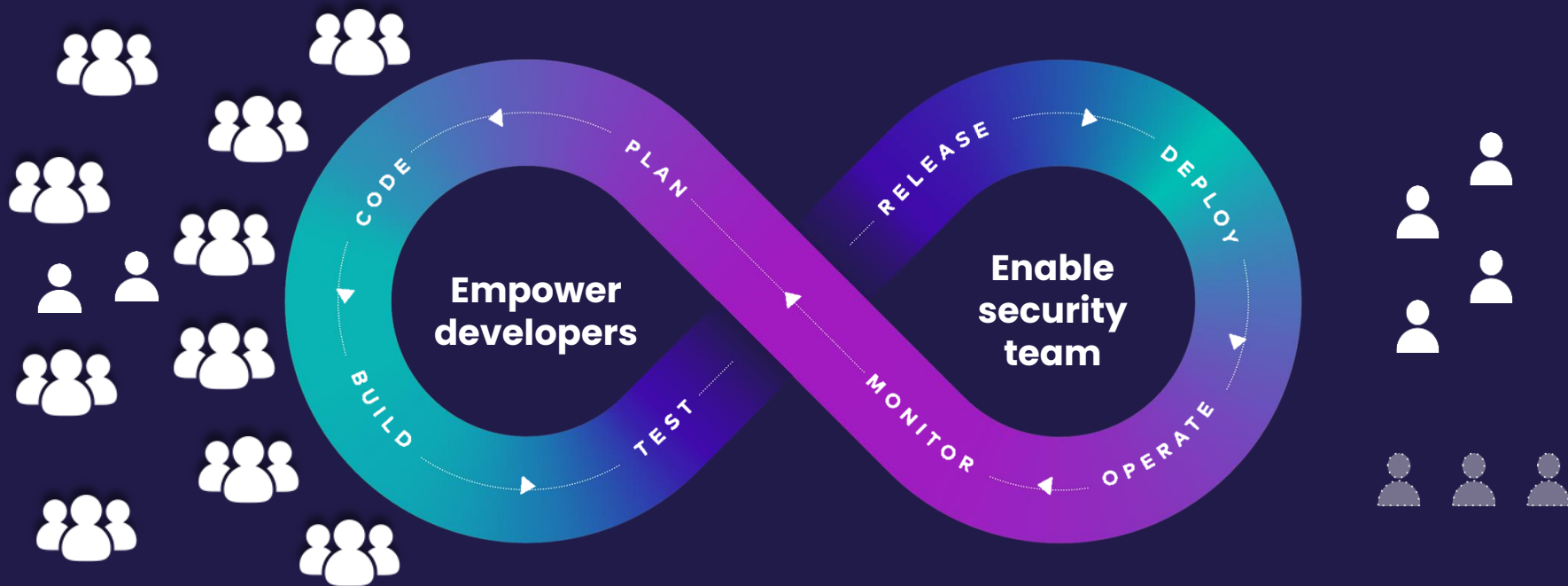


snyk

Develop fast.
Stay secure.

DevOps requires dev first security

Empower developers to build applications securely within the entire development process



32M global developers

*Understanding the Significance of the Worldwide Developer
Forecast, 2020–2025: Part-Time Application Developers Lead Growth*

4.19M global cybersecurity staff; 2.7M staff shortage

Source: (ISC)² Cybersecurity Workforce Study, 2021

The modern application

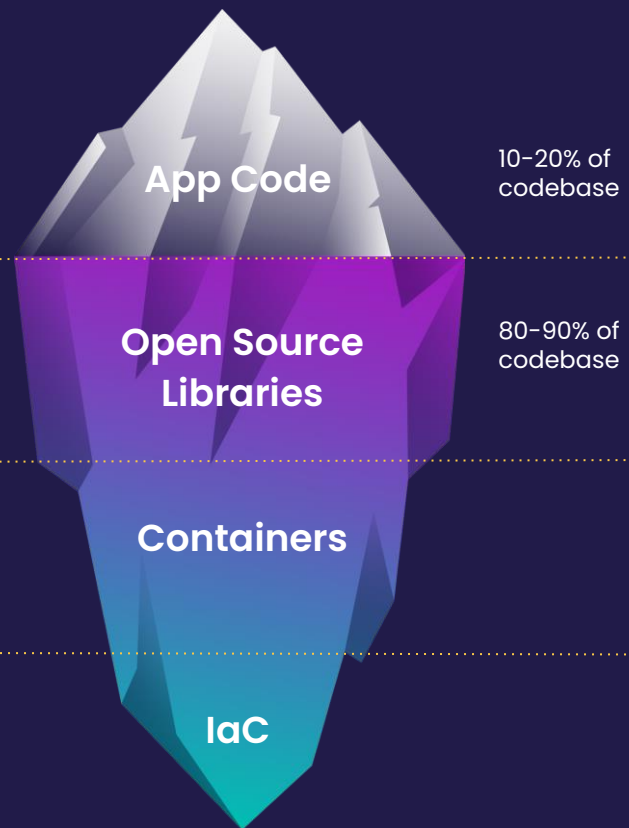
A New Risk Profile

Deployed daily – waterfall approach doesn't scale. Scans can't take hours.

80% of vulnerabilities found in indirect dependencies

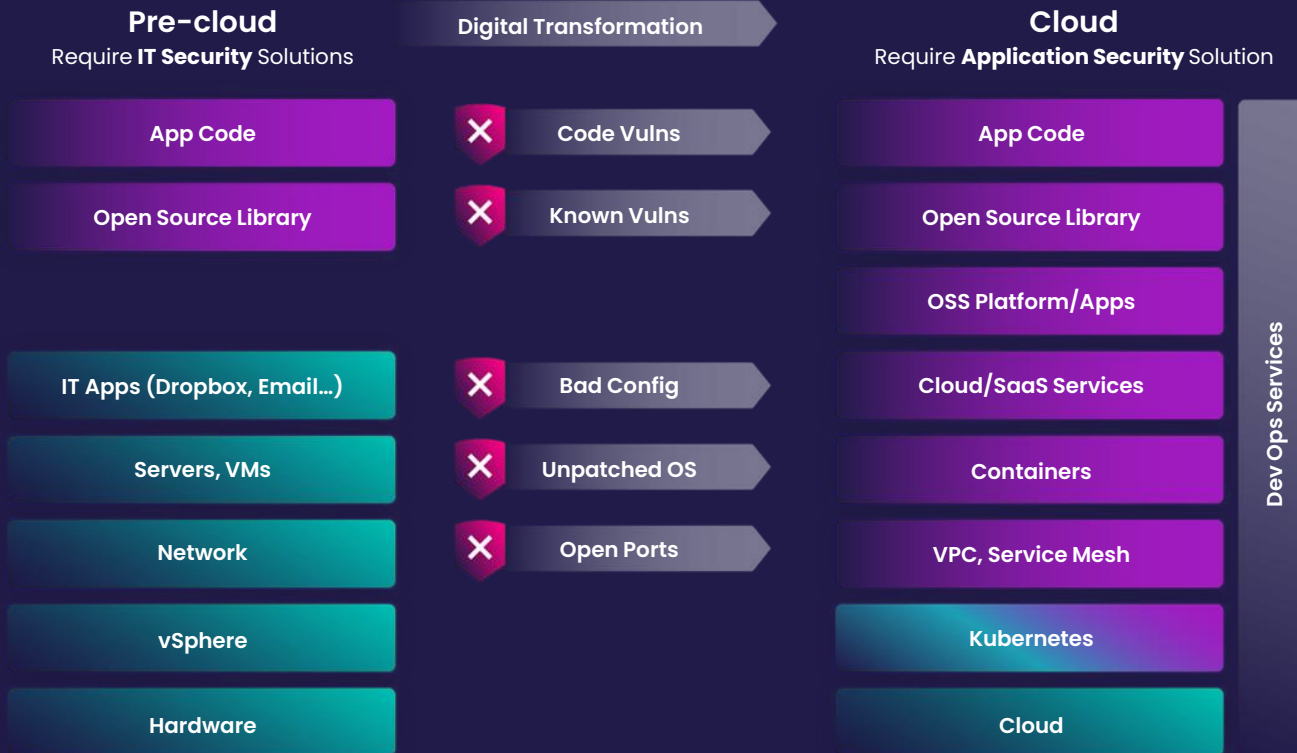
100s of Linux packages, and their vulnerabilities, inherited with base images

#1 cloud vulnerability is misconfiguration
[NSA]



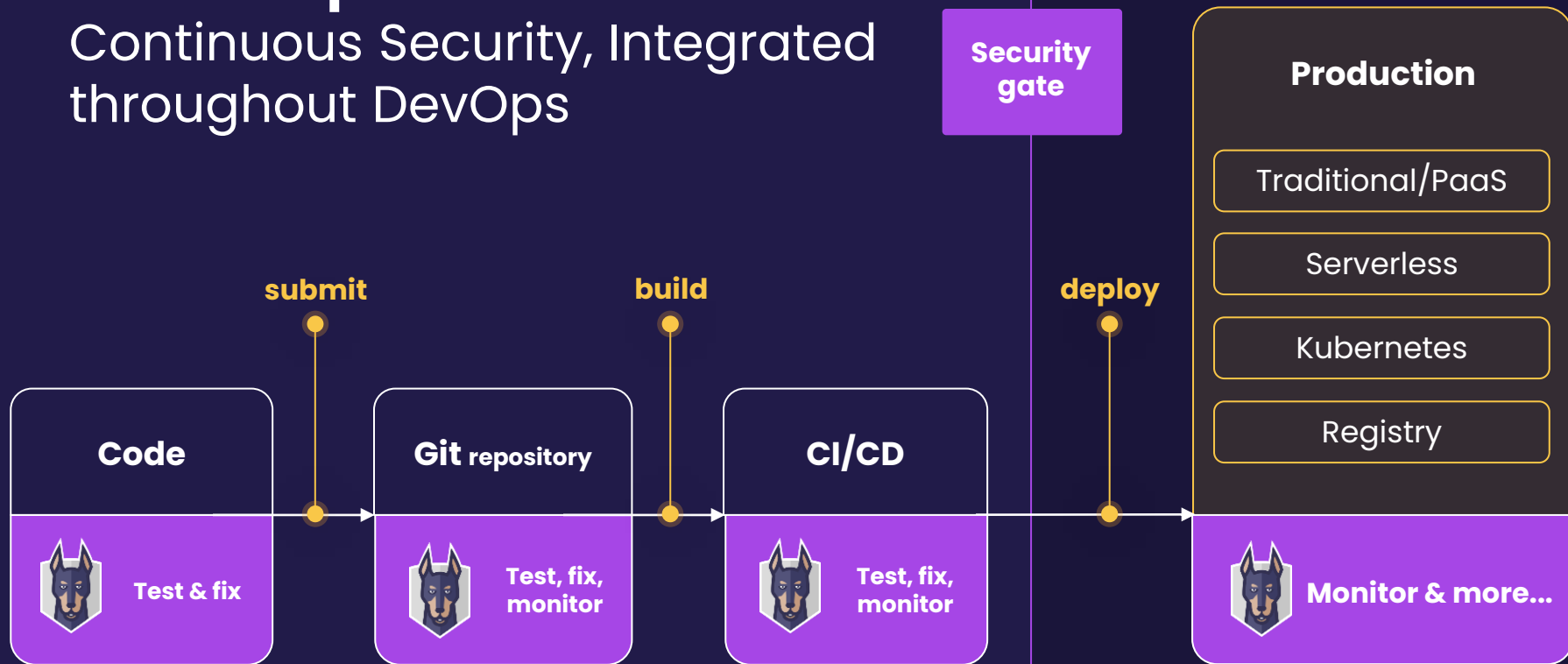
Cloud turns IT into App Services

Dev
IT/Op



DevSecOps:

Continuous Security, Integrated throughout DevOps





Developer Security Platform



Snyk Code



Snyk Open Source



Snyk Container



Snyk IaC

Developer Experience

Application intelligence

Security intelligence

Empowerment

Extensibility

Governance

Founded on belief that developers can and should handle security

Snyk is all about DEV

- Developers **drive adoption!**
- Need to love it to use it
- Otherwise **'work around it'**

snyk.io



What does DEV product mean?

- Self serve usage
- Tight GitHub integration
- Robust CLI
- Super clean CI/CD integration
- **Easy fix** that doesn't require a lot of developer time and expertise
- Broad use in open source projects - leading indicator of **"what's right"**
- Avoid mistakes of others designed to serve a central administrator first, and be **pushed down** on development.

snyk.io



Thank you!



snyk

snyk

Additional slides

Our expertise. Your success.

Continuously helping you make the most out of Snyk

Snyk's Customer Success programs provide the expertise and resources you need to successfully implement your application security program and maximize the return on your investment with Snyk.

- **Flexible**
Get the right level of support for your team
- **Expert**
Leverage Snyk's experience with developer-led application security
- **Ongoing**
Realize value throughout your journey with Snyk



Onboarding



Scaling



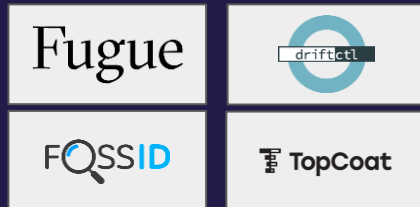
**Sustained
Success**



snyk

Snyk's Last 12 Months

M&A



New Alliances



Partner Progress

- Partnered with Google on Assured Open Source program
- Snyk Technical Alliance Partner program launched with Atlassian, Sysdig, Docker, Hashicorp, Stackhawk
- Joined ServiceNow TAP program
- Strategic Atlassian partner - exclusive first-party integration in Bitbucket Cloud
- OpsGenie integration
- Exclusive first-party integration with AWS CodePipeline
- Snyk vulnerability database powers Amazon Inspector, Dynatrace Application Security Module
- AWS Security Competency
- Red Hat Container Certification
- IaC integration with Terraform Cloud Enterprise



Snyk Code – Find and fix vulnerabilities in application code in real time



Snyk Learn – Security education designed for developers

Product Enhancements

Q2 2021

- Snyk Team plan
- JetBrains IDE Support for Open Source and Code
- Project Attribute Policies
- Elixir Support for Open Source
- Maven plugin 2.0
- Code in Free Plan
- Critical Severity
- Snyk IaC CLI - Terraform Plan Scanning
- GitHub Code Scanning Support for Open Source
- CloudFormation Support in IaC
- Container Kubernetes Workloads Automation
- Visual Studio IDE plugin for Open Source

Q4 2021

- Snyk Learn released
- Snyk Apps
- Snyk Open Source.NET remediations
- Snyk Open Source in VS Code
- Snyk Code Local Engine Beta
- Snyk IaC ARM file support
- Acquisition of driftctl
- Snyk IaC Custom Rules
- Snyk Open Source fixes in CLI

Q3 2021

- Malicious Packages
- Container - Automatic Base Image Detection
- Social Trends
- Snyk Policies
- Snyk Code Python and PHP
- Snyk Code Priority Score
- Jenkins plugin
- Additional Container Registries
- Improve Reachable Vulnerabilities(Java)
- Snyk IAC CLI Ignore
- New Smaller and Faster CLI

Q1 2022

- Unmanaged C/C++ in Snyk Open Source
- IaC, Container, and Snyk Advisor in JetBrains IDEs
- Native integration with Atlassian Bitbucket
- IaC drift management
- IaC integration with Jira and central reporting
- Terraform variable support
- All Snyk products available self-serve
- Self-serve SSO

Snyk helps companies develop fast & stay secure



Customers

1800+



Quarterly
Tests

332M+



Raised

\$850M



Globally
Distributed

13 Hubs

Remote Snykers all
over the world

PROTECTED BY SNYK

Google



intuit



asurion



snyk

Driven By Strong Values



Care Deeply



Ship It



One Team



Think Bigger

And Committed to ESG

Snyker Impact

Snykers' volunteering and mentorship of non-profits

Snyk Technology Impact

Snyk product donations and discounts to non-profits

Snyk Community Impact

Donations to diversity-leading non-profits at DevSecCon

Snyk Business Practices

Commitment to carbon neutrality

Snyk Intel Provides Cutting-Edge Security Intelligence



Find More

>3x

More vulnerabilities covered than next publicly available database

Know Sooner

>92%

Of JavaScript vulnerabilities in National Vulnerability Database were added to Snyk Database first

Identify Accurately

Low False Positives

Thanks to continuous and deep quality controls

Fix Smarter

Remediation Insights

Hand-curated data and enriched metadata to guide prioritization and remediation decisions

Trusted by



snyk

Integrated with development tools



Docker Visual Studio 2019 VS Code



WebStorm PyCharm buildah



PhpStorm GoLand Eclipse



IntelliJ RubyMine Snky CLI

Coding



GitHub GitHub Enterprise



Bitbucket Cloud Bitbucket Server



Azure Repos GitLab

Source Control



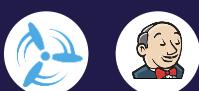
CircleCI Snky API



BitBucket Pipelines AWS Code Pipeline



Azure Pipelines TeamCity



Concourse Jenkins

CI/CD



IBM Cloud VMWare Tanzu Heroku



Kubernetes Azure Functions Cloud Foundry



Docker & others AWS Lambda RedHat Openshift

Runtime



Harbor Quay



npm Enterprise Private Registry Amazon ECR



Artifactory Google Container Registry



Docker Hub Azure Container Registry

Registries



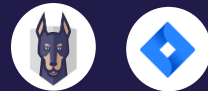
Brinqa Fortify SSC



Nucleus Security Vulcan



Kenna Security RiskSense



Snky API Jira



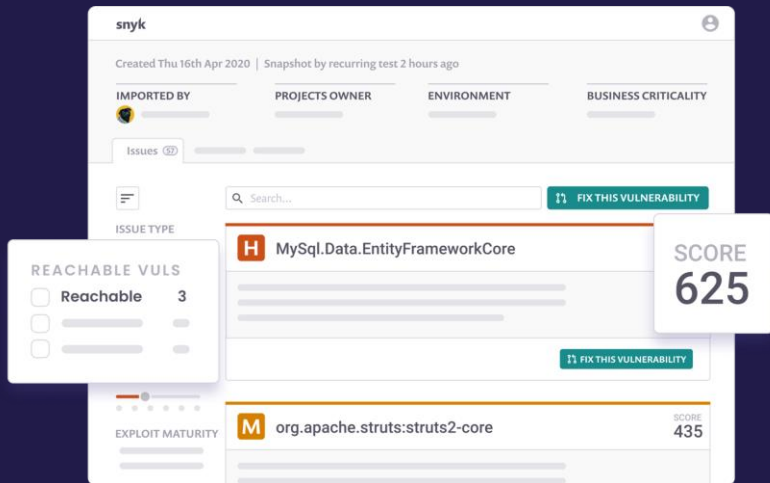
micro focus Slack

Issue Management

Developer-first prioritization

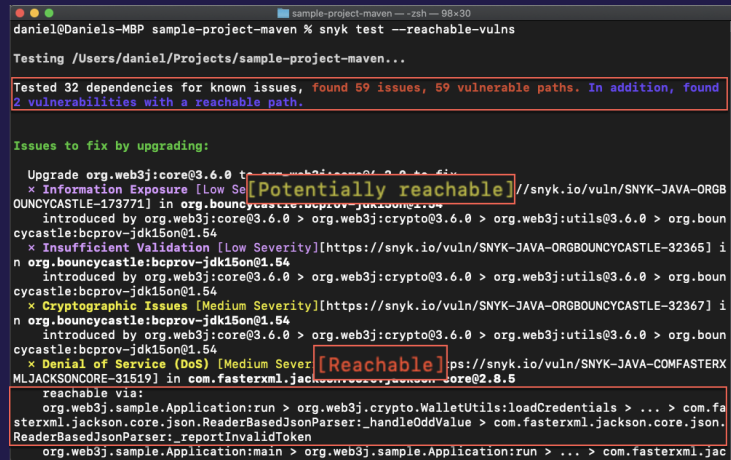
Focus remediation efforts on the issues posing the greatest risk

Instant prioritization



Priority scoring and exploitability indicators
for fast and accurate triaging

Deep application context



Reachability indicators for context-informed
prioritization

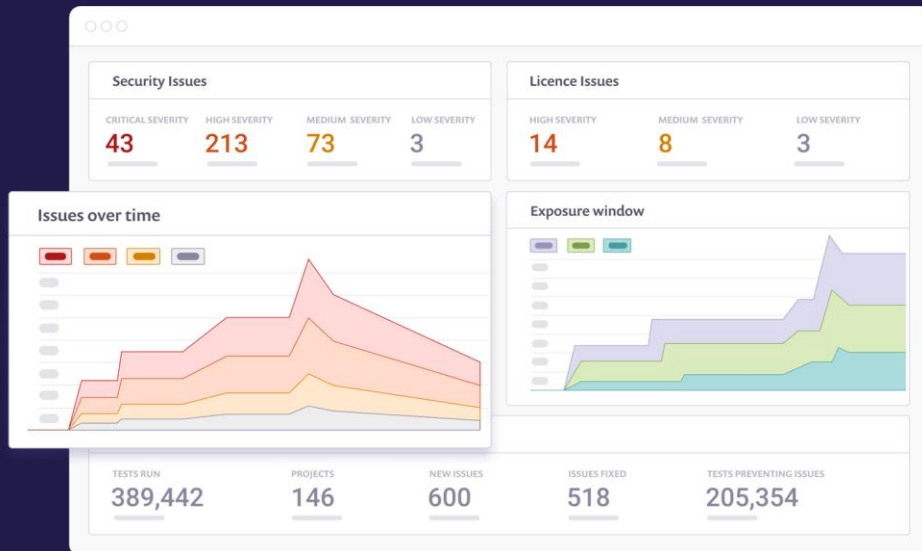
Governance at scale

Overall security status

Monitor the risk and exposure over time and the actions taken to secure

Dependency health

Track overall health status, identify the deprecated packages and take action accordingly



Actionability

Find issues with available solution, filter and implement automatically.

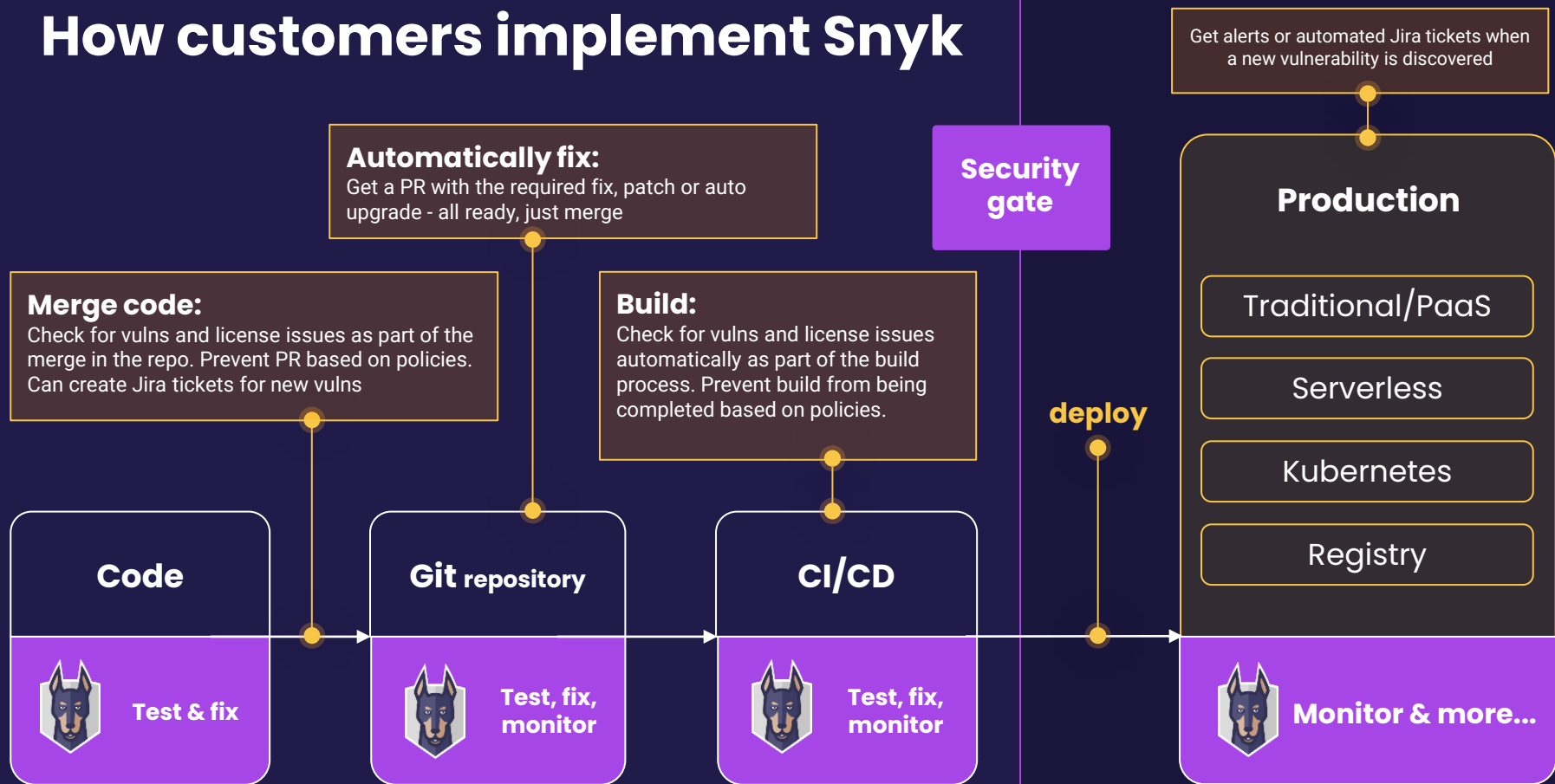
Policies

Manage security and license compliance using automated and fully-customizable rules.

Project management

Manage your security and legal posture across your different projects more efficiently.

How customers implement Snyk



Snyk Extensibility & API

Tune Snyk's security automation to fit into existing development workflows

- ✓ User-friendly and easy to implement
- ✓ Client libraries for Python, Ruby, Go, PHP, JavaScript
- ✓ Supported across Snyk products
- ✓ Tech solutions for custom requirements



**Automated security
testing**



**Security management
at scale**



**Vulnerability
monitoring**



**Incident
management**


“

API is an important requirement for us when deploying new tools. We believe in actionability and making it as easy as possible for developers to take action, and Snyk's API enabled us to build a tool that integrates security into the processes developers are already using. ”

LUNAR[®]

Flexible deployment options to meet your business needs

Provided as Software-as-a-Service (SaaS), Snyc's deployment options offer ease of use and scalability while also providing the required level of data protection.

Snyk developer security platform		
		
As multi-tenant SaaS	As single-tenant SaaS	
The simplest and most cost-effective way to use Snyk's developer security platform.	Private Cloud on AWS – an isolated instance of the Snyk developer security platform.	
<ul style="list-style-type: none">• Data encryption in transit & at rest• GDPR, Soc 2, ISO 27001/270017	<ul style="list-style-type: none">• Data residency (US, EU)• Single Sign-On	<ul style="list-style-type: none">• Audit logs• 99.9% uptime SLA

PROTECTED BY SNYK

Google



Intuit

Telstra

ASOS
discover fashion online

asurion

New Relic

snyk

Lessons learned from Apache Struts: a vulnerability that lead to a real-life hack

EQUIFAX

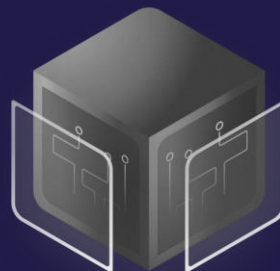
Apache Struts (CVE-2017-5638) attacks timeline: +150M People had highly personal data exposed



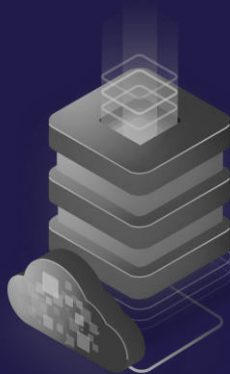
Snyk products



Code



Container



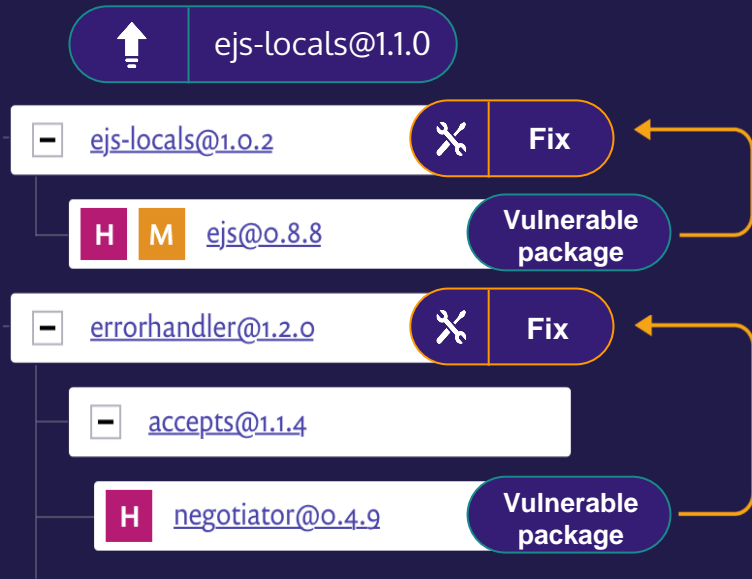
Infrastructure
as Code



Open Source

Automated Remediation

Solving the complex fix logic



Single-click fix pull request



Be license compliant as early as coding

Start early

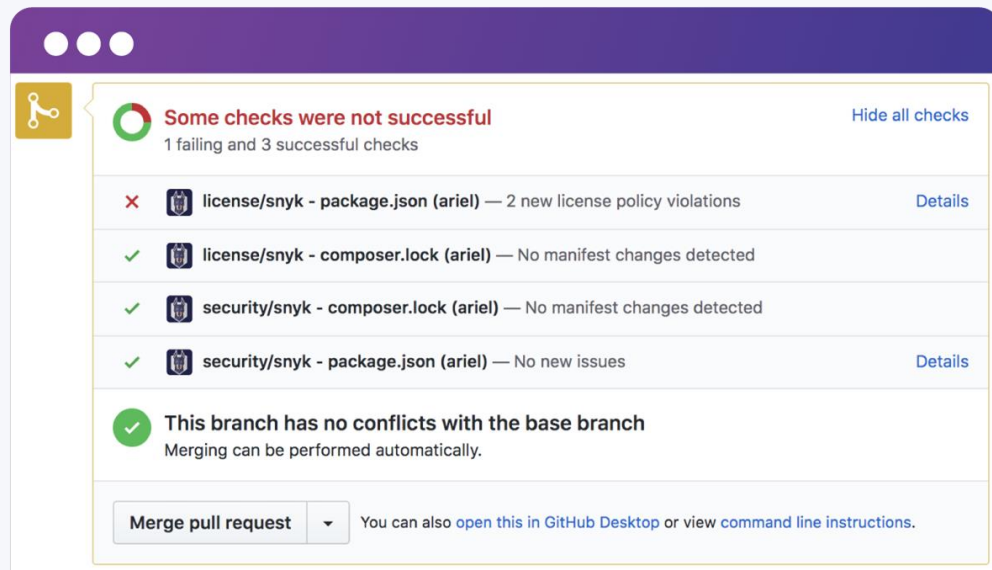
Verify compliance at every stage of development

Scan

Get visibility to all the licenses that are being used.

Comply

Define policies and take automatic actions to verify compliance.



Copyright info

BOM report

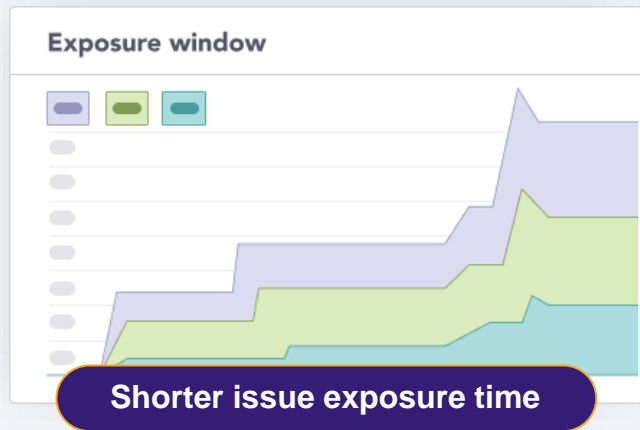
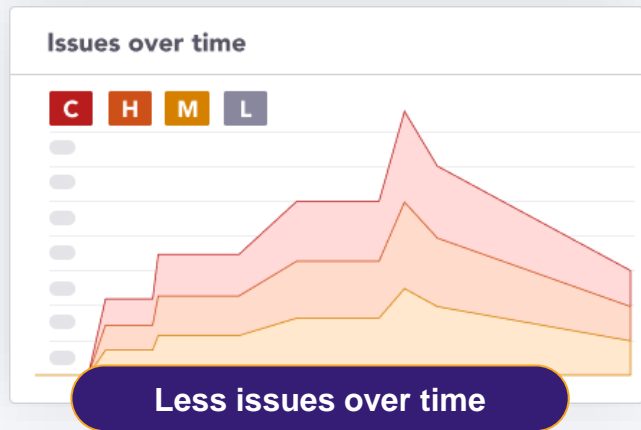
Policies

Gating non-compliant
packages

Legal team actionable
instructions

Automated Remediation

Fix MORE issues, QUICKER



Accelerating MTTF (mean time to fix)

Automated Remediation

Automation and patching

Single-click fix pull request

Automatically calculates the minimal direct dependency version upgrade needed



Uniquely developed and tested patches

- backporting the original fix, tested rigorously
- minimal changes required without breaking changes



Of vulnerabilities instances can't be fixed by an upgrade



patches are applied each month by Snyk's customers

Snyk Intel Vulnerability DB – data and insights



Enriched data from numerous vulnerability databases

Such as CVE, NVD and more. Data derived from these resources is analysed, tested and enriched, before being included in the database



Proprietary research for new vulnerabilities

Our Security team is working to uncover severe vulnerabilities in key components - 66 zero-day vulnerabilities discovered in 2021



Threat Intelligence systems

Listen to chatter on security bulletins, Jira boards, Github commits; to automatically identify vulnerabilities yet to be reported. For example, Apache Airflow and Marked



Community relationship

Snyk collaborates with the community and operates bug bounties for new disclosures, resulting in hundreds of community disclosures, such as f2e-server



Collaboration with academia

The team partners with PhD academia labs such as Berkeley, Virginia Tech and Waterloo, to exchange tools, methods and data. Findings are then exclusively disclosed by Snyk

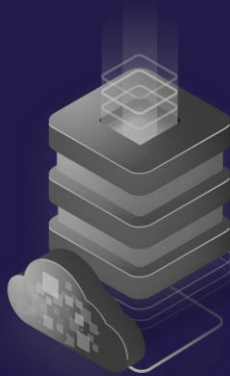
Snyk products



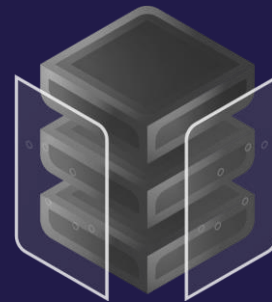
Code



Container

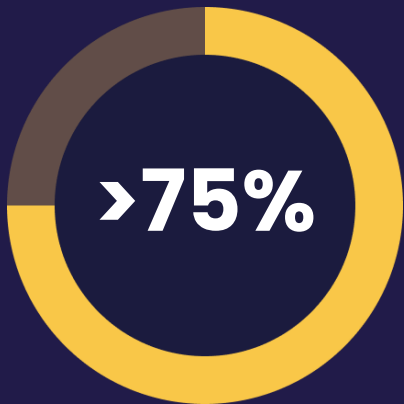


Infrastructure
as Code



Open Source

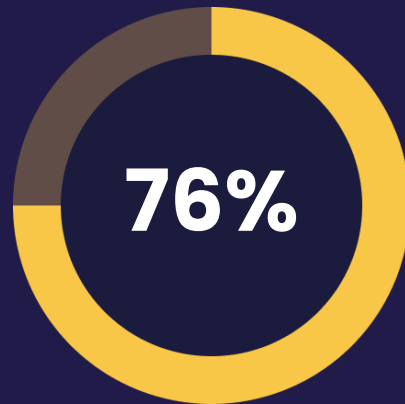
Containers are fast becoming mainstream, but vulnerabilities often go unchecked



of global organizations will
be running containerized
applications in production
by 2022



The top 10 most popular
images have more than 30
vulnerabilities



of the top 1,000 Docker
containers have severe
known vulnerabilities

Snyk Container

Build and maintain secure containers



Detecting

container vulnerabilities
throughout the development
process



Remediating

automatically to minimize
exposure and reduce time-to-
fix



Monitoring

continuously, and protecting
the image after the initial
scan

Detecting container vulnerabilities throughout the development process



Application vulnerabilities



Operating system vulnerabilities



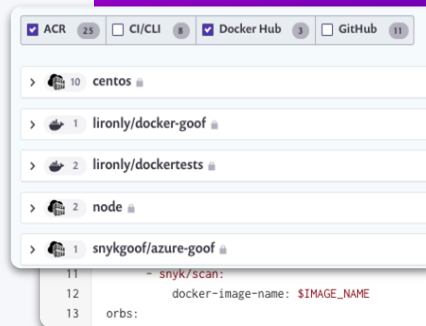
Kubernetes configuration issues

```
X High severity vulnerability found in libssh2/libssh2-1
Description: Integer Overflow or Wraparound
Info: https://snyk.io/vuln/SNYK-LINUX-LIBSSH2-451807
Introduced through: curl@7.64.0-4
From: curl@7.64.0-4 > curl/libcurl@7.64.0-4 > libssh2/libssh2-1@1.
Introduced in your Dockerfile by 'RUN apt-get update && apt-get ins
ca-certificates curl'
```

Start early, test images locally

t.apps/redis-master				Overview	History	Settings
Kind	Deployment	Secure configuration	Root	TRUE		
Cluster	Production	See configuration	CPU limits	SET		
Namespace	default		Memory limits	MISSING		
Revision	1		Seccomp	MISSING		
Pod labels	app: redis role: master tier: backend		Drop capabilities	FALSE		

Find vulnerable workloads in Kubernetes clusters



Integrate security into your CI/CD pipelines and container registries and test as you build

Remediating automatically to minimize exposure and reduce time-to-fix

HIGH SEVERITY

Improper Input Validation

Vulnerable module: bash

Introduced through: bash@4.3-11+deb8u1

Fixed in: 4.3-11+deb8u2

Dockerfile instruction: Introduced by your base image (node:6.14.2-slim)

Get straight to the version of the package which fixes the vulnerability

Open pull requests for updating base images in the Dockerfile.

Recommendations for base image upgrade

	BASE IMAGE	VULNERABILITIES
Current image	node:6.14.2-slim	169
Minor upgrades	node:6.17.0-slim	104
Major upgrades	node:11.15.0-slim	90
Alternative upgrades	node:12.8.0-buster-slim	47

Follow base image recommendations to reduce your total vulnerability exposure

Open a fix PR

github.com/snyk

Vulnerabilities with a fix

An upgrade or patch is available to fix the vulnerable dependencies.

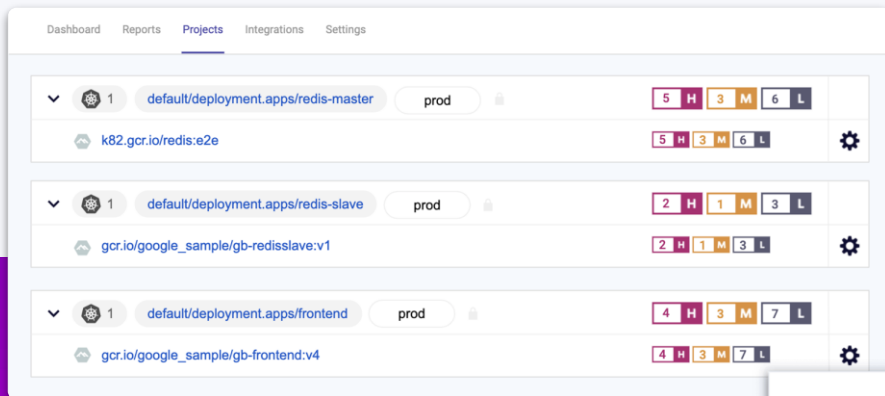
- H** Regular Expression Denial of Service (ReDoS) in debug
- H** Content & Code Injection (XSS) in marked
- H** Regular Expression Denial of Service (ReDoS) in fresh

[OPEN A FIX PR](#)

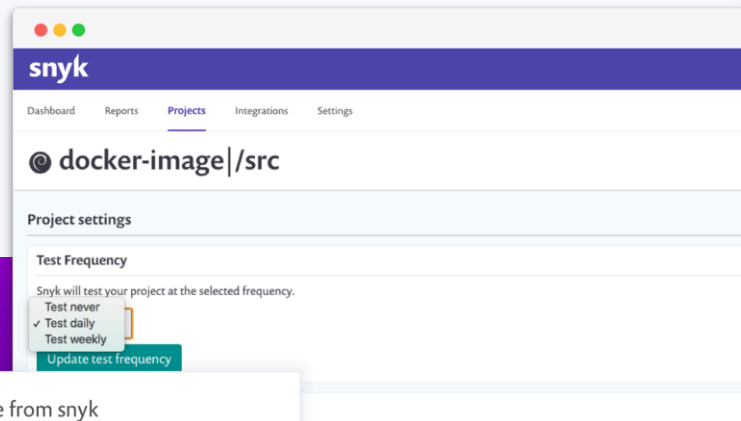
Monitoring continuously to protect the image after the initial scan



Monitor your Kubernetes application for insecure configurations, prioritise accordingly



Monitor your images for newly discovered vulnerabilities



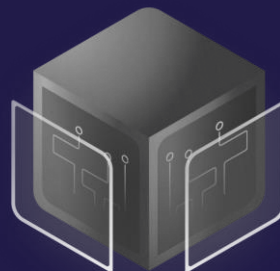
New message from snyk

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

Snyk products



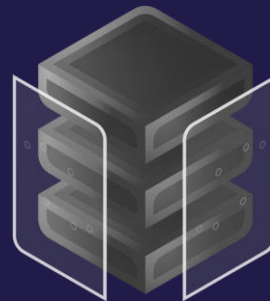
Code



Containers



Infrastructure
as Code



Open Source

IaC

Growing usage and risks

2 M+

Kubernetes config files publicly
accessible on Github

267 K+

Terraform

250 K+

Azure ARM

90 K+

AWS
CloudFormation

600 K+

Compose

>50%

Teams have
workloads deployed
with IaC

45%

Teams adopted
automated IaC
scanning in SDLC

No. 1

Concern for teams since
moving to a cloud-native
platform

1. *Snyk State of Cloud Native Application Security Report, 2021.*

Misconfiguration of database assets is a growing problem.

—Verizon DBIR 2021



67%

Of misc. error incidents caused by misconfiguration

619

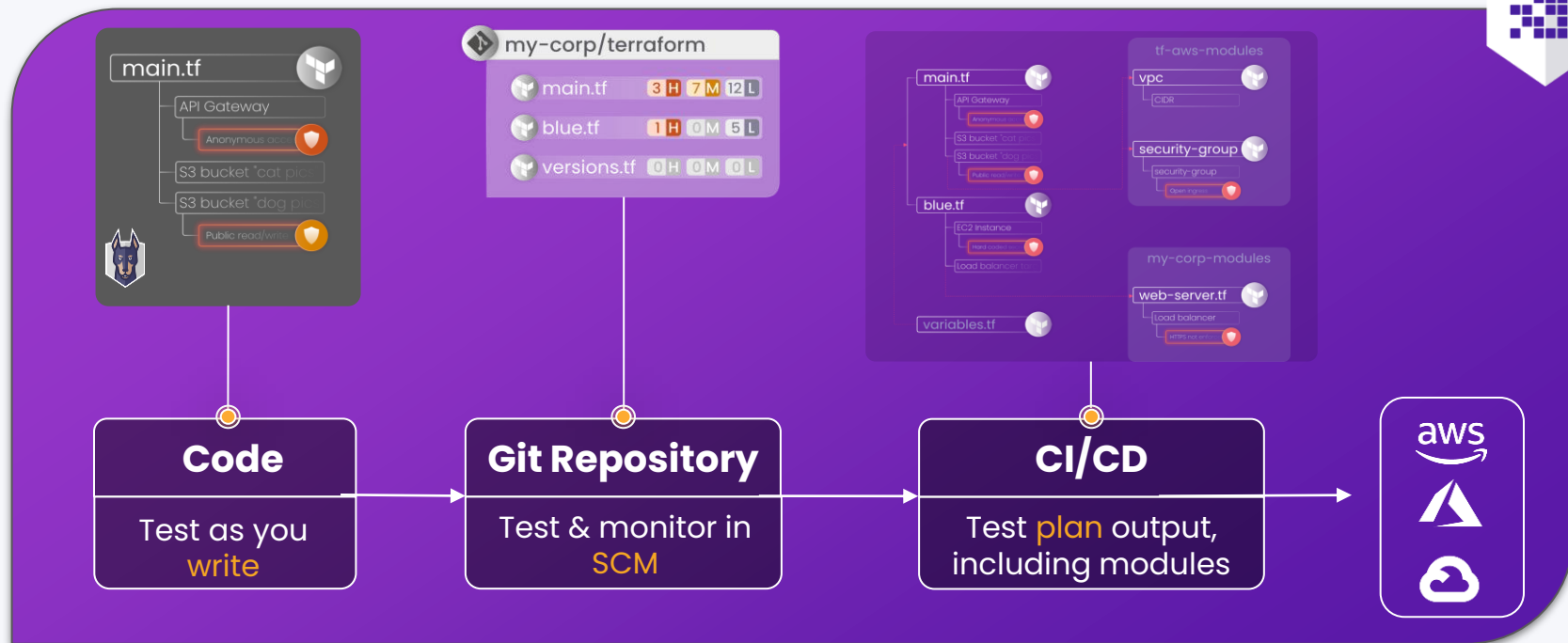
Breaches due to misconfigurations alone in 2020–2021

#6

On the list of top action varieties involved in breaches

Infrastructure Security Built for Developers

Write, Plan and Apply IaC Securely



Securing against industry best practices and CIS benchmarks



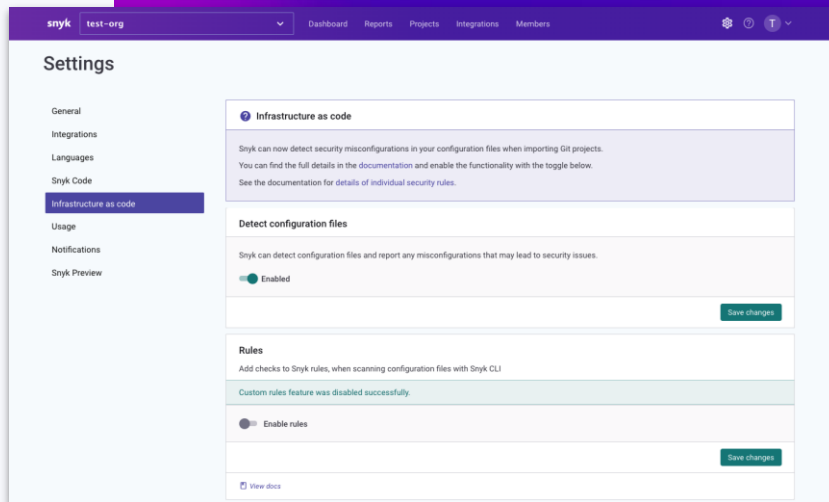
Industry best practice rulesets for Terraform, CloudFormation, ARM, and Kubernetes formats and AWS, Azure, and GCP.



Expanding ruleset backed by CIS benchmarks and threat-modelling research by Snyc security engineers.



Custom policies powered by Open Policy Agent (OPA)/Rego.



Detecting misconfigurations throughout the infrastructure lifecycle



Prevent misconfigurations from reaching production by fixing issues at the source.



Maximize developer adoption with integrations keeping them in their preferred workflows.



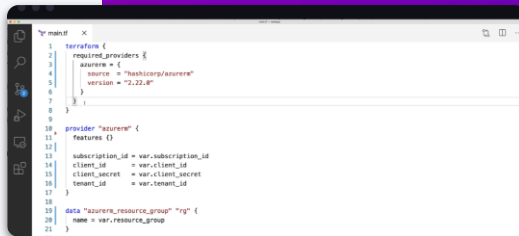
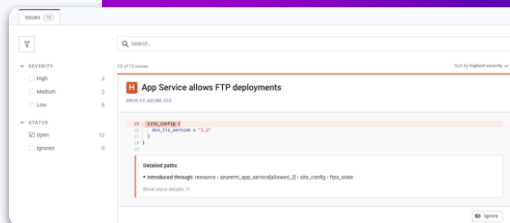
Monitor for cloud infrastructure drift and unmanaged resources in your cloud environments.

```
$ snyk iac test deployment.yaml
```

```
Testing deployment.yaml...
```

```
Infrastructure as code issues:
```

```
X Container is running as root [High Severity]
[SNYK-CC-K8S-10] in Deployment
  introduced by input > spec > template > spec >
  containers[snykit] > securityContext > runAsNonRoot
```



Start early in the development process, test IaC locally or in the IDE

Quickly import Git repositories into Snyk. Automate importing of new projects using the powerful Snyk API.

Streamline security & compliance in Terraform with our run tasks integration

Empowering developers to secure their cloud & app configurations




Zero developers in on the critical issues with actionable fix advice.



Issue, impact, and remediation shown directly in line with misconfigured code



Severity scoring and linked policy violation for greater security context on the issue

 **Non-encrypted S3 Bucket**
SNYK-CC-TF-4

```
20 resource "aws_s3_bucket" "blog-files" {
21   bucket = "blog-static.purpledoble.com"
22   acl    = "public-read"
23   policy = file("policy.json")
24 }
```

Detailed paths

- Introduced through: input › resource › aws_s3_bucket[blog-files]

[Show less details](#)

This issue is...

Non-encrypted S3 Bucket

The impact of this is...

A non-encrypted S3 bucket increases the likelihood of unintentional data exposure

You can resolve it by...

For AWS provider < v4.0.0, set `server_side_encryption_configuration` block attribute. For AWS provider >= v4.0.0 add `aws_s3_bucket_server_side_encryption_configuration` resource.

[Ignore](#) [Full details](#)

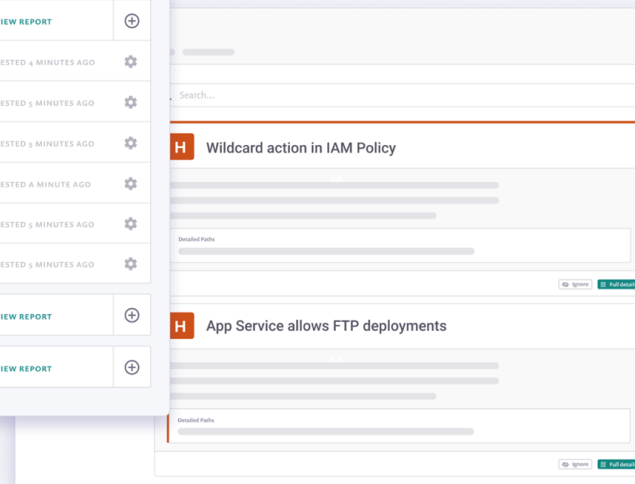
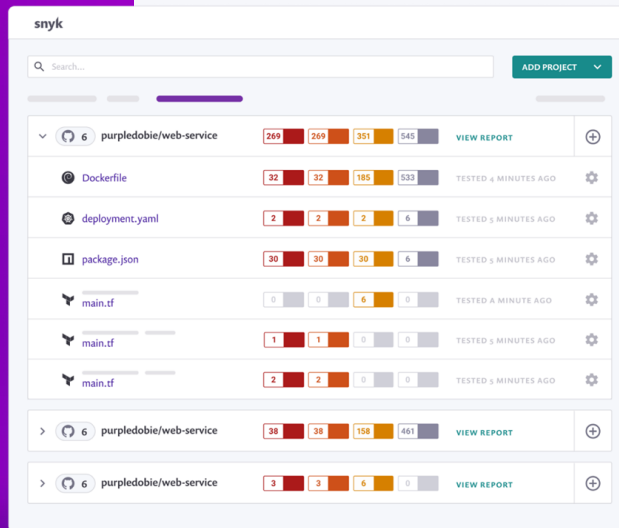
```
19
20 resource "aws_s3_bucket" "blog-files" {
21   bucket = "blog-static.purpledoble.com"
22   acl    = "public-read"
23   policy = file("policy.json")
24 }
25
26 website {
27   index_document = "index.html"
28   error_document = "error.html"
29   routing_rules = <<EOF
30   {}
31   "Condition": {
32     "KeyPrefixEquals": "docs/"
```



Snyk IaC

Code to cloud, and back to code

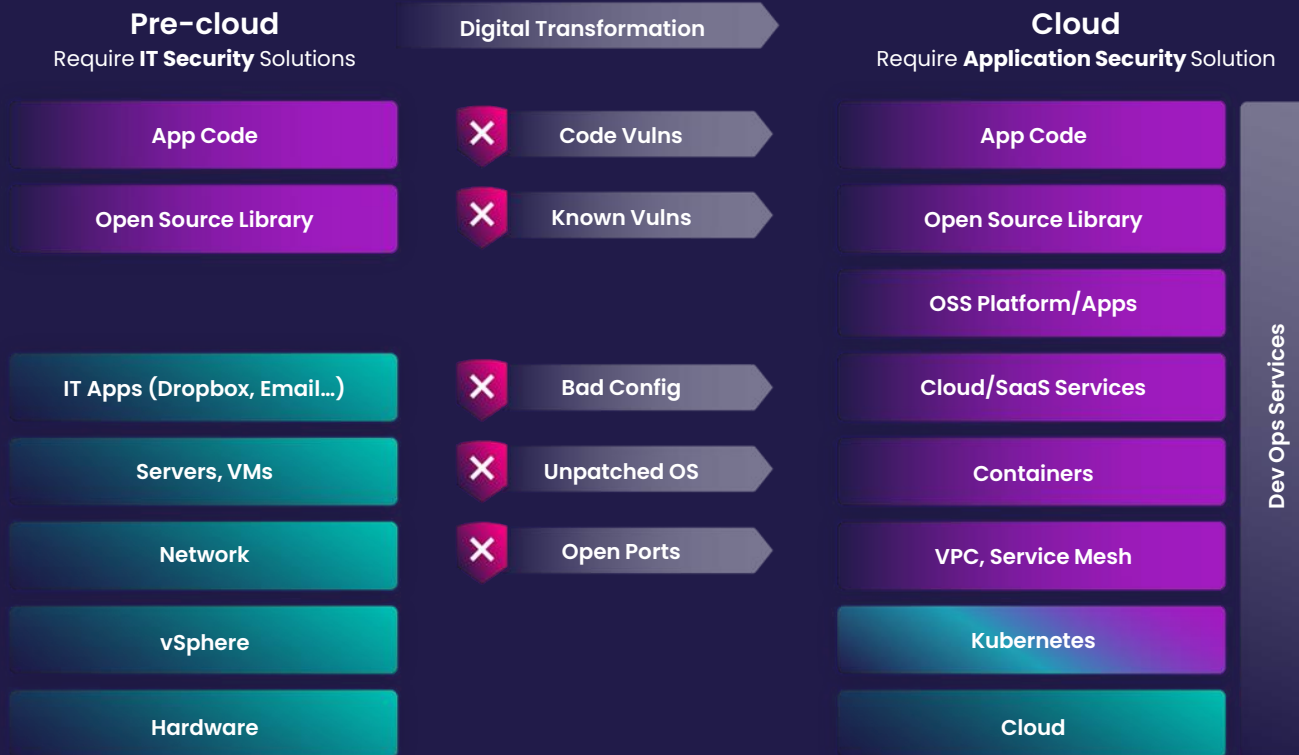
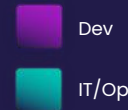
- **Maximize developer adoption**– seamless integrations into developer workflows, minimizing downtime and navigation through security tooling.
- **Secure against the best**– enforce best practice security rulesets, custom policies, and compliance frameworks from code to CI/CD.
- **Drive faster remediation** – deliver actionable fix guidance on the riskiest issues to developers, in-line with code.
- **Centralized insights and reporting** – gain visibility into configuration issues with reports available on misconfiguration status overtime.



Snyk Cloud

Following four slides explain the vision behind the Fugue acquisition and the direction of the future Snyk Cloud product

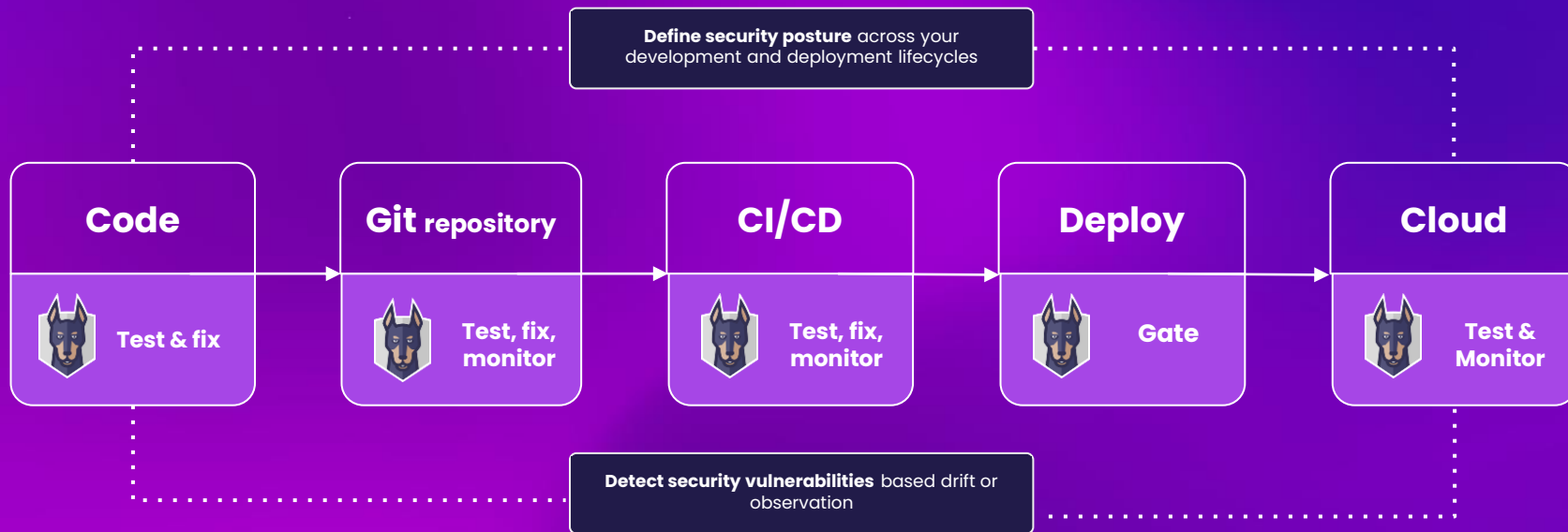
Cloud turns IT into App Services





Code to Cloud, and back to Code:

Secure from your desired state in code to your real-time state in the cloud





Code to Cloud, and back to Code:

Empower Cloud security, Security, and Development teams with visibility across their estates

Cloud | Security

How secure is **all** of my organization's infrastructure?

All Apps



Test & Monitor

Developer

Code



Test & fix

Git repository



Test, fix, monitor

CI/CD



Test, fix, monitor

Deploy



Gate

App on Cloud



Test & Monitor

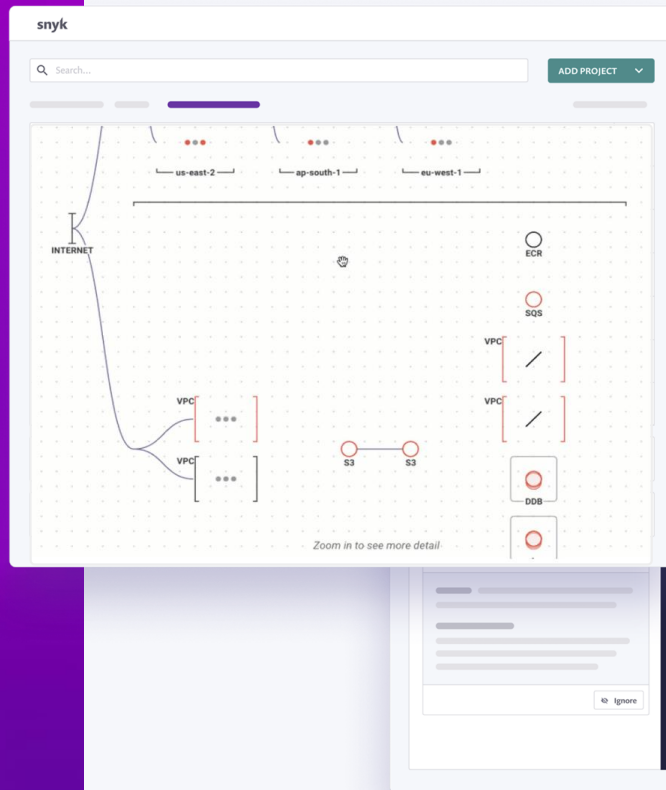
How secure is my application's infrastructure across my development pipeline?



Snyk IaC + Cloud

Code to cloud, and back to code

- **Developer First**- bring production insights left to improve the developer experience with
 - Security issue context
 - Actionable fix advice
- **Holistic application view** - enable developers to take ownership of their application security from writing IaC files in their IDE to the real-time state of the cloud
- **Faster remediation** - close the feedback loop between cloud and production security insights and developer workflows
- **Reduce the most risk**- prioritize issues based on risk, not just finding the most amount of issues



```
resource "aws_vpc" "example" {
  cidr_block = var.cidr
}

resource "aws_default_security_group" "default" {
  vpc_id = aws_vpc/example.id

  ingress {
    protocol = -1
    self     = true
    from_port = 0
    to_port   = 0
  }
}
```

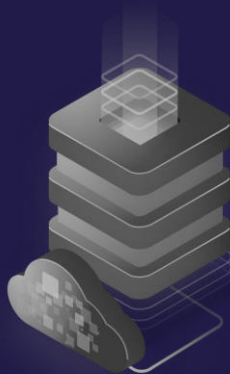
Snyk products



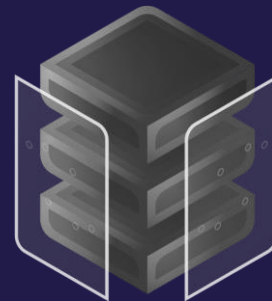
Code



Containers



Infrastructure
as Code



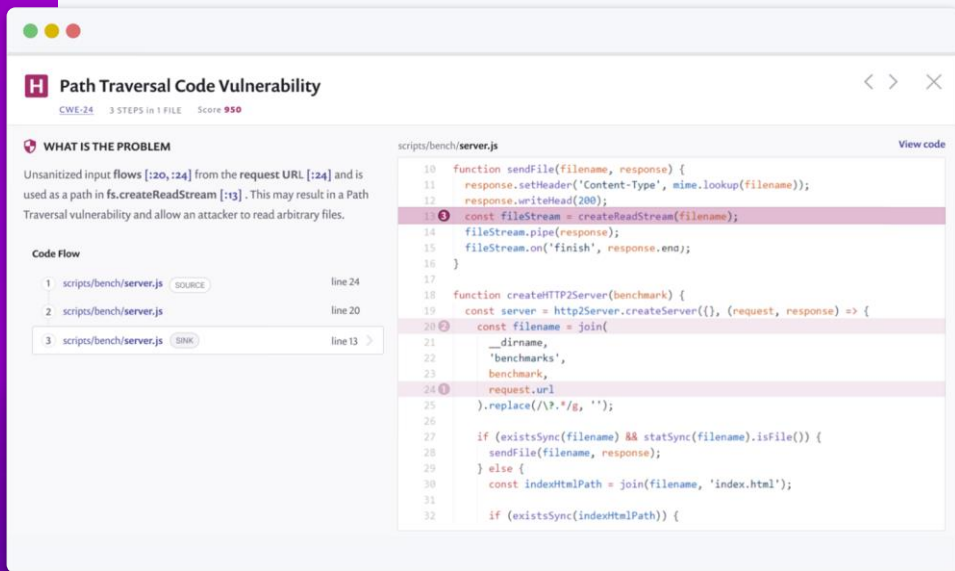
Open Source



Snyk Code

- **Integrated Platform** – Snyk offers all elements for a modern software supply chain
- **Dev Friendly** – Works how and where developers work
 - IDE and Git integration
 - *Actionable* fix recommendations based on real-world data.
- **Real-Time** – 10 – 50x faster than traditional SAST solutions enables securing while developing vs afterwards
- **Improve Accuracy** – Machine learning algorithms continuously trained on the world's code to unveil security and performance bugs

SAST Re-imagined as a dev-first solution

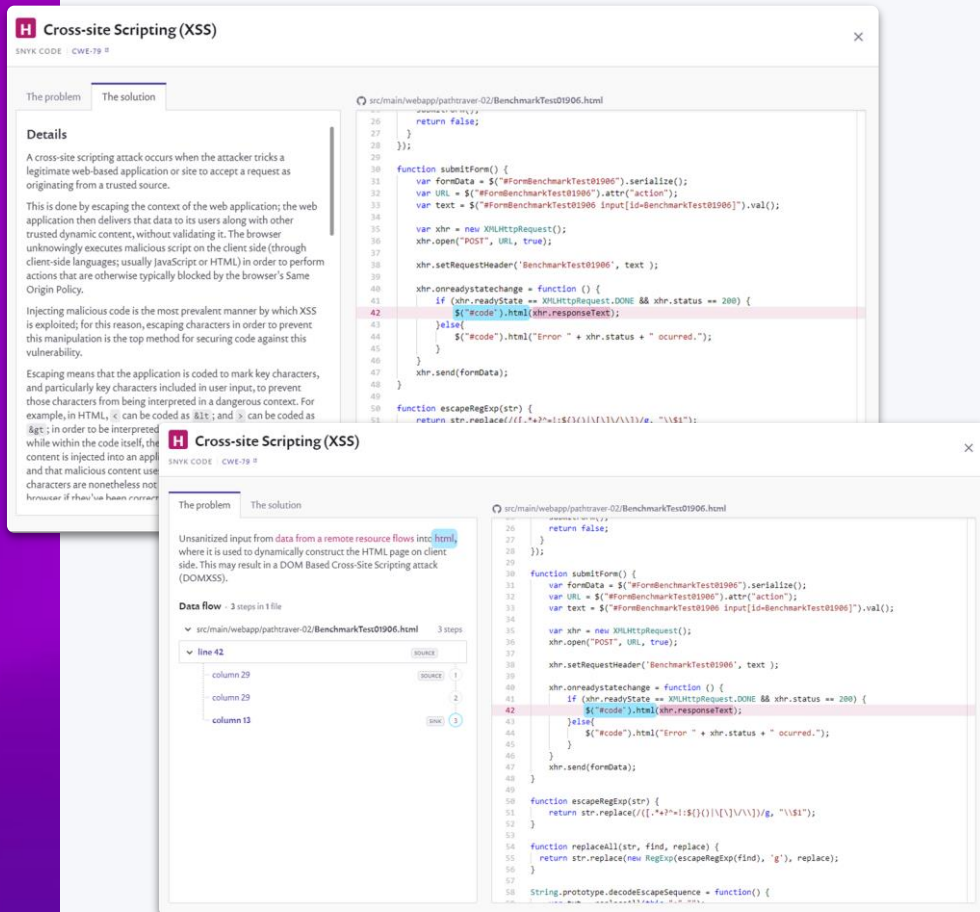




Snyk Code

SAST Re-imagined as a Dev-first solution

- **Dev Friendly** - Works how and where developers work
 - IDE and Git integration
 - Actionable fix recommendations based on real-world data.
- **Real-Time** - 10 - 50x faster than traditional SAST solutions enables securing while developing vs afterwards
- **Unparalleled Accuracy** - Machine learning algorithms trained on the world's code reduces false positives to near-zero

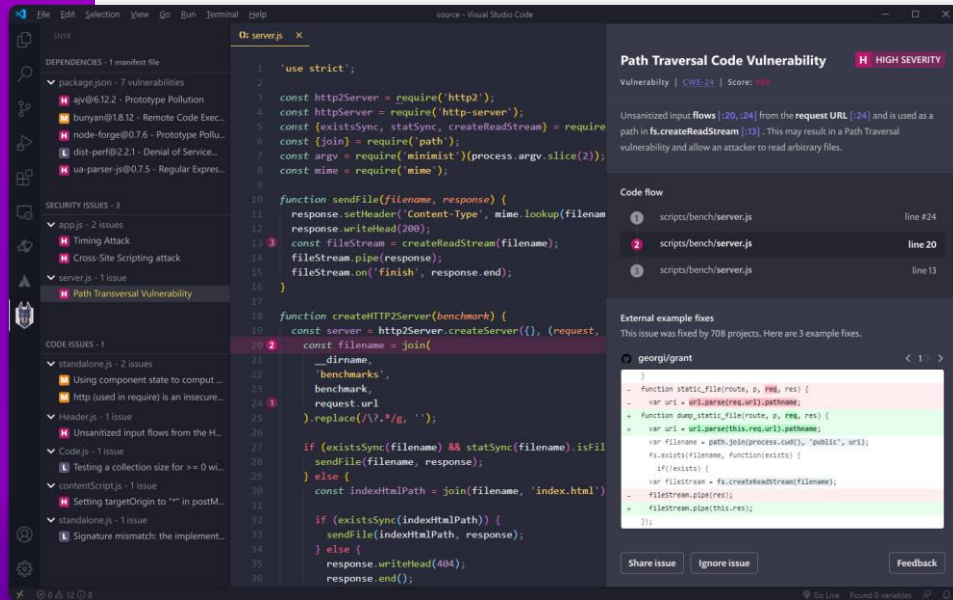




Snyk Code

SAST Re-imagined as a Dev-first solution

- **Dev Friendly** - Works how and where developers work
 - IDE and Git integration
 - Actionable fix recommendations based on real-world data.
- **Real-Time** - 10 - 50x faster than traditional SAST solutions enables securing while developing vs afterwards
- **Unparalleled Accuracy** - Machine learning algorithms trained on the world's code reduces false positives to near-zero



Deprecated Slides

These slides are from older versions of the Intro Deck and are set to be deleted from future revisions of this deck.