RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SP03-R09

The Future is Hybrid: Key Considerations for Cloud and DevOps

Lamar Bailey

Director, Security Research & Development
Tripwire
@btle310

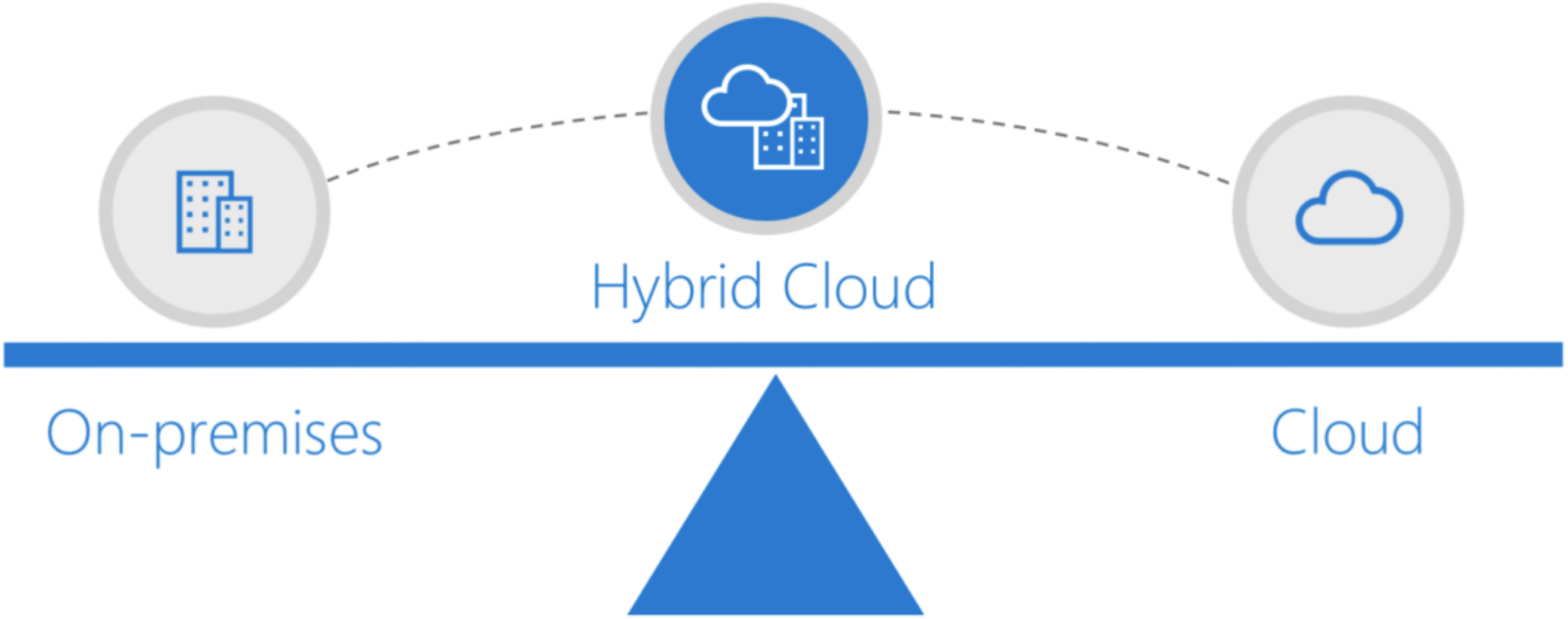
Agenda

- Shifting Landscape
- Cloud Asset Security
- Cloud Security Posture
- Case Study
- Q&A

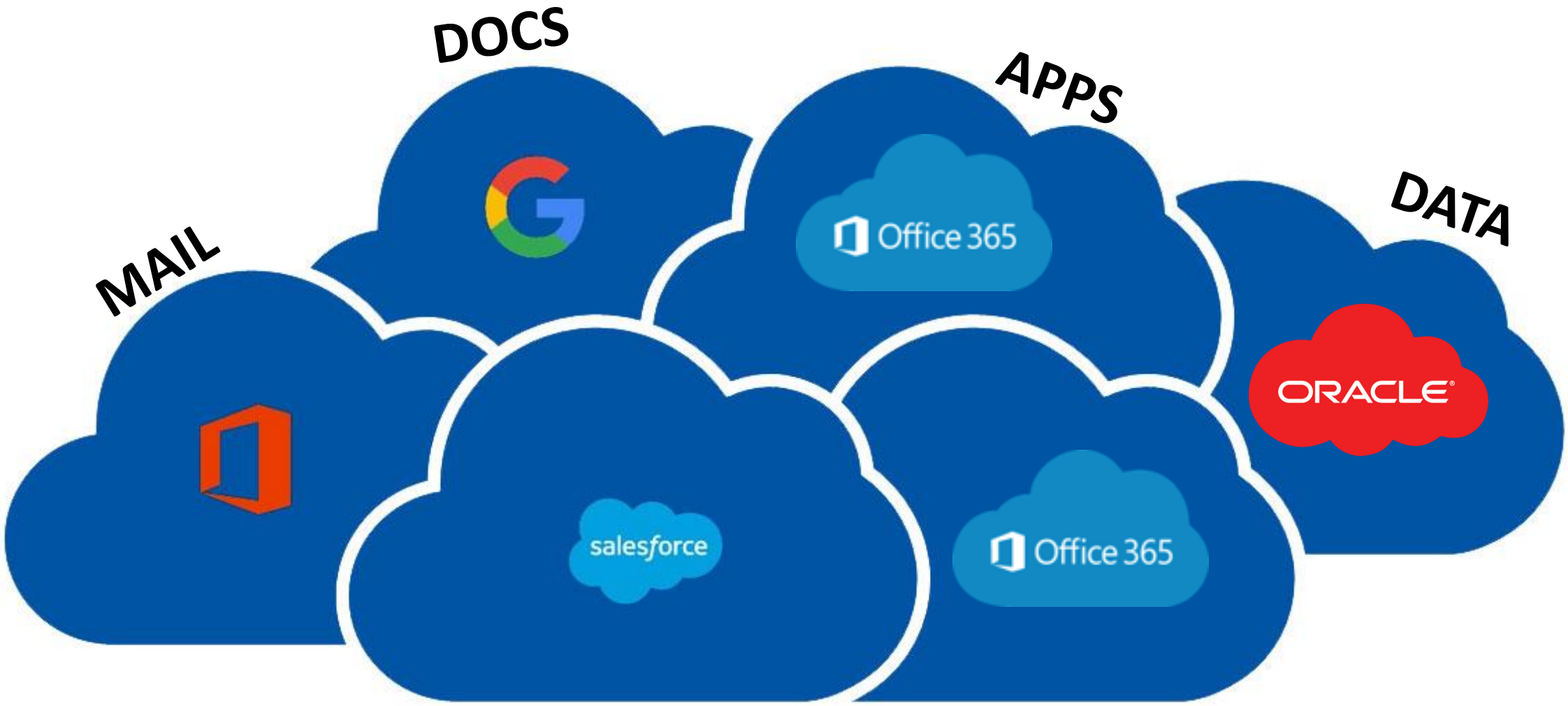
RSAConference2019

Shifting Landscape

Hybrid Landscape



Who Secures the Cloud?



Responsibility and Control

- App configuration
- Application
- Server configuration
- Operating system
- Antivirus
- Network

IaaS

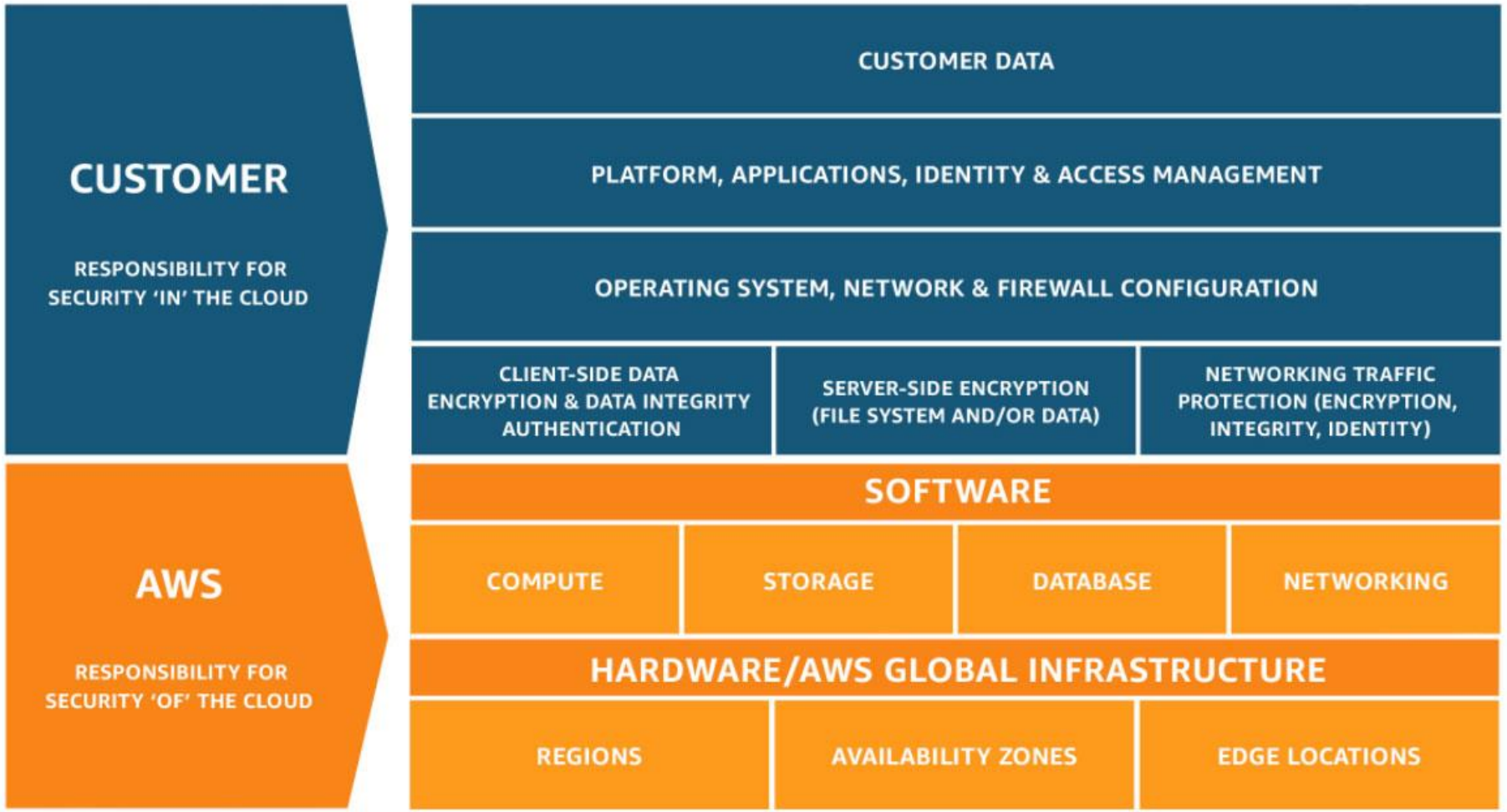
- App configuration
- Application
- Server configuration

PaaS

- App configuration

SaaS

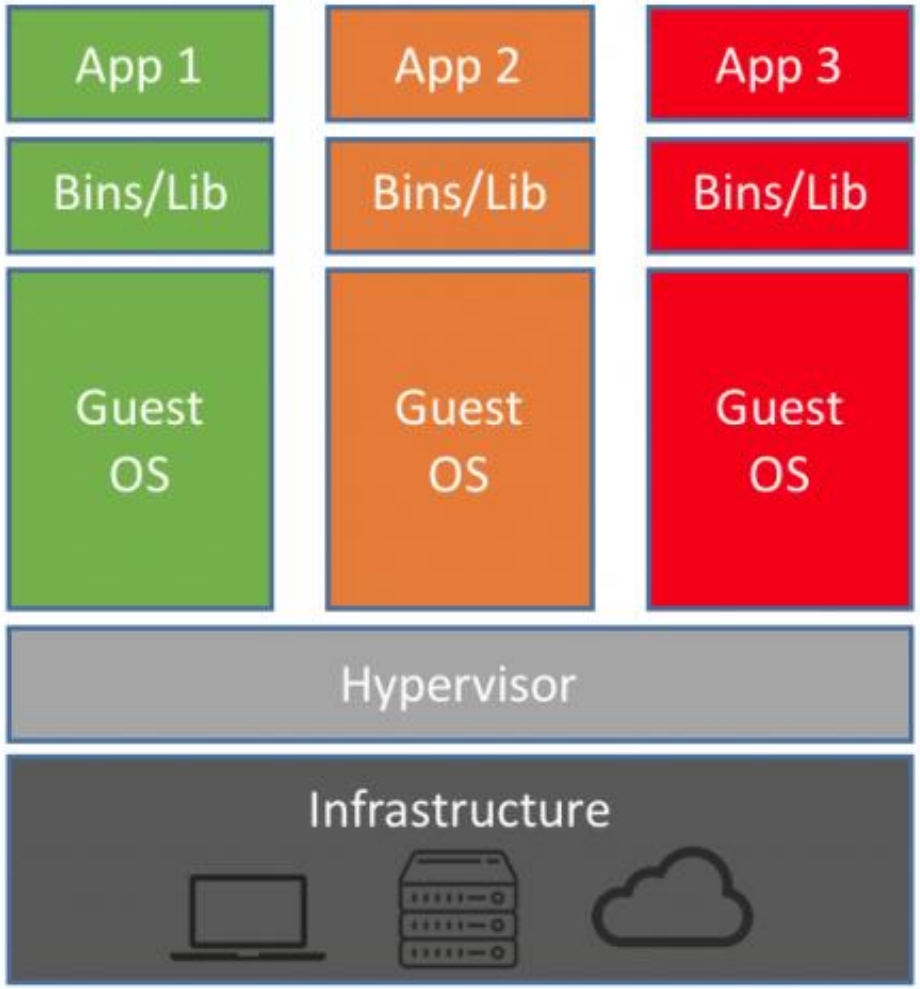
The AWS Security Model



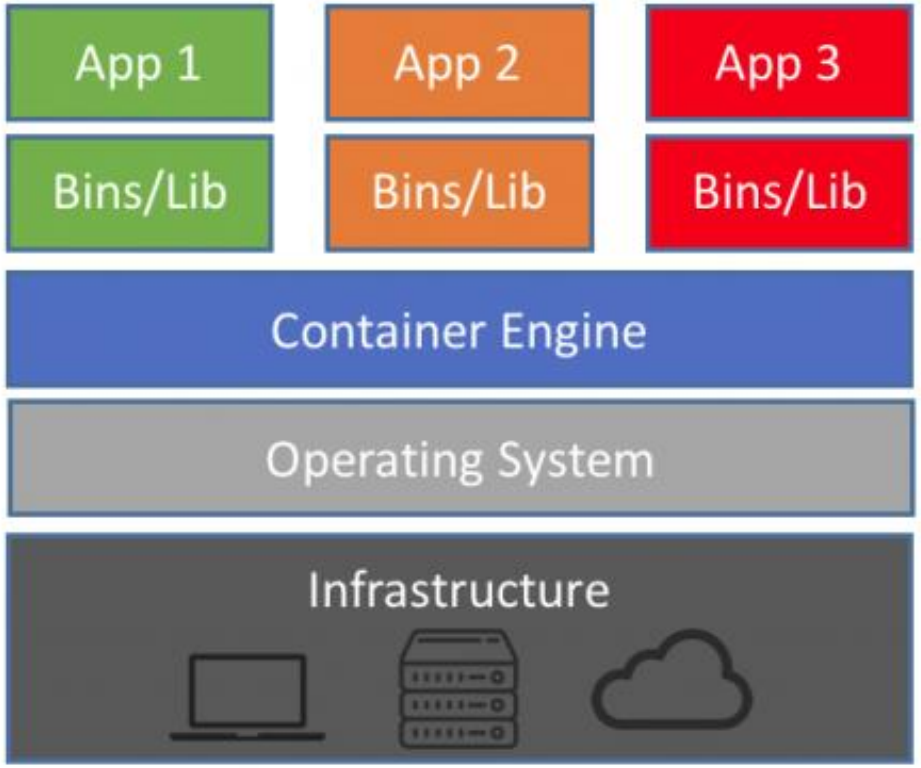
RSAConference2019

Cloud Asset Security

What is Moving to the Cloud?

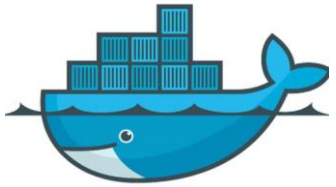


Machine Virtualization



Containers

Shifting Left with Containers



Containers Deployed with Unacceptable Risk

Without pre-deployment assessment of images, containers are pushed to production that are vulnerable or contain misconfigurations

Images in Repositories Become Vulnerable

Newly discovered vulnerabilities may make stored images vulnerable without any changes to the images themselves

Production Assessment is Too Late

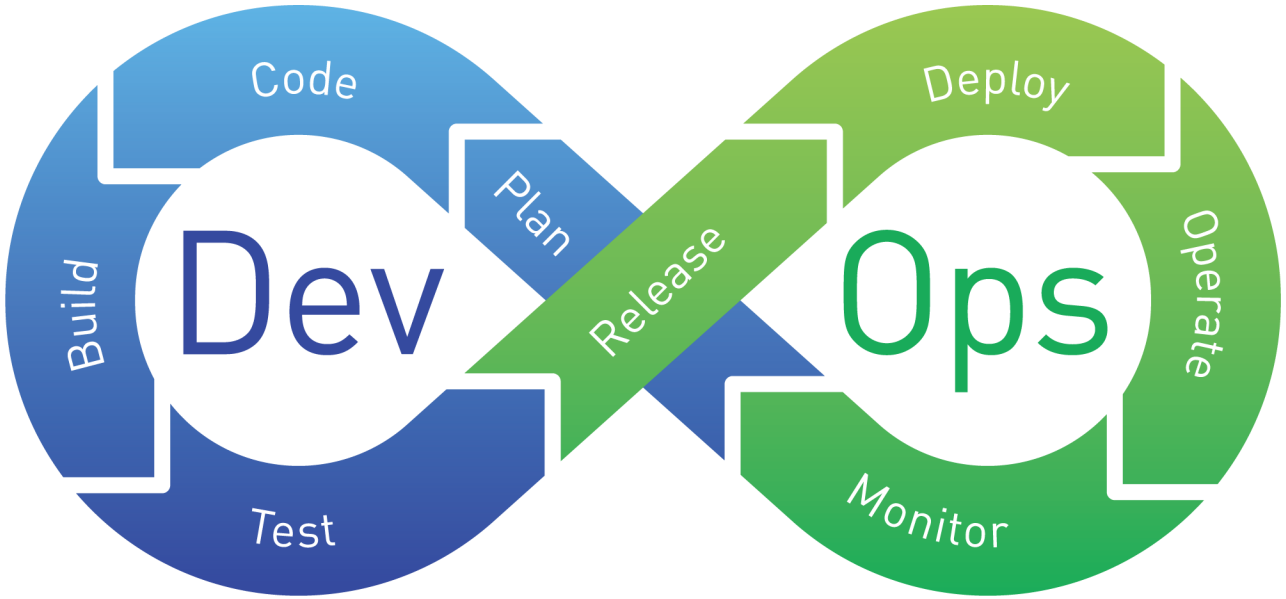
The majority of infosec tools are built for assessment of production systems, leaving assessment incomplete or too late for containers

tripwire

kubernetes

amazon web services

docker



Microsoft Azure

puppet

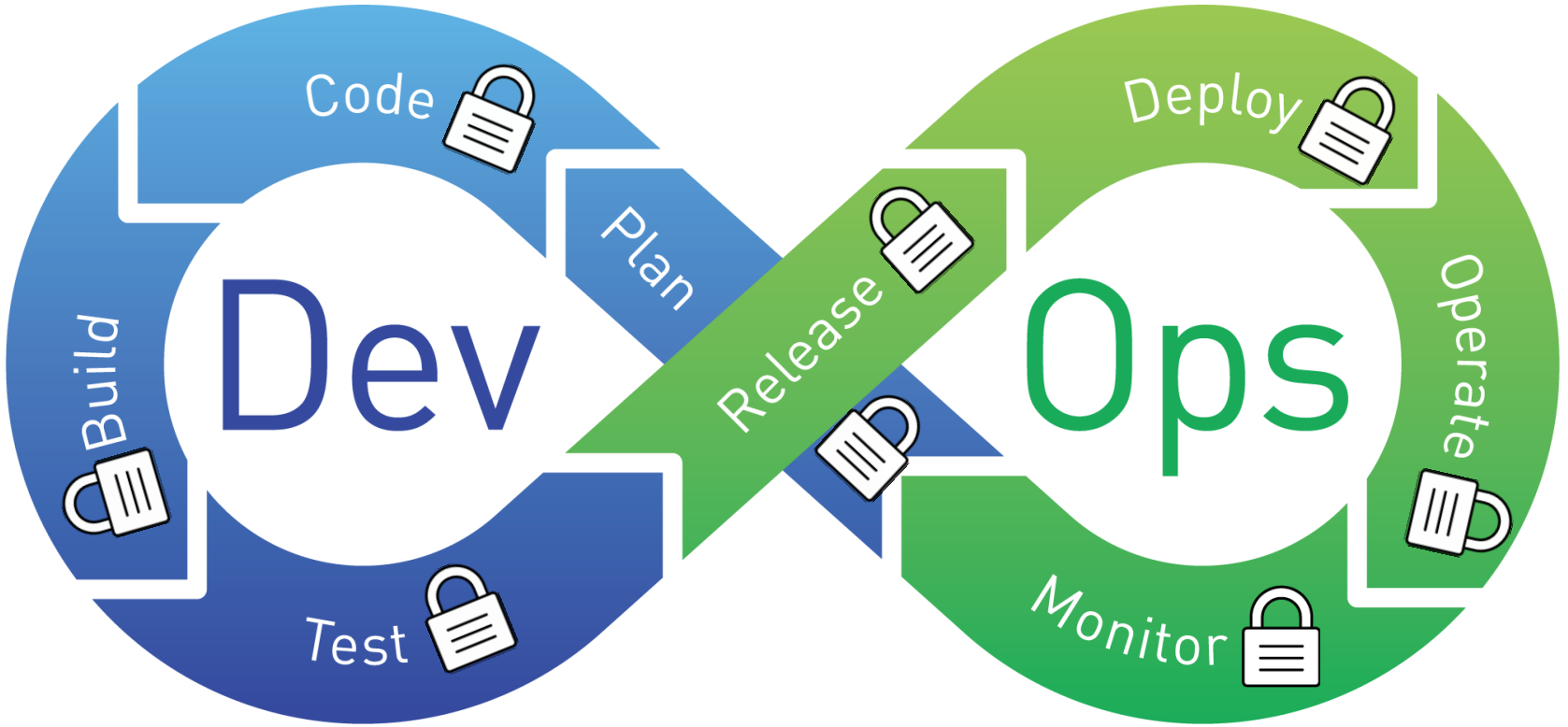
Google Cloud Platform

tripwire

ANSIBLE

CHEF

What is DevSecOps?



Putting the Sec in DevOps

Secure the Toolchain

- Lock down DevOps infrastructure
- Monitor DevOps scripts
- Establish and monitor security policies for DevOps tools

Automate

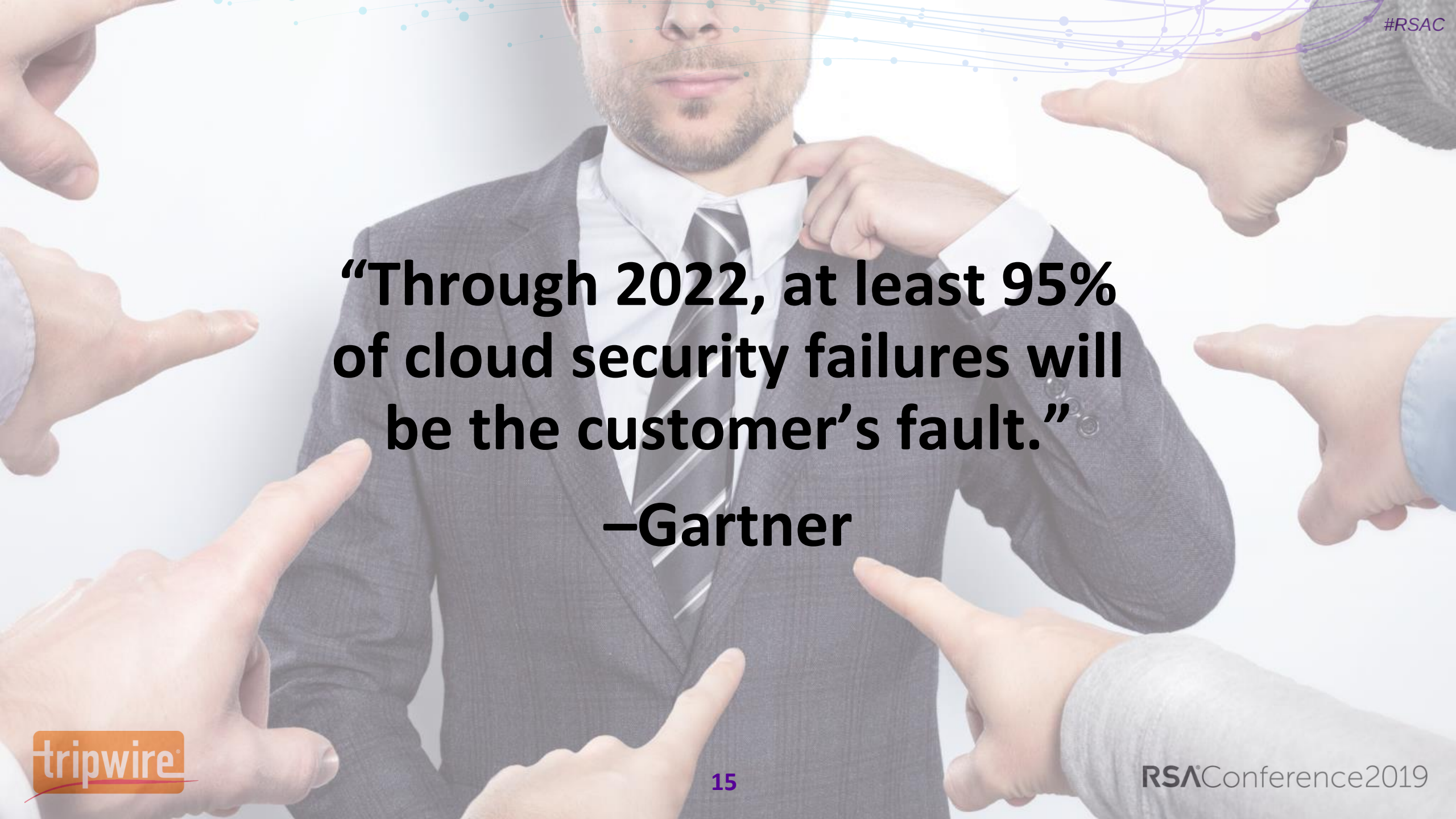
- Orchestrate security products with DevOps tools
- Reconcile changes made by DevOps tools automatically

Shift Left

- Add security to the DevOps process prior to deployment
- Check images and containers pre-deployment
- Monitor production for integrity

RSAConference2019

Cloud Security Posture Management



“Through 2022, at least 95% of cloud security failures will be the customer’s fault.”

–Gartner

hacking - AWS account hacked! Amazon isn't helping. What can I do ...
https://serverfault.com/.../aws-account-hacked-amazon-isnt-helping-what-can-i-do

My AWS Root Account Was Hacked (and it was my fault) | Roberto ...
https://www.linkedin.com/.../my-aws-root-account-hacked-fault-roberto-dwayne-mon...

AWS Developer Forums: My AWS account got hacked? ...
https://forums.aws.amazon.com/thread.jspa?messageID=750056

Hacker Puts Hosting Service Code Spaces Out of Business - Threatpost
https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of.../106761/

AWS Account hacked, bill of 2000$:(– ashnvishy
https://ashnvishy.wordpress.com/2016/03/29/aws-account-hacked-bill-of-2000/

Mea Vita: Carpe Diem: $5,000 Security Breach
blog.joemoreno.com/2014/04/5000-security-breach.html

My AWS account was hacked and I have a $50,000 bill, how can I ...
https://www.quora.com/My-AWS-account-was-hacked-and-I-have-a-50-000-bill-how...

Most Common Mistakes

Direct Connectivity to Internet

SSH/RDP Open to Public Internet

Data Stores Exposed

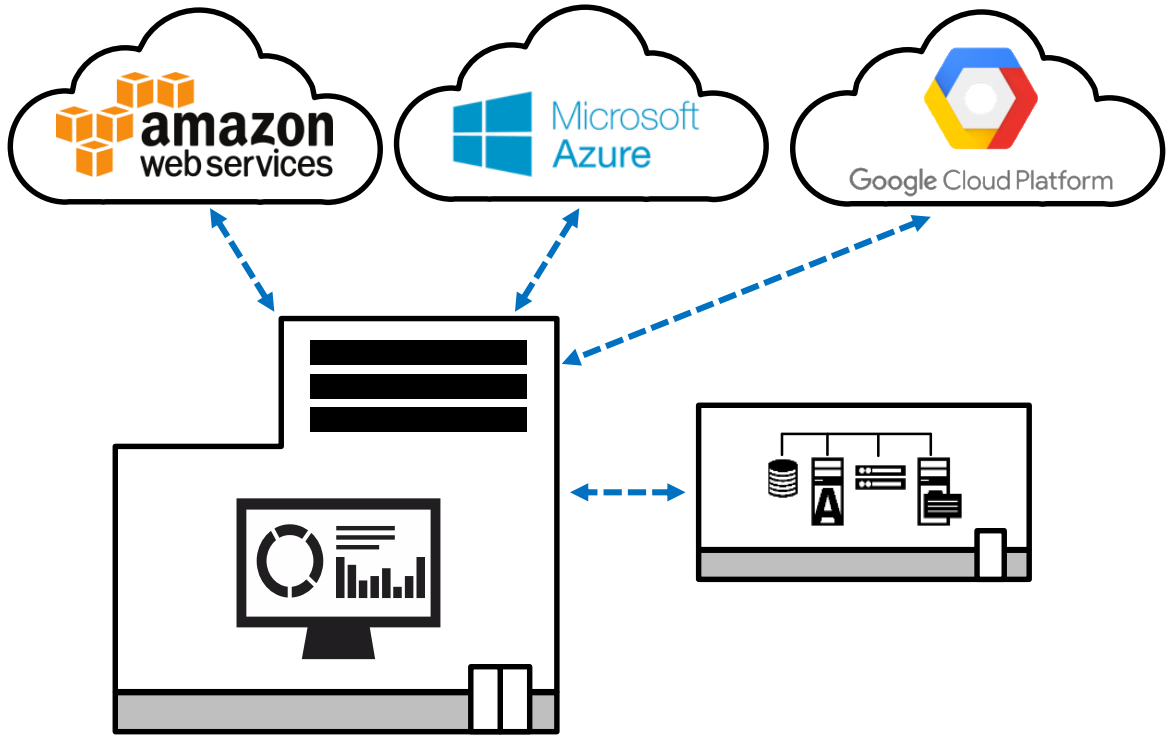
Unprotected APIs

Lack of Access Control

Lack of Encryption

Cloud Security Posture Management

- Ensure the **secure configuration** of cloud provider accounts to prevent incidents
- **Monitor** cloud management accounts for changes that could result in breaches, non-compliance, downtime or surcharges
- Gain **visibility** across your entire hybrid environment, including multiple AWS, Azure & GCP accounts



“Swivel Chair” Problems

RSAConference2019

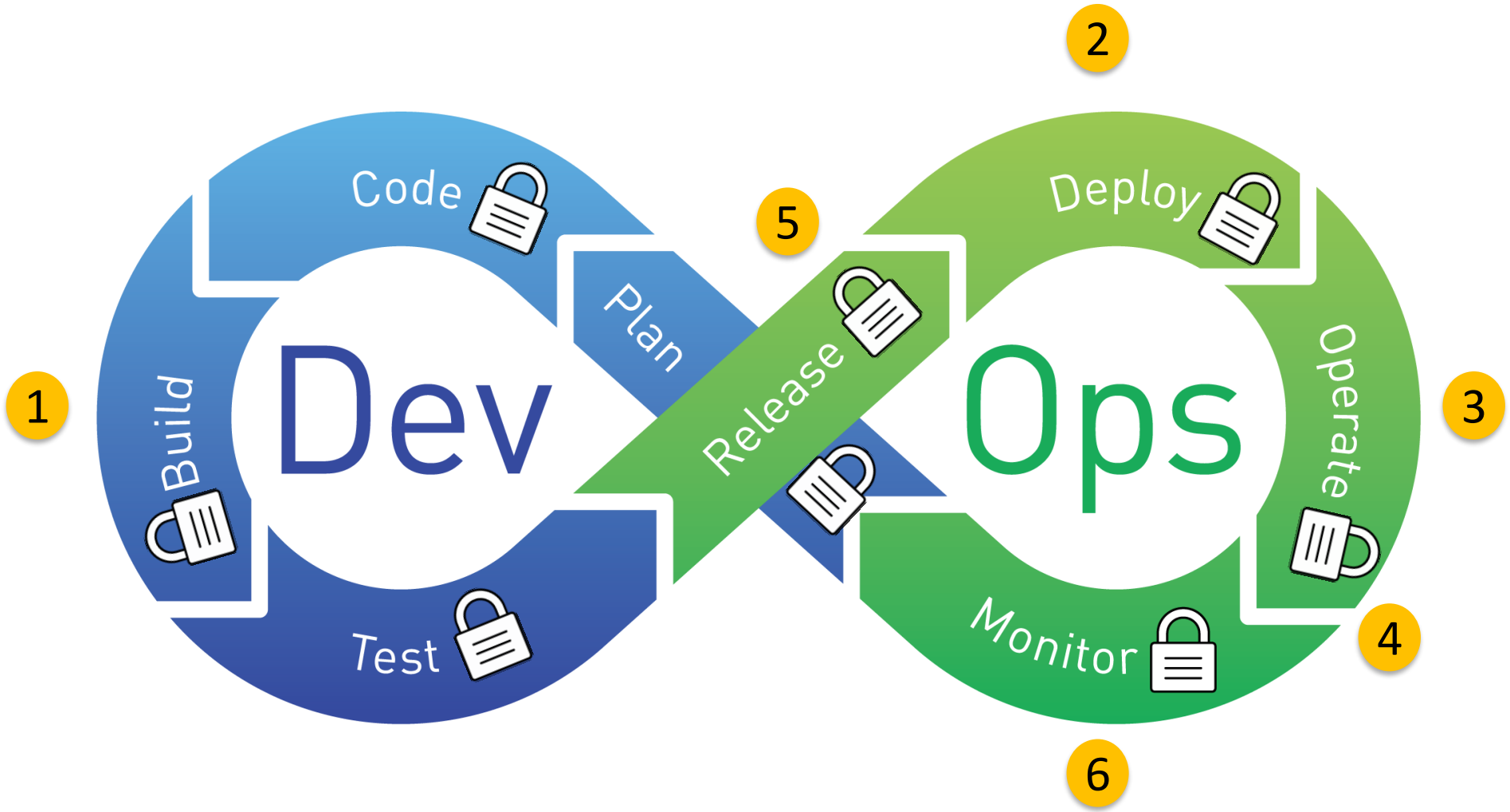
Case Study

Securing a Multinational Bank's Hybrid Cloud Enterprise

Business Needs

- Dependable **risk assessment and configuration control**
- **Reduced attack surface** through integration with DevOps teams and orchestration tools
- Systems deployed automatically meet approved images' **risk levels and configurations**
- **Change monitoring** on elastic systems
- Instant **vulnerability assessment** on individual servers after unauthorized configuration changes

Solution


1
2
3
4
5
6
Code
Plan
Build
Test
Release
Deploy
Operate
Monitor
Dev
Ops

RSAConference2019

Takeaways

Takeaways

- If security is a **bottleneck**, expect to be avoided
- DevOps will continue to grow – implement security solutions that work at the **speed of DevOps**
- Hybrid environments require **hybrid solutions**
- **Stop** buying swivel chairs
- Have a plan and **don't lose your donkey**

RSAConference2019

Q&A