2025 KCD WASHINGTON DC

Velocity Meets Security

Scaling securely with Kubernetes

Rodrigo Bersa

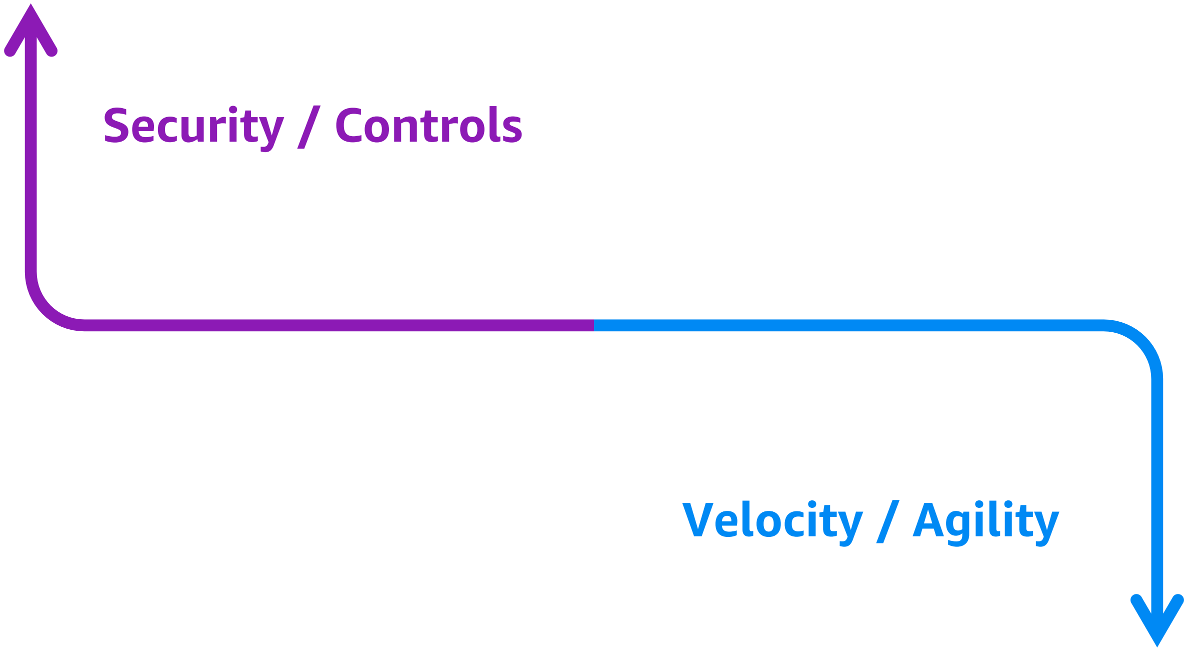
Sr. WW Containers Specialist SA
Amazon Web Services

Raj Saha

Founder, Stealth EdTech Startup
Former Principal SA at AWS

The challenge

Traditional technology consumption



Security / Controls

Velocity / Agility

The goal

Balance between control and agility

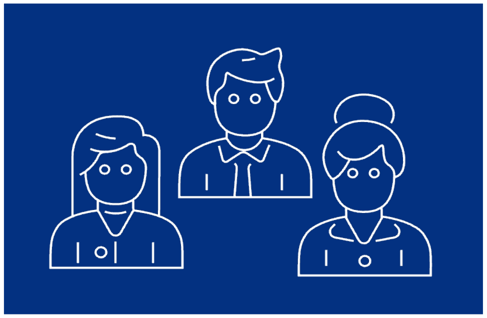
Security / Controls

Velocity / Agility

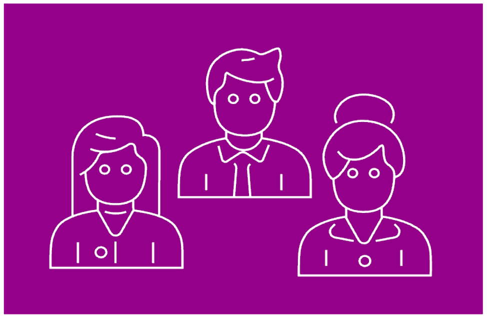
Enable
Provision
Operate
Secure

Experiment
Be productive
Empower
Self-service

The operational model evolution

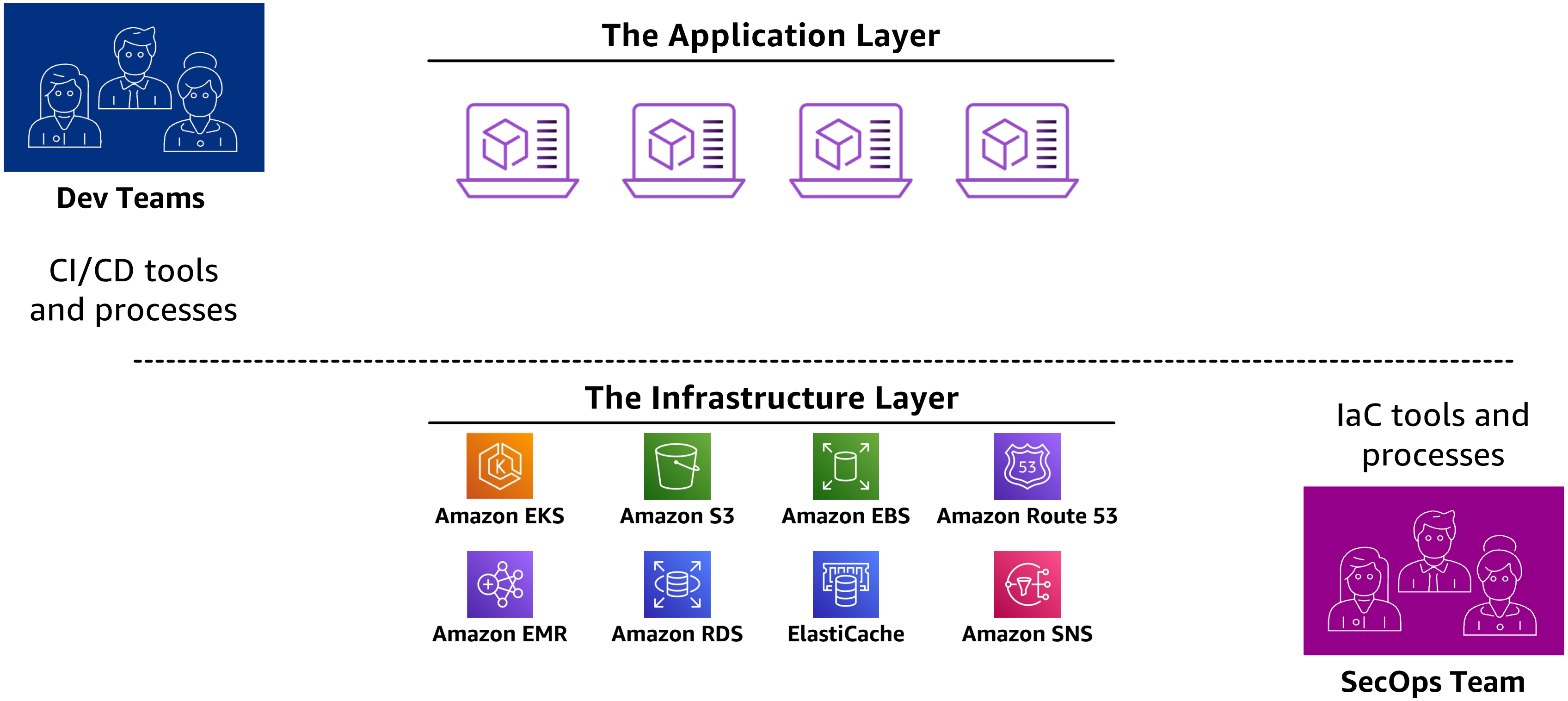


Dev Teams



SecOps Team

The operational model evolution



Dev Teams

CI/CD tools and processes

The Application Layer

The Infrastructure Layer

Amazon EKS

Amazon S3

Amazon EBS

Amazon Route 53

Amazon EMR

Amazon RDS

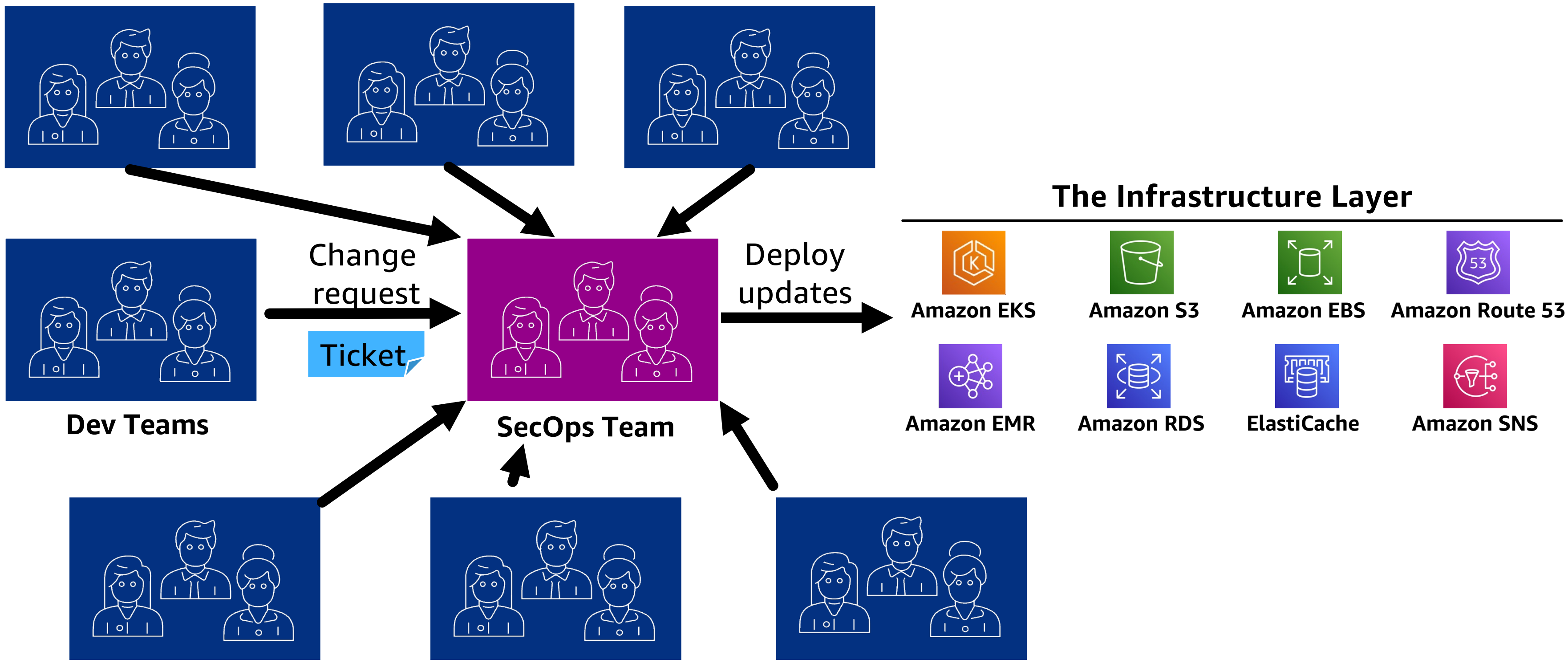
ElastiCache

Amazon SNS

IaC tools and processes

SecOps Team

The operational model evolution



Change request

Ticket

Dev Teams

SecOps Team

Deploy updates

The Infrastructure Layer

Amazon EKS

Amazon S3

Amazon EBS

Amazon Route 53

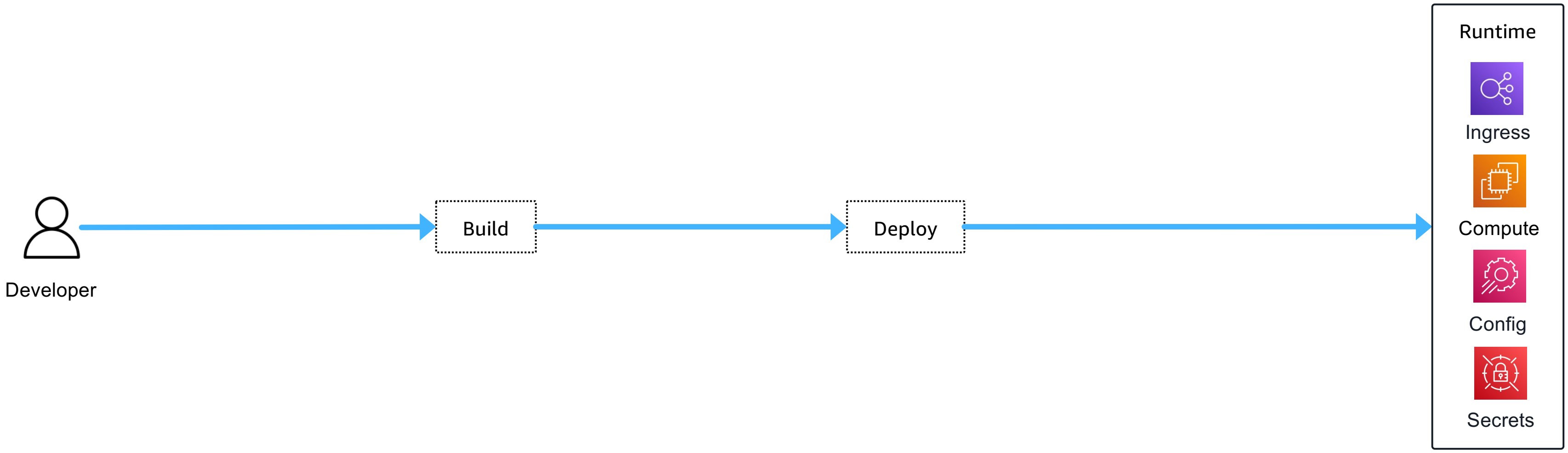
Amazon EMR

Amazon RDS

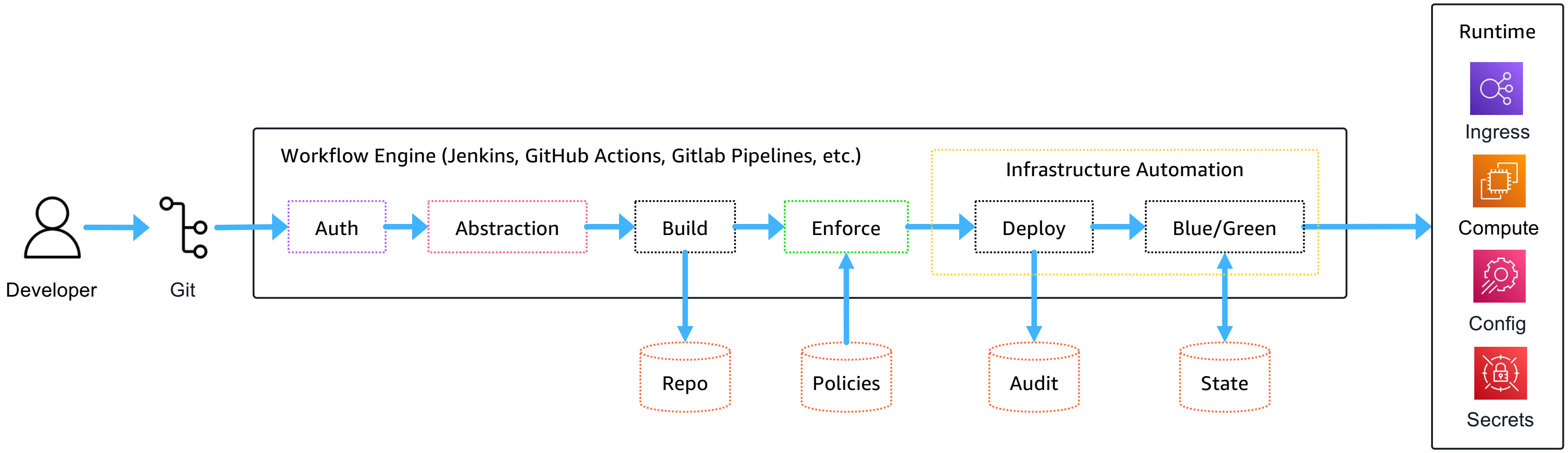
ElastiCache

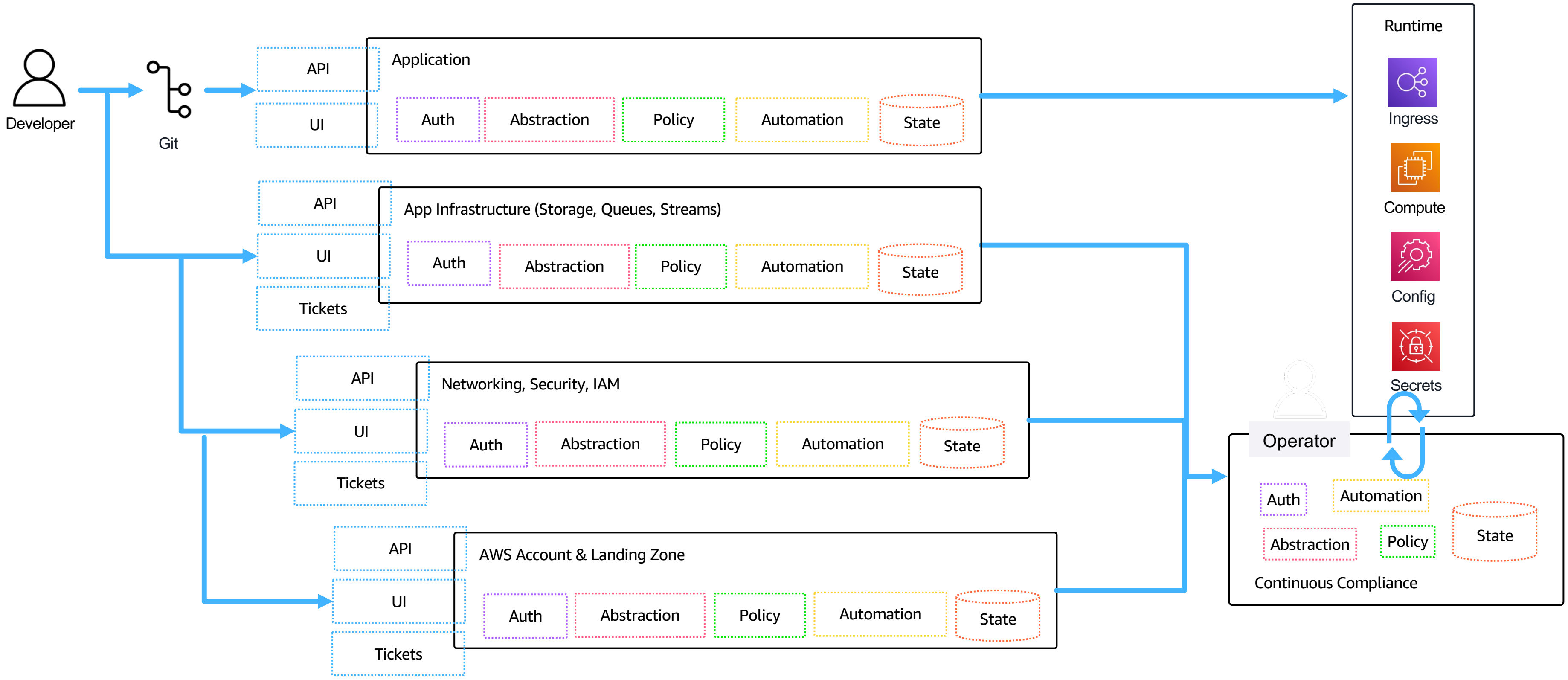
Amazon SNS

CI/CD Pipeline Evolution



CI/CD Pipeline Evolution




Developer
Git
API
UI
Application
Auth
Abstraction
Policy
Automation
State
API
UI
Tickets
App Infrastructure (Storage, Queues, Streams)
Auth
Abstraction
Policy
Automation
State
API
UI
Tickets
Networking, Security, IAM
Auth
Abstraction
Policy
Automation
State
API
UI
Tickets
AWS Account & Landing Zone
Auth
Abstraction
Policy
Automation
State
Runtime
Ingress
Compute
Config
Secrets
Operator
Auth
Automation
Abstraction
Policy
State
Continuous Compliance

Large-scale environments challenges

Scaling to millions of users

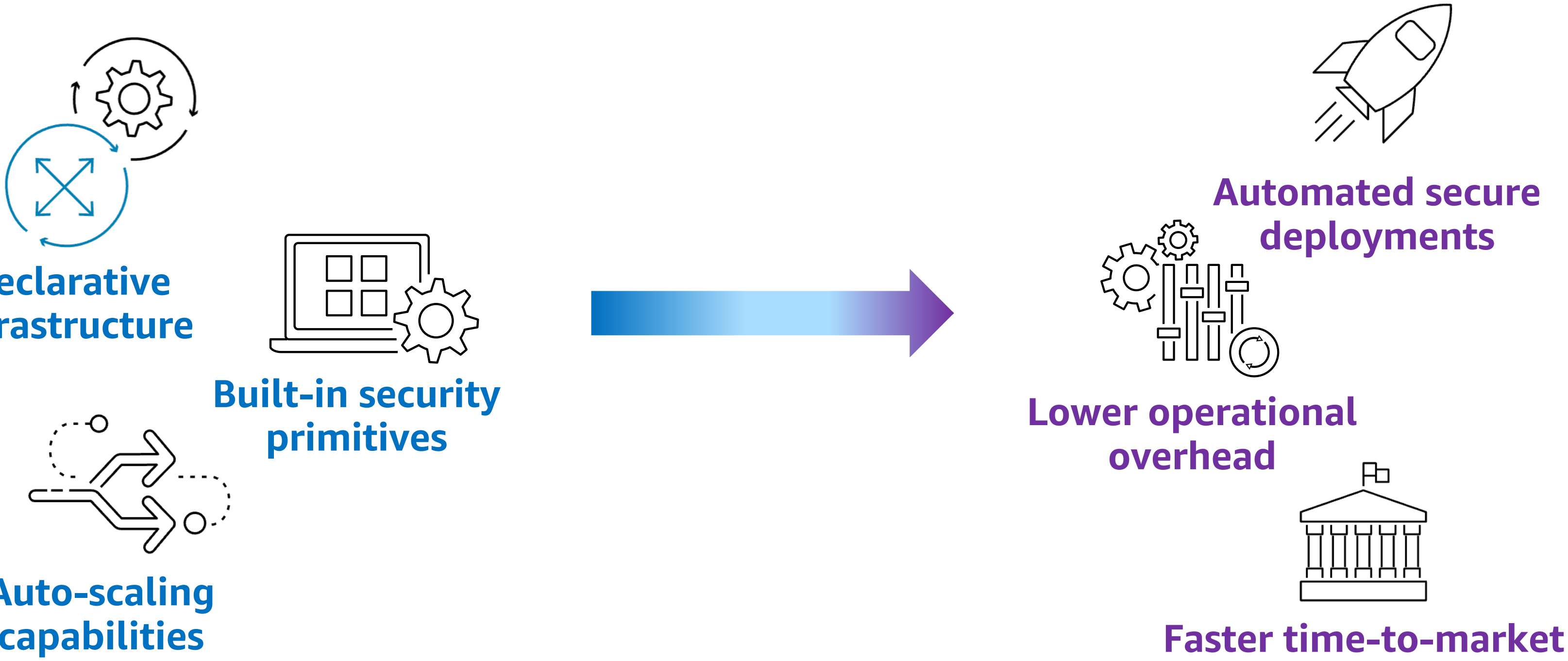
Consistent security

Multi-tenancy

Resource isolation

Centralized observability

Why Kubernetes?



Declarative infrastructure

Built-in security primitives

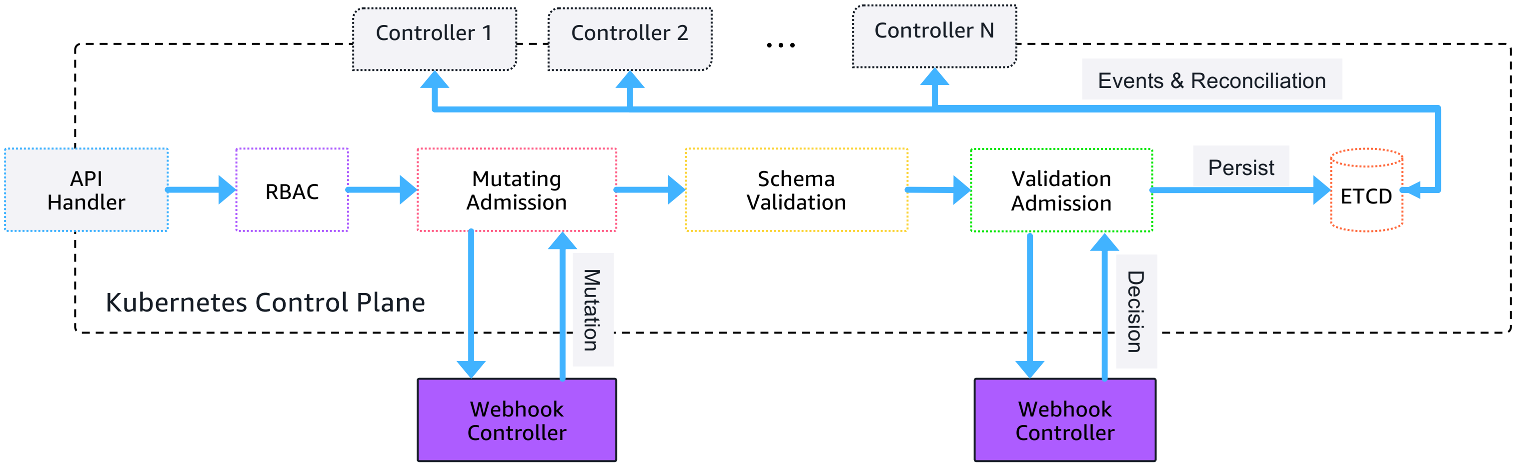
Auto-scaling capabilities

Automated secure deployments

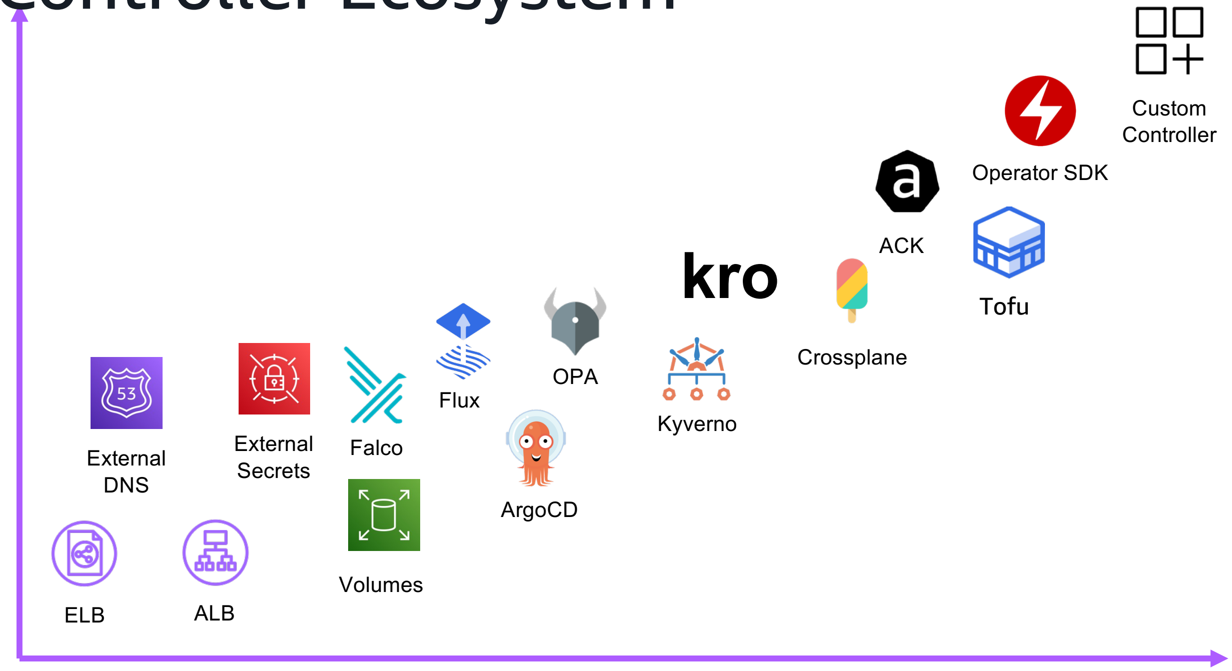
Lower operational overhead

Faster time-to-market

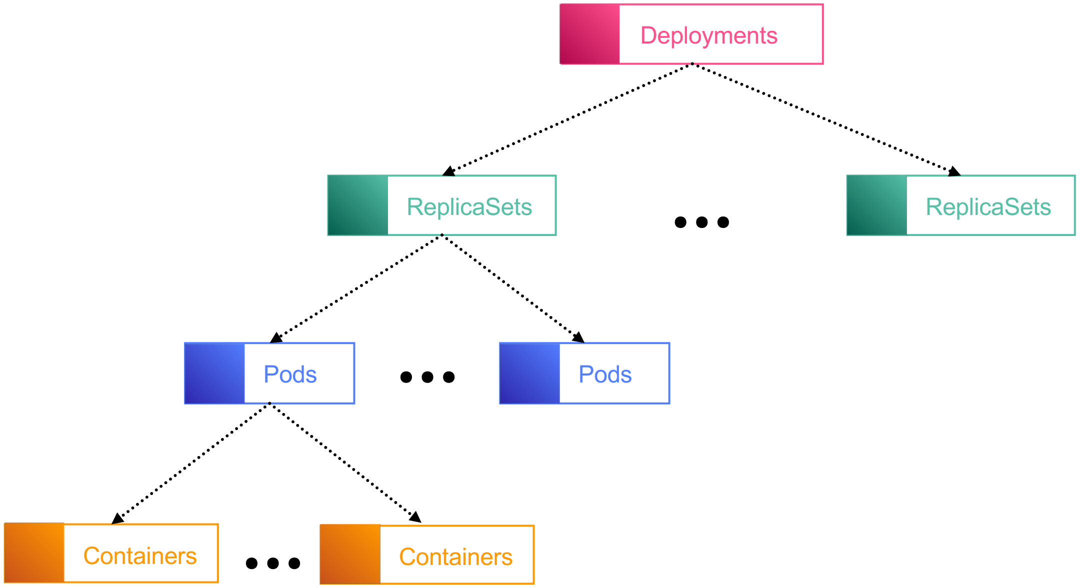
What if we used Kubernetes as the Platform Framework?



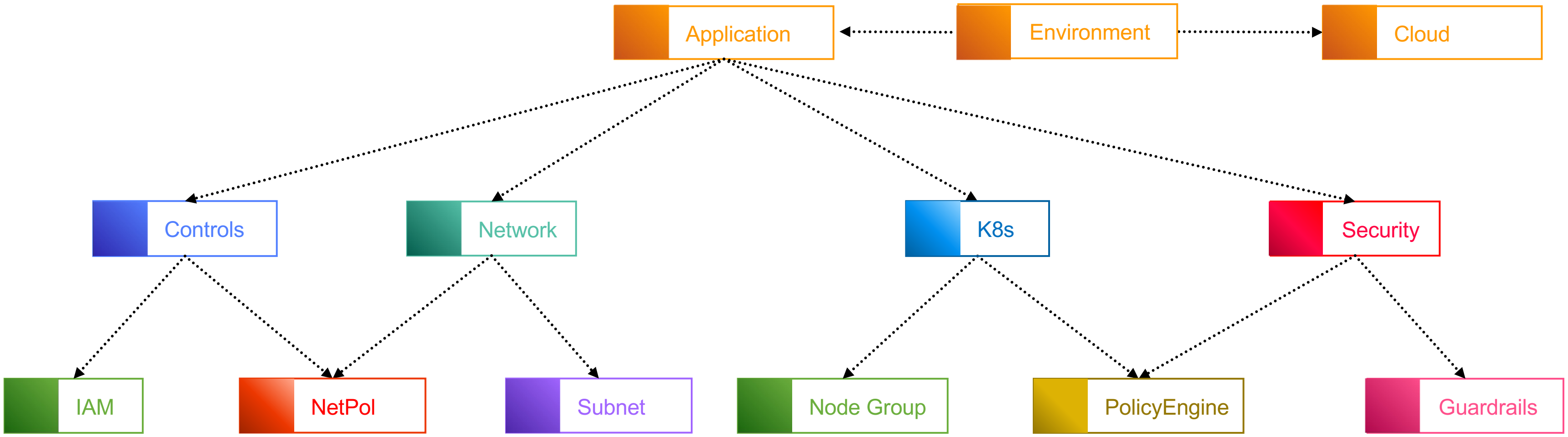
Large Controller Ecosystem



Composable Abstractions



Composable Abstractions

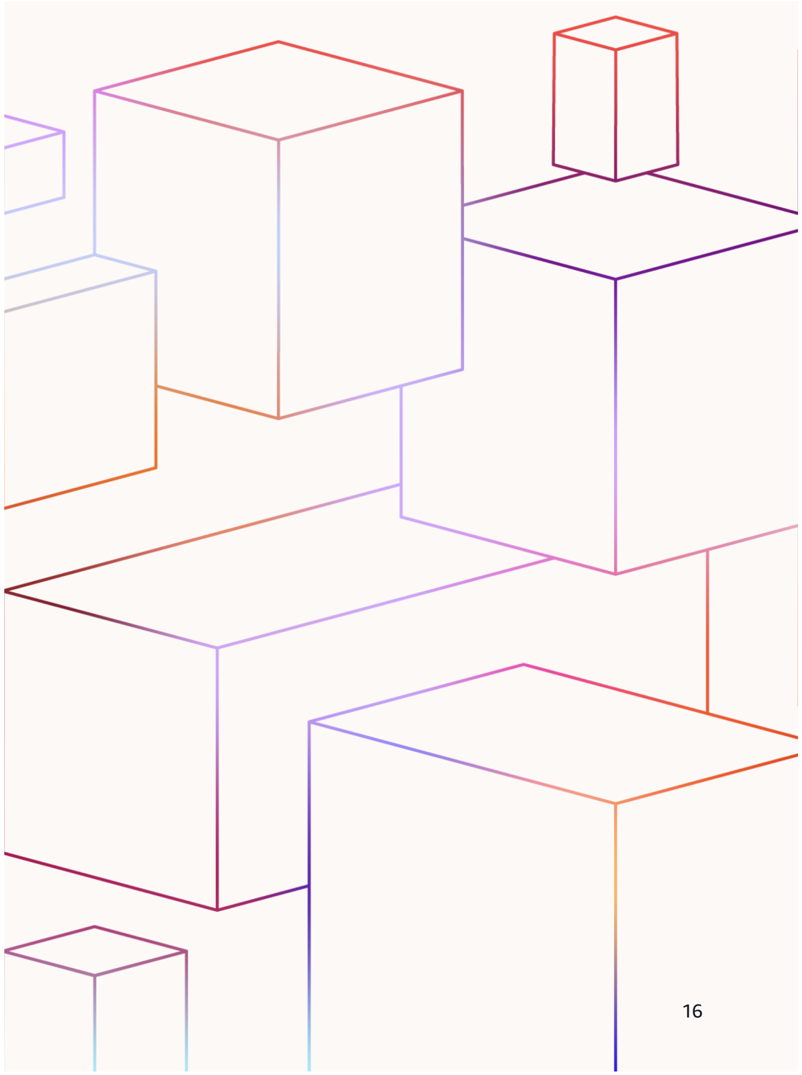


Native security features

Role-based access controls (RBAC)

Network Policies and Pod Security Standards

Resource Quotas and Limits

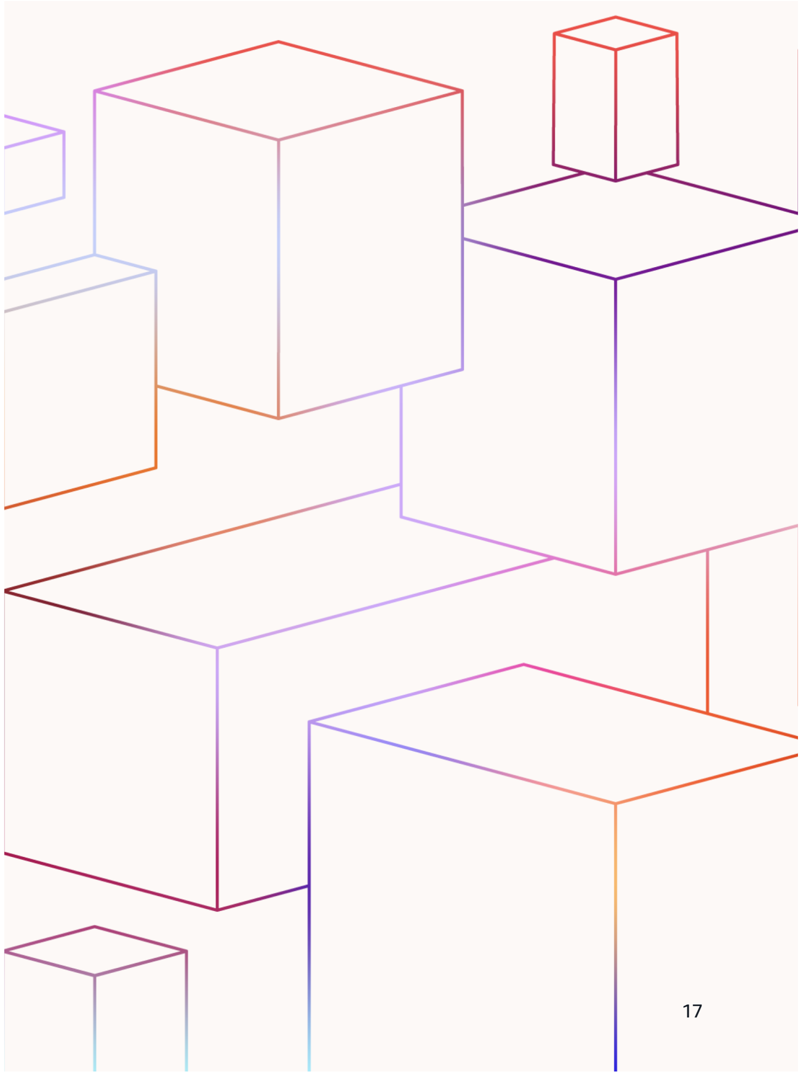


Security-as-Code

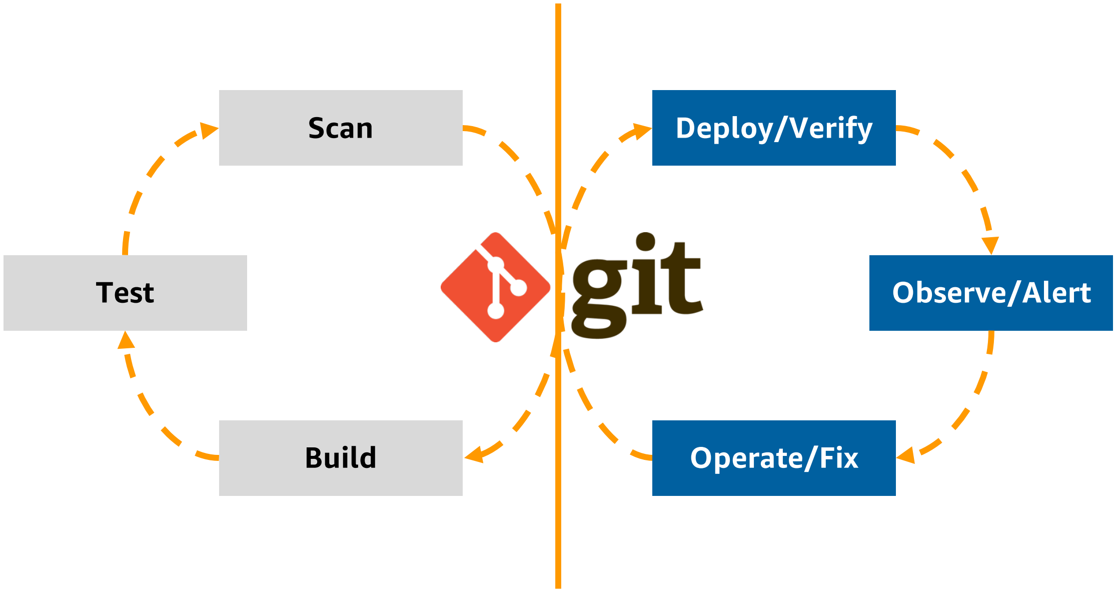
Open Policy Agent

Kyverno

CEDAR ACCESS CONTROL FOR KUBERNETES



GitOps: Infrastructure and Security Automation



Immutability Firewall

GitOps: Infrastructure and Security Automation

Infrastructure Controllers

Configuration

Shift-left Security

Development

- Pre-commit hooks
- Image scanning in CI

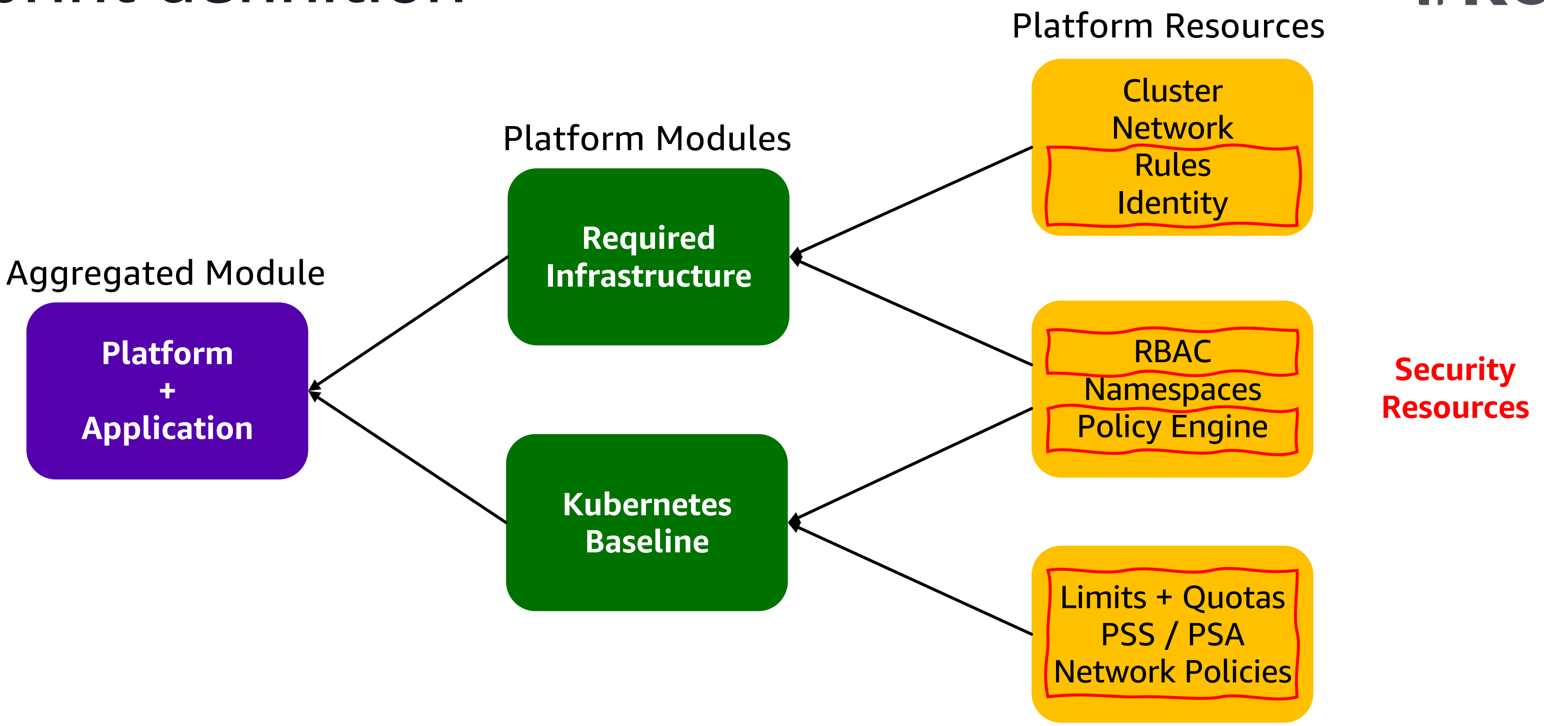
Deployment

- Admission controllers
- Policy enforcement

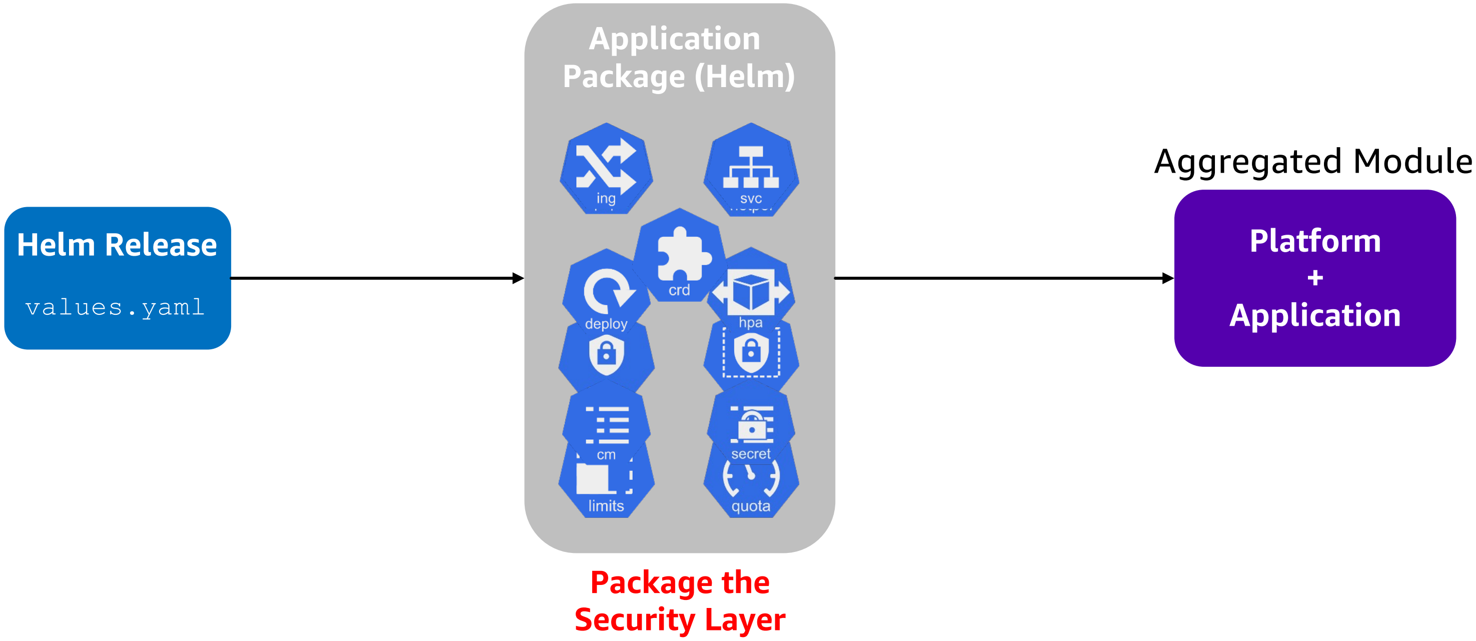
Runtime

- Continuous scanning
- Automated response

Blueprint definition



Packaging application with Helm



Helm Release

values.yaml

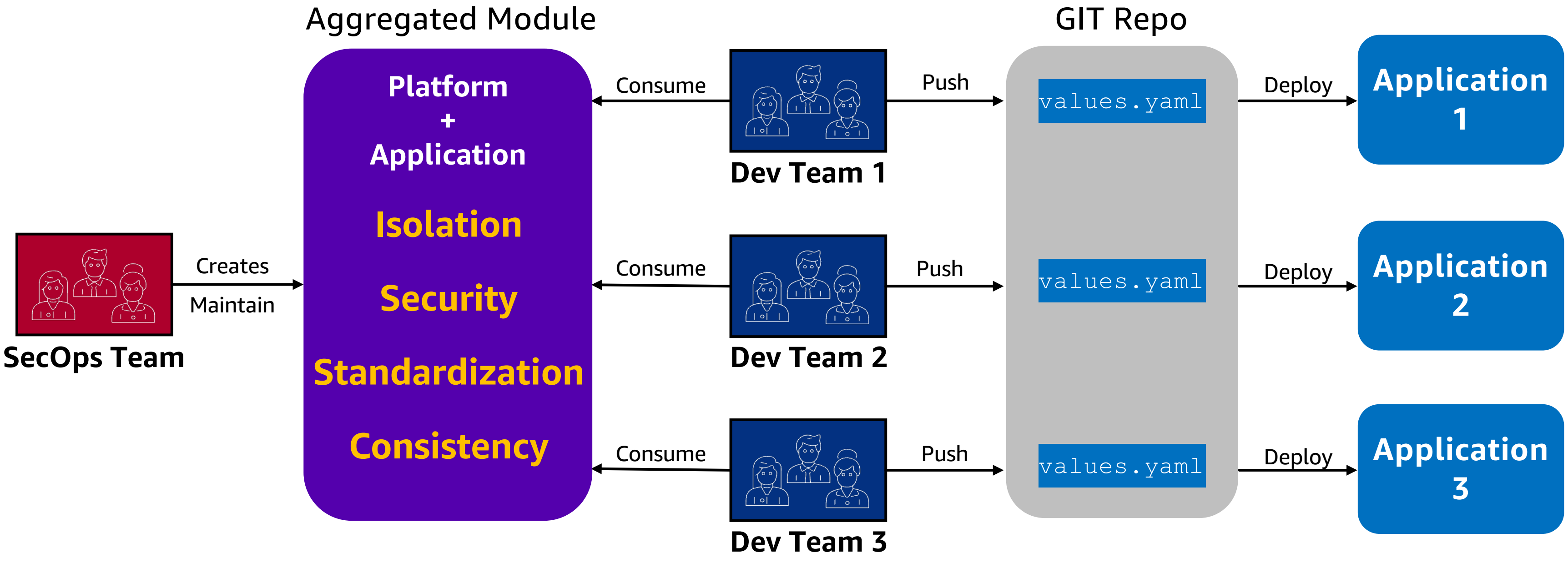
Application Package (Helm)

Package the Security Layer

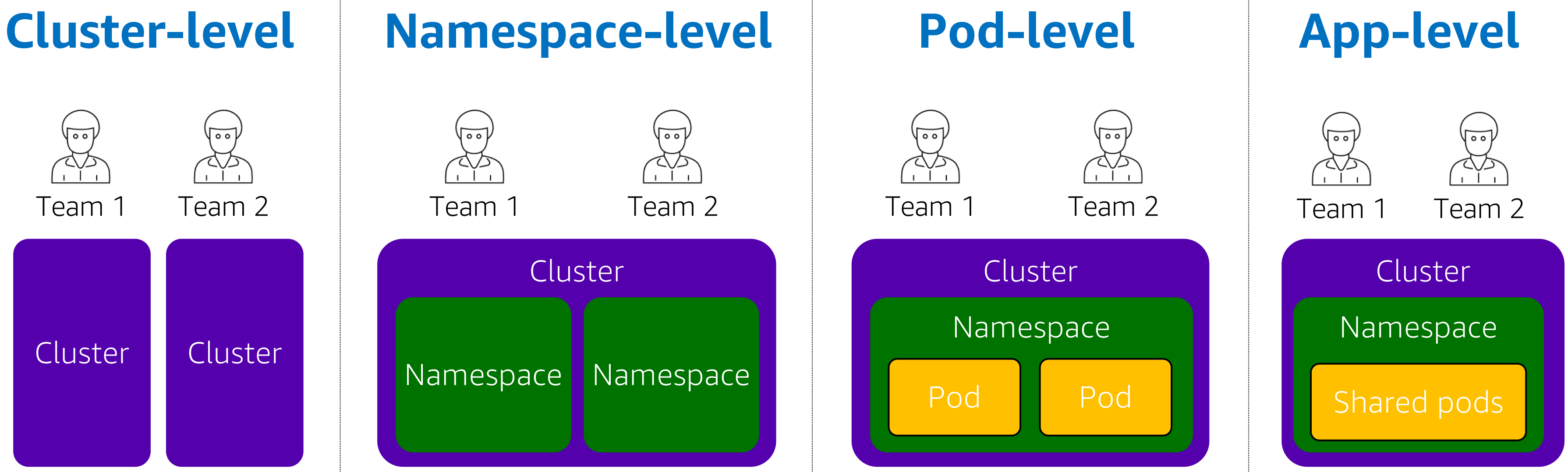
Aggregated Module

Platform + Application

Leverage Platform Engineering Strategy



Multi-tenancy: Isolation models & Team Autonomy



Cluster-level

Team 1

Team 2

Cluster

Cluster

Namespace-level

Team 1

Team 2

Cluster

Namespace

Namespace

Pod-level

Team 1

Team 2

Cluster

Namespace

Pod

Pod

App-level

Team 1

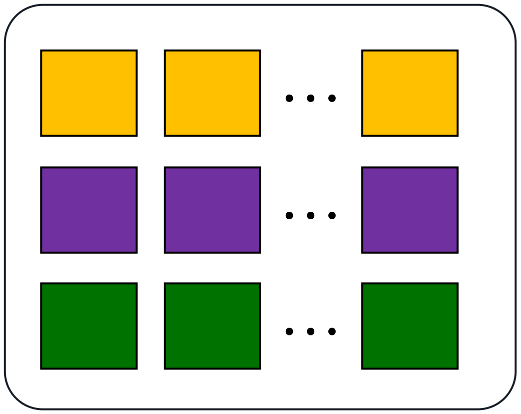
Team 2

Cluster

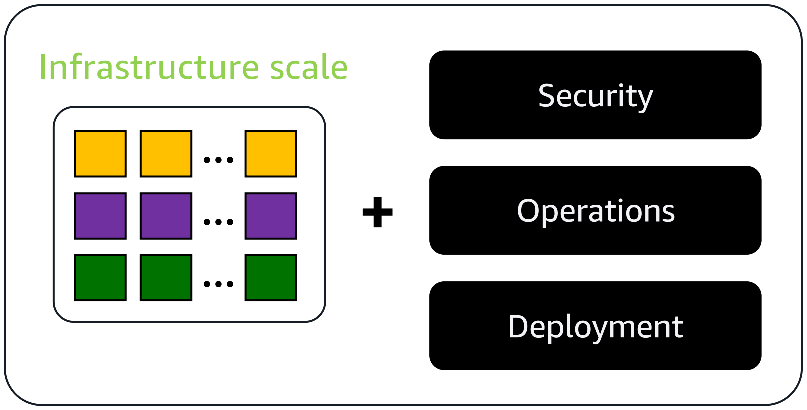
Namespace

Shared pods

Broadening your view of scale



Scale your infrastructure to support multi-Team workloads



Scale your business to achieve agility, innovation, efficiency, and growth with embedded security

Key Takeaways

- Security enables velocity
- Shift Left & Automate
- Platform Engineering Approach
- Test security

  (before someone else does)

2025 KCD WASHINGTON DC

Thank You!

Rodrigo Bersa
bersa
rodrigobersa

Raj Saha
cloudwithraj
cloudwithraj