Chaos Architecture

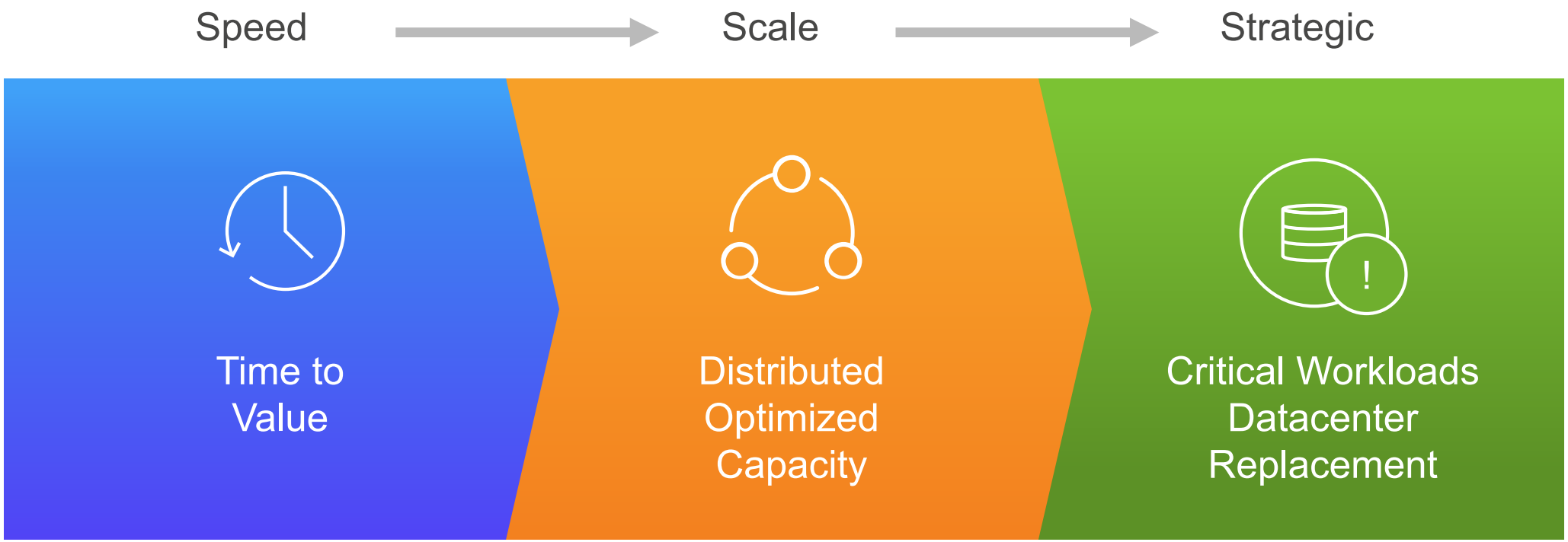
A Cloud Native Availability Model

Adrian Cockcroft

@adrianco

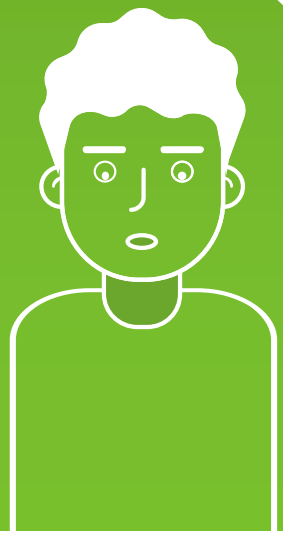
AWS VP Cloud Architecture Strategy

Pathway for Digital Transformation



As an architect my role wasn't to tell other people what the architecture should be.

It was to ask awkward questions…

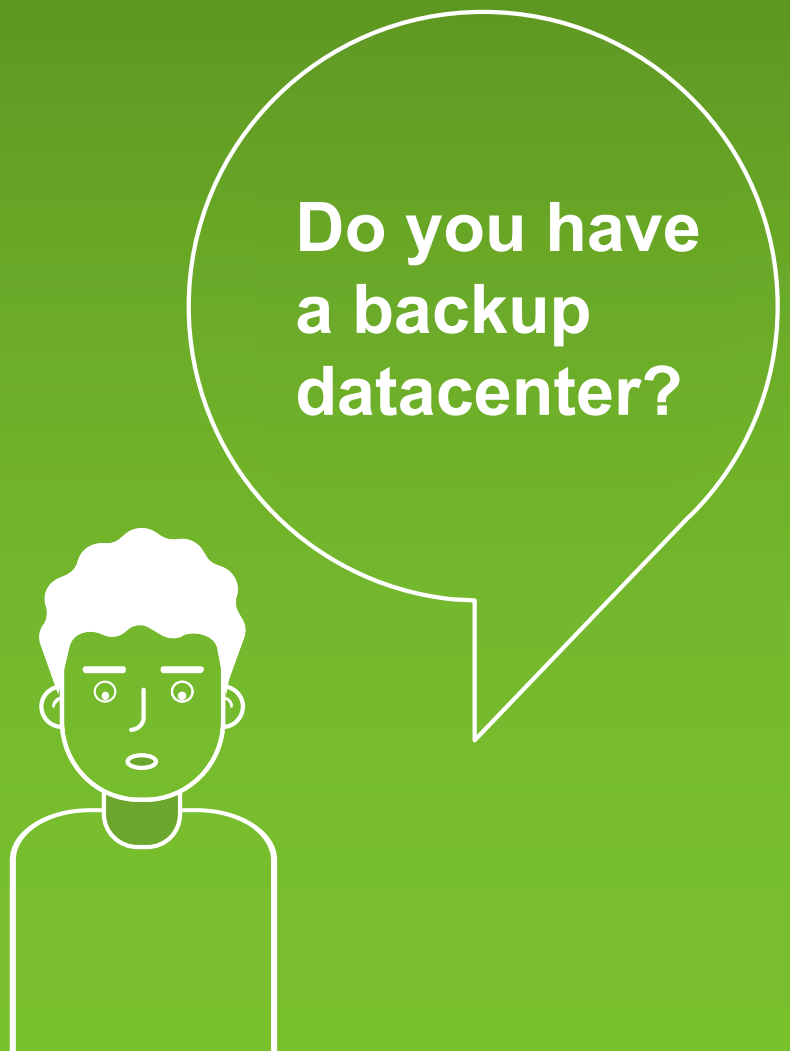


What should your system do when something fails?

- Stop?
- Carry on with reduced functionality?

Permissive failure, what's the real cost of continuing?

See ***Memories, Guesses, and Apologies***
by Pat Helland



How often do you failover apps to it?

How often do you failover the **whole datacenter** at once?

“Availability Theater”

A fairy tale…

Once upon a time, in theory, if everything works perfectly, we have a plan to survive the disaster we thought up in advance.

How did that work out?

Forgot to renew domain name… SaaS vendor

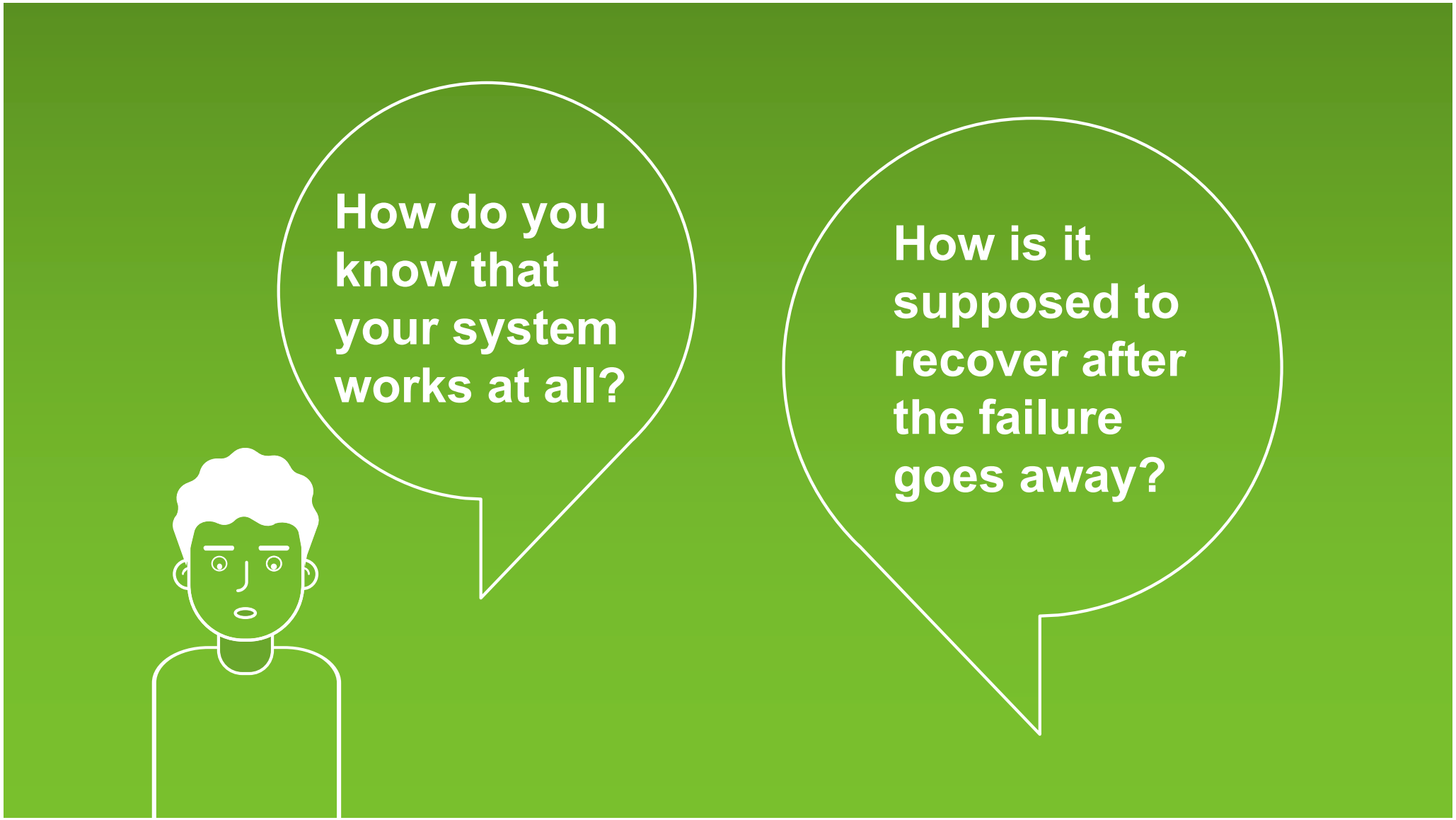
Didn’t update security certificate and it expired… Entertainment site

Datacenter flooded in hurricane Sandy… Finance company, Jersey City

Whoops! **YOU, tomorrow**

“You can’t legislate against failure, focus on fast detection and response.”

—Chris Pinkham


How do you know that your system works at all?
How is it supposed to recover after the failure goes away?

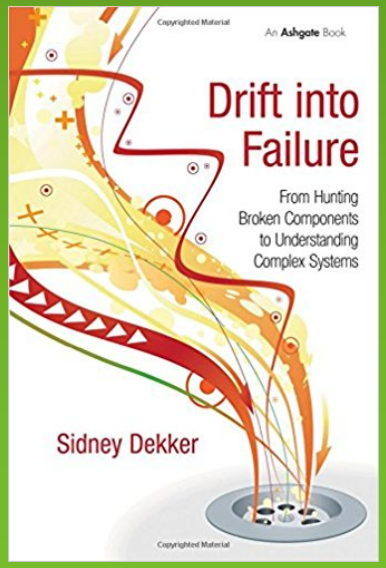
acmqueue

The Network Is Reliable

ACM Queue 2014

Bailiss & Kingsbury

@pbailiss @aphyr



Drift Into Failure

Sydney Dekker

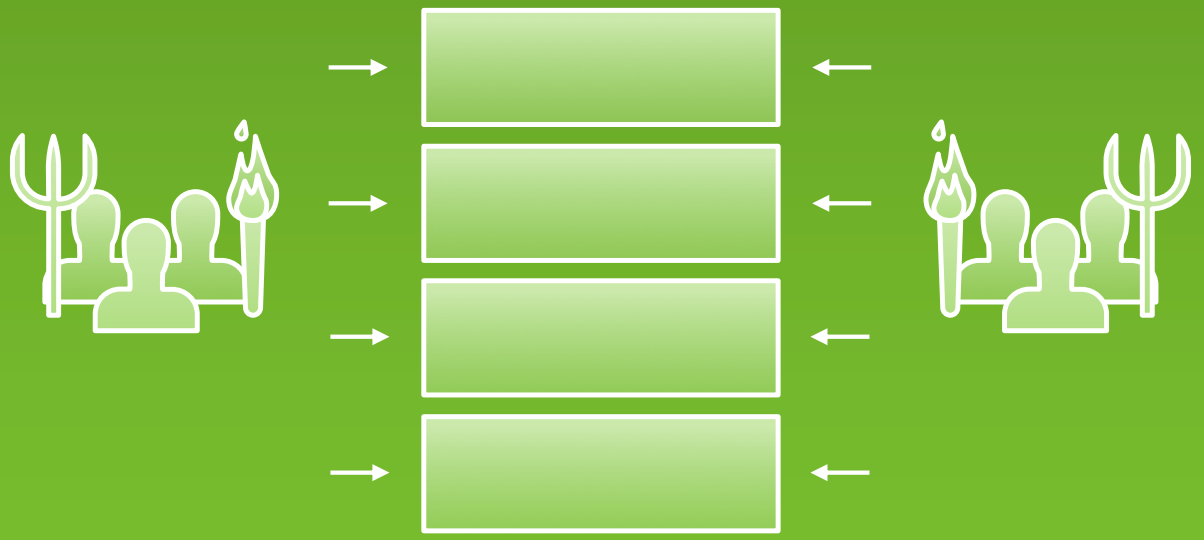
Release It!

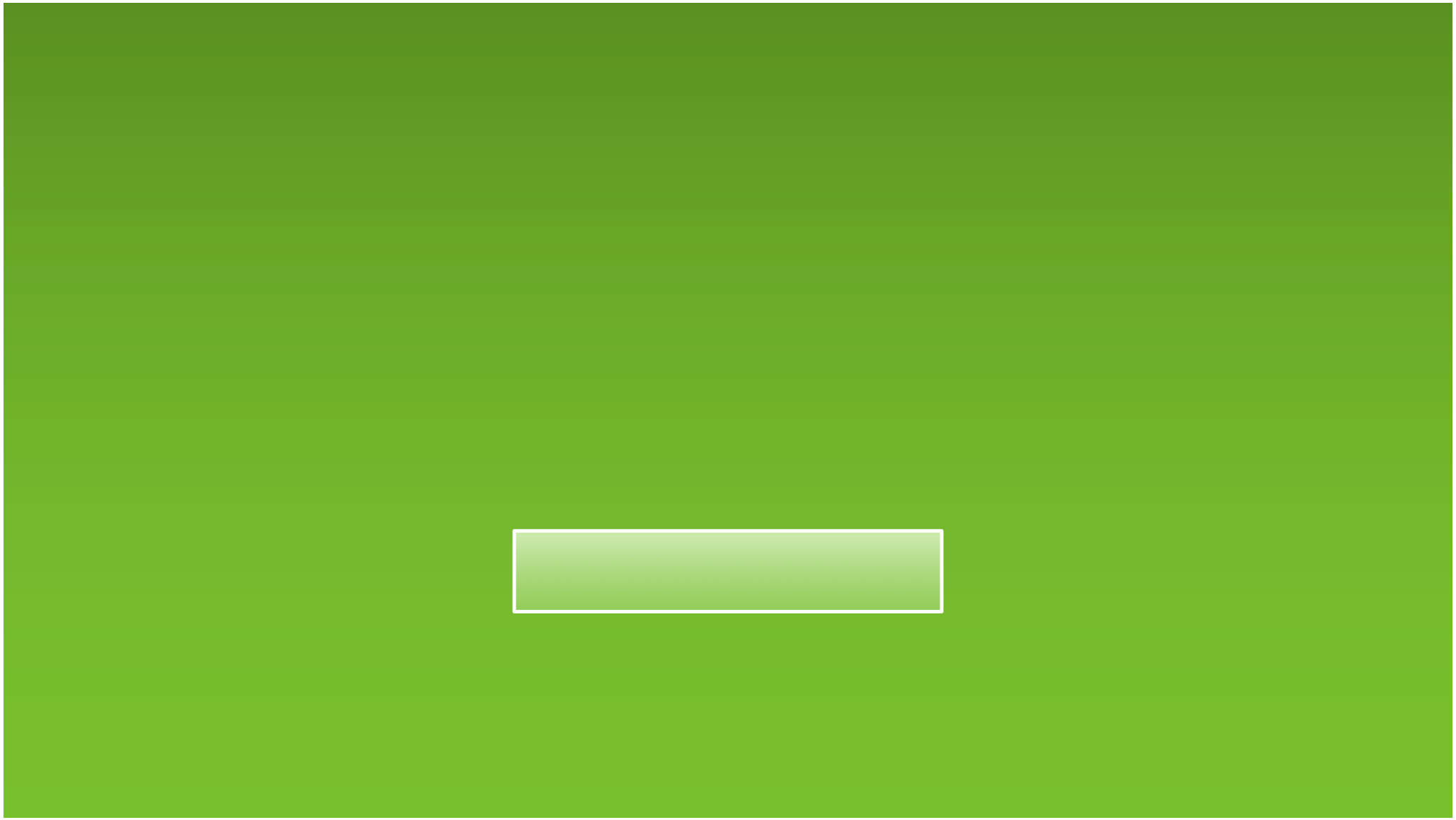
Second Edition 2017

Michael Nygard

Chaos Architecture

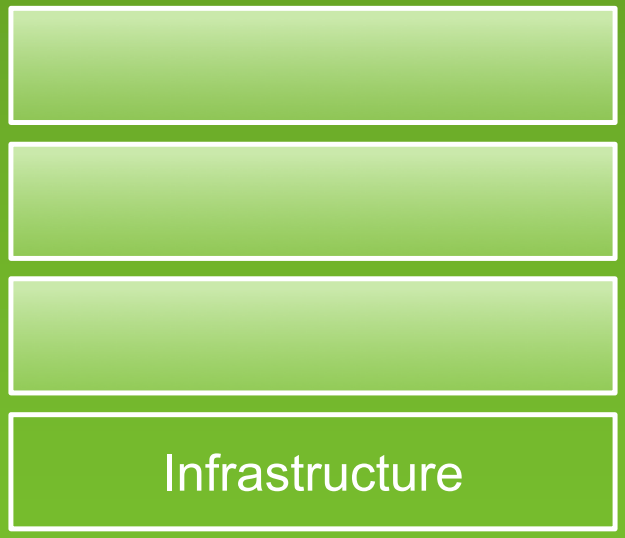
Four layers
Two teams
An attitude

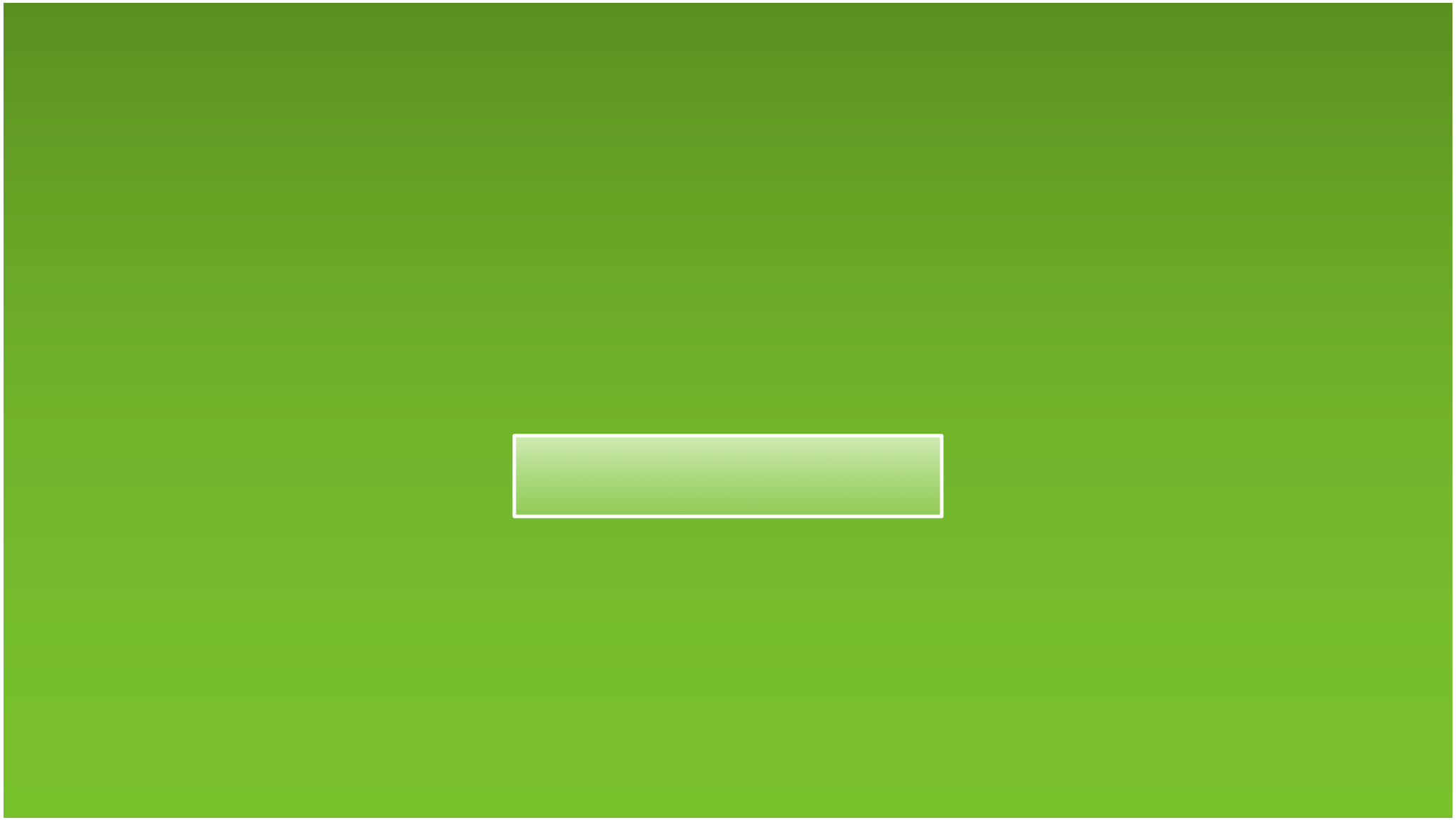




Infrastructure and Services

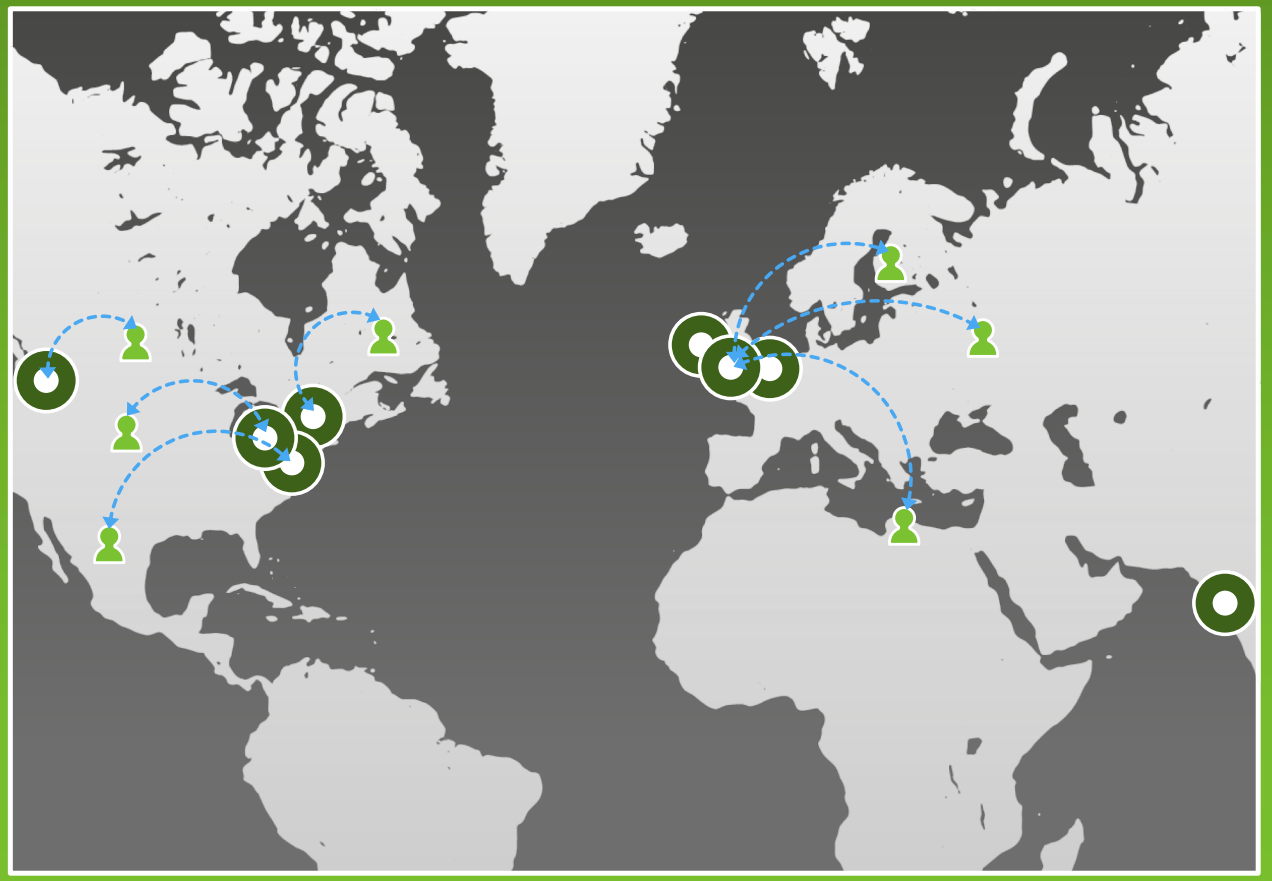
No single point of failure


Infrastructure



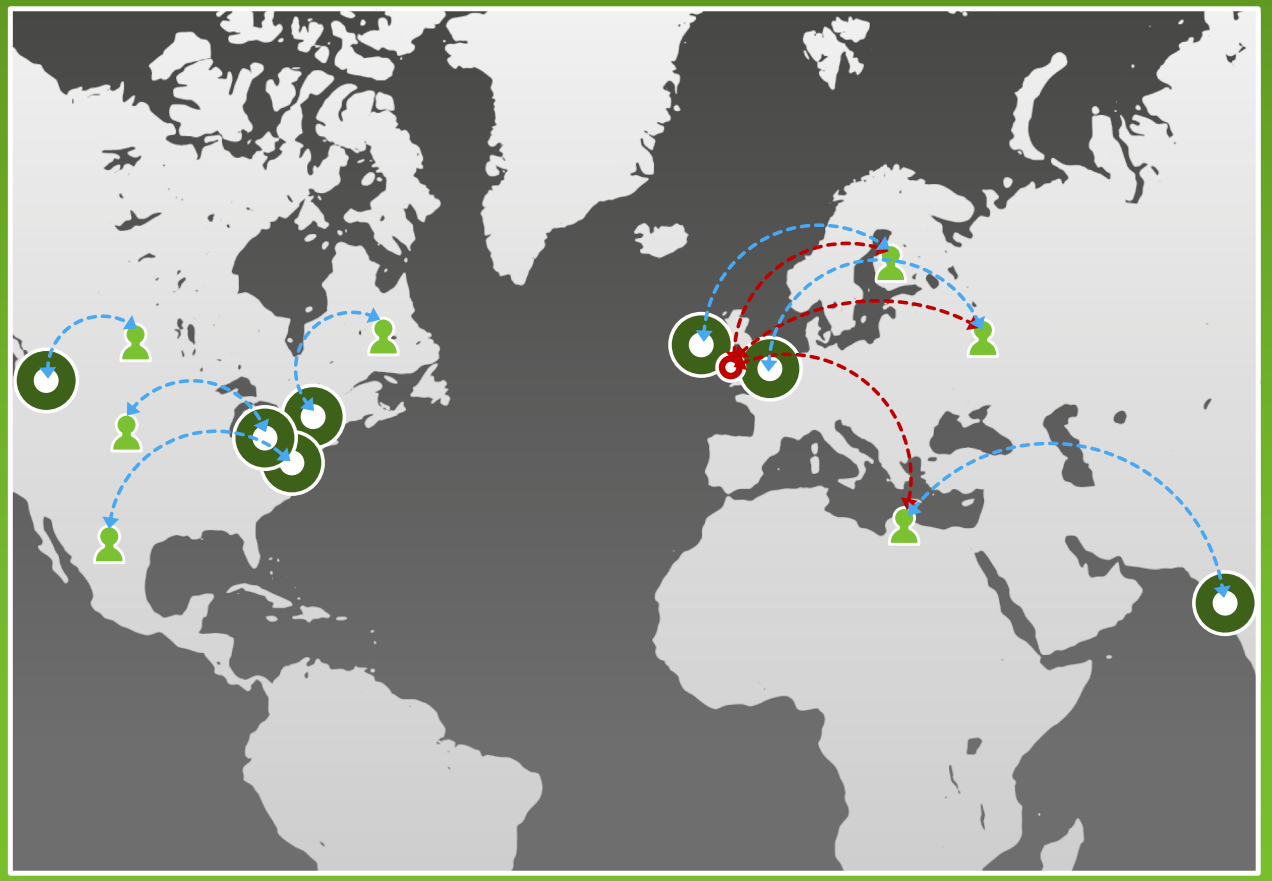
Switching and Interconnecting

Data replication
Traffic routing
Avoiding issues
Anti-entropy recovery



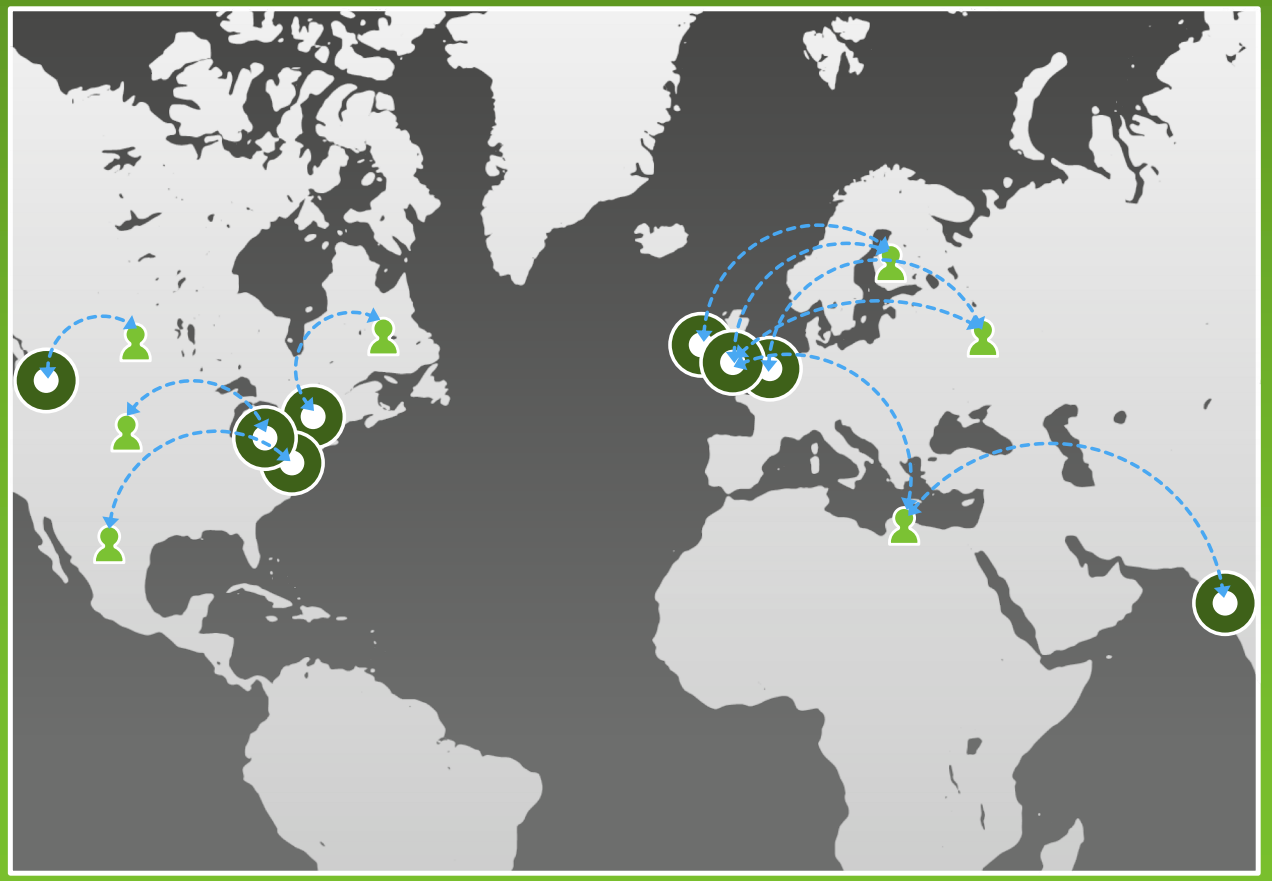
Switching and Interconnecting

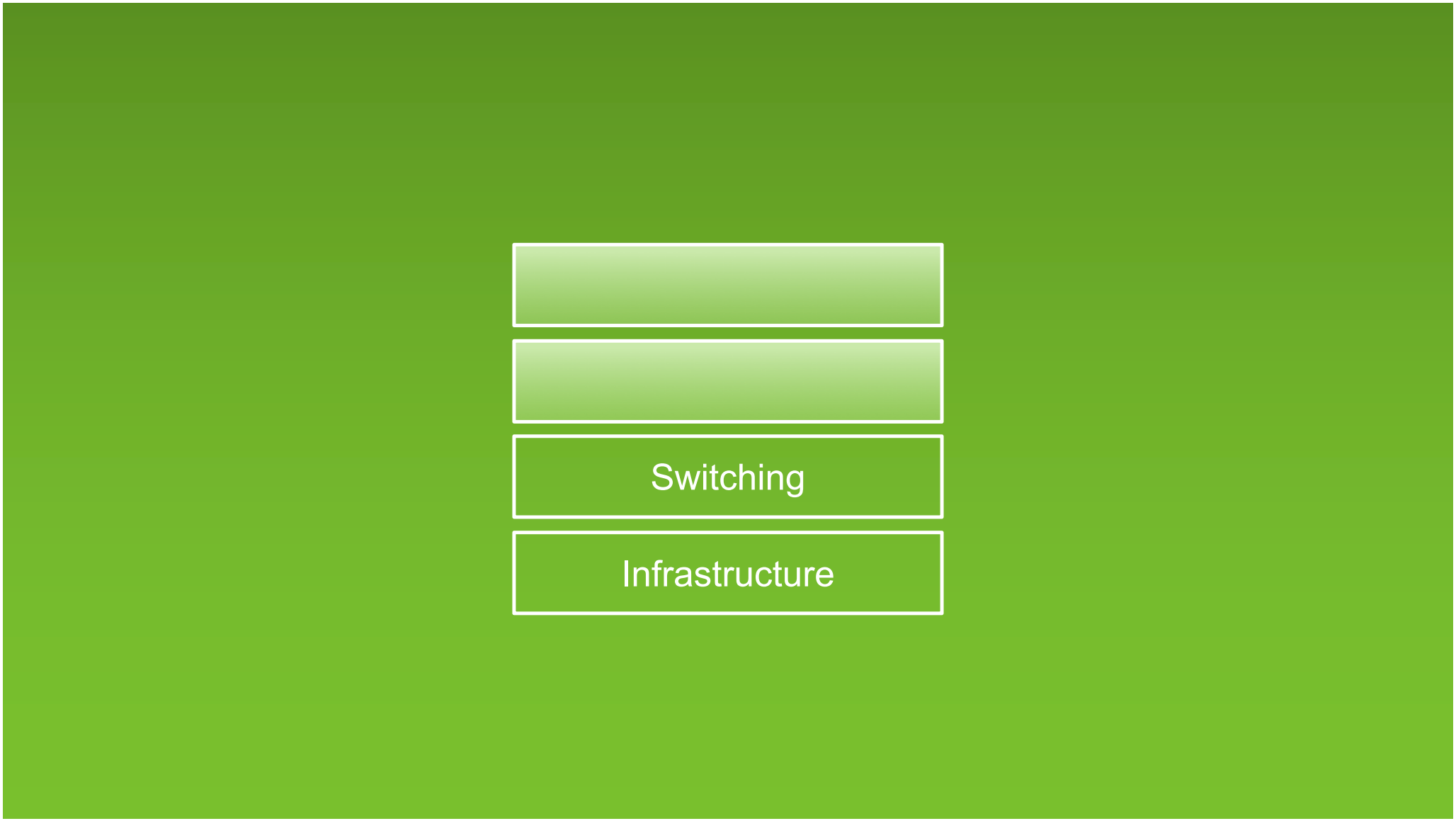
Data replication
Traffic routing
Avoiding issues
Anti-entropy recovery

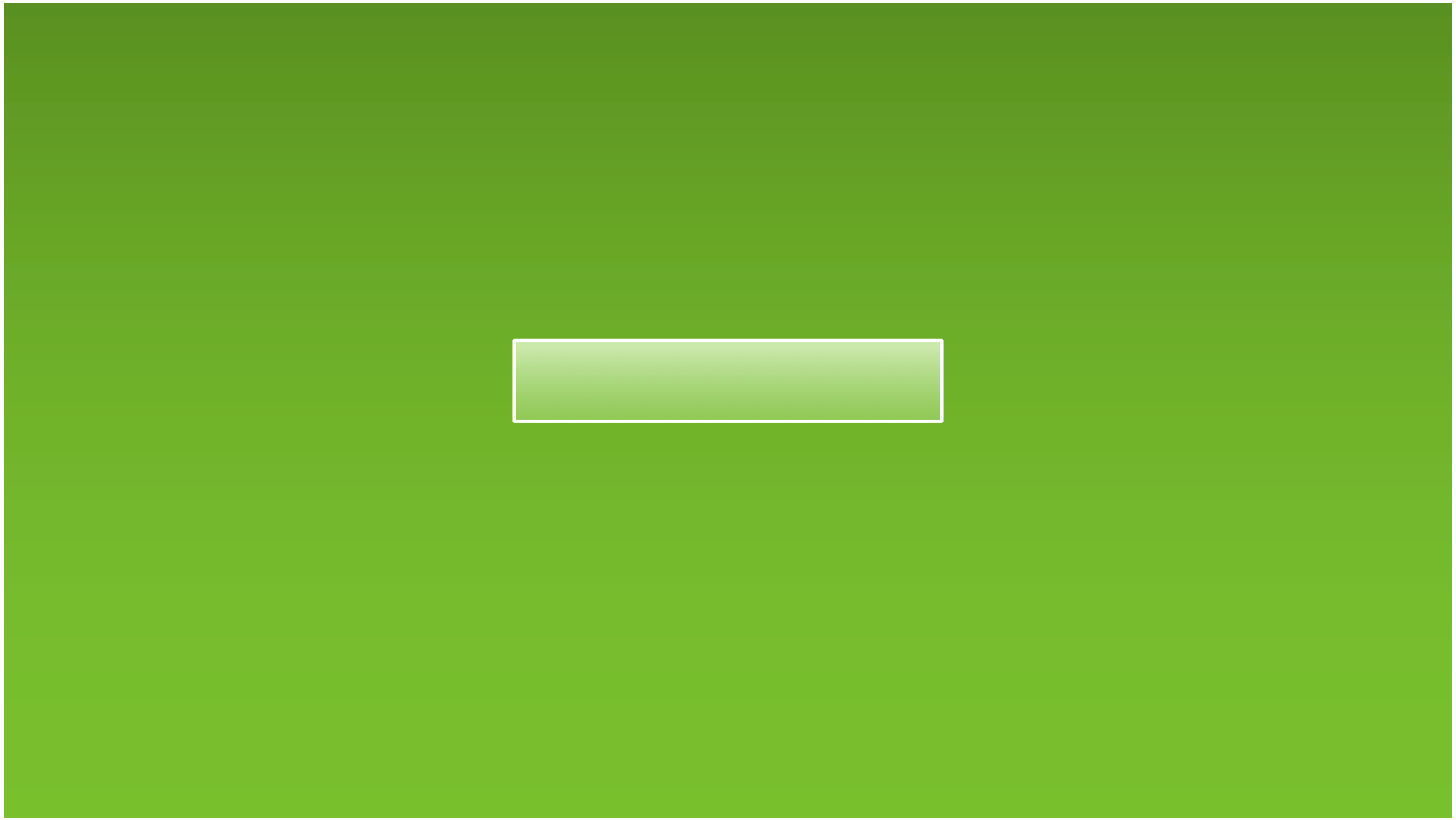


Switching and Interconnecting

Data replication
Traffic routing
Avoiding issues
Anti-entropy recovery




Switching
Infrastructure

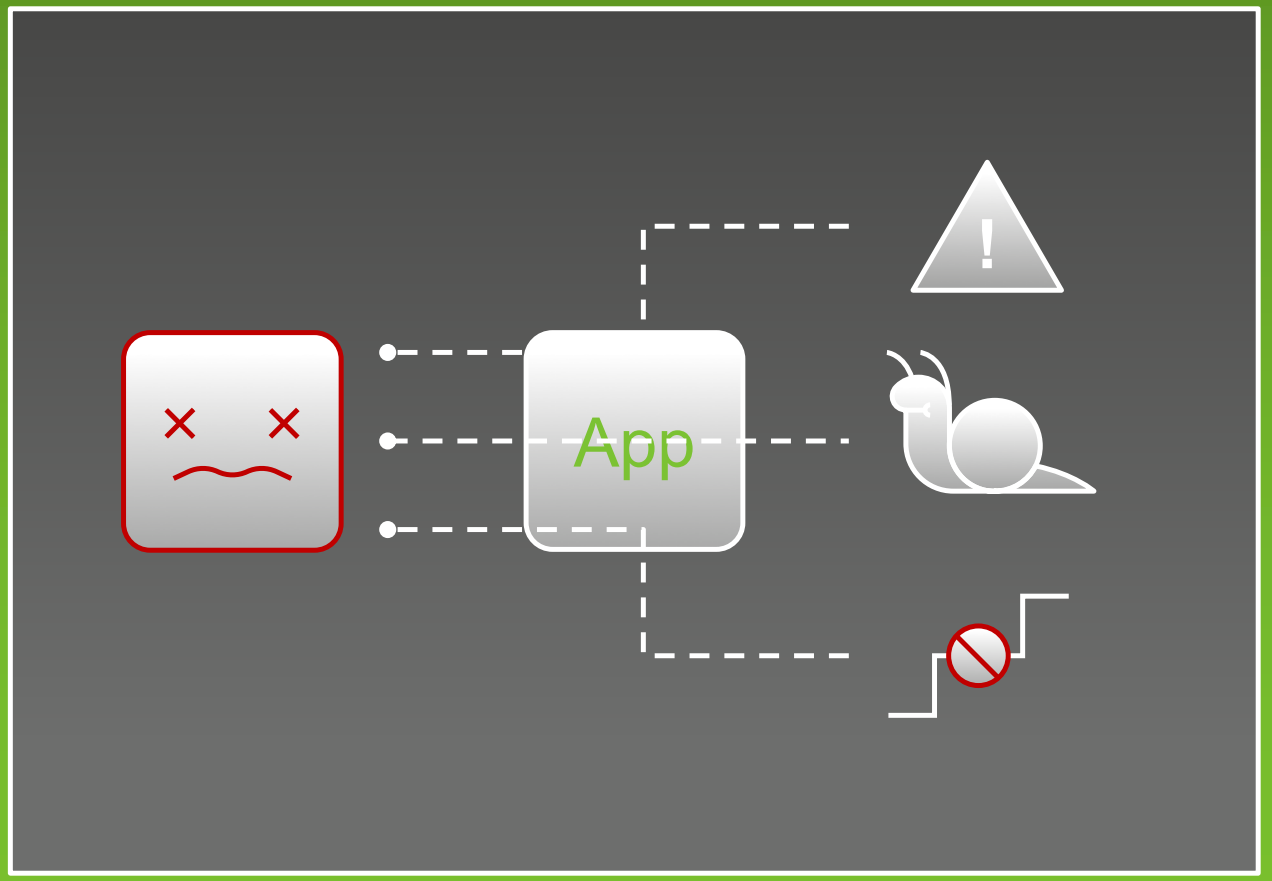


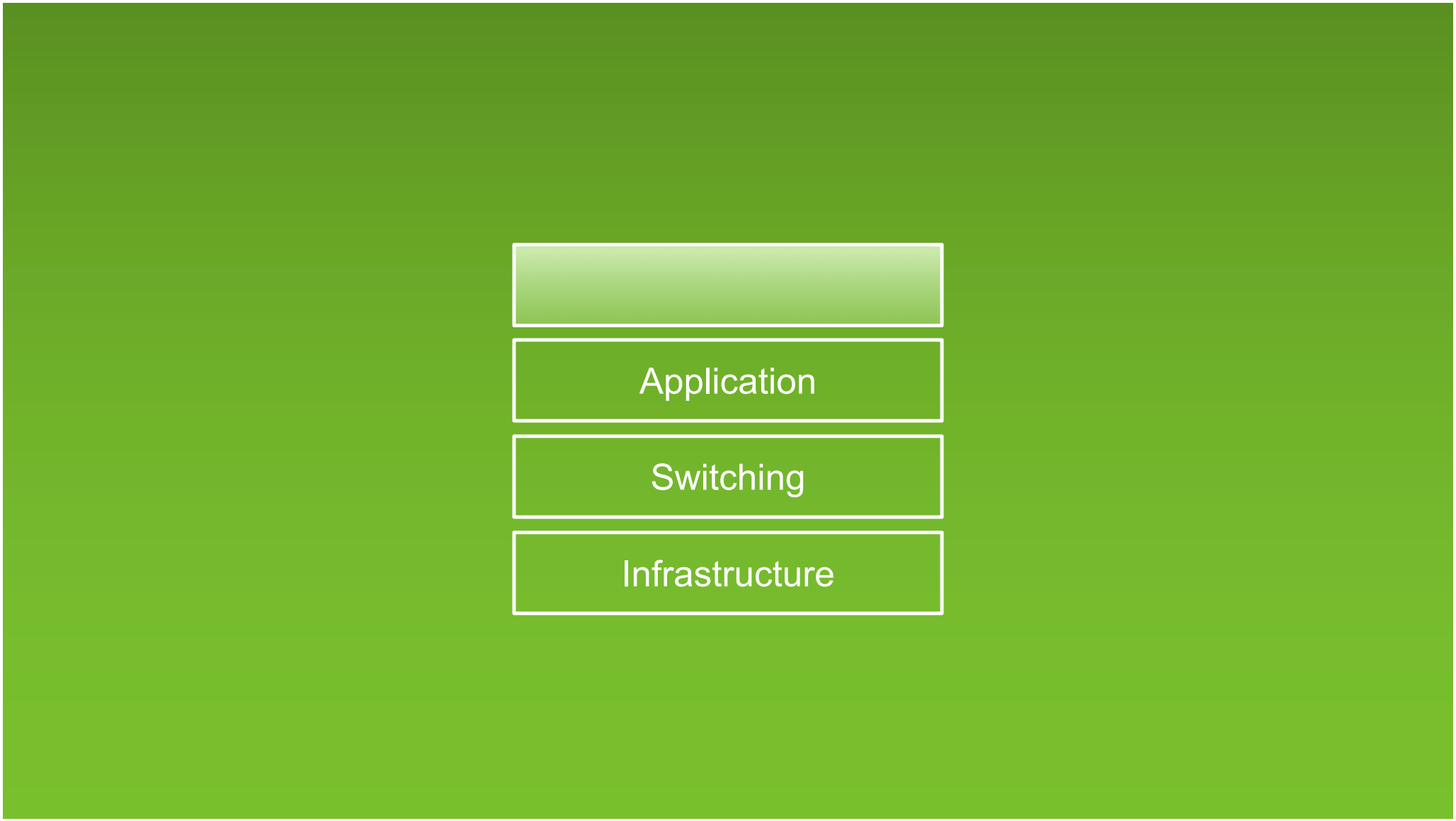
Application Failures

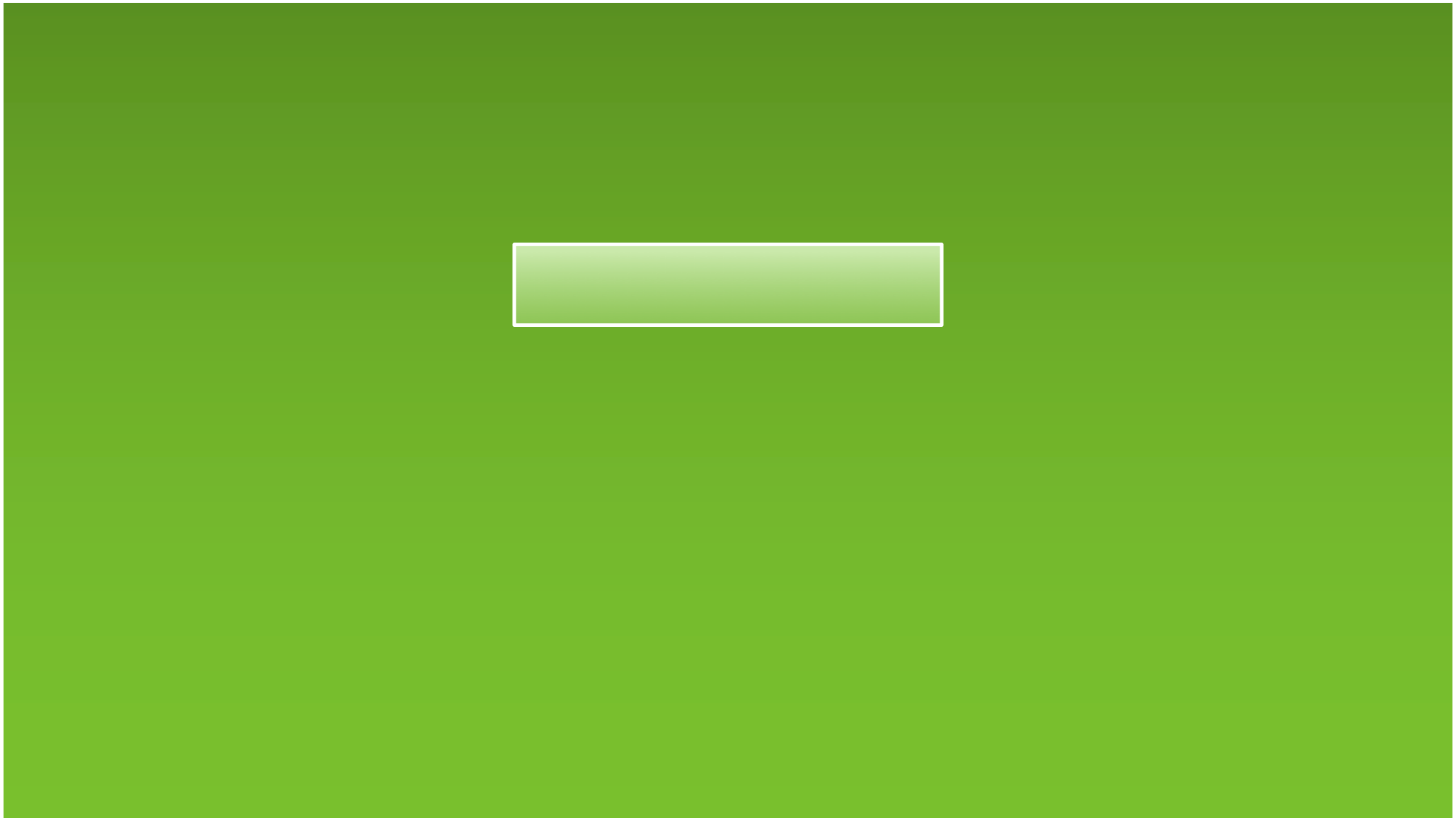
Error returns

Slow response

Network partition

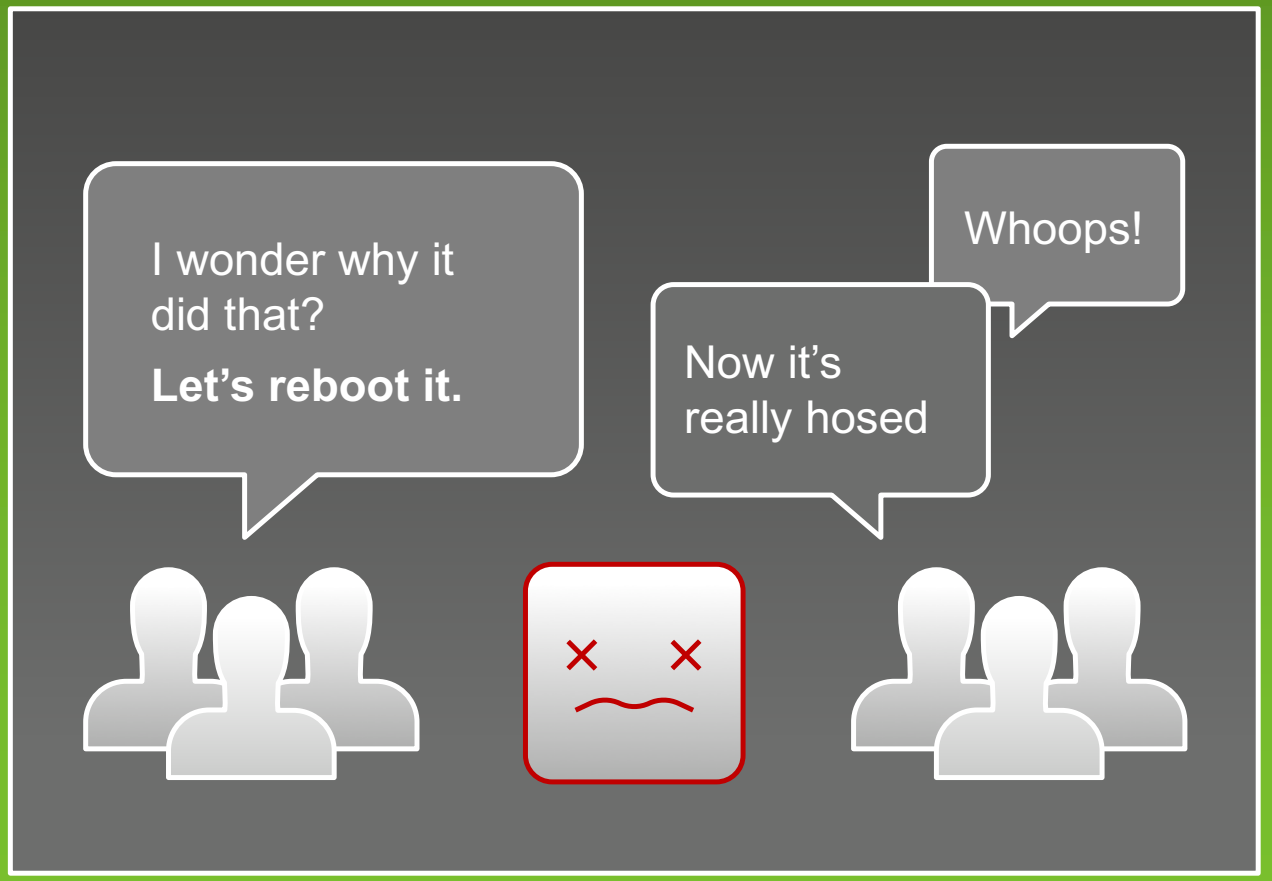



Application
Switching
Infrastructure



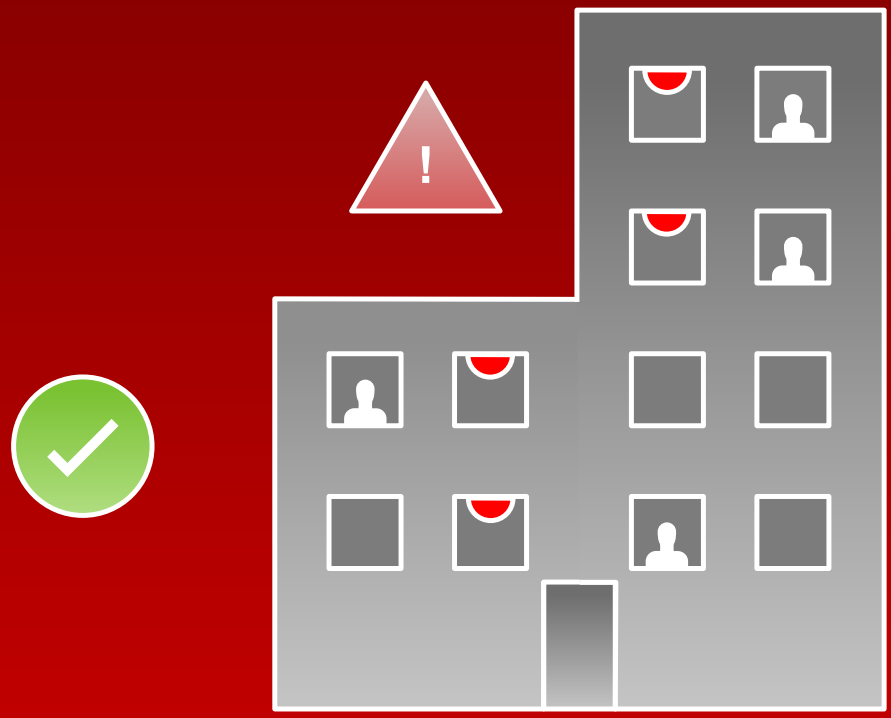
People

Unexpected application behavior often causes people to intervene and make the situation worse



People Training

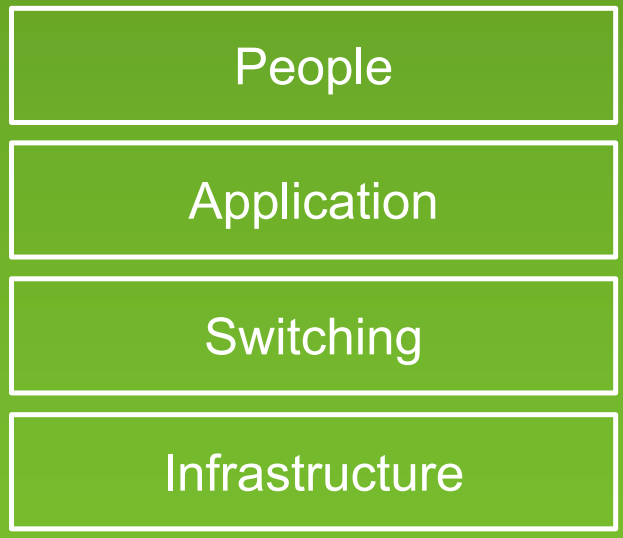
A fire drill is a boring routine where we make everyone take the stairs and assemble in the parking lot



People Training

Fire drills save lives in the event of a real fire, because people are trained how to react

Who runs the "fire drill" for I.T.?



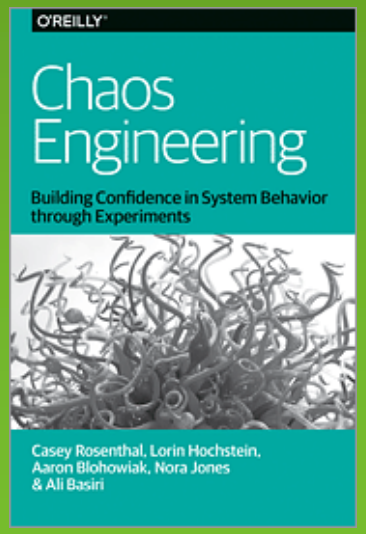
Chaos Engineering Team

People

Application

Switching

Infrastructure



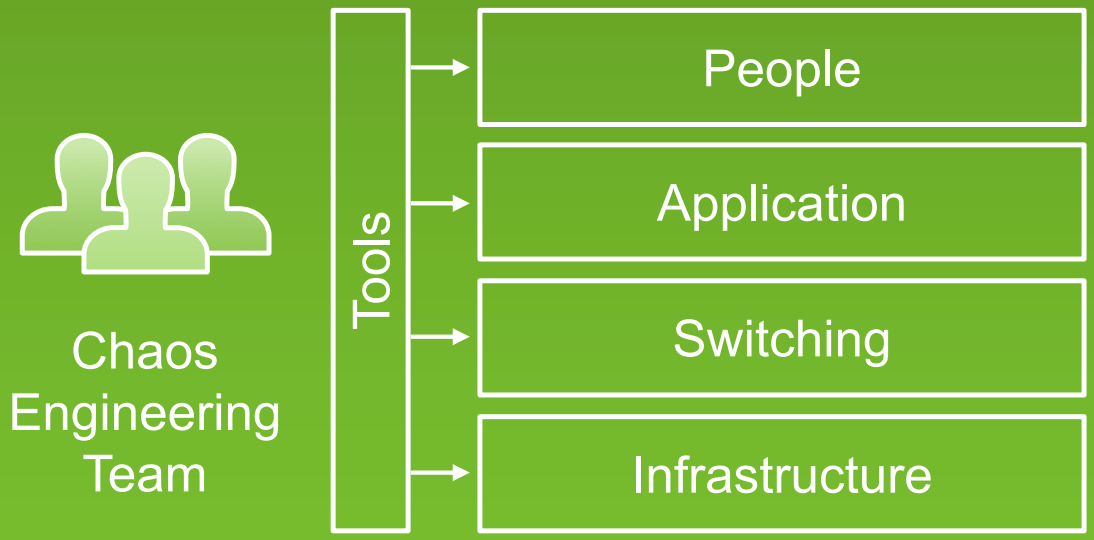
Chaos Engineering Team

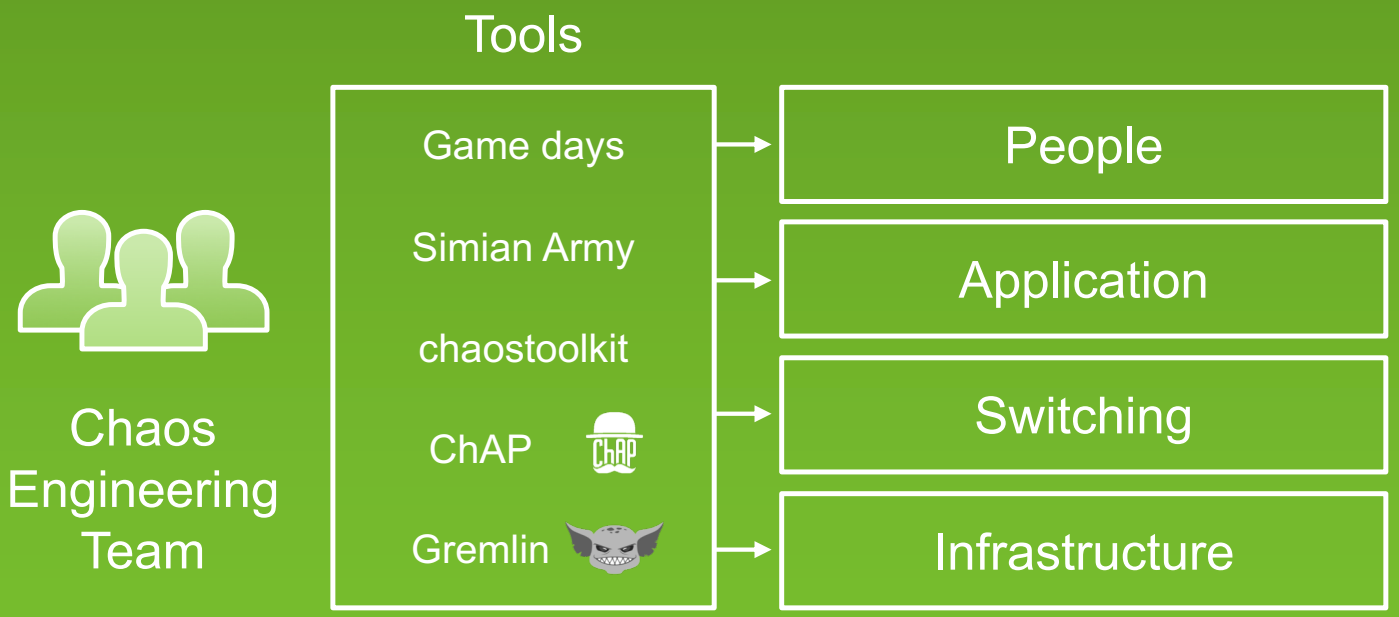
People

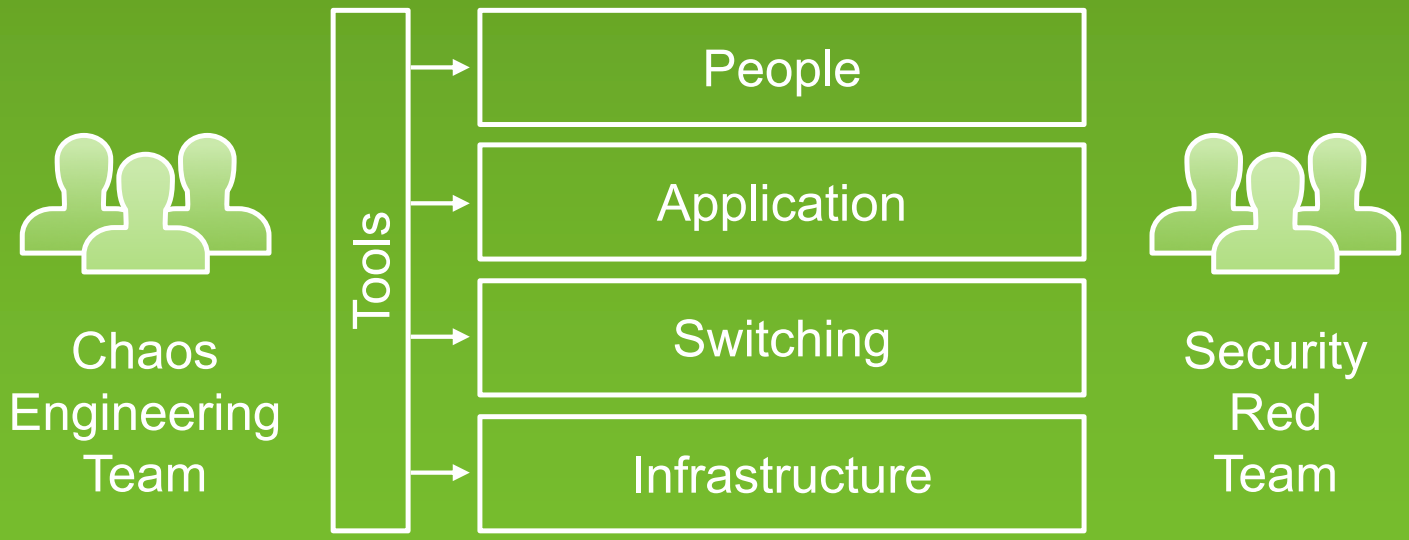
Application

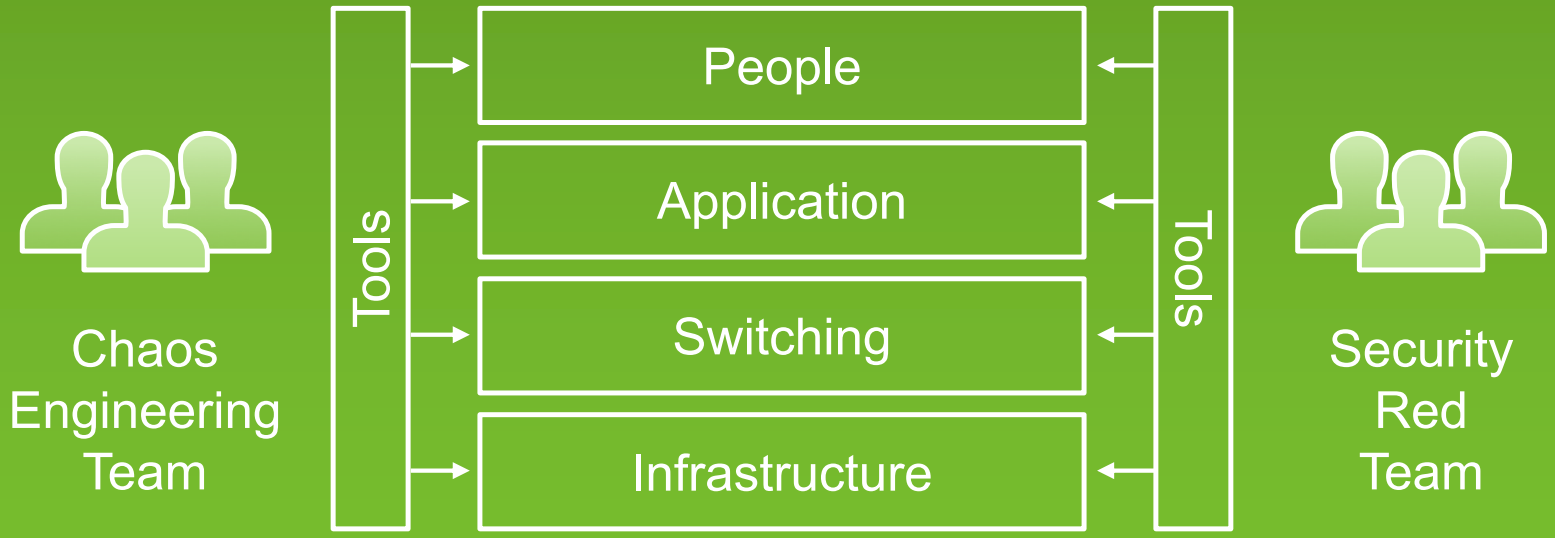
Switching

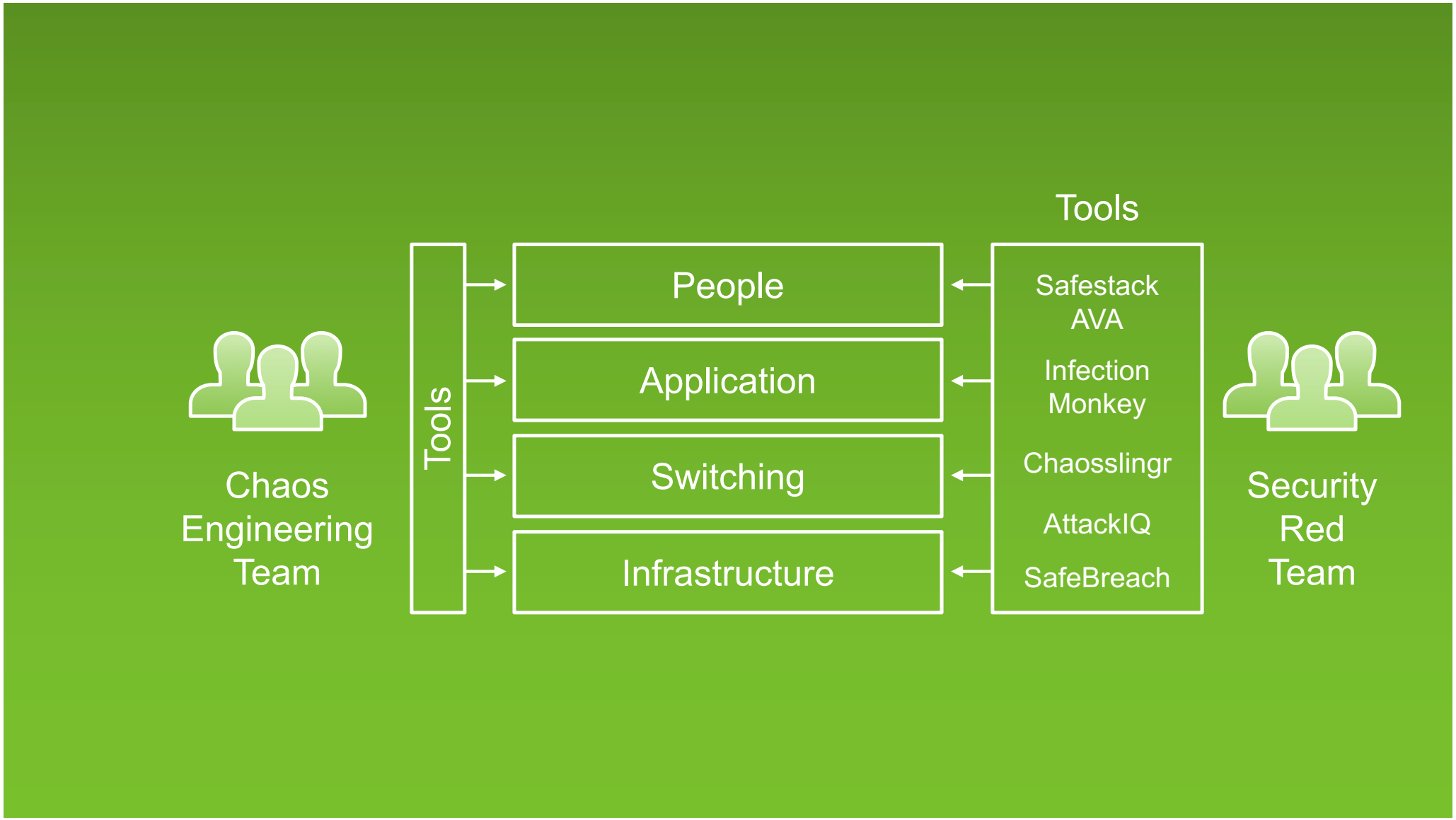
Infrastructure


Chaos
Engineering
Team
Tools
People
Application
Switching
Infrastructure


Tools
Chaos Engineering Team
Game days
Simian Army
chaostoolkit
ChAP
Gremlin
People
Application
Switching
Infrastructure


Chaos
Engineering
Team
Tools
People
Application
Switching
Infrastructure
Security
Red
Team


Chaos
Engineering
Team
Tools
People
Application
Switching
Infrastructure
Tools
Security
Red
Team


Tools
Chaos Engineering Team
Tools
People
Application
Switching
Infrastructure
Safestack AVA
Infection Monkey
Chaosslingr
AttackIQ
SafeBreach
Security Red Team

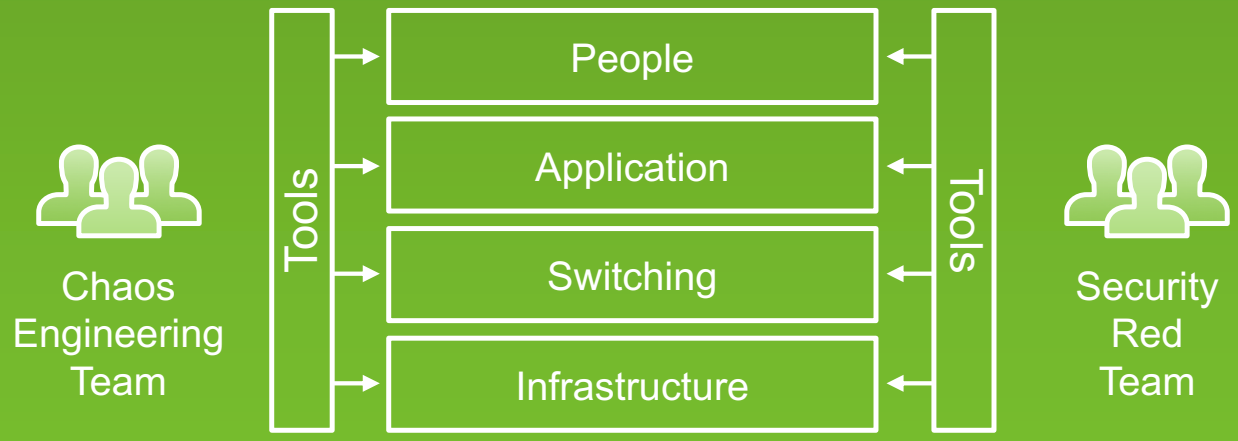
Chaos Architecture

Four layers

Two teams

An attitude—

Break it to make it better

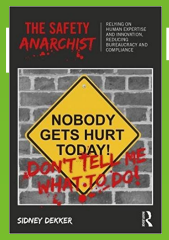


Break it to make it safer

For more on the “New View” of Safety see:
Todd Conklin’s Pre-accident podcast
John Allspaw’s stella.report

Synoptic Illegibility

You can’t write down exactly what **really** happens, so you can’t write a synopsis or run-book. System safety is an emergent
rty



The Safety Anarchist
Sydney Decker

Failures are a system problem—lack of safety margin

Not something with a root cause of component or human error


Blindfolded on a cliff edge,
what would you do?

Hypothesis testing

- We think we have safety margin in this dimension, let's carefully test to be sure
- In production
- Without causing an issue

Chaos testing ensures that you have:

Experienced Staff

Robust Applications

Dependable Switching Fabric

Redundant Service Foundation

Cloud Native Chaos in Practice

Mechanisms for AWS and Kubernetes

AWS Mechanisms

Amazon Aurora DB Cluster Fault Injection Queries

Crash master or replica
Fail a replica
Disk failure or congestion

ALTER SYSTEM SIMULATE *percentage_of_failure* PERCENT READ REPLICA FAILURE [TO ALL | TO "replica name"] FOR INTERVAL *quantity* { YEAR | QUARTER | MONTH | WEEK | DAY | HOUR | MINUTE | SECOND };

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/AuroraMySQL.Managing.FaultInjectionQueries.html

AWS Mechanisms

IAM Region Restriction

Simulate regional API issues by changing the list of permitted regions

```
{ "Sid": "RegionRestricted", "Effect": "Allow", "Action": “*”, "Resource": "*", "Condition":
        {"StringEquals": {"aws:RequestedRegion": [ "eu-west-1"]}}
}
```

https://aws.amazon.com/blogs/security/easier-way-to-control-access-to-aws-regions-using-iam-policies/

Kubernetes Mechanisms

Gremlin Attacks

Gremlin runs a daemon on each node that manages and induces failures and network blocking

https://www.gremlin.com/community/tutorials/how-to-install-and-use-gremlin-with-kubernetes/

Kubernetes Mechanisms

Open Source Chaos Toolkit

Chaos Toolkit defines experiments, executes them and generates reports – chaostoolkit.org

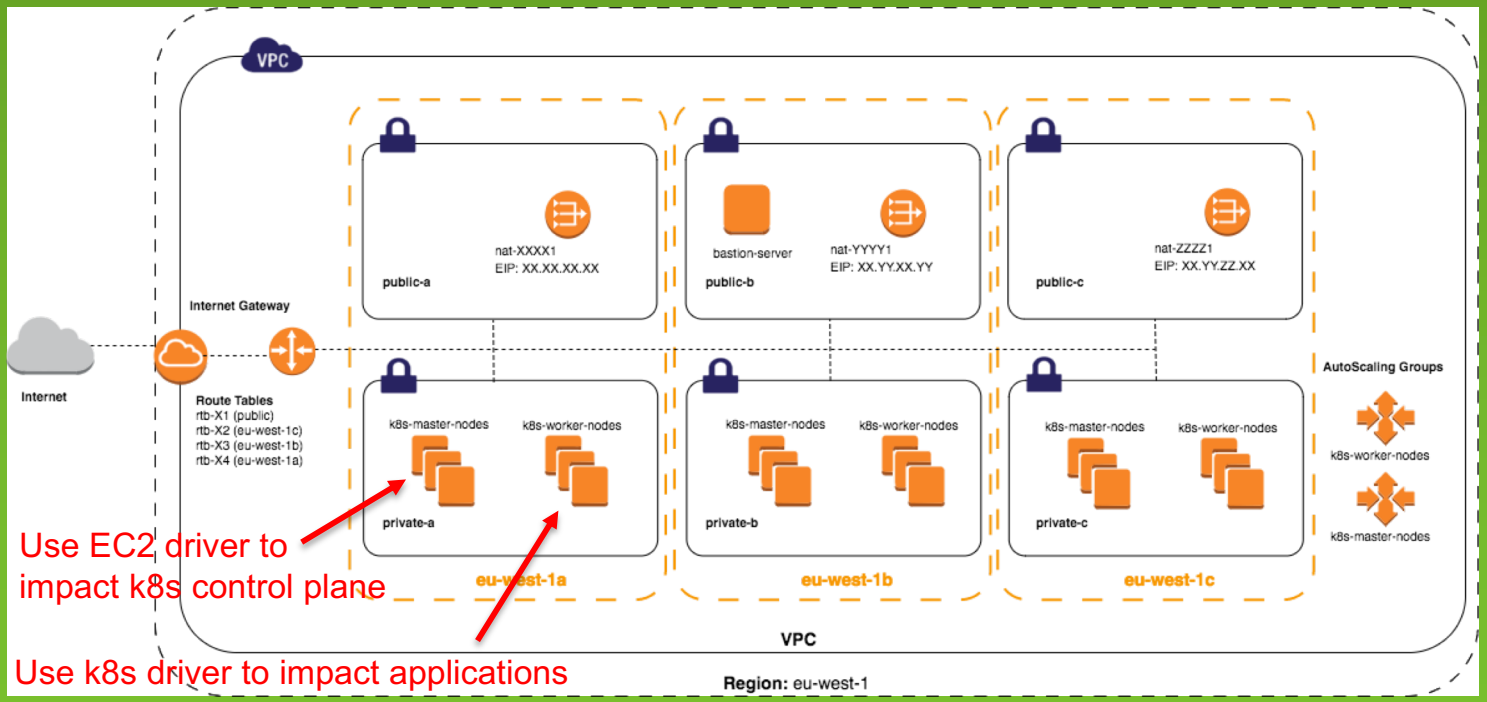
Drivers for Gremlin, EC2 and Kubernetes etc.

Included in Kubernetes on AWS Workshop

https://medium.com/chaos-toolkit/make-applications-more-resilient-on-kubernetes-by-adding-chaos-engineering-70a4c282609f

CNCF Chaos Working Group

Open Source Chaos Toolkit



Introduction https://medium.com/chaosiq/a-pinch-of-chaos-engineering-at-kubecon-604614b73871
Image from https://kubecloud.io/ha-kubernetes-cluster-on-aws-kops-makes-it-easy-2337806d0311

Expensive and custom disaster recovery is being replaced by low cost, portable, automated chaos engineering.

Chaos Architecture

A Cloud Native Availability Model

Adrian Cockcroft

@adrianco

AWS VP Cloud Architecture Strategy