Multi-account AWS Architecture with Terraform

… our journey.

Zachary Wilson
Partner / Engineer
SwitchCase Group
zach@switchcasegroup.com

Starting with context

- About Me
  - Meetup attendee
    - and Presenter!!!
  - Engineer
  - Partner
- About SwitchCase Group

SwitchCase Group Companies

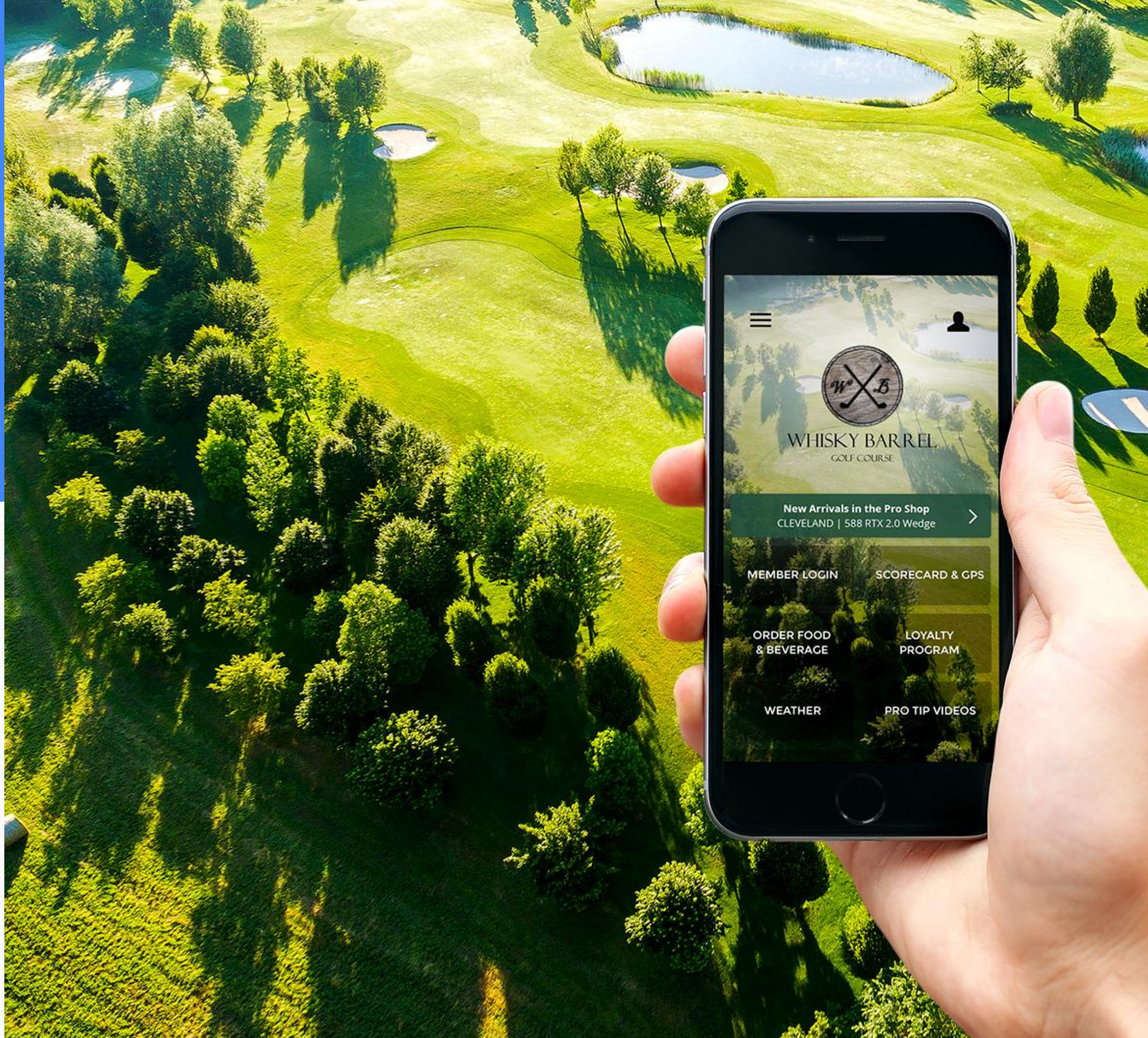
Gallus Golf

InstantEncore

Interactive Fitness

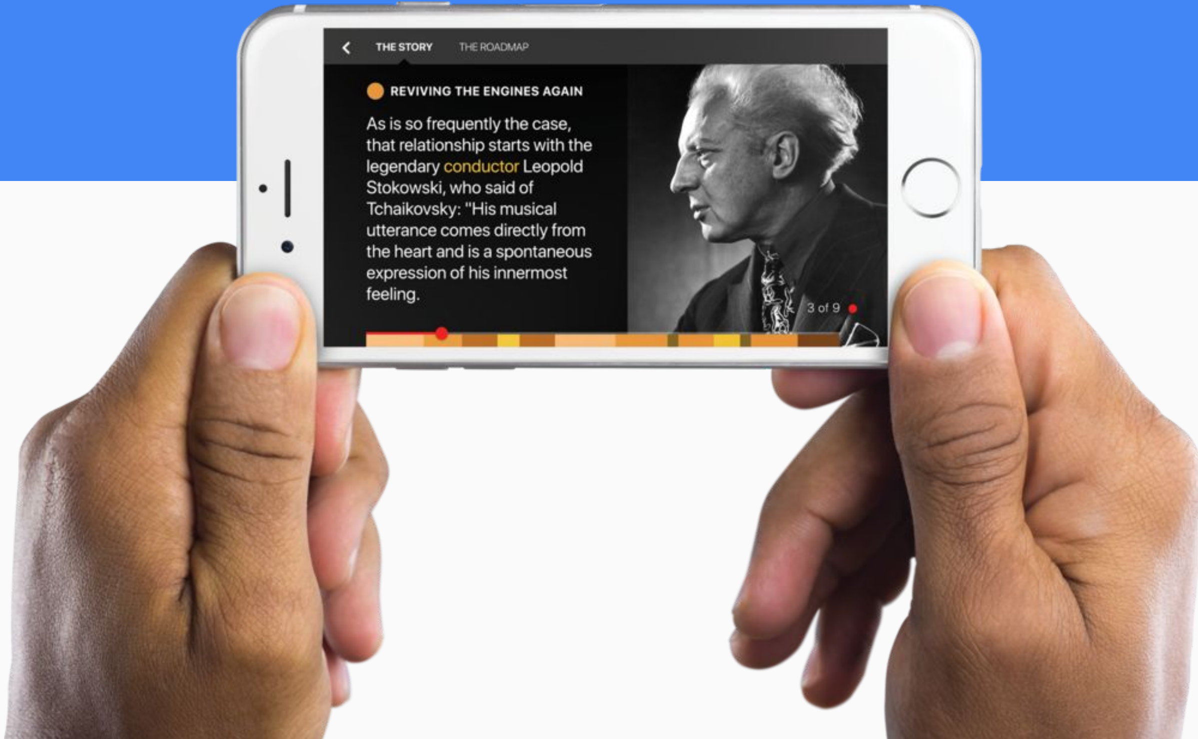
Gallus Golf

Provides branded mobile apps and social software for over 700 golf courses worldwide. Our products enhance the golf experience in order to attract new customers and book more rounds with existing customers.



InstantEncore

Powers mobile apps for over 200 arts organizations worldwide. Enhances the performance experience and promotes ongoing attendance by using mobile technology to engage with the audience.

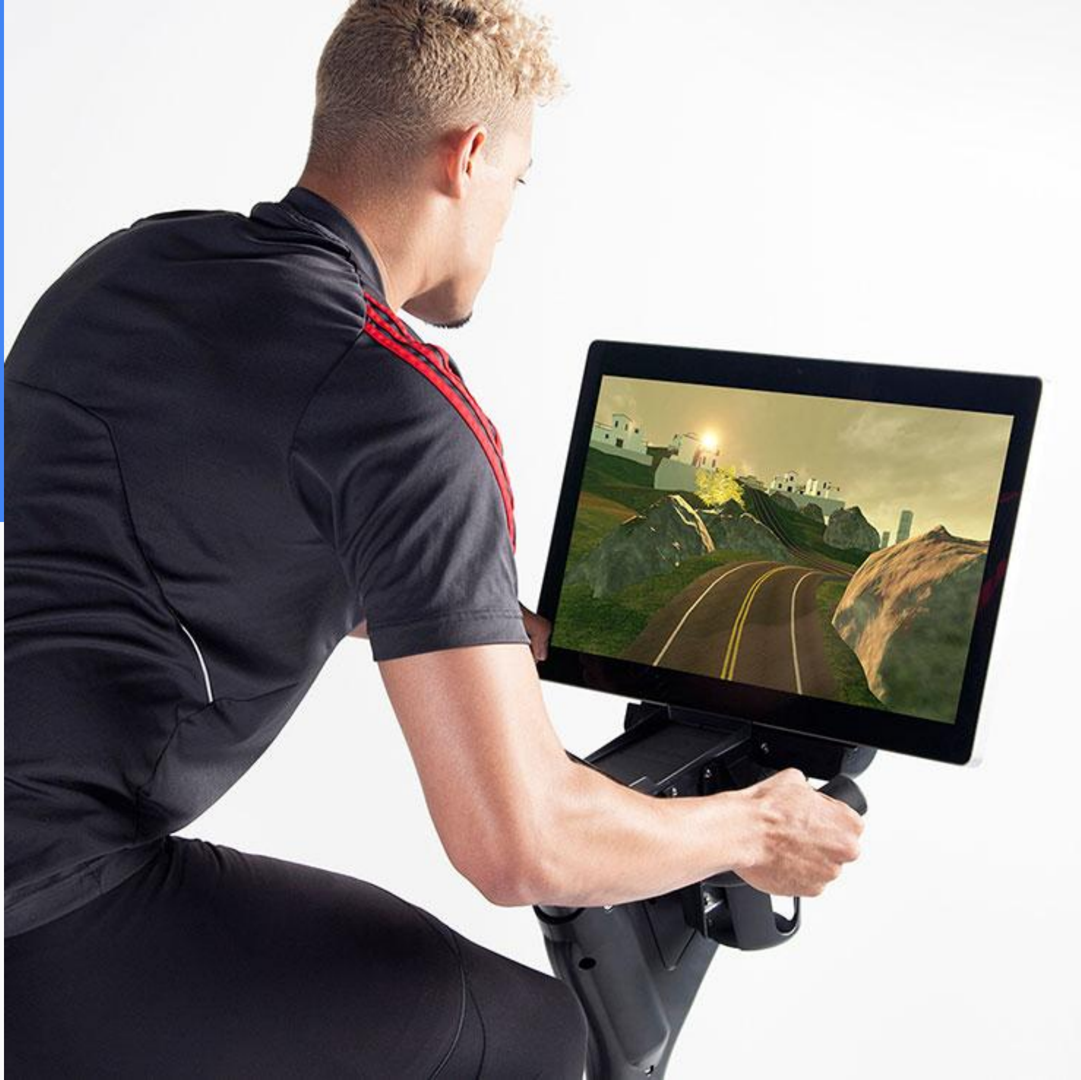


REVIVING THE ENGINES AGAIN

As is so frequently the case, that relationship starts with the legendary conductor Leopold Stokowski, who said of Tchaikovsky: "His musical utterance comes directly from the heart and is a spontaneous expression of his innermost feeling.

Interactive Fitness

It’s not just about bikes – it’s about helping you build your business. The Expresso product line has revolutionized the indoor exercise industry by blending eye popping virtual reality with a classic cardio workout.



SwitchCase Group Companies

Gallus Golf

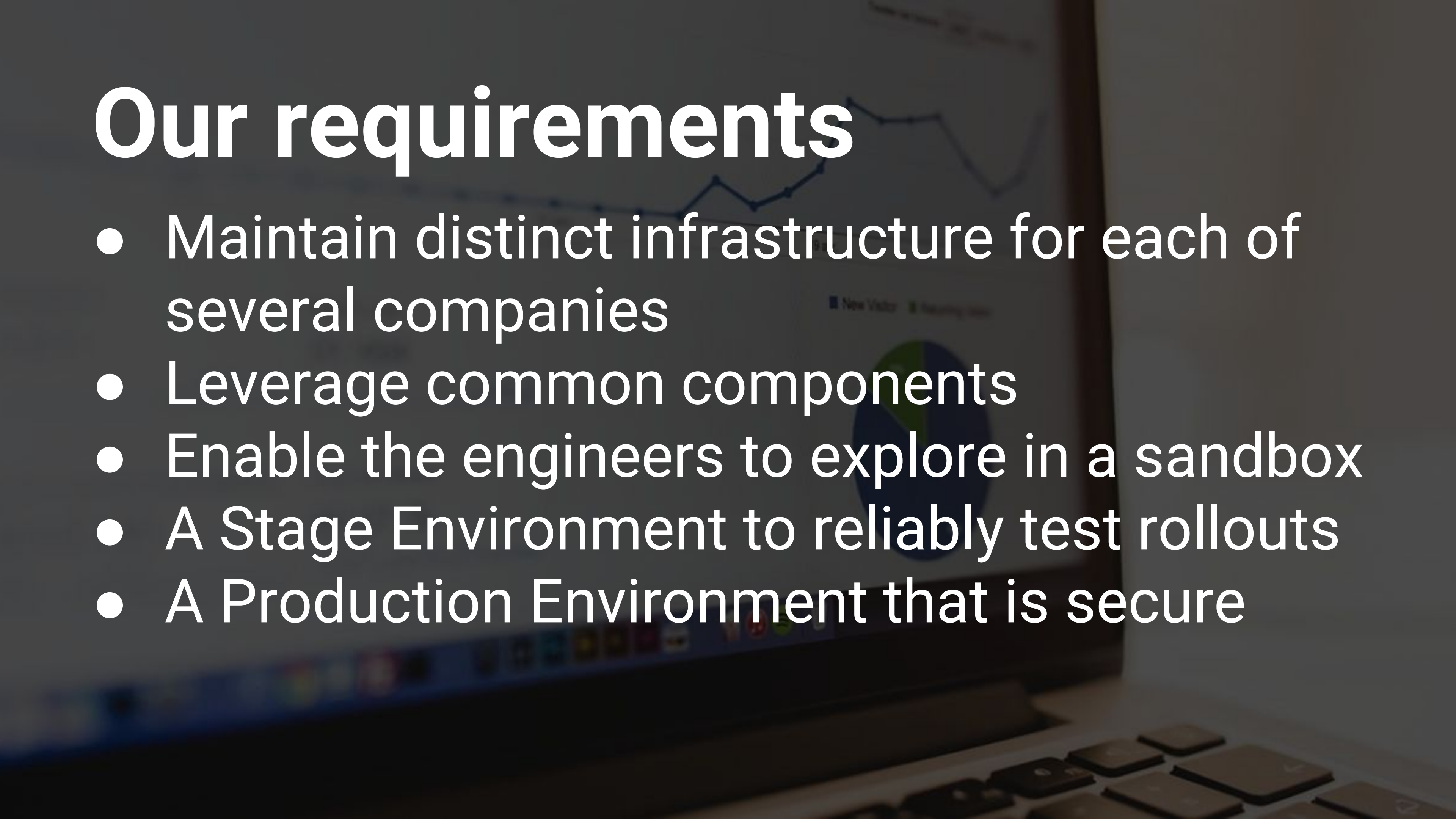
InstantEncore

Interactive Fitness

All technology businesses,
each with its own infrastructure needs.

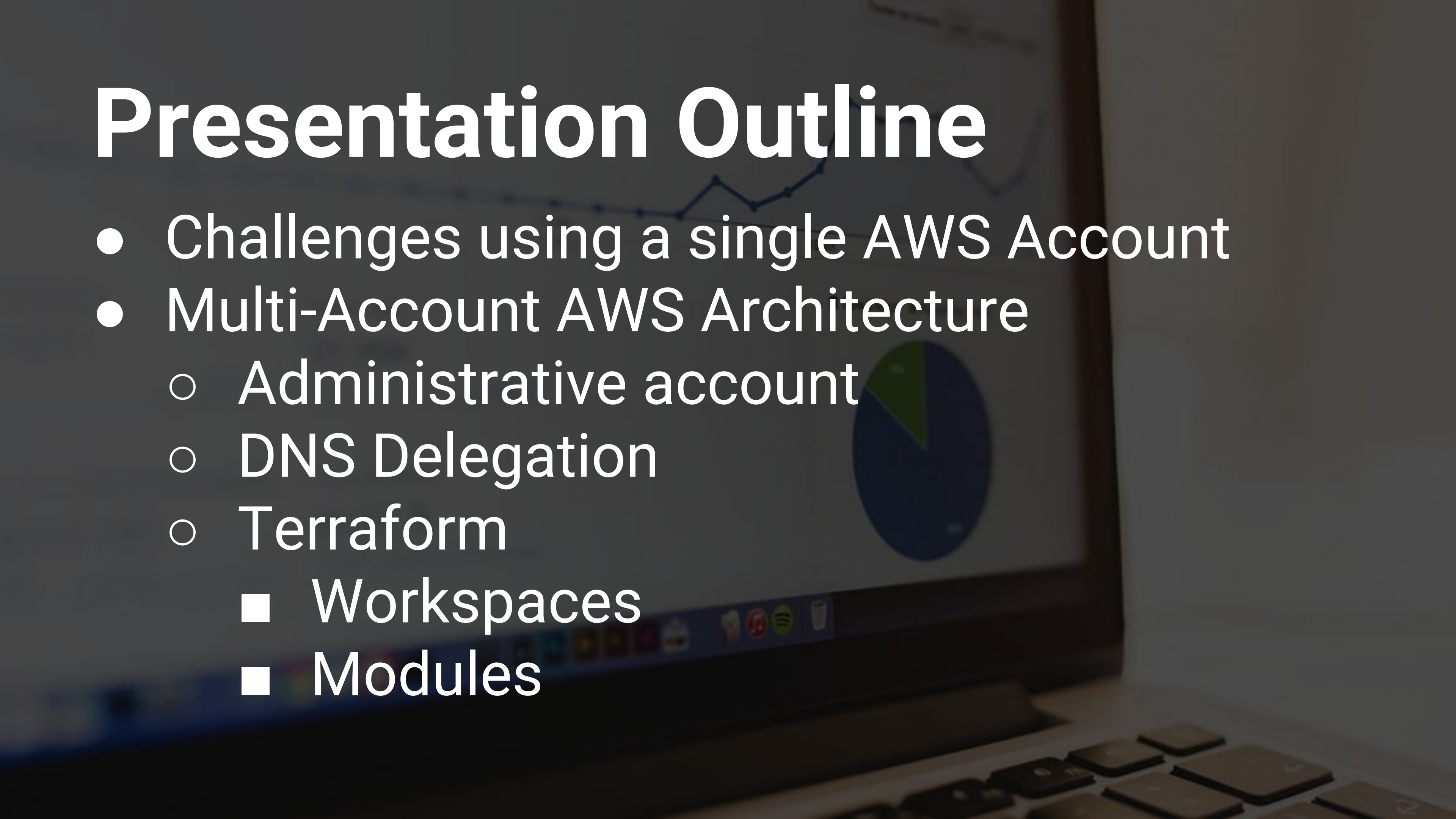
Shared Engineering Team

Each company has access to SwitchCase’s Engineering team. This model brings efficiencies, and helps companies grow quickly without the investment in their own fully staffed engineering team.



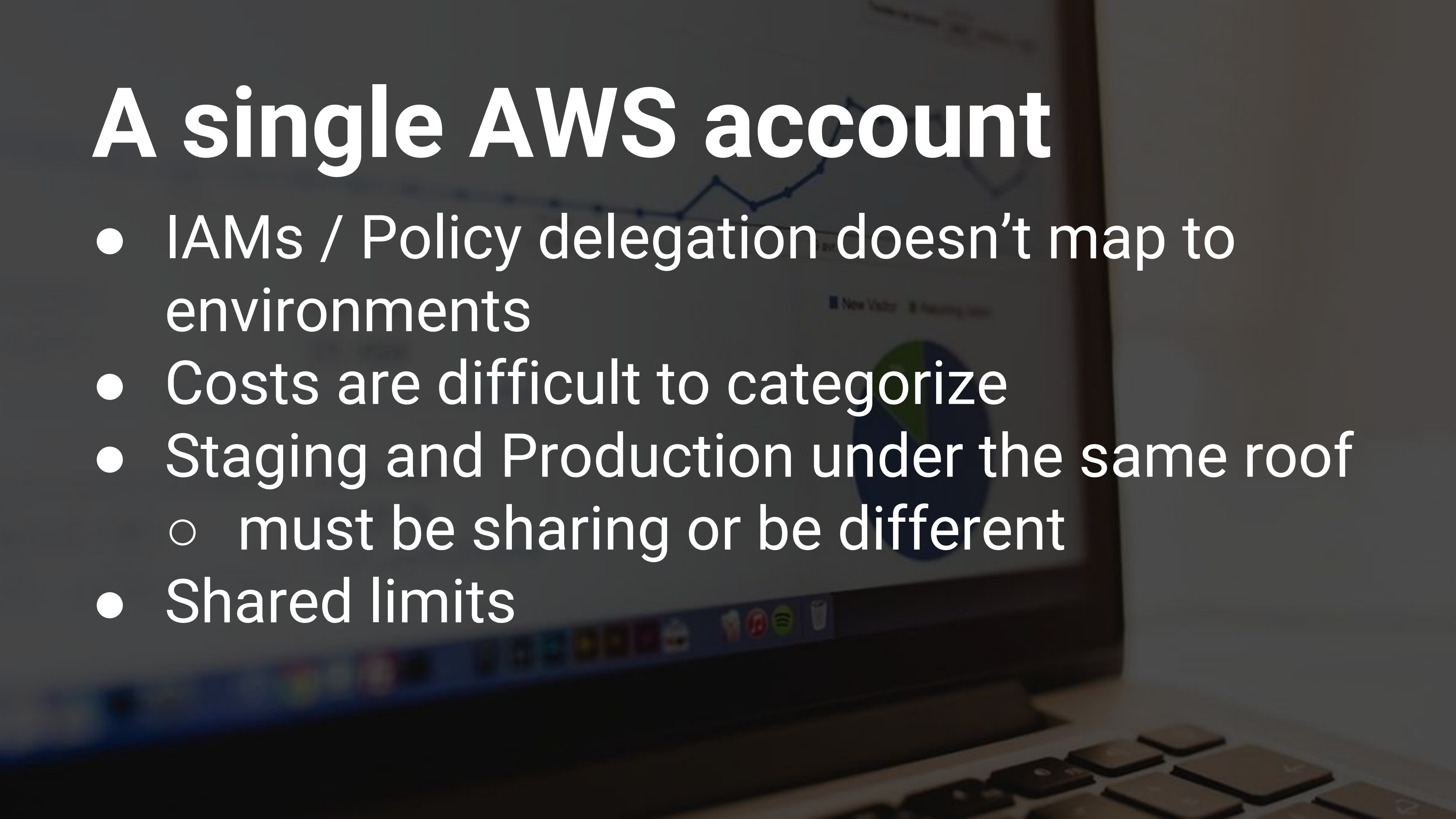
Our requirements

- Maintain distinct infrastructure for each of several companies
- Leverage common components
- Enable the engineers to explore in a sandbox
- A Stage Environment to reliably test rollouts
- A Production Environment that is secure



Presentation Outline

- Challenges using a single AWS Account
- Multi-Account AWS Architecture
  - Administrative account
  - DNS Delegation
  - Terraform
    - Workspaces
    - Modules



A single AWS account

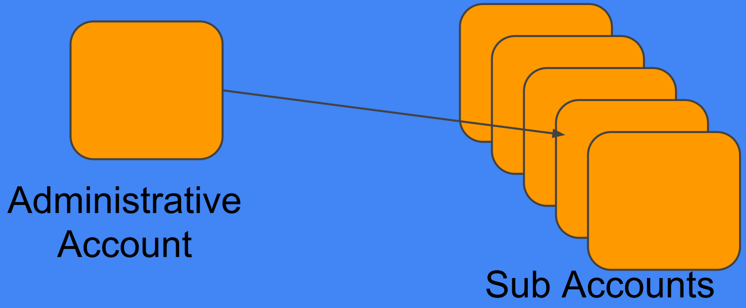
- IAMs / Policy delegation doesn’t map to environments
- Costs are difficult to categorize
- Staging and Production under the same roof
  - must be sharing or be different
- Shared limits

Multi-Account AWS Architecture

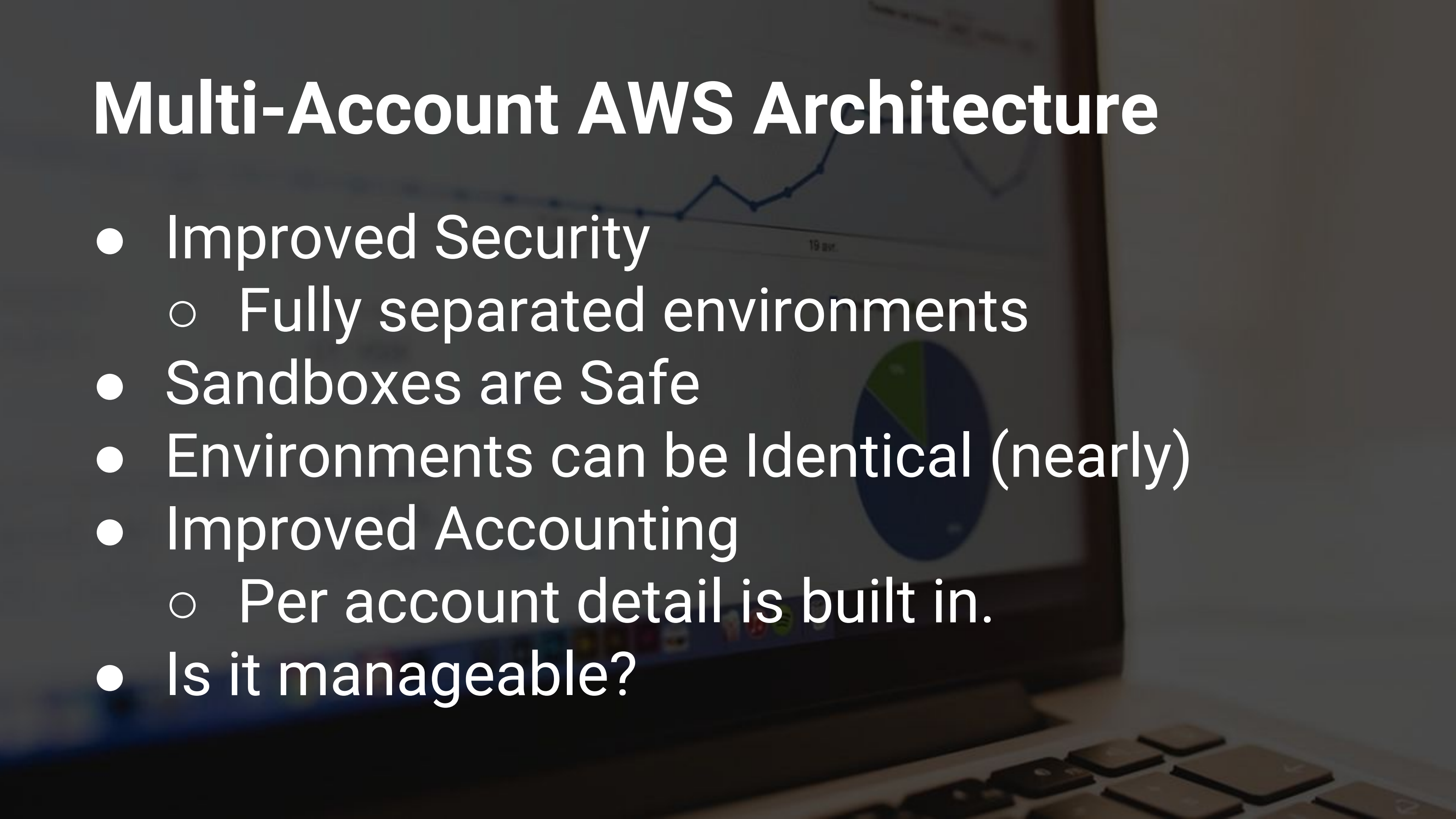
Using a number of separate AWS accounts to isolate different teams and environments.

Multi-Account AWS Architecture

Using a number of separate AWS accounts to isolate different teams and environments.



Multi-Account AWS Architecture

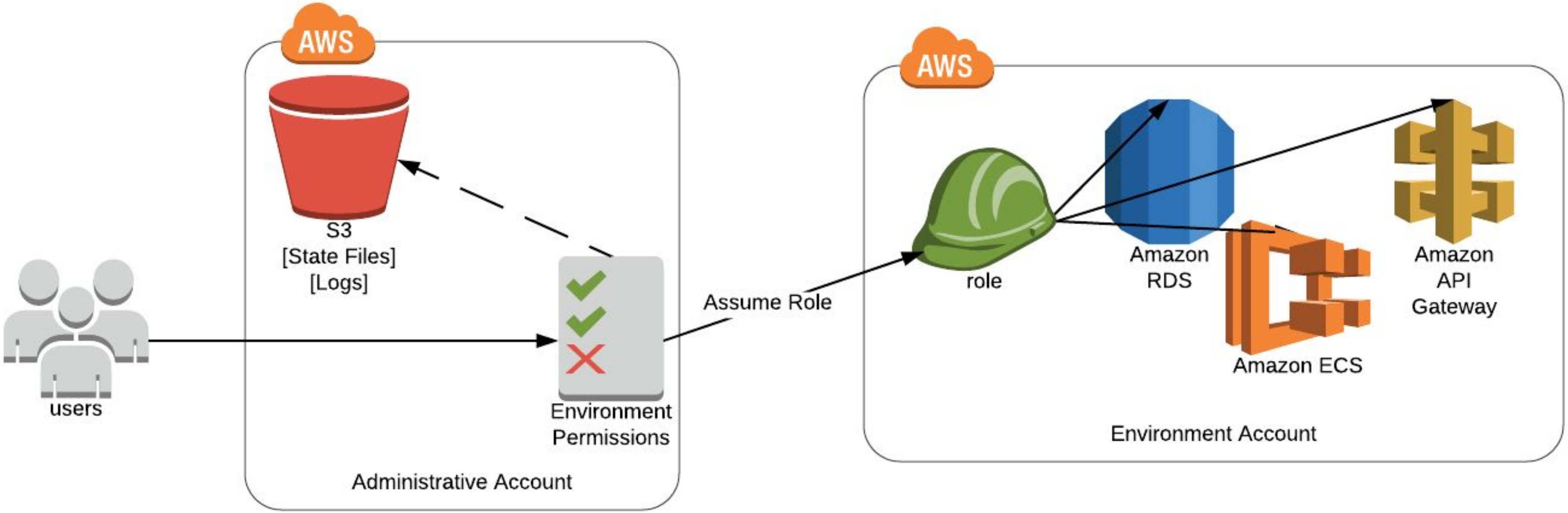


- Improved Security
  - Fully separated environments
- Sandboxes are Safe
- Environments can be Identical (nearly)
- Improved Accounting
  - Per account detail is built in.
- Is it manageable?

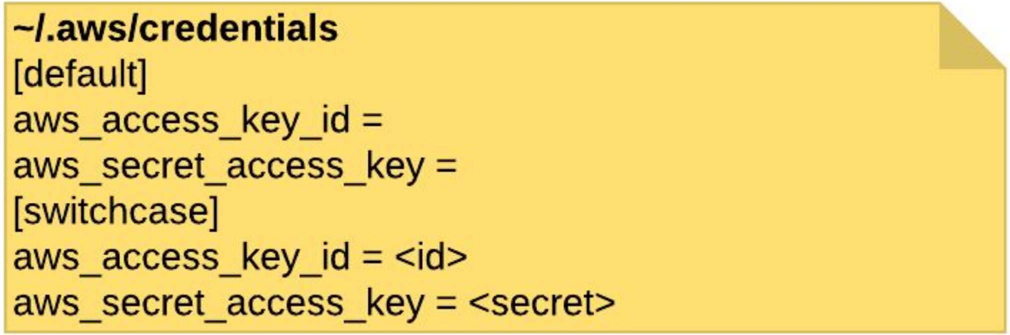
Multi-Account AWS Architecture

- AWS Organizations
  - Create groups of AWS accounts
  - Aggregates the billing up to one account
- IAMs
  - Create Users
  - Create Policies
    - Delegate Access to member accounts
    - Assume Role

Assume Role

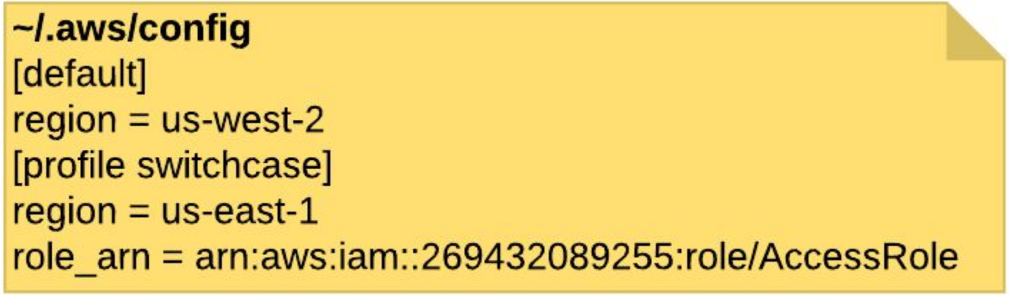

AWS
S3
[State Files]
[Logs]
users
Environment Permissions
Administrative Account
Assume Role
AWS
role
Amazon RDS
Amazon API Gateway
Amazon ECS
Environment Account

Assume Role: Developer



~/.aws/credentials

```
[default]
aws_access_key_id =
aws_secret_access_key =
[switchcase]
aws_access_key_id = <id>
aws_secret_access_key = <secret>
```



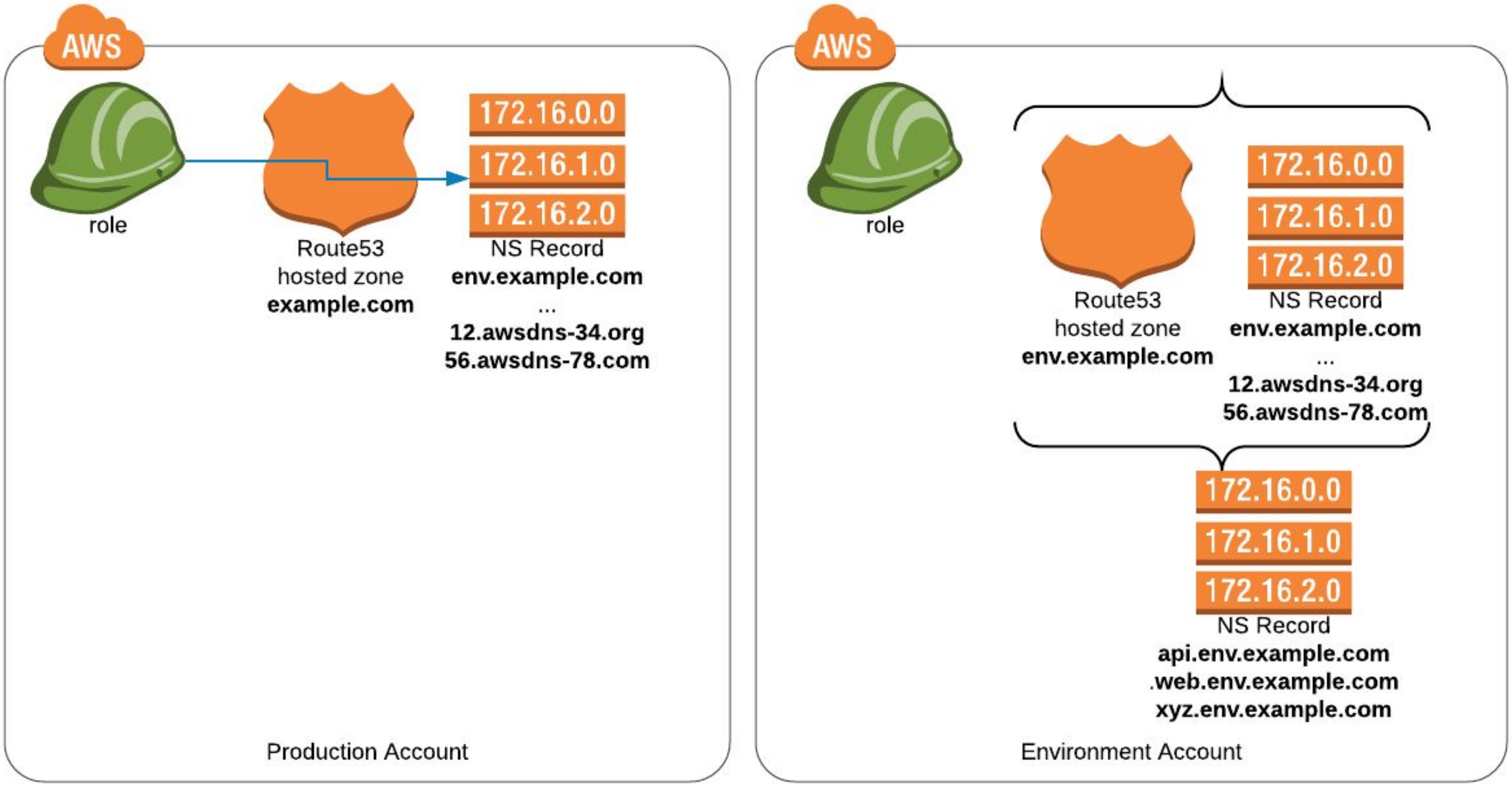
~/.aws/config

```
[default]
region = us-west-2
[profile switchcase]
region = us-east-1
role_arn = arn:aws:iam::269432089255:role/AccessRole
```

Multi-Account AWS Architecture

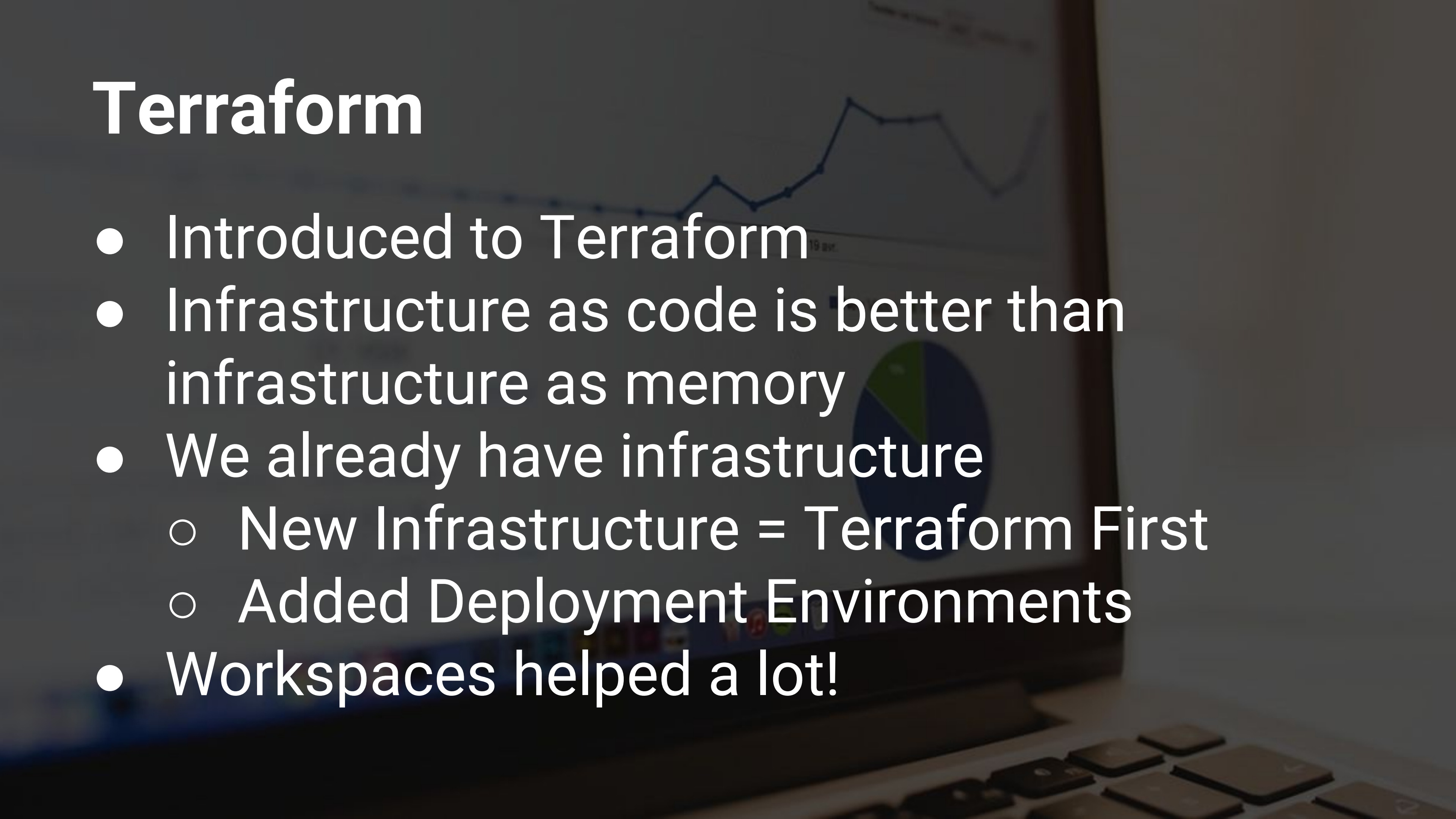
- Our Implementation (not our invention)
  - Terraform Docs
- Administrative Account
  - IAM Users
  - S3 Buckets
  - *Master Account
    - Member Accounts

Blue: Account Bootstrap Terraform



Terraform

Write, Plan, and Create Infrastructure as Code

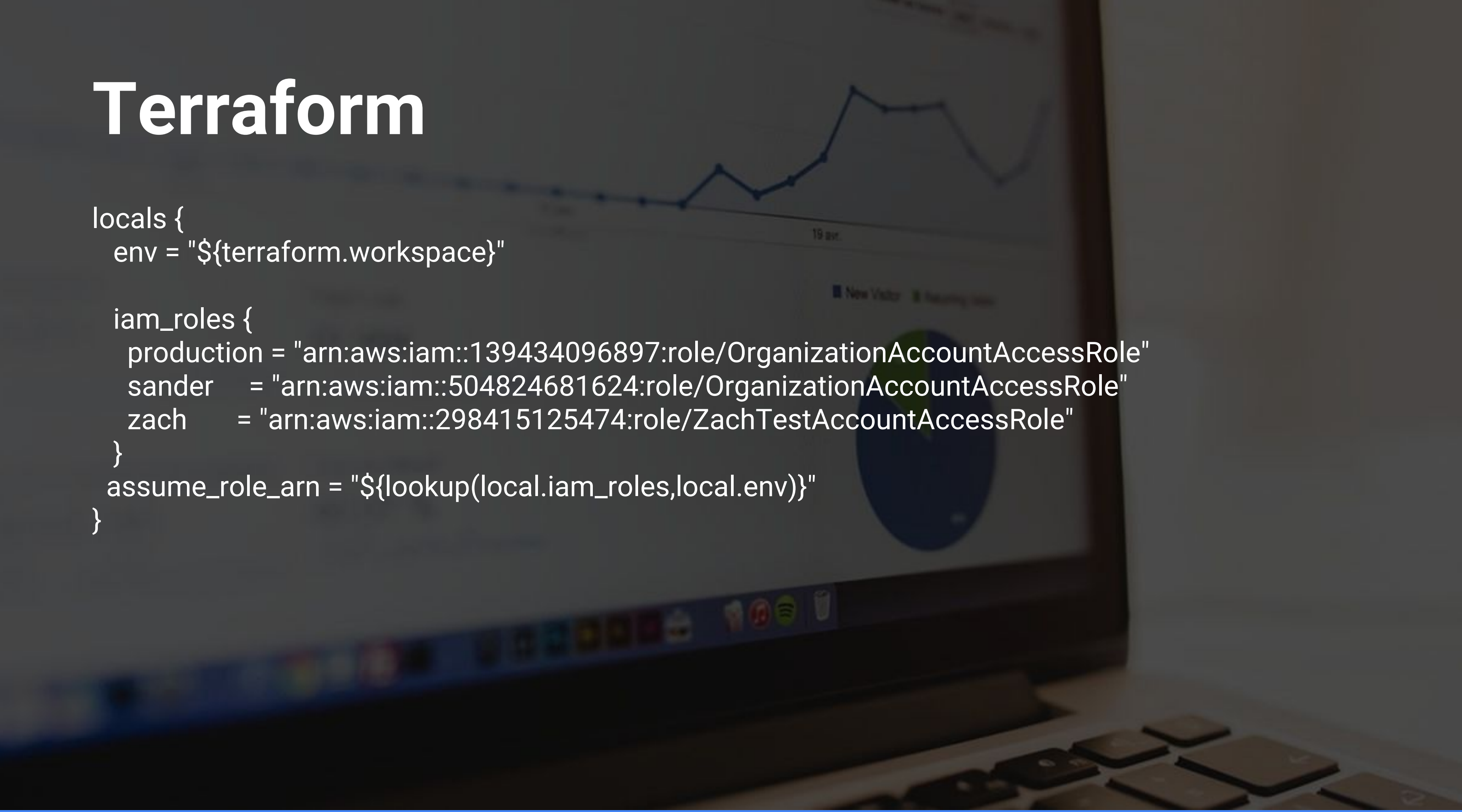


Terraform

- Introduced to Terraform
- Infrastructure as code is better than infrastructure as memory
- We already have infrastructure
  - New Infrastructure = Terraform First
  - Added Deployment Environments
- Workspaces helped a lot!

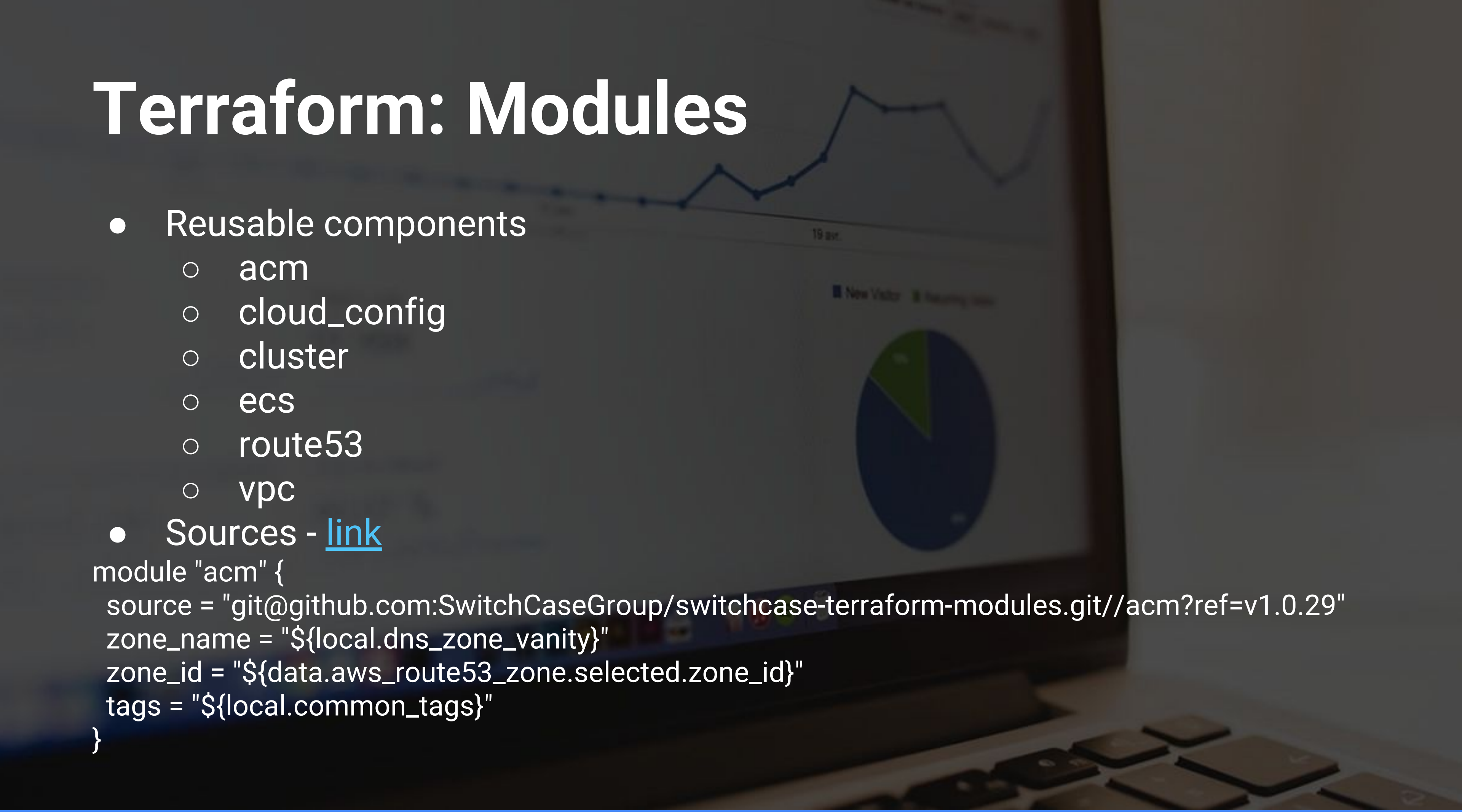
Terraform

- Workspaces
  - terraform workspace select zach
  - Terraform Workspace == AWS Account
    - workspace zach = zach’s AWS sandbox
    - workspace stage = stage AWS account
    - workspace production = production AWS account
- Locals



Terraform

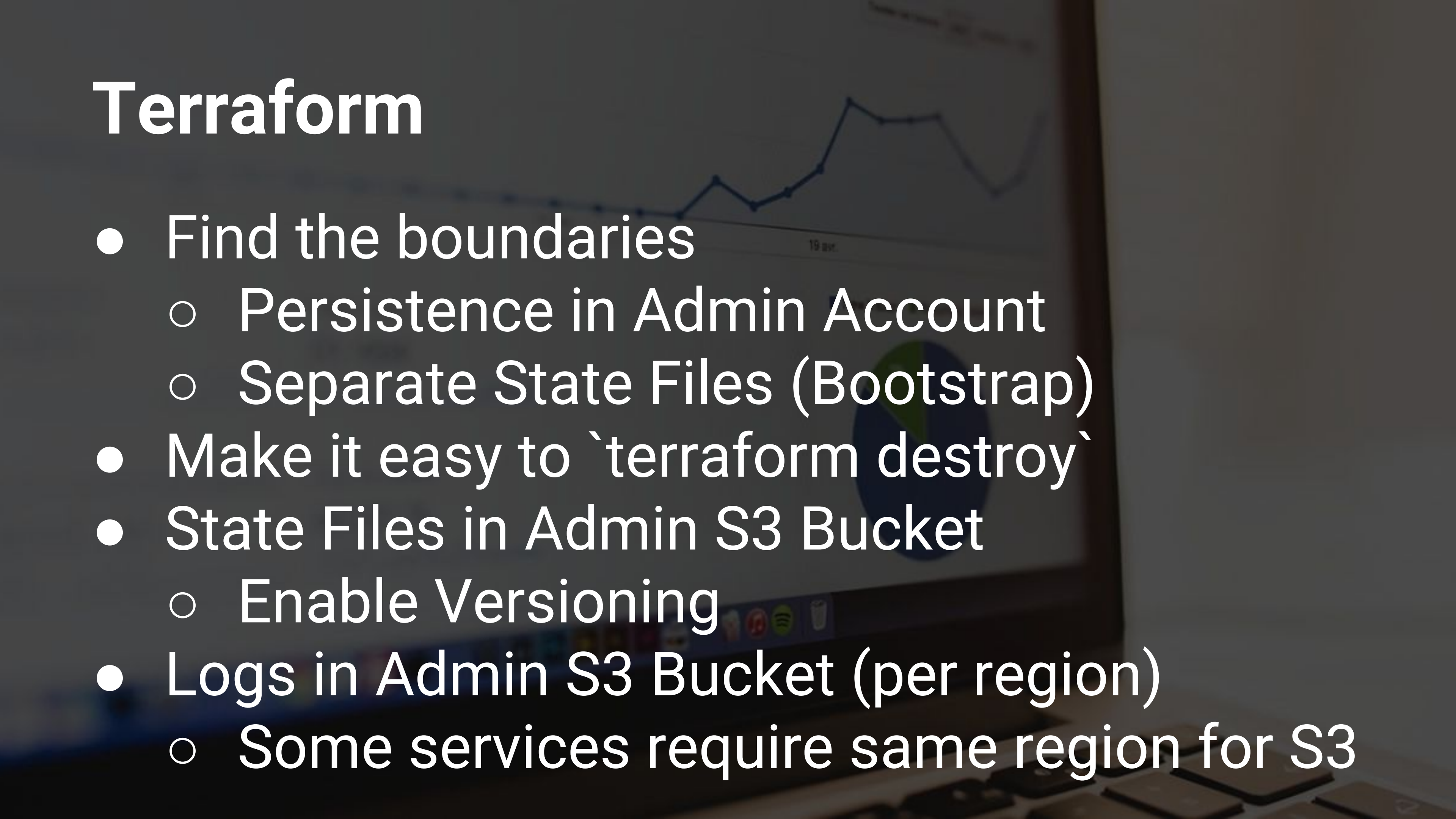
```
locals {
   env = "${terraform.workspace}"

   iam_roles {
     production = "arn:aws:iam::139434096897:role/OrganizationAccountAccessRole"
     sander     = "arn:aws:iam::504824681624:role/OrganizationAccountAccessRole"
     zach       = "arn:aws:iam::298415125474:role/ZachTestAccountAccessRole"
   }
  assume_role_arn = "${lookup(local.iam_roles,local.env)}"
}
```



Terraform: Modules

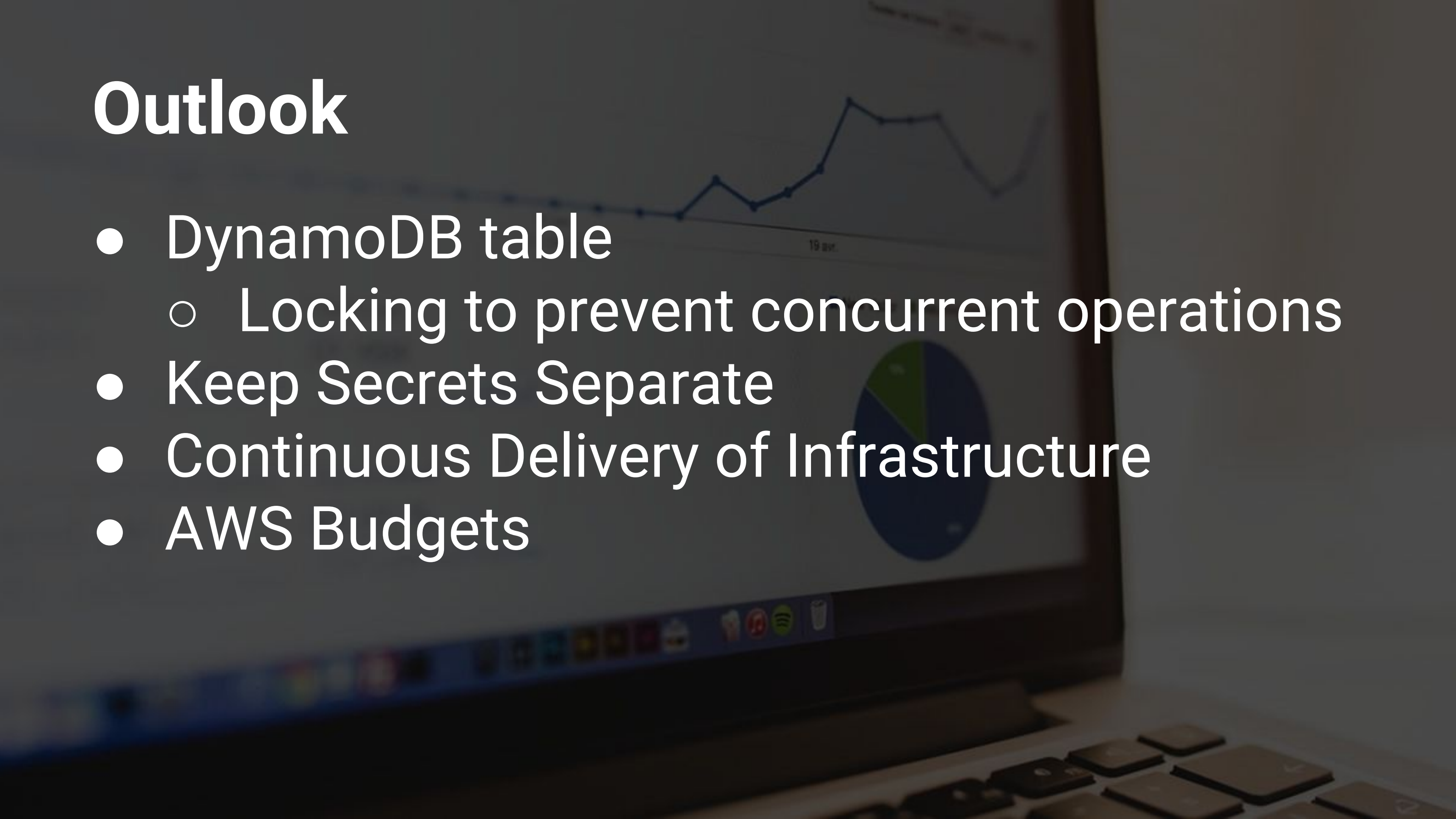
- Reusable components
  - acm
  - cloud_config
  - cluster
  - ecs
  - route53
  - vpc
- Sources - link

```
module "acm" {
  source = "git@github.com:SwitchCaseGroup/switchcase-terraform-modules.git//acm?ref=v1.0.29"
  zone_name = "${local.dns_zone_vanity}"
  zone_id = "${data.aws_route53_zone.selected.zone_id}"
  tags = "${local.common_tags}"
}
```



Terraform

- Find the boundaries
    - Persistence in Admin Account
    - Separate State Files (Bootstrap)
- Make it easy to `terraform destroy`
- State Files in Admin S3 Bucket
    - Enable Versioning
- Logs in Admin S3 Bucket (per region)
    - Some services require same region for S3



Outlook

- DynamoDB table
  - Locking to prevent concurrent operations
- Keep Secrets Separate
- Continuous Delivery of Infrastructure
- AWS Budgets

Questions & Discussion

Come work with us!

We are always looking for great engineers
We are always looking to start the next company

Zachary Wilson
Partner / Engineer
SwitchCase Group
zach@switchcasegroup.com