

Infrastructure Layers

Cloud API + Terraform = Empathetic GitOps

Infrastructure Engineer

“Simple”

“Complexity kills people”



Business

Problems

Ideas take months to reach customers

New hires take months to be valuable

Unknown security state

Uncontrollable infra spend

Engineering

Services take months to reach customers

New hires take months to train

Unknown infra state

Uncontrollable tech debt

Problem

Engineering Culture

Known infra state

Datacenter "think"

Service Menu

Takeaways

Solution

Infrastructure Layers

Git

Cloud APIs

Terraform Modules

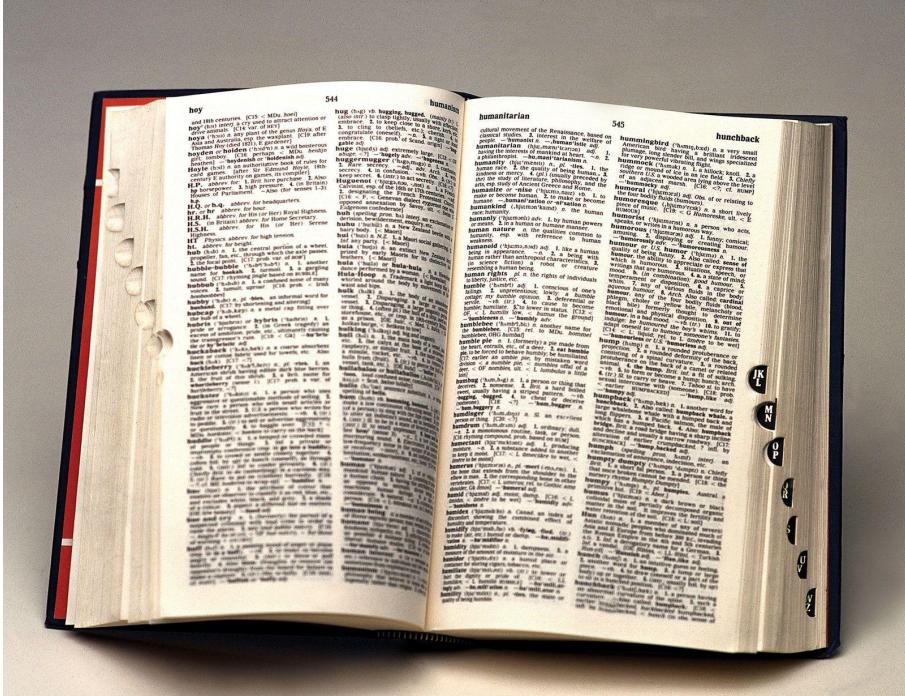
Empathy based Infrastructure Culture



Definitions

Definitions

- “The Cloud”
- “DevOps”
- Infrastructure as Code (IaC)
- Infrastructure Layers
- Git & GitOps
- “State”
- Zero Trust

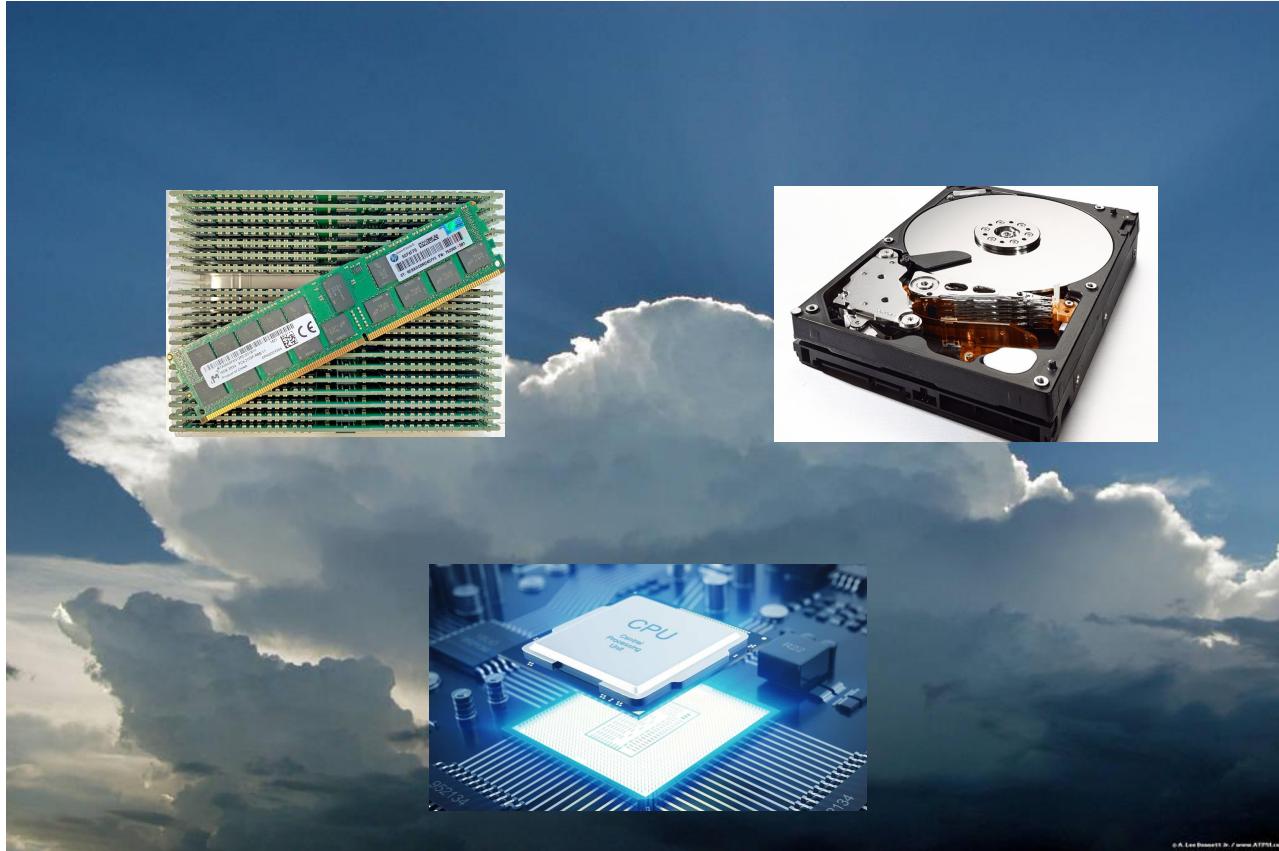


“The Cloud”

A collection of physical machines pooled together and offered to end users to run workloads.



“The Cloud”

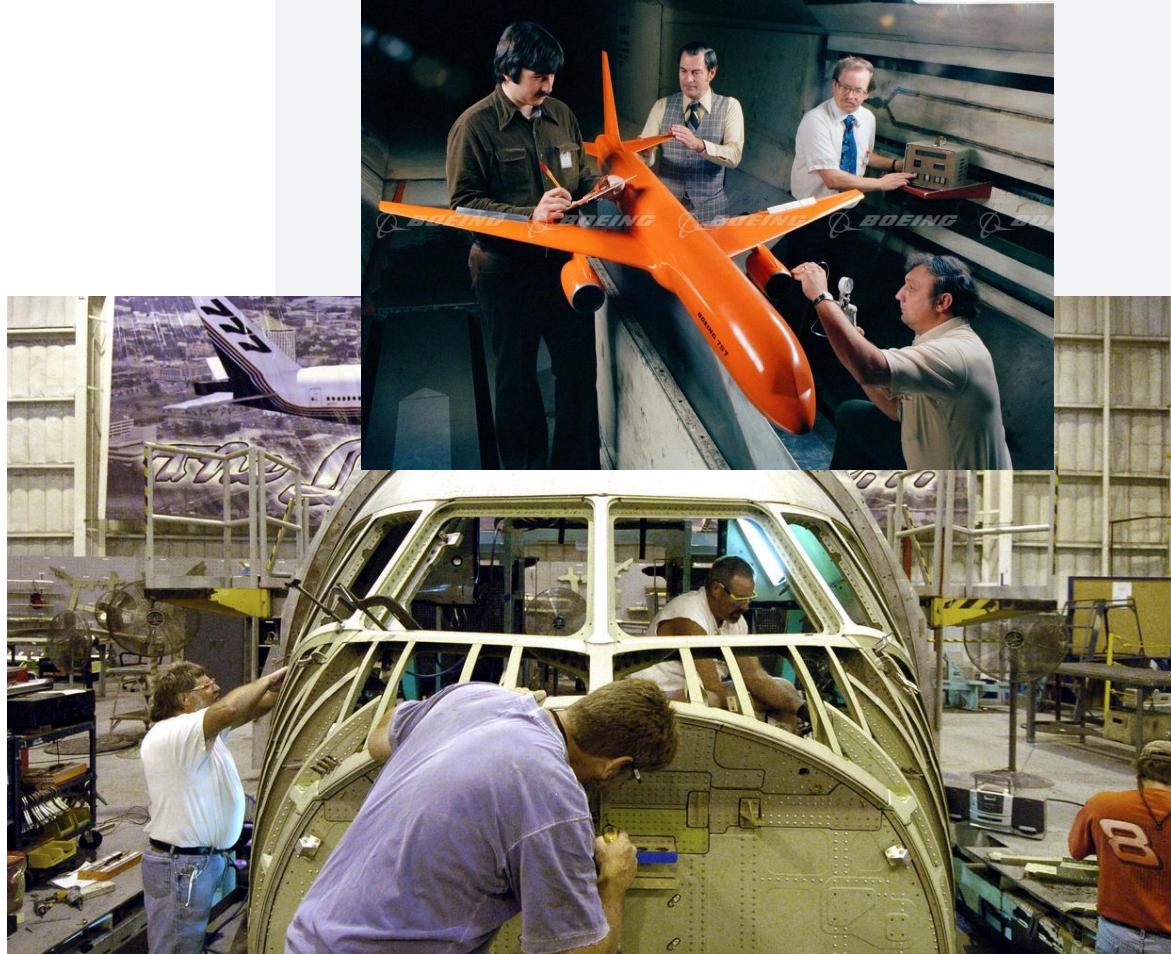


© A. Lee Bennett Jr. www.ATPM.com

“DevOps”

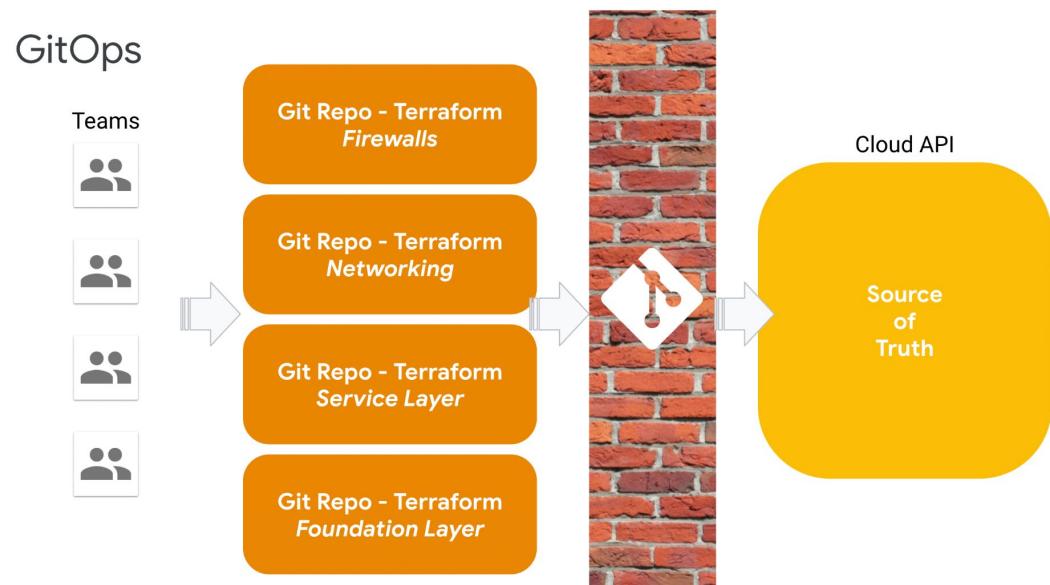
*A collection of
humans working
together to ship value
to the customers.*

- Not a team
- Not a title



“Infrastructure as Code aka IaC”

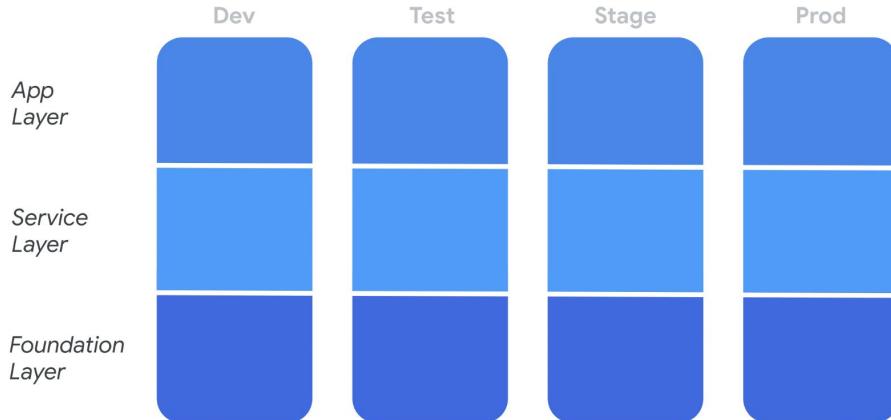
*Suggesting your own
desired state of the
infrastructure, in
code, in a
Git Pull Request.*



“Infrastructure Layers”

*Grouping of the IaC
into silo'd Git Repos in
order to provide
empathy for all
engineers involved.*

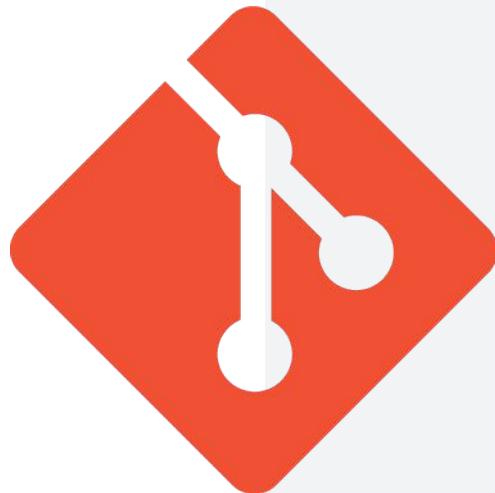
Layers vertically segment



“Git & GitOps”

*Git: distributed
version control system*

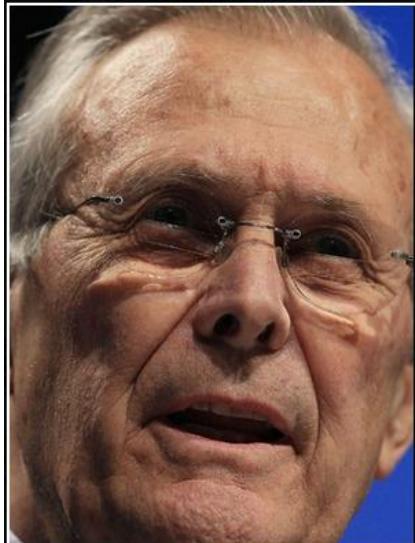
GitOps: “Git + CiCd”



git

“State”

The source of truth



There are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns - the ones we don't know we don't know.

— Donald Rumsfeld —

AZ QUOTES

“Zero Trust”

Nothing is trusted =

- *No person*
- *No device*
- *No network*



The only outcome of trust is some type of betrayal

Datacenter to the Cloud

A Brief History

“Datacenter think”

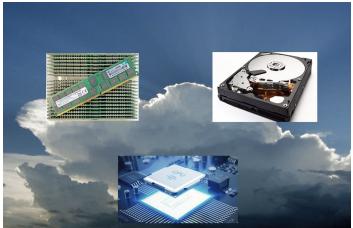
A building & a cage with lots of:

- people
- power
- access methods
- bare metal



The "CLOUD"

- No buildings & no cages
- less people
- no power
- less access methods
- no bare metal



amazon.com Your Amazon.com Make Money See all 43 Product Categories Your Account Cart Your Lists Help

Program Overview | Marketplace | Associates | Advantage | Web Services | WebStore By Amazon | Paid Placements | On-demand Publishing

Welcome to Amazon Web Services

Amazon Web Services provides developers with direct access to Amazon's robust technology platform. Build on Amazon's suite of web services to enable and enhance your applications. We innovate for you, so that you can innovate for your customers. Browse developer innovations in our [Solutions Catalog](#) to see the possibilities!

What's New?

Amazon EC2: Now in Unlimited Beta and Launching New Instance Types (October 16, 2007)
The Amazon EC2 Beta is now open to all developers and any developer can sign up to start using Amazon EC2 today. Additionally, Amazon EC2 has launched "Large" and "Extra Large" instance types to provide more memory, CPU, and instance storage, and are based on 64bit technology. The Large Instance is equivalent to roughly four Small Instances (original instance), and the Extra Large Instance is roughly equivalent to eight Small Instances. This was a popular request from customers that we're very happy to address with this release. [Read more details about these Instances.](#)

Announcing "AWS Start-Up Challenge": Win \$100,000 Plus an Investment Offer From Amazon (September 12, 2007)
AWS has just launched the AWS Start-Up Challenge, a contest for entrepreneurs and software developers that will award the winner \$50,000 in cash, \$50,000 in AWS credits, an investment offer from Amazon.com, and more. What are you waiting for? [Submit your idea now.](#)

Amazon Flexible Payments Services (Amazon FPS) - Limited Beta (August 2, 2007)
Amazon Web Services has opened a limited beta of Amazon Flexible Payments Service (Amazon FPS). Amazon FPS is the first payments service designed from the ground up specifically for developers. The set of web services APIs allows the movement of money between any two entities, humans or computers. It is built on top of Amazon's reliable and scalable payment infrastructure. Learn more about this [new service.](#)

Start Using Amazon Web Services

1. [Create your free Amazon Web Services account](#)
2. [Explore our web services](#)
3. [Build your application](#)

In the News

RightScale wins "Best in Show" at VentureNet (October 22, 2007)
RightScale is named "company to watch" by a committee of venture capital investors for their management platform built on Amazon Elastic Compute Cloud.

AWS Update at Web 2.0 Summit (October 18, 2007)
Amazon Web Services Vice President Adam Selipsky spoke at Web 2.0 Summit about the latest things happening in AWS.

WordPress using Amazon S3 (October 9, 2007)
WordPress founder Matt Mullenweg states on his blog that WordPress is now using Amazon S3 as its primary storage.

Students Learn Cloud Computing (October 8, 2007)
Phil Windley gives his students at Brigham Young University hands-on experience using Amazon EC2, SQS and S3.

Your Web Services Account

- Create scalable and reliable apps
- Build new solutions and make money
- Join an innovative developer community
- Sign-up today

AWS Start-Up Challenge

Enter the AWS Start-Up Challenge to win \$100,000 in cash and AWS credits, and an offer from Amazon.

4 Days Left till October 28

AWS Blog

Read the exciting and innovative developments around Amazon Web Services from the words of our Evangelists. [AWS Blog](#)

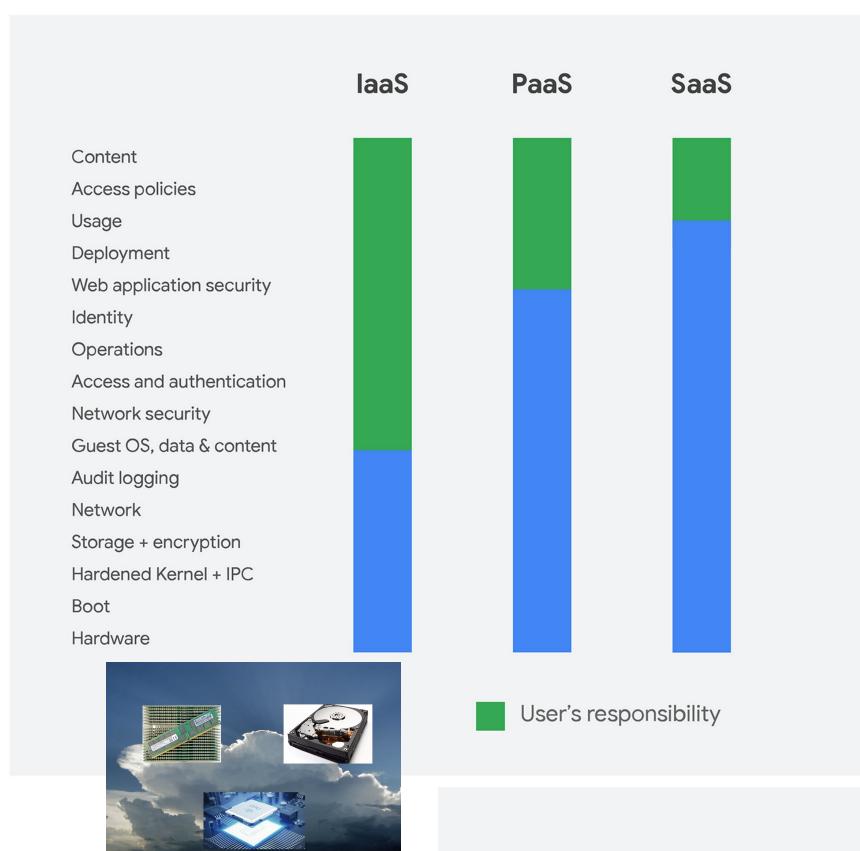
“

Cloud native techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.

”



“Cloud Shared Responsibility Model”



Infrastructure as Code

“ A server should be like a phoenix, regularly rising from the ashes.”



Martin Fowler

Phoenix Servers

Prevent:

- Configuration Drift
- Snowflake Server

Allow:

- Rise from the Ashes



Two deployment paths to a Phoenix Server

Imperative:

- specifics

Declarative:

- consumables

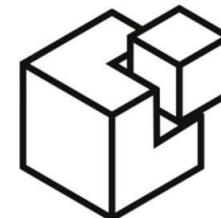


distributed
infrastructure state
development hosted in
Git

desired infrastructure
state promotion with Git
pull requests



Past Configuration Tools had Challenges



To deliver a **no humans in production, self-healing, secure-by-default infrastructure via GitOps, Infrastructure as Code must be API driven.**

API Driven IaC

Terraform *only* speaks to APIs

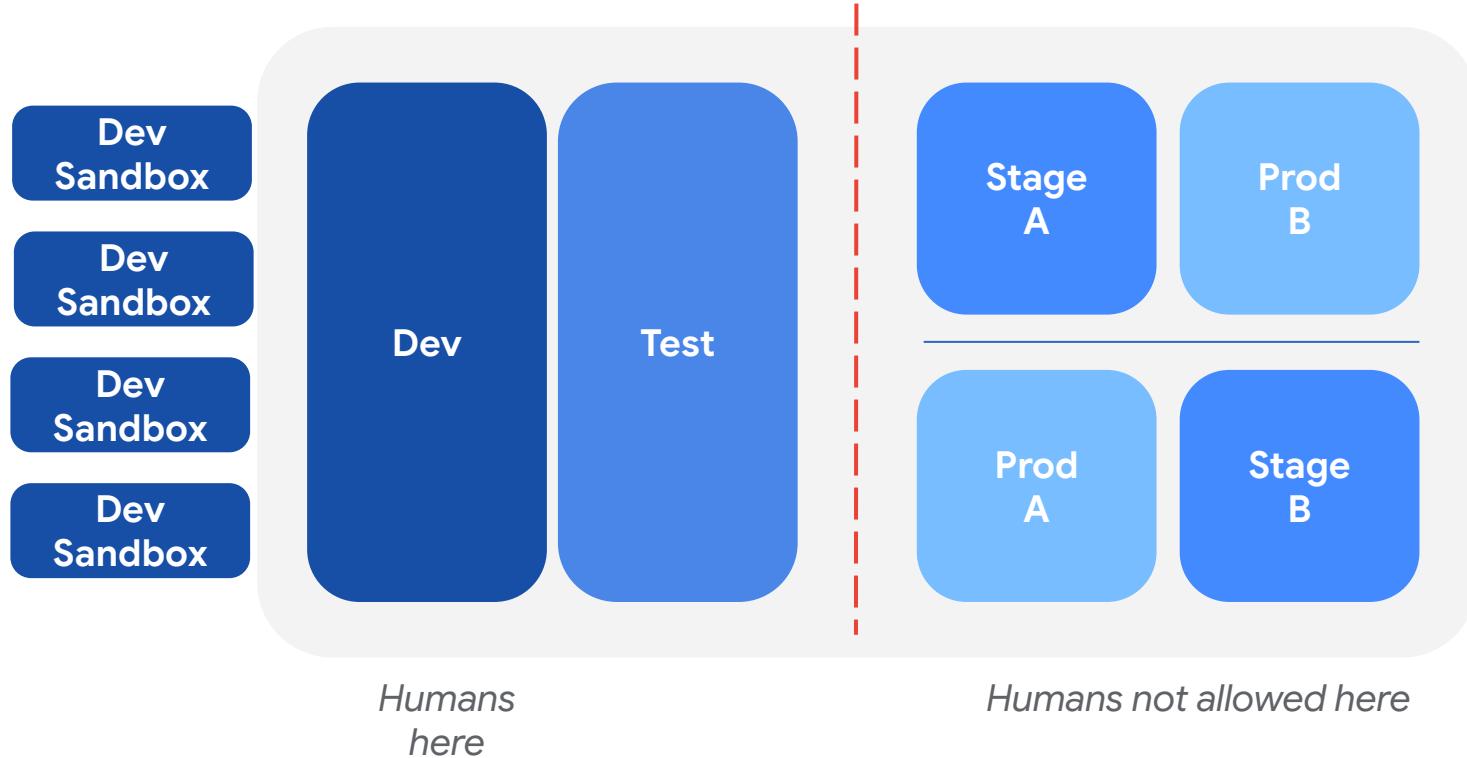
- Cloud native approach
- Declare state via HCL
- Resource Graph stores desired state
- Cloud API stores source of truth
- Written in Go



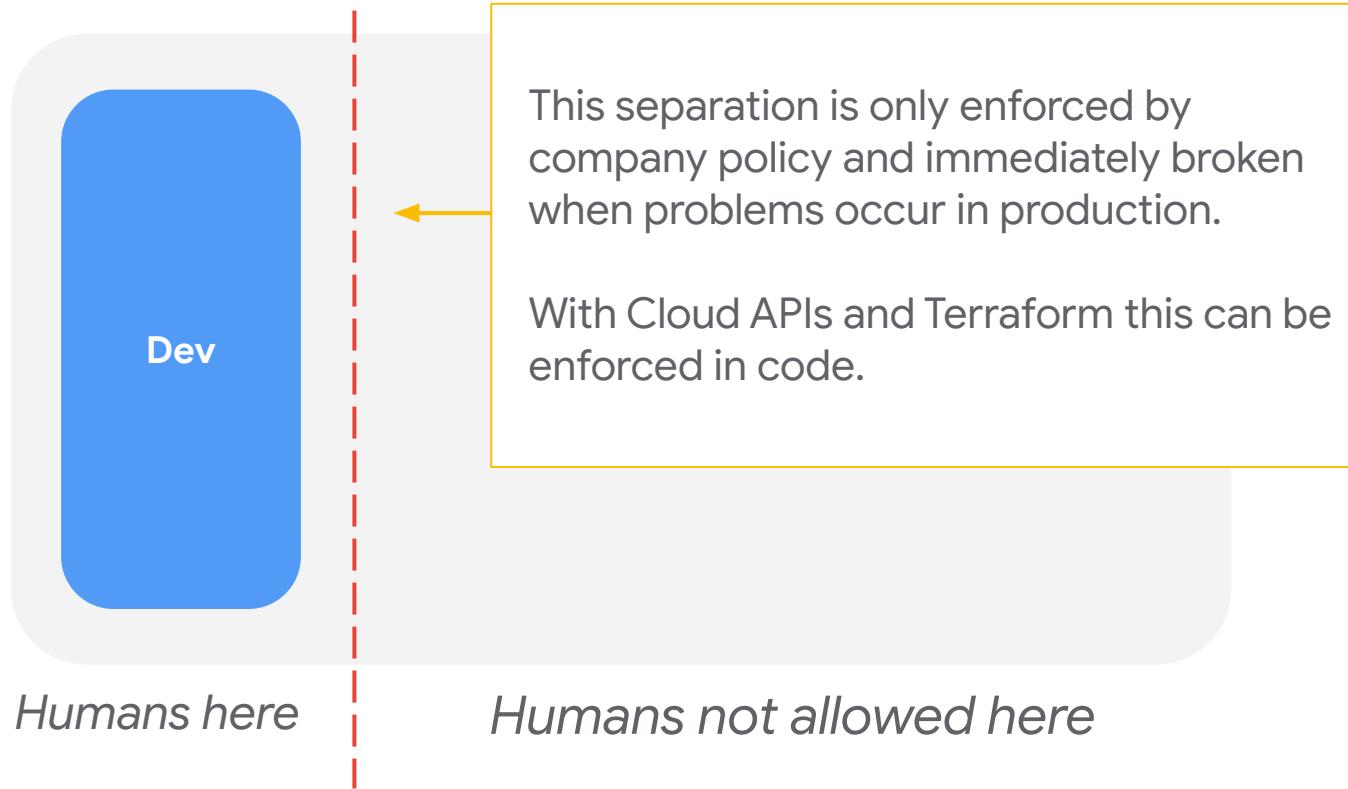
HashiCorp
Terraform

Infrastructure Layers

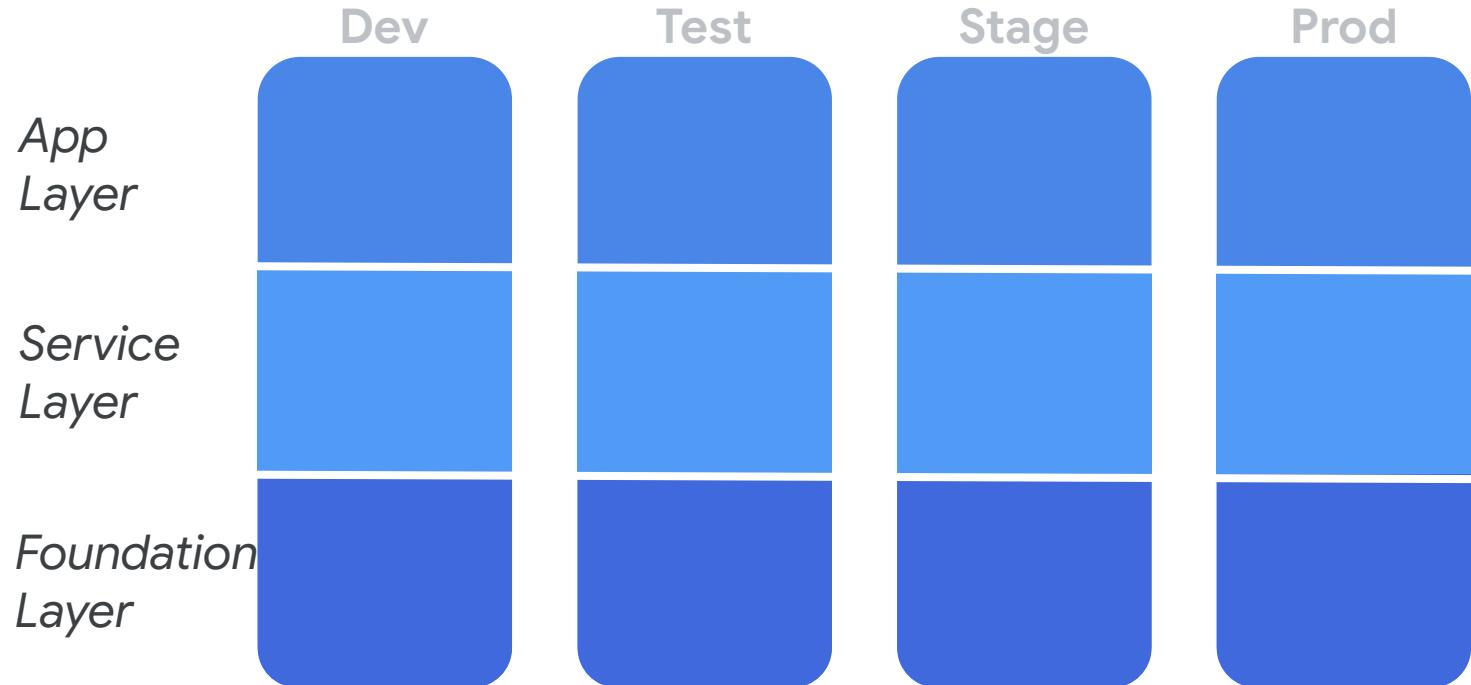
Environments separate horizontally



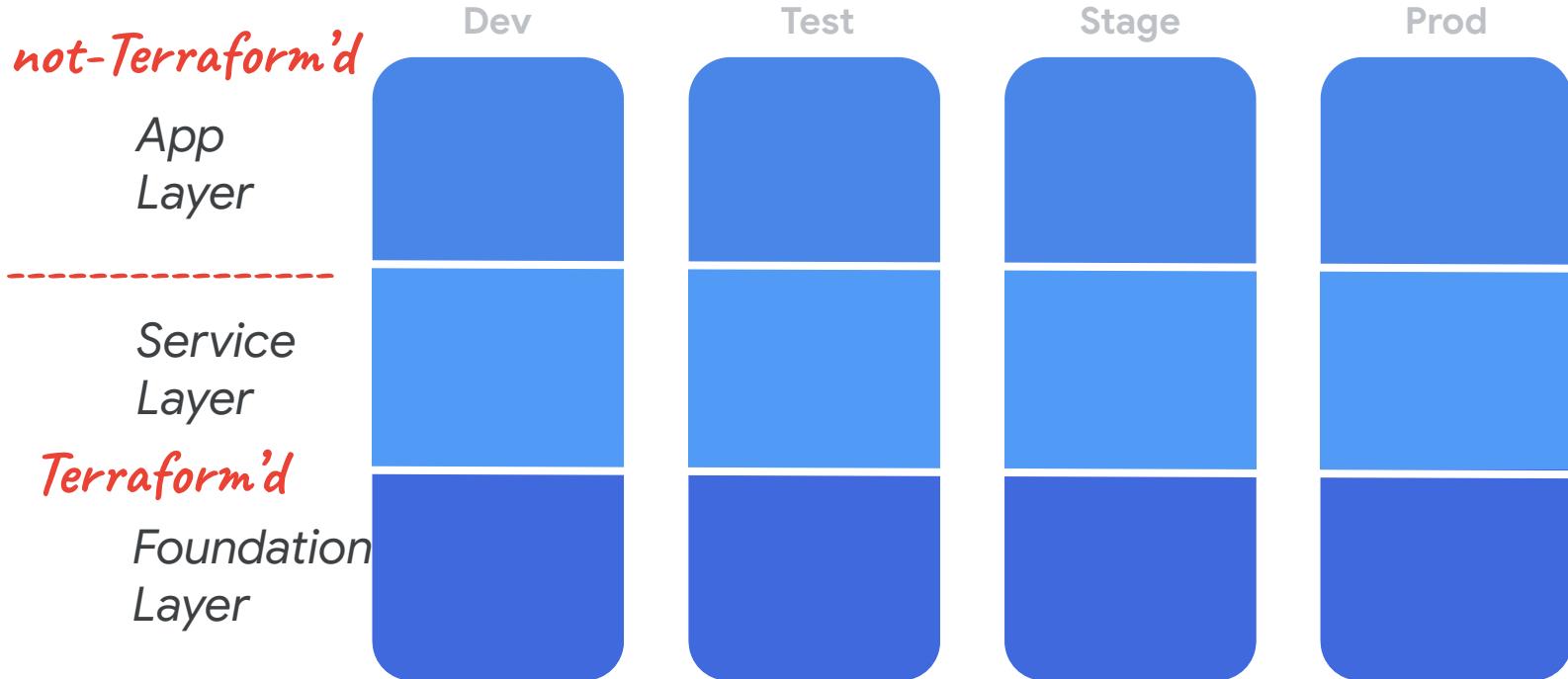
Separation is subjective



Layers vertically segment



Layers vertically segment



Infrastructure Layers segmentations

Foundation

GCP Organization
GCP Folders
GCP Projects
AWS Organizations
Azure Organizations
Security
Networking
IAM
Logging
Firewalls

Service

GCP Services
GKE - GCE - CloudSQL
AWS Services
EKS - EC2 - RDS
Azure Services
AKS - AzureVM - AzureSQL
Argo/Artifactory
Logging
App Firewalls

App

Application binaries
Containers
Helm Charts
Database data

Segmentation of Responsibility

Security

*Security
Logging*

Networking
Monitoring
Observability
Auditing

Ops

*Security
Logging*

Networking
Monitoring
Observability
Versioned States
Scaling
Healing

Dev

*Security
Logging*

Application Logic
Database Data
Versioned State
Observability Ticks

Segmentation of Responsibility

This segmentation allows each team to focus on their area of responsibility providing empathy for other teams

Security

Security Logging

- Networking
- Monitoring
- Observability
- Auditing

Ops

Security Logging

- Networking
- Monitoring
- Observability
- Versioned States
- Scaling
- Healing

Dev

Security Logging

- Application Logic
- Database Data
- Versioned State
- Observability Ticks

GitOps

*Git interface for the
Desired Infrastructure State*

GitOps

Teams



Git Repo

Desired
Infrastructure
State

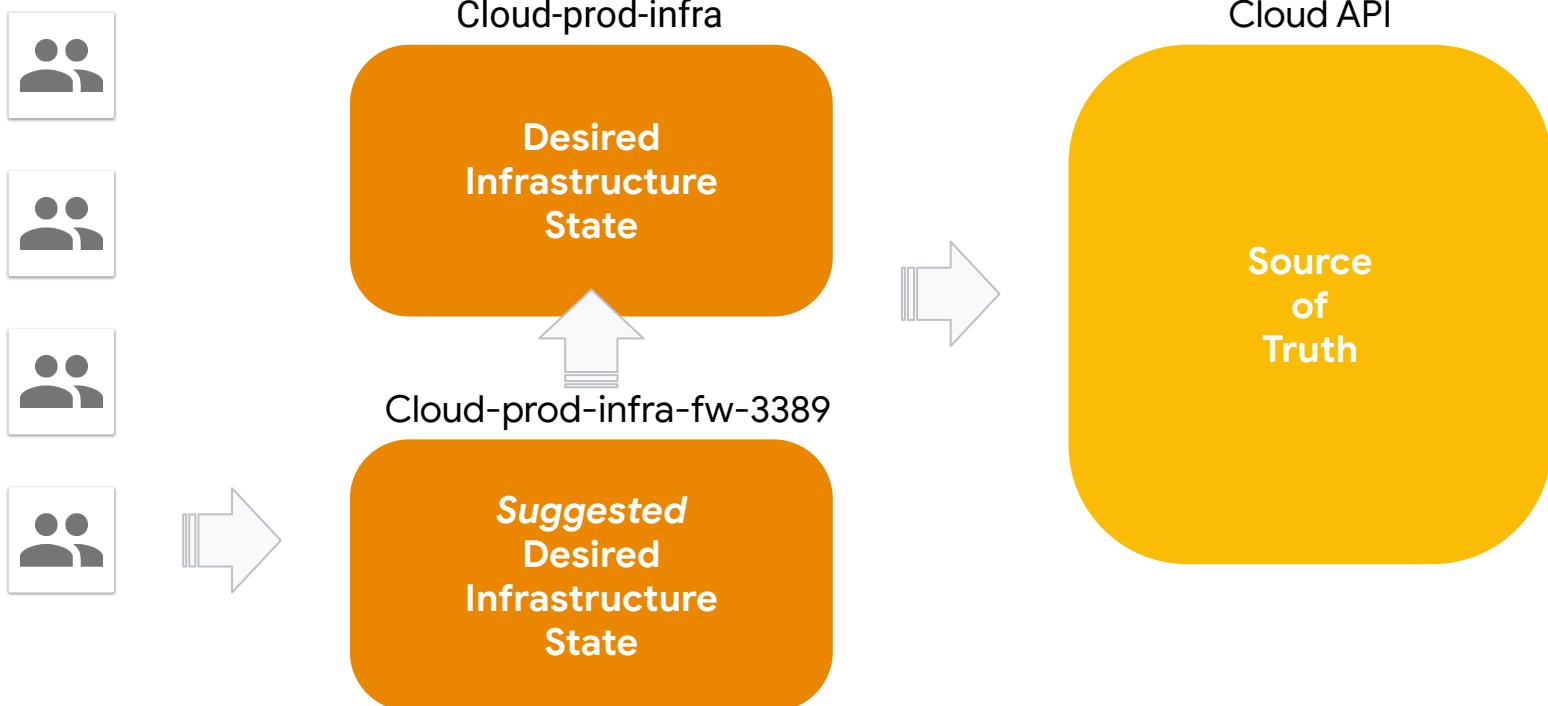


Cloud API

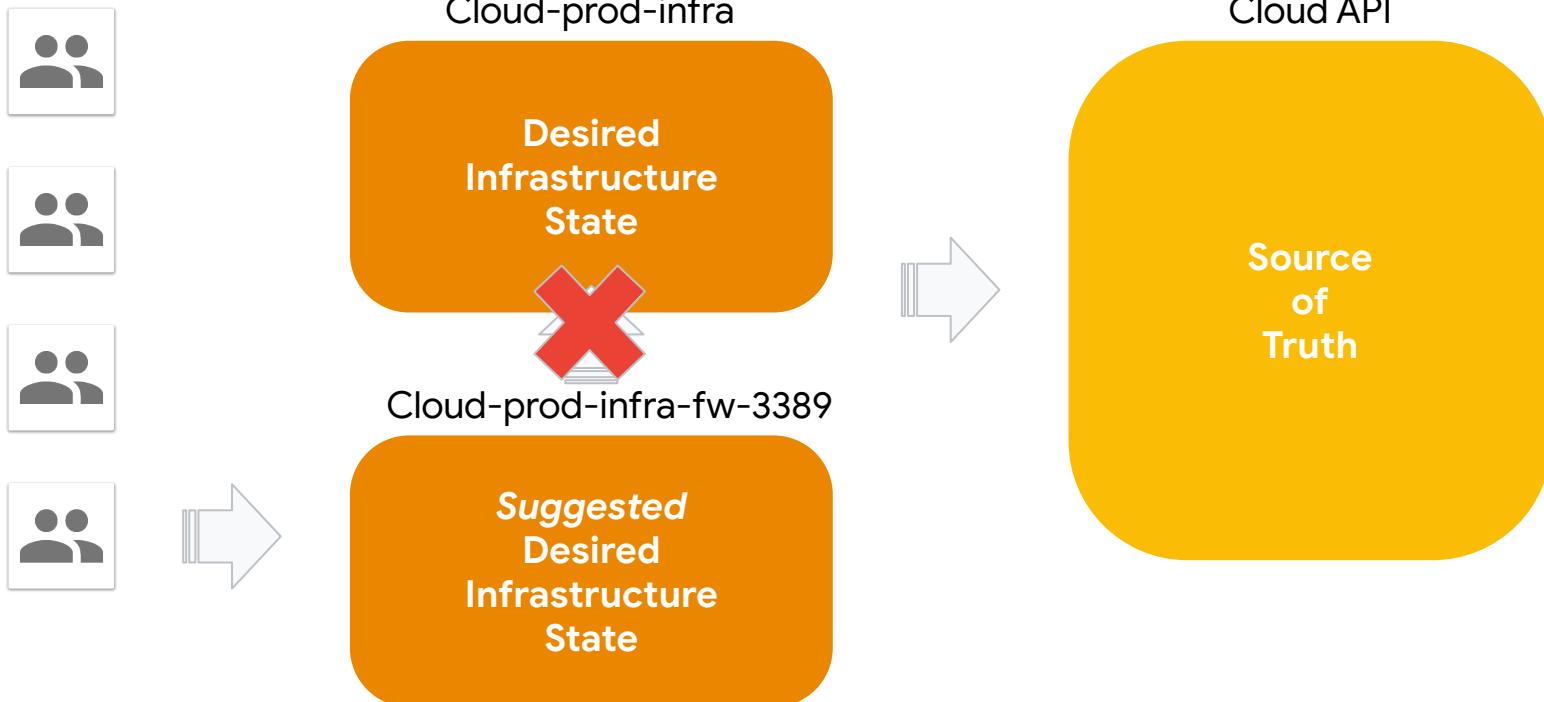
Source
of
Truth



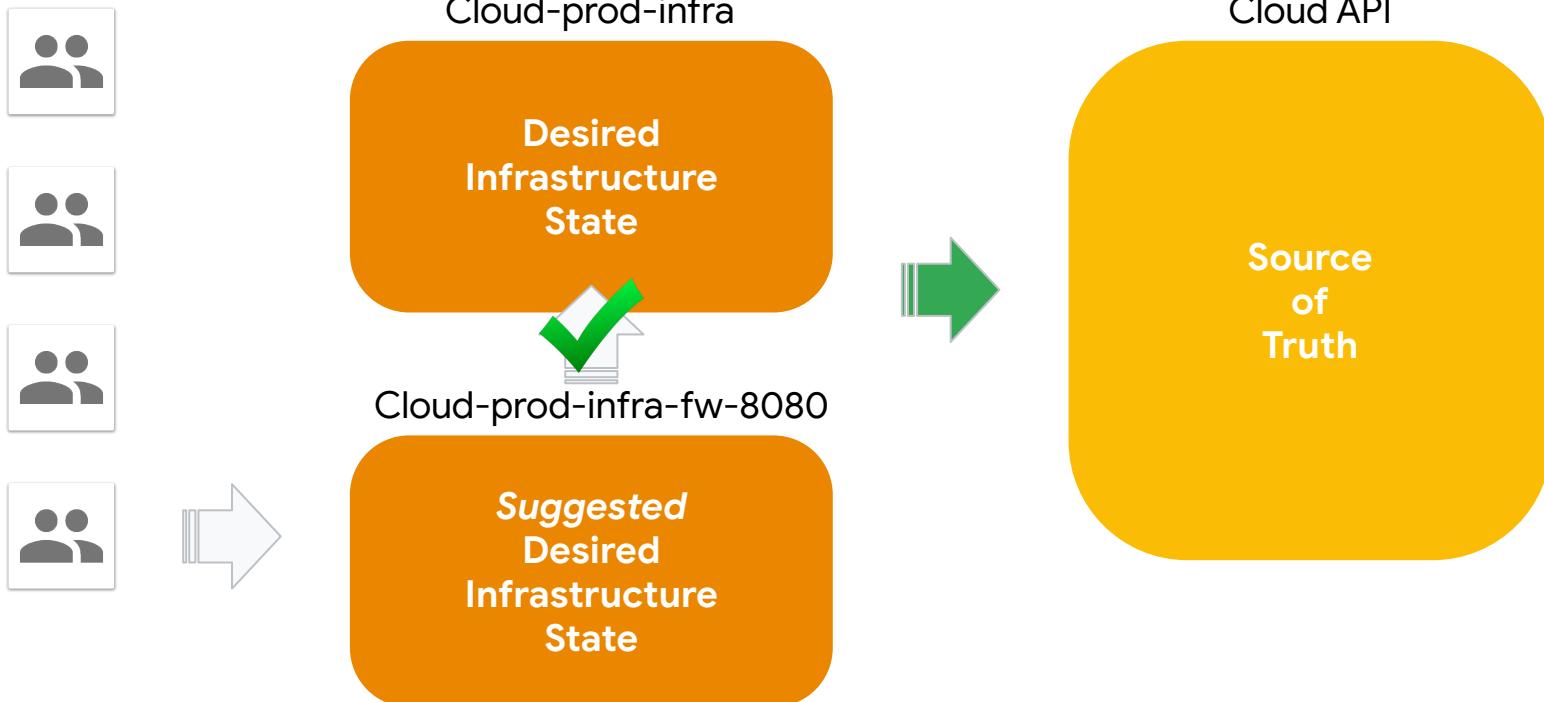
Git Pull Requests



Git Pull Requests



Git Pull Requests



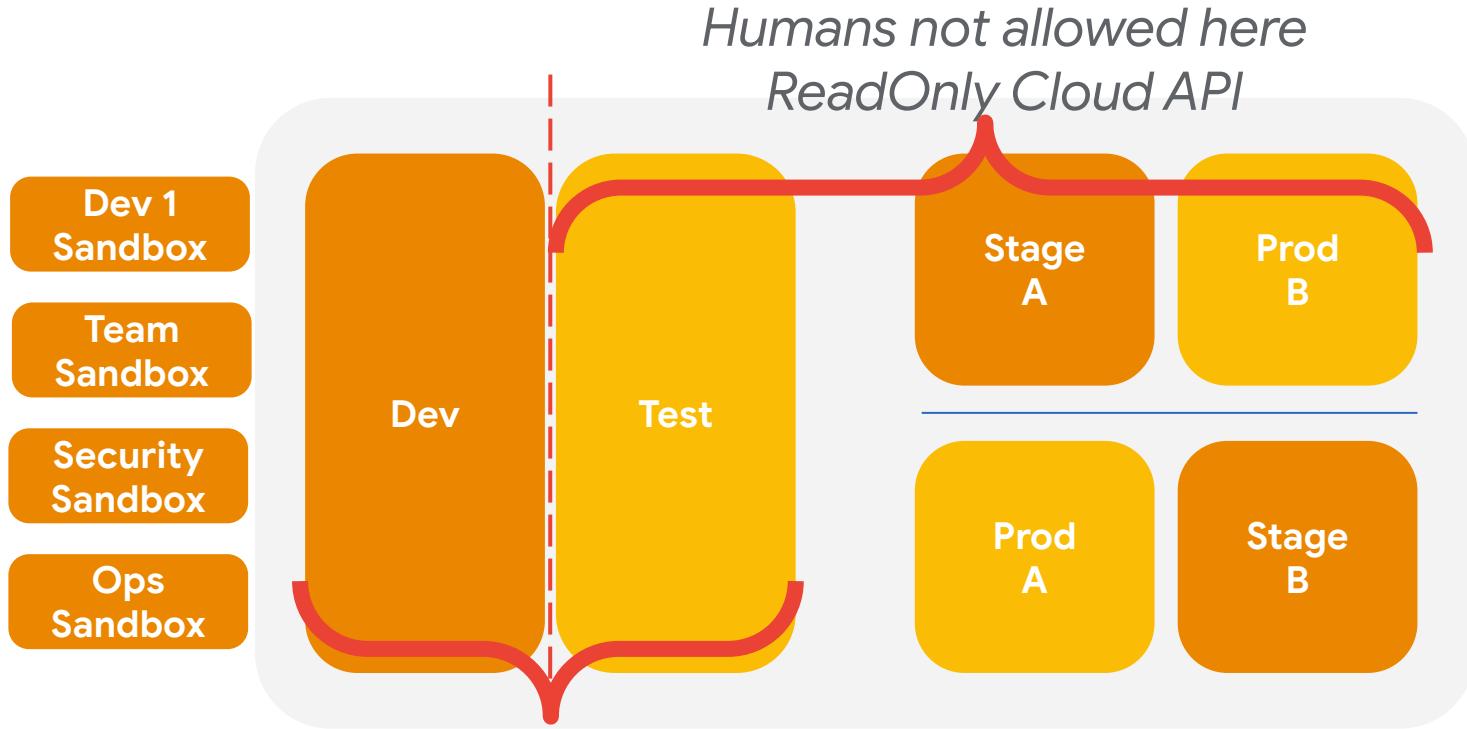
Mad Scientist Laboratory



Mad Scientist Laboratory



Code Lifecycle Across Environments



App Code + IaC = Productionalized

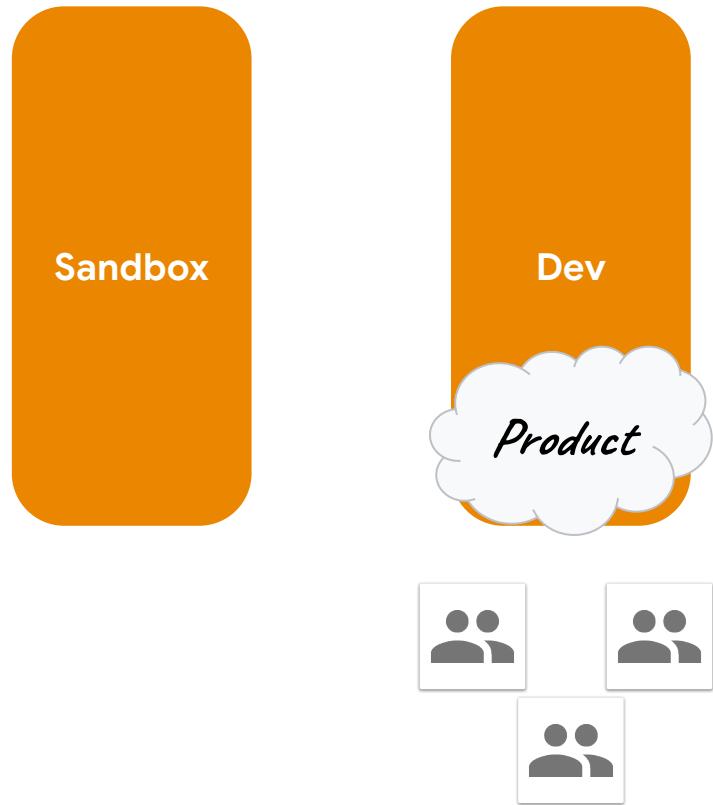
The Sandbox

- Confined anarchy
- Empower engineers to experiment & learn
- NO - infrastructure-as-code
- YES - Web Consoles!!
- Only rule = *security perimeter preventing opening to the public web*



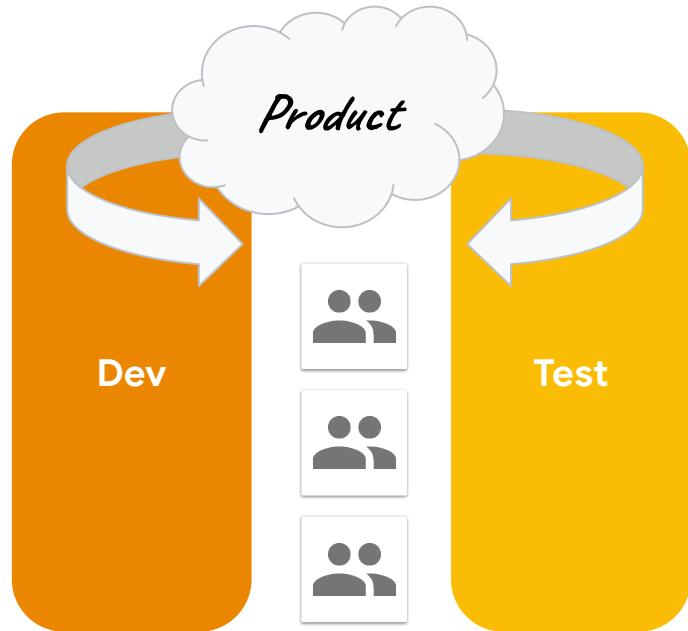
Promote to Dev for Integration Collaboration

- Dev, Ops, Security collaborating Git PR
- Goal is productionalization of product
- App Code + IaC
- Vetting of:
 - Security
 - Scaling
 - Healing



Promote to Test for Prod testing

- Product ready for Prod promotion
- NO - humans in Test
- ONLY - IaC in Test



GitOps

Teams



Git Repo - Terraform
Firewalls

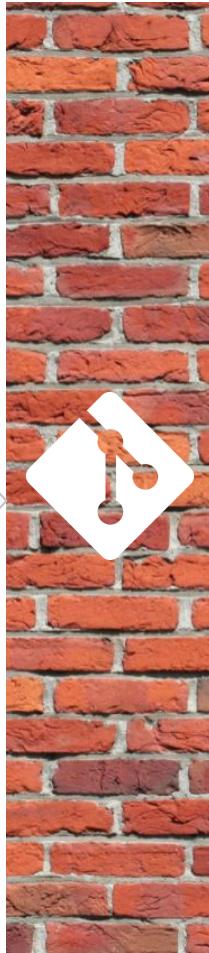
Git Repo - Terraform
Networking

Git Repo - Terraform
Service Layer

Git Repo - Terraform
Foundation Layer

Cloud API

Source
of
Truth



Service Buffet

Teams



Optical Translator App



Julia Math Suite



Hugo Go Website



GCP BigQuery



Cloud API

Source
of
Truth



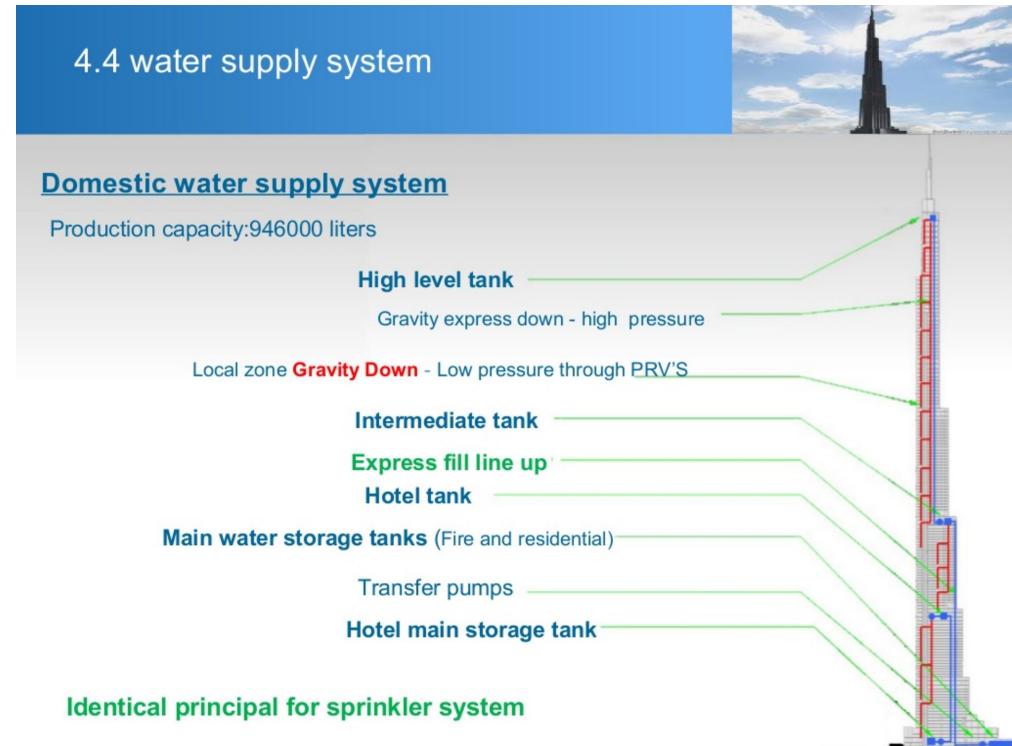
Security
Sanctity

“ The security of the infrastructure is designed in progressive layers... ”

Google Infrastructure Security Design Overview



Simplicity
+
Known State
=
Security



Simplicity
+
Known State
=
Security



Virus Scanning is making payments for the car that was repossessed 12 years ago

BTR.sys deployed to the Windows source code and signed by Microsoft

2009

CVE-2021-24092: 12 Years in Hiding – A Privilege Escalation Vulnerability in Windows Defender

• KASIF DEKEL / FEBRUARY 10, 2021

Executive Summary

In this post, we disclose a severe vulnerability in Windows Defender that allows attackers to escalate privileges from a non-administrator user. Windows Defender is deeply integrated into the Windows operating system and is installed by default on every Windows machine (more than 1 billion devices).

2021 CVE-2021-24092

CVE Published





Infrastructure Layers Outcomes

Self-Healing

Self-healing infrastructure turns
Saturday at 2am problems into
Monday 10am problems.

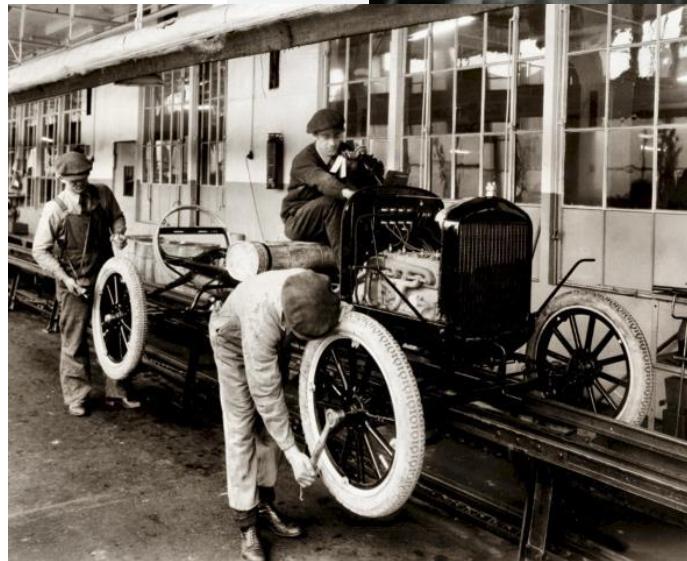
Having the right people in the right
frame of mind to solve hard
problems.



Infrastructure Culture as a Recruiting Tool

Eliminate toil to:

- retain the talent you already have
- bring in new talent
- let engineers enjoy solving unique problems



Eliminating Toil

"TOIL IS THE KIND OF WORK TIED TO
RUNNING A PRODUCTION SERVICE THAT
TENDS TO BE MANUAL, REPETITIVE,
AUTOMATABLE, TACTICAL, DEVOID OF
ENDURING VALUE, AND THAT SCALES
LINEARLY AS A SERVICE GROWS."

From here