RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART3-W11

7 Steps to Maintain Security Across Your Cloud Estate

Jason Needham

Sr. Director of Cloud Security
VMware
jneedham@vmware.com

Casey Lems

Cloud Security Architect
VMware
clems@vmware.com

RSAConference2020

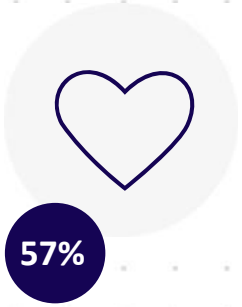
What's Required for Public Cloud Security? How are These Environments Different?

The Promise:

Speed, Agility, and Customer Delivery Drive Multicloud Adoption

Improve speed of service delivery

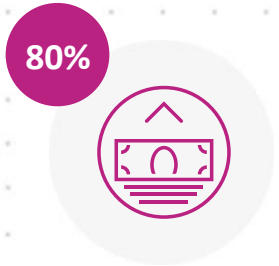
Flexibility to react to changing markets



Improve customer support or services*

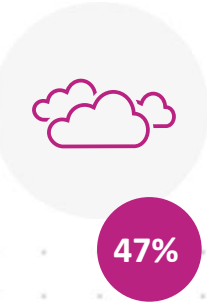
The Reality:

Operational Challenges Take Over



Will overshoot their cloud IaaS budgets**

Will accidentally expose data or services †



Do not optimize cloud workloads ‡

* 2018 IDG Cloud Computing study
**Gartner, Ten Moves to Lower Your AWS IaaS Costs 15 October 2018

† Gartner, Innovation Insight for Cloud Security Posture Management, 25 January 2019
‡ Forrester Analytics Global Business Technographics Infrastructure Survey, 2018

What Do You See as Biggest Public Cloud Security Threats?

42%

Unauthorized access

42%

Insecure interfaces /APIs

40%

Misconfiguration of the cloud platform /wrong setup

Source: 2019-Cloud-Security-Report-ISC2

Hijacking of accounts, services or traffic

External sharing of data

Malicious insiders

Malware/ransomware

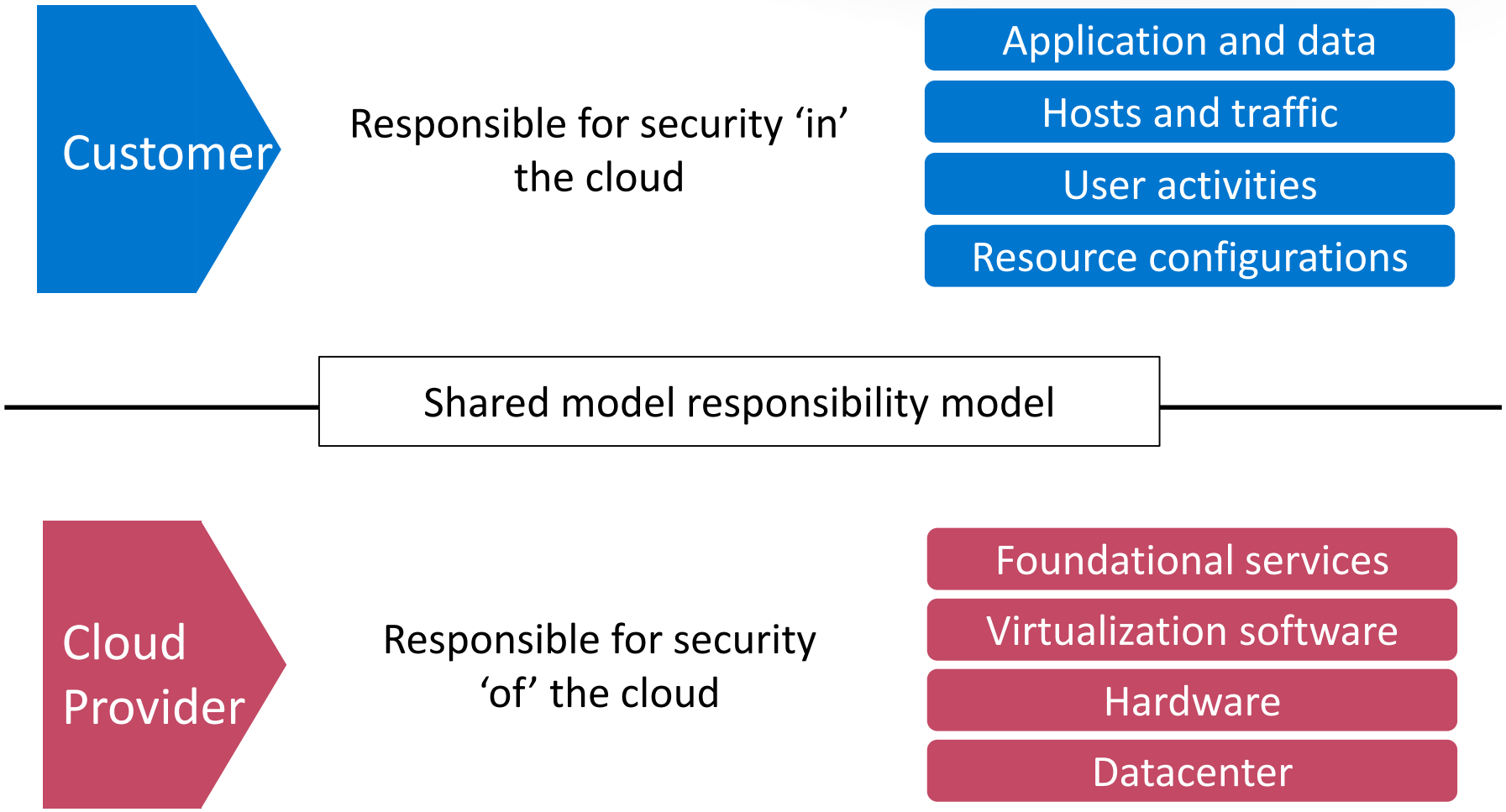
Traditional Security Control Challenges

Constantly changing environment

Missing resource identity

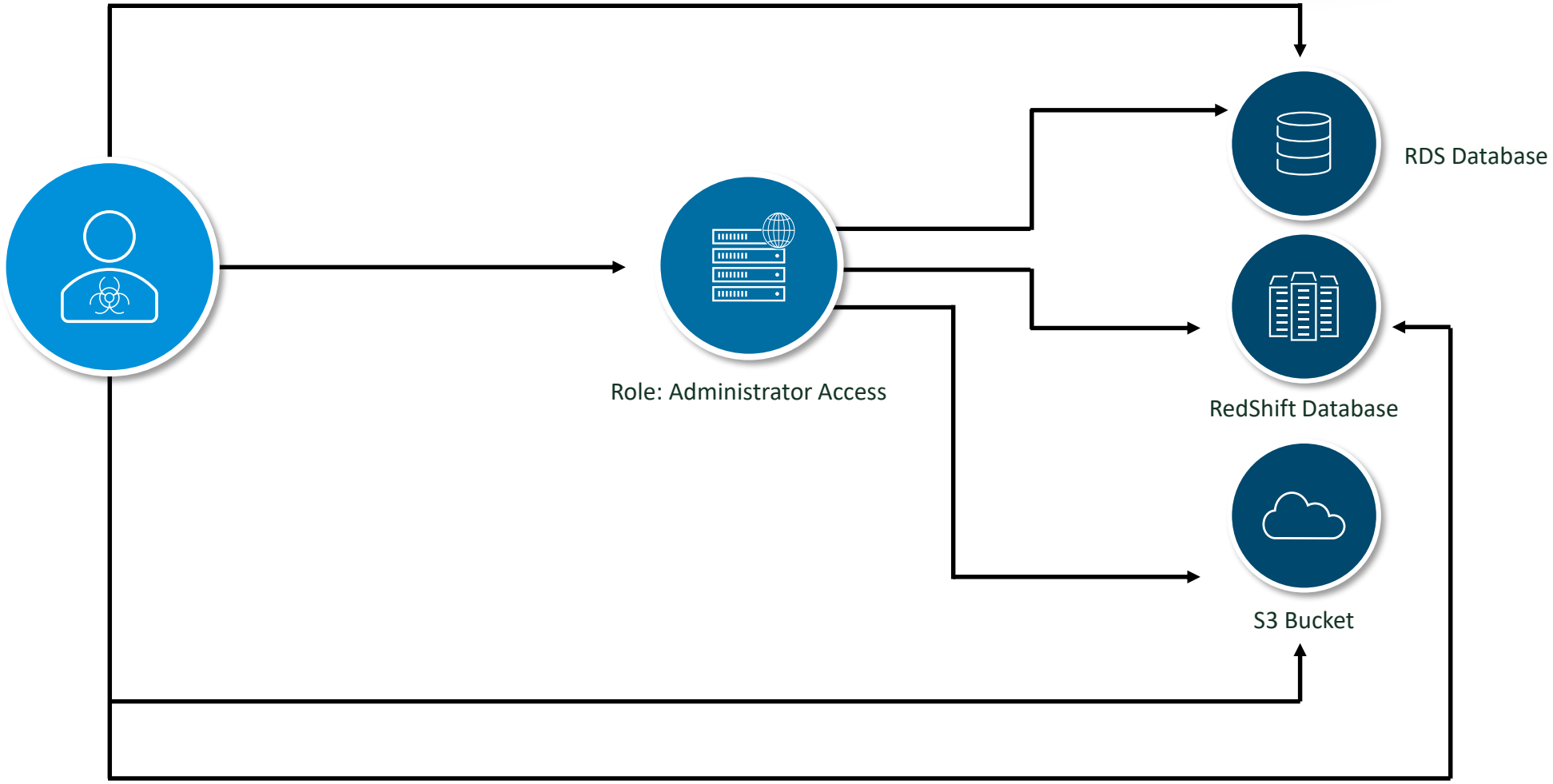
No Single Firewall Policy

Customers Are Responsible For Security “In” The Cloud



Common Cloud Vulnerabilities

Highly privileged virtual machines



VMware IT Secures Over 7000+ Cloud Accounts with Secure State

Public Cloud Environment

amazon web services

Microsoft Azure

80M
Objects

4B
Events/Day

"Secure State is a better fit for us as we scale. We **secure over 80M cloud objects and process over 4 billion events everyday**. Secure State gives us the right set of alerts, both quickly and intelligently compared to other security solutions we have used in the past."

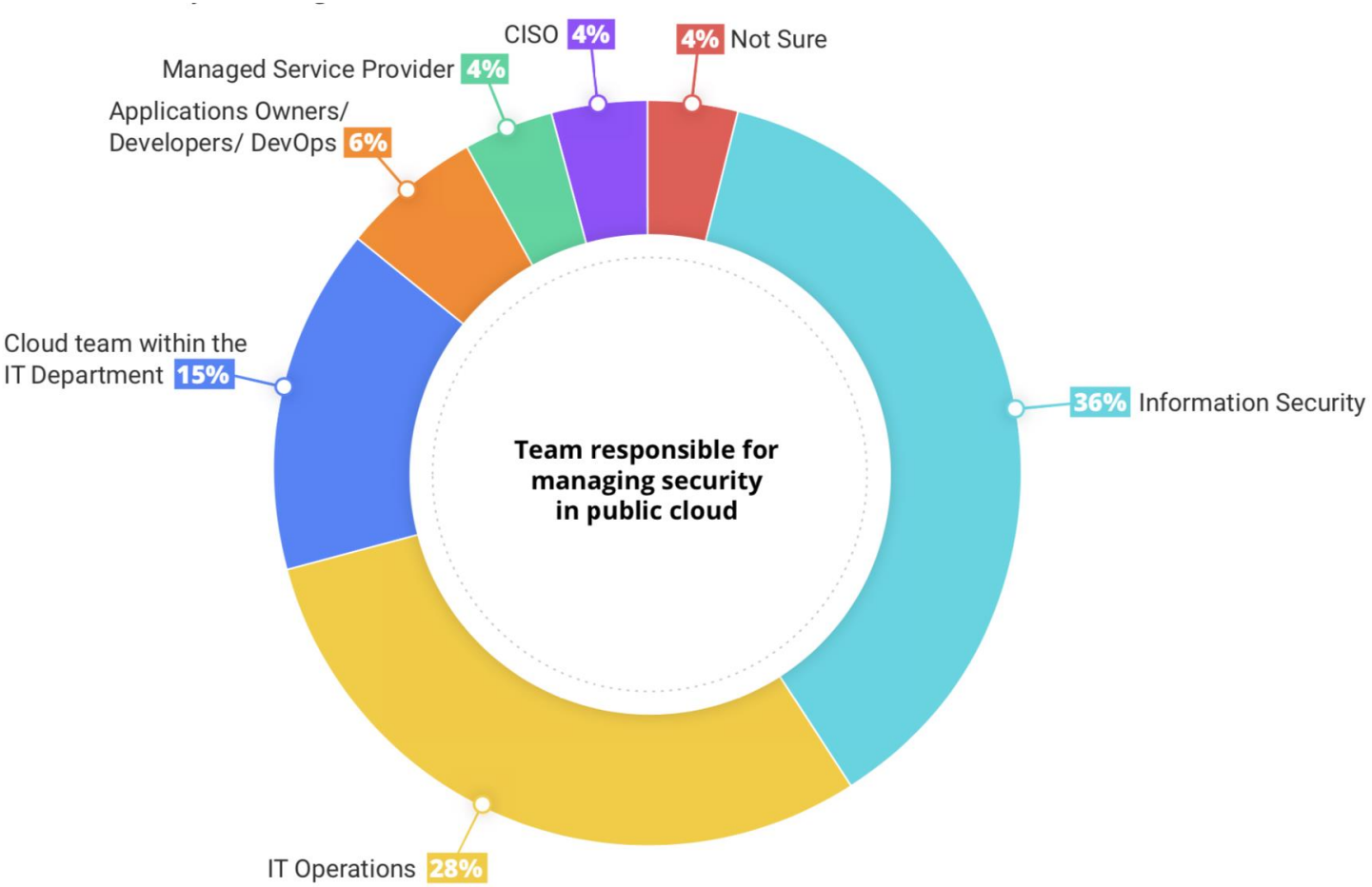
Sandeep Poonen, Director of Security

RSAConference2020

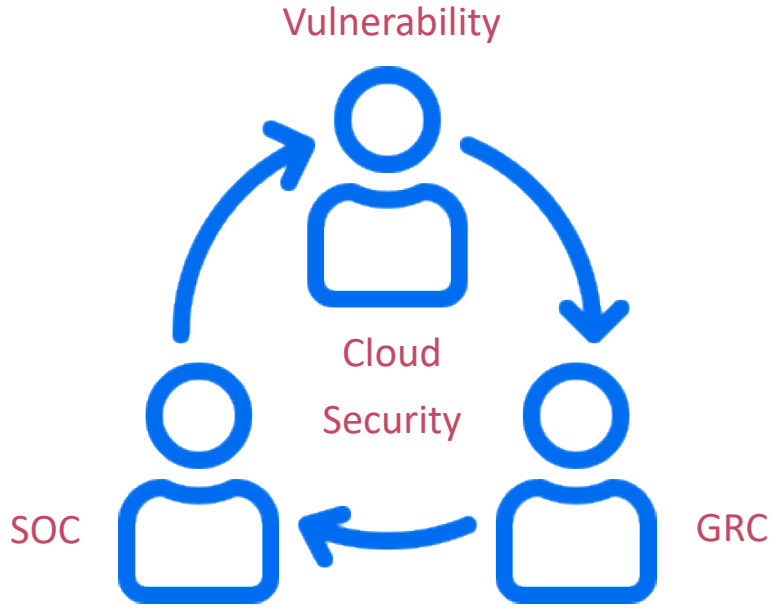
7 Steps to Managing Your Cloud Security Estate

1. Clarify Internal Responsibility

Who Is Responsible for Cloud Security?



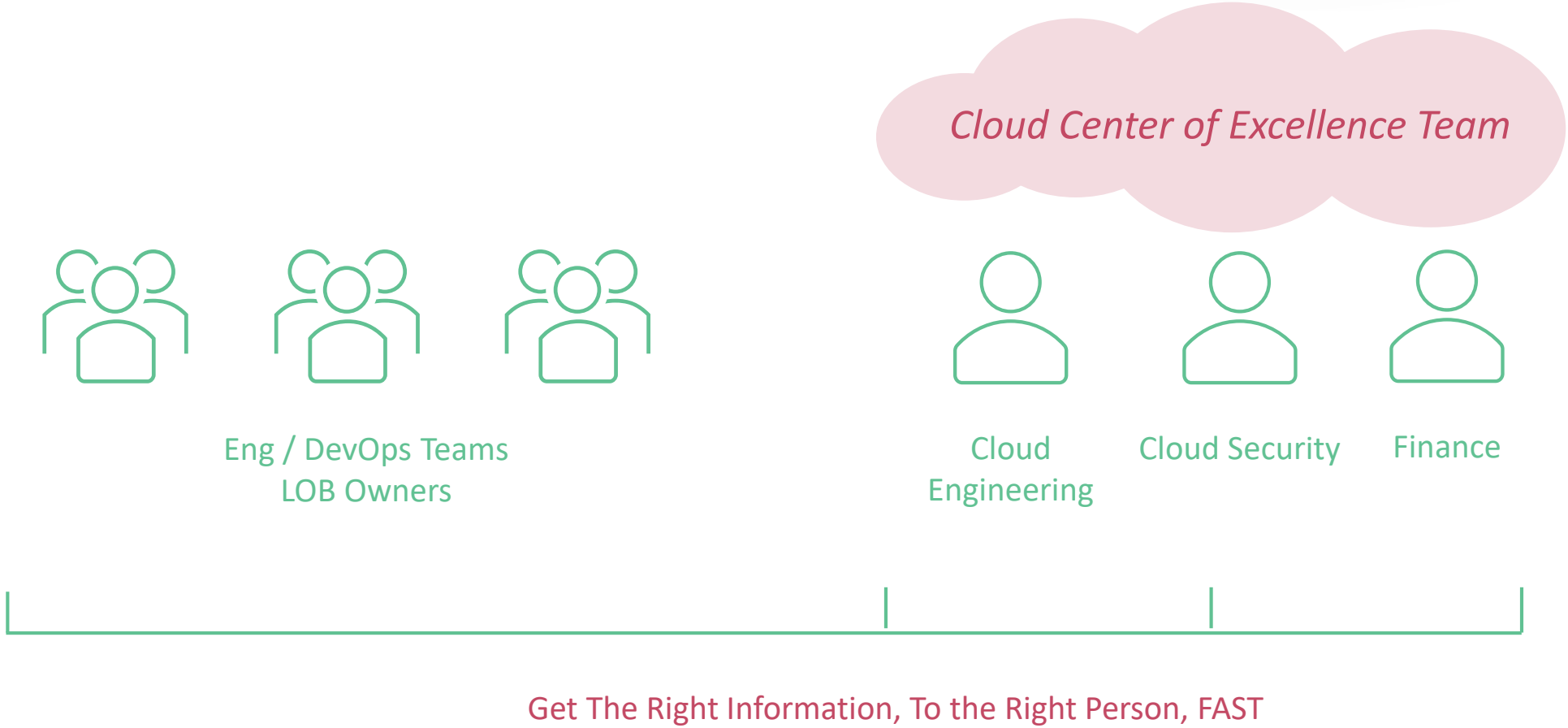
Who Owns this Within Security Itself?



Source: CSA_Cloud_Security_Complexity_Report_2019

2. Communication

Equip Cloud Teams To Better Manage Risk



3. Asset Visibility – Have a Collection Plan

#1 Critical Control for Center for Internet Security (CIS)

- Solution Designed for Cloud Asset Visibility
  - Different Assets Types: Account / Owners / IaaS / PaaS / Serverless
  - Different Designs: Services In Isolation vs Relationships & Dependencies
- Frequency: Weekly, day, near real-time
  - Dynamic / Ephemeral
  - Open APIs / More Sources of Change
- Coordinated Approach
  - Every team pulling inventory data is costly and can disrupt operations and deployment
- Security and Service Owner Accessible

4. Define Your Standards – Create a Governance Program

1 Controls

Provider Hardening Guides and Standards

2 Target Environments

Dev / Test

Internal Services

Production SaaS

Business Wide Standards

3 Exceptions

Accept Risk, Workflow and documentation

Example:

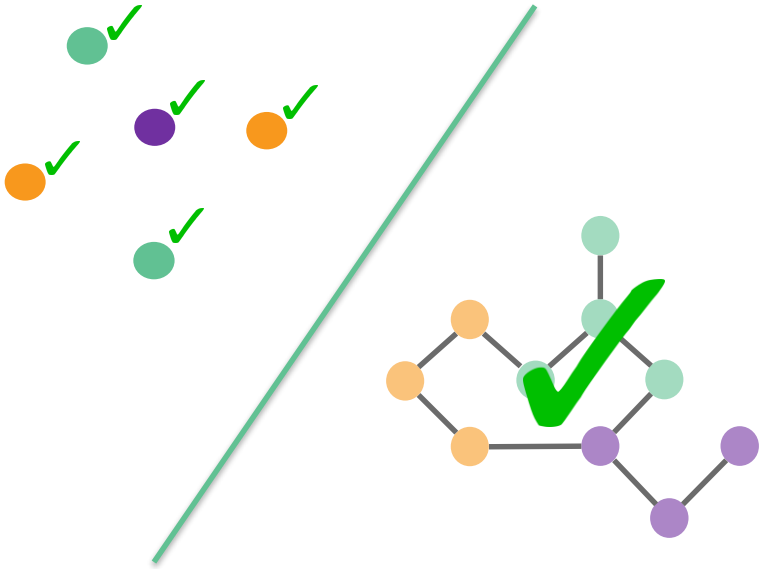
EC2 Instance is Publicly Accessible and has elevated privileges for S3 Buckets
-> CIS AWS, NIST 800-171, EU-GDPR

All Production SaaS Accounts

Whitelist / Suppress accepted EC2 instances with Tag App1

5. Detect Vulnerabilities – At Cloud Speed

Faster Is Better	Smart / AI Anomalies	Isolated vs Holistic Conditions



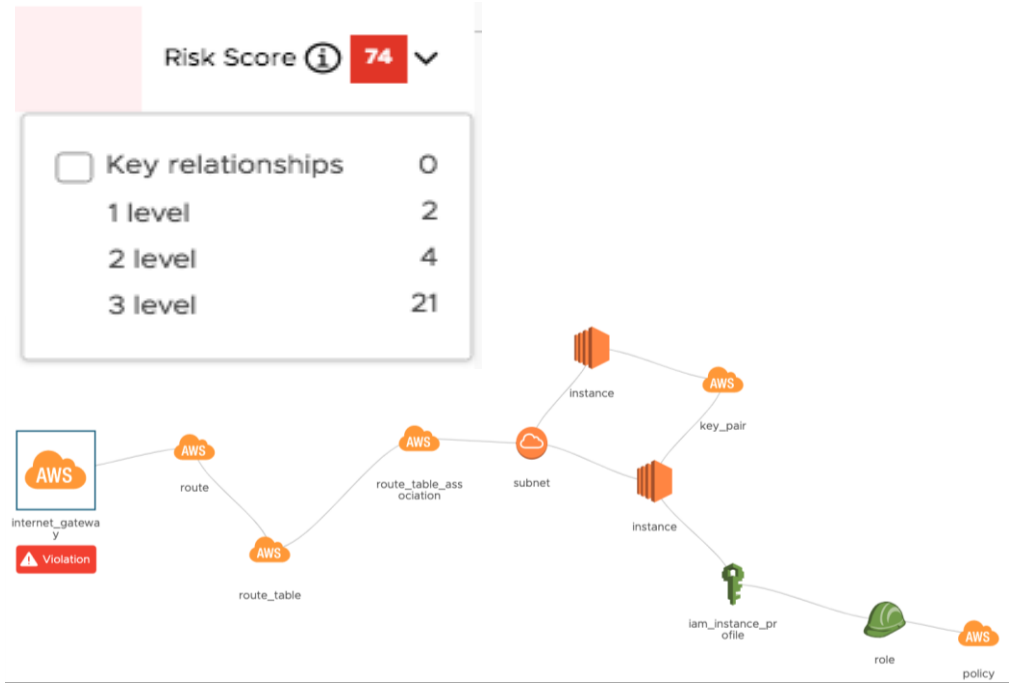
VMware Secure State

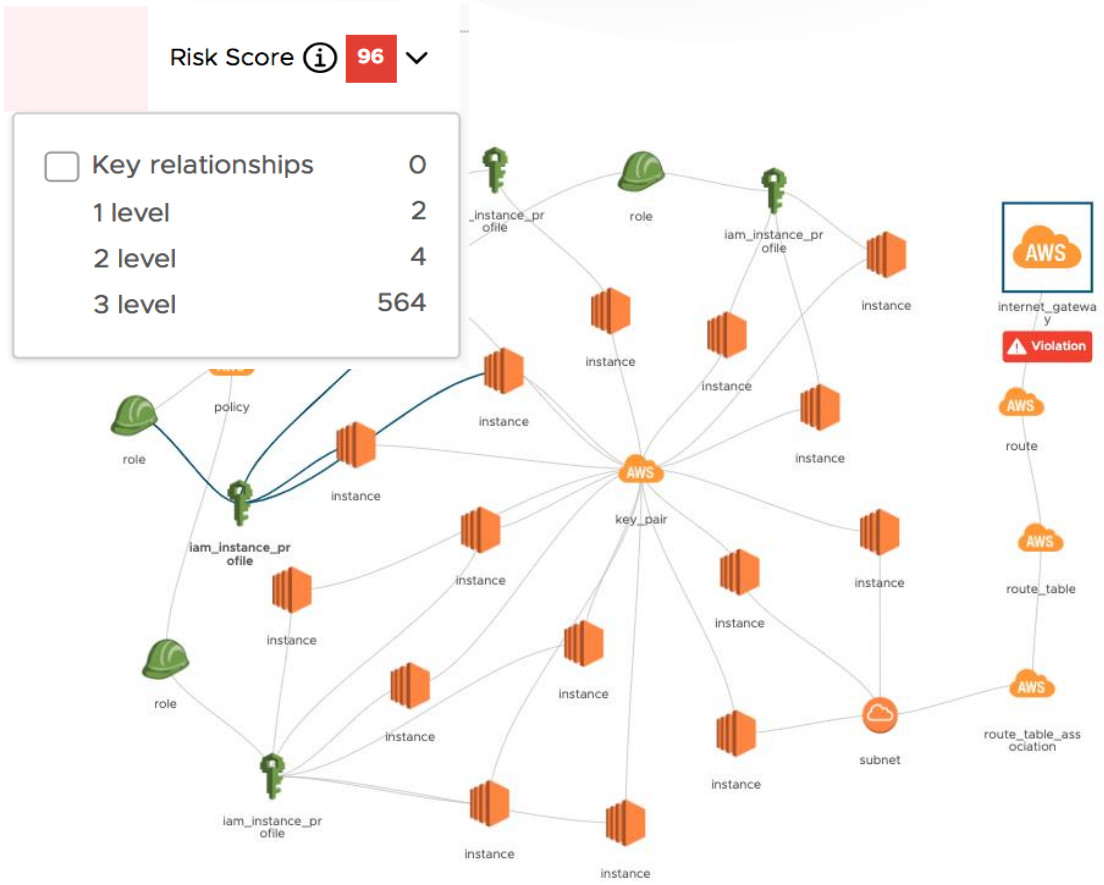
Interconnected Cloud Security Monitoring

Event Based Micro-Inventory

Real-Time Insights

Simplified, Risk-based Prioritization





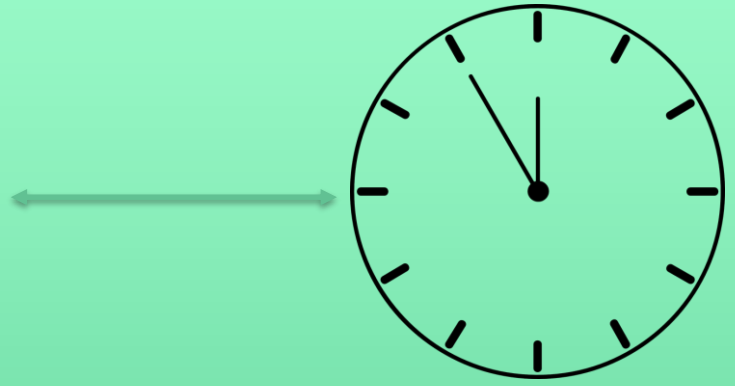
6. Remediating Issues – Building Trust and Success

Evolution from Manual to Automated Remediation and Guardrails

Manual Actions

Manual with Approvals

Automated Guardrails

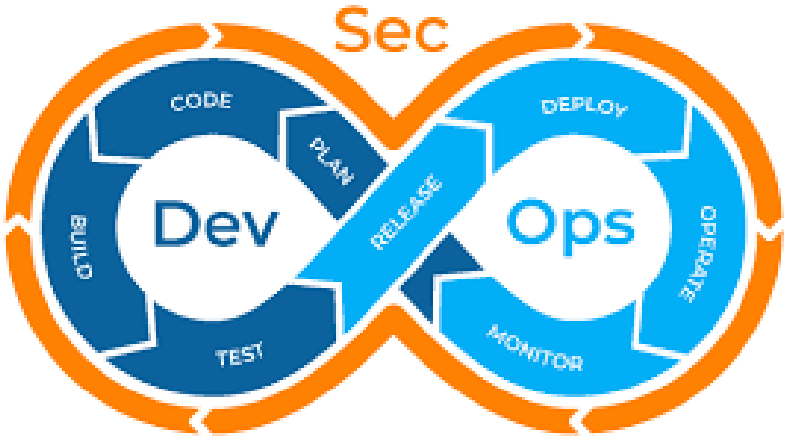


Existing Resources

New Resources

7. Shift Left / Security As Code

Integrate with DevOps and CI/CD Pipeline



aws CERTIFIED

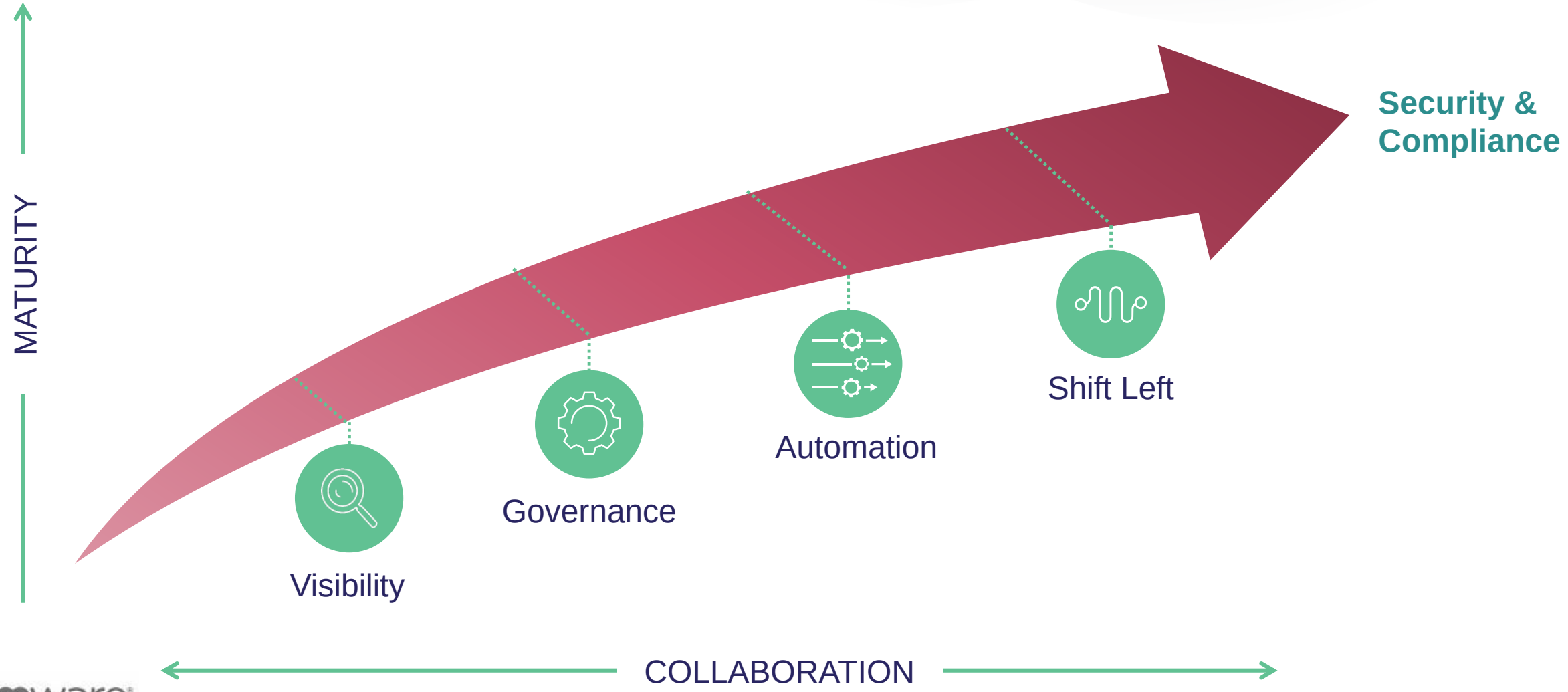
CloudFormation

RSAConference2020

Applying At Your Company

Cloud Security Journey

Effectively Manage Cloud Risk



7 Steps In Review

Steps	Key Guidance
1. Clarify Responsibilities	All Teams Not Just Security
2. Communication Plan	For All Resources Not Just
3. Asset Visibility	LOB Owners Have App Context
4. Define Standards	Identify Controls with Minimal Exceptions
5. Automate Detection	Prioritize Risk
6. Automate Responses	Coordinated Responses
7. Shift Left	Proactive Security Mindset

RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PART3-W11

7 Steps to Maintain Security Across Your Cloud Estate

Jason Needham

Sr. Director of Cloud Security
VMware
jneedham@vmware.com

Casey Lems

Cloud Security Architect
VMware
clems@vmware.com