# Can we (really) trust developers to handle security?

**Lawrence Crowther**
Head of Solutions Engineering
Snyk, APJ

snyk

# Digital Transformation Changed the Way Developers Work

## Yesterday

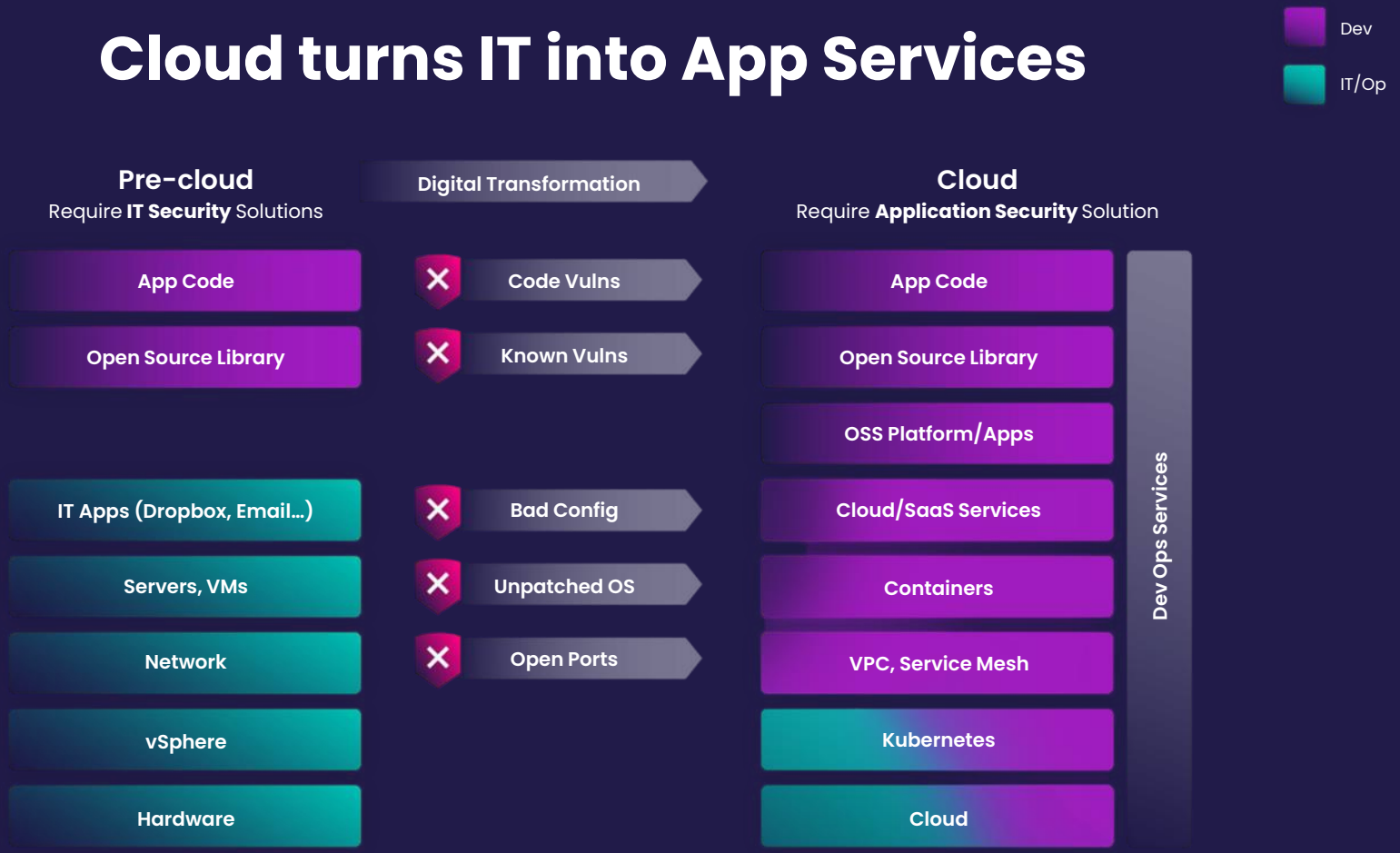
- Sporadic Deployment (Months) 
- Siloed Devs and Ops 
- Rigid Dev Model 
- Limited Supply Chain 

## Today

- Continuous Deployment 
- DevOps 
- Agile Dev Model 
- Vast & Opaque Supply Chain 

snyk

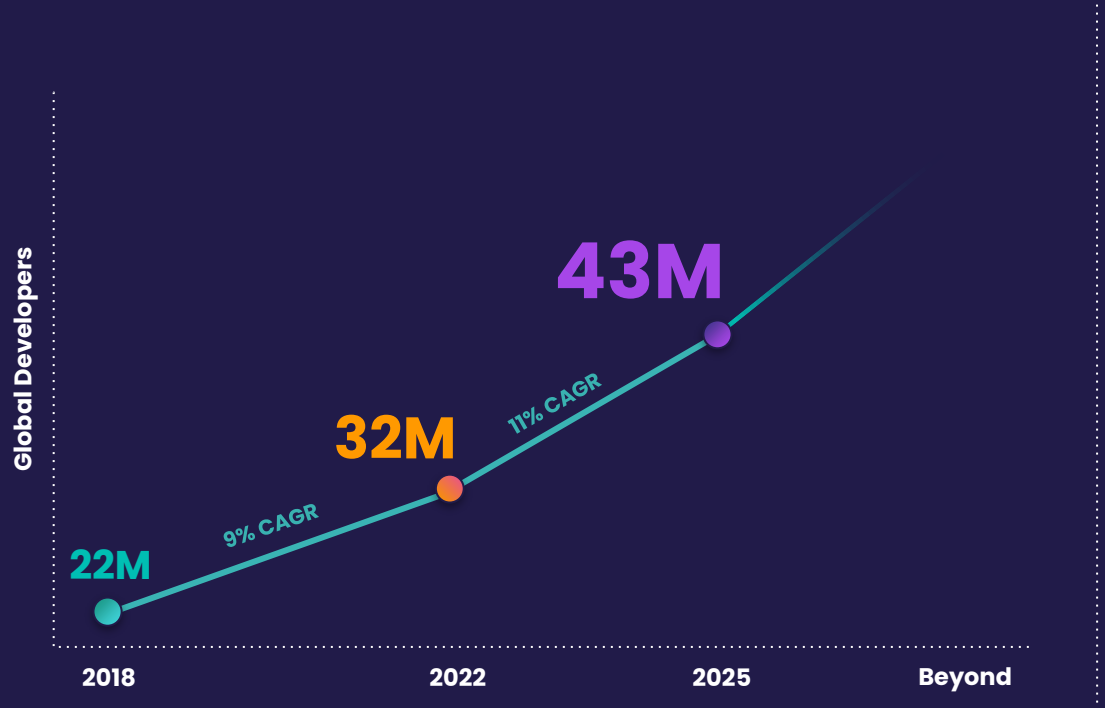
# Cloud turns IT into App Services




snyk

# Developer Growth Is Outpacing Security

## The World Is Increasingly Reliant on Developers




## Security Talent Shortages Prevent Scaling

**600K**

**Unfilled Cybersecurity Positions in the US**

**3.5M**

**Cybersecurity Job Openings Globally by 2025**

**164%**

**Next 5-Year Growth in Demand for App Development Security**

*Source: IDC, White House, US Department of Commerce, Cybersecurity Ventures, Truist Security Research. Note: 2021 developer figure extrapolated based on 2020-2025 CAGR of 10.5%. US unfilled cybersecurity positions in the past year as of September 2021.*

snyk

# And the only way to scale security is to empower developers

*"The ratio of engineers in Development, Operations, and Infosec in a typical technology organization is **100:10:1**.*

*When Infosec is that outnumbered, without automation and integrating information security into the daily work of Dev and Ops, Infosec can only do compliance checking, which is the opposite of security engineering—and besides, it also makes everyone hate us."*

**—Gene Kim**
*10 Tips for Integrating Security Into DevOps*, DZone


snyk

# Dev-first Security

snyk

# 4 Key Principles of a Dev First Security Program

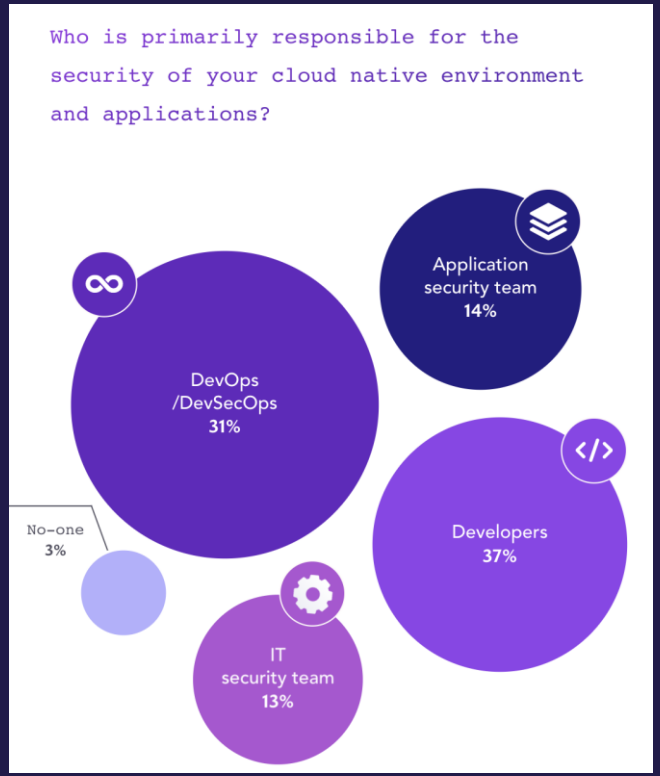
1. Change in ownership

# Security isn't just for the security team

"Developers are **three times more likely** to view security as their responsibility versus their security peers"

Source: State of Cloud Native Application Security

https://snyk.io/state-of-cloud-native-application-security/

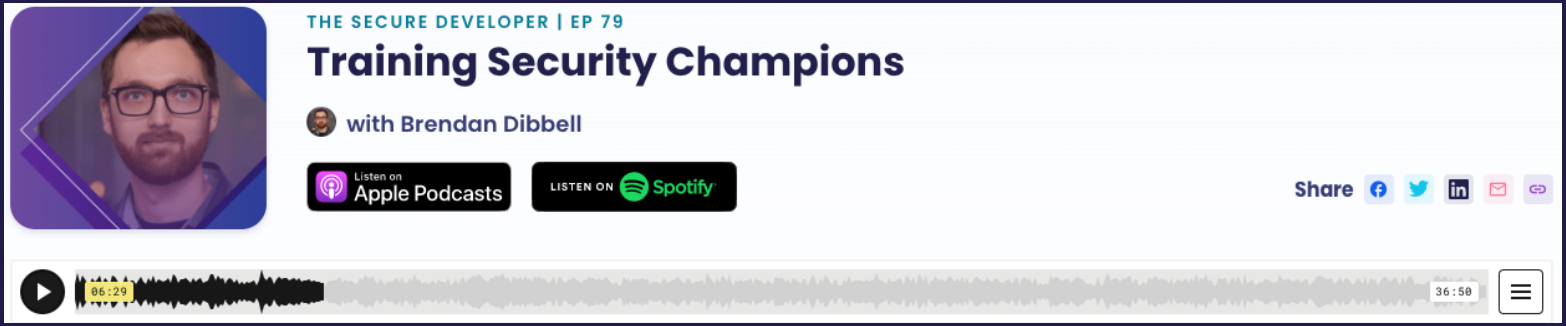


## shared ownership model

***"When everybody owns something, nobody owns it, and nobody has a direct interest in maintaining or improving its condition."*** **Milton Friedman**

## balanced ownership

# Security Ownership




*"Instead of focusing on doing all of the things, we really want to focus on how do we give our engineers the tools that they need to take ownership of security."*

Brendan Dibbell
Application Security Engineer Team Lead
Toast

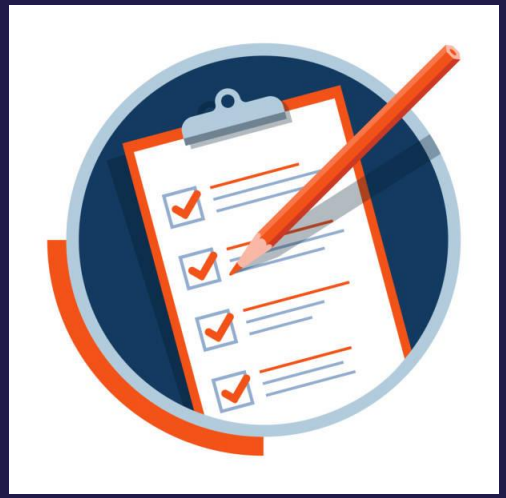
snyk

# 4 Key Principles of a Dev First Security Program

1. Change in ownership
2. Design for the developers

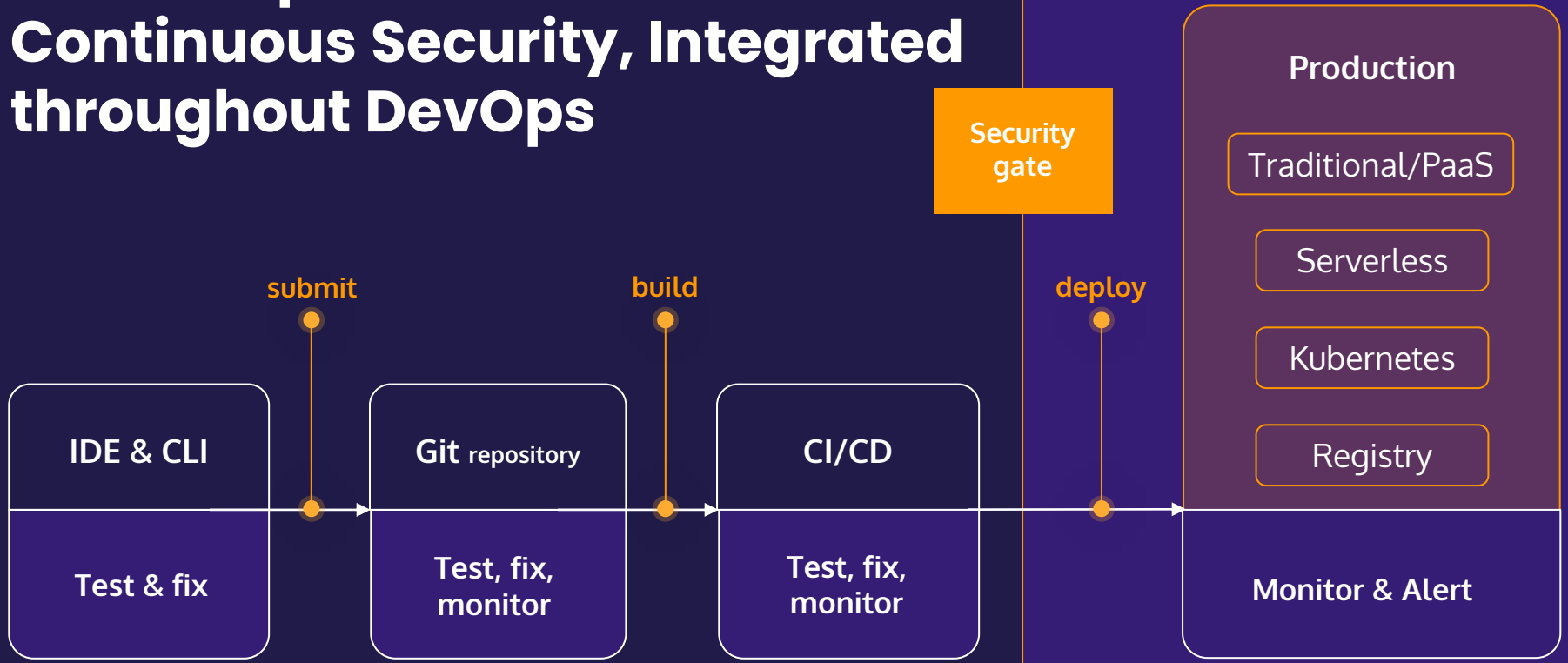
# What’s the goal?

**Security Audits**

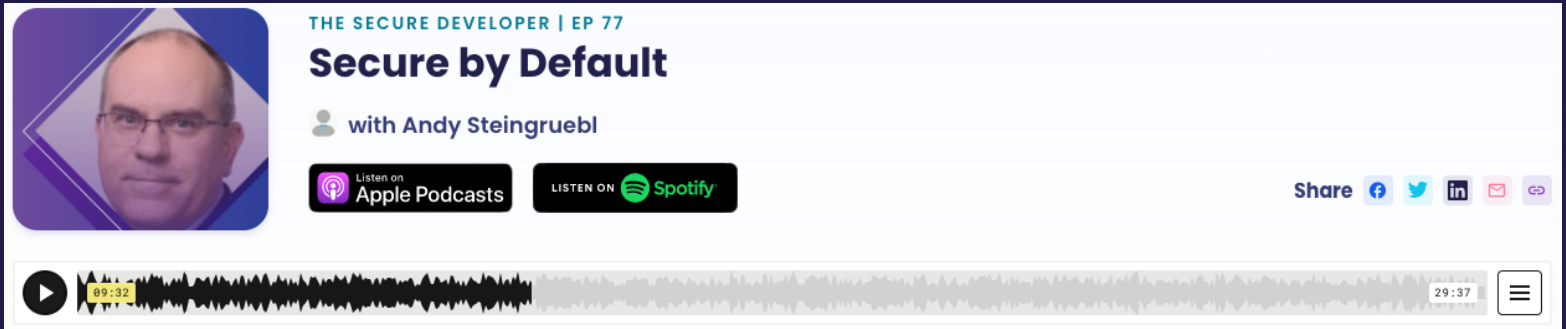


**Developers Fix**

# DevSecOps: Continuous Security, Integrated throughout DevOps



# Meet the Developers Where They Are




*"It's meeting people where they are and trying to integrate with existing workflows of how people do their job, making things easy and safe by default."*

Andy Steingruebl
Chief Security Officer
Pinterest

snyk

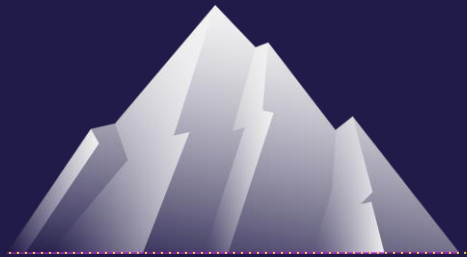
# 4 Key Principles of a Dev First Security Program

1. Change in ownership
2. Design for the developers
3. Bring the cloud into appsec

snyk

# The modern application

## A new risk profile for developers



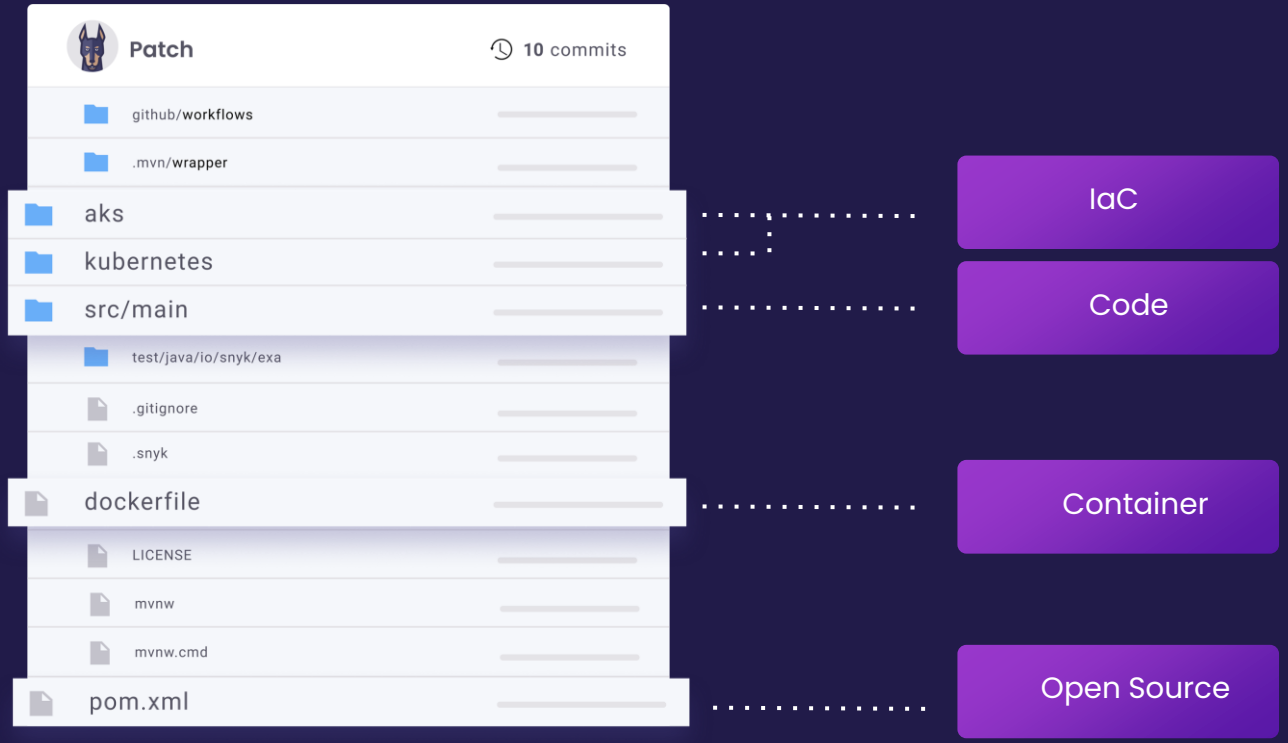
**Code**

- **Software deployed daily** - 'waterfall' approach doesn't scale. Scans can't take hours.
- **10-20% of code is custom** - and digital transformation increases pressure to deliver more and faster.

snyk

# The modern application

## The Developer's View




snyk

# Gartner AST Critical Capabilities

| 2020 | | 2021 | | 2022 | |
|---|---|---|---|---|---|
| 15.4 | SAST | 12 | SAST | 10 | SAST |
| 13 | DAST | 11 | DAST | 6 | DAST |
| 6 | IAST | 8.4 | IAST | 9 | IAST |
| 13.4 | SCA | 12.4 | SCA | 12 | SCA |
| 11.4 | Mobile AST | 6 | Mobile AST | 8 | Mobile AST |
| 1.6 | Business Critical Apps | 2 | Business Critical Apps | 2 | Business Critical Apps |
| 13 | API Testing & Discovery | 11.6 | API Testing & Discovery | 14 | API Testing & Discovery |
| 14 | SDLC Integration | 11 | Lifecycle Integration | 9 | Lifecycle Integration |
| 12.2 | Automation & Speed | 7 | Infrastructure as Code | 8 | Infrastructure as Code |
| | | 4 | Container Security Scanning | 9 | Container Security Scanning |
| | | 2 | Fuzzing | 3 | Fuzzing |
| | | 12.6 | Developer Enablement | 10 | Developer Enablement |

# 4 Key Principles of a Dev First Security Program

1. Change in ownership
2. Design for the developers
3. Bring the cloud into appsec
4. Develop your champions

snyk

# Security Champions


- Embedded
- Experienced
- Empathetic

# Security Champions


*"When I think about security champions and successful models, it's either where out of engineering or development teams, you actually identify several folks that are responsible for security."*

Rinki Sethi
Vice President and Chief Information Security Officer
Twitter

snyk

# 4 Key Principles of a Dev First Security Program

1. Change in ownership
2. Design for the developers
3. Bring the cloud into appsec
4. Develop your champions

snyk

snyk


Develop fast.

**Stay secure.**