RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: CLS-M02

The Coming Cloudpocolypse: Disrupting the Cloud Shared Responsibility Model

Rich Mogull

SVP Cloud Security/CEO
FireMon/Securosis
https://www.linkedin.com/in/richmogull/

Chris Farris

Cloud Security Nerd
PrimeHarbor Technologies, LLC
https://www.linkedin.com/in/jcfarris/

Disclaimer

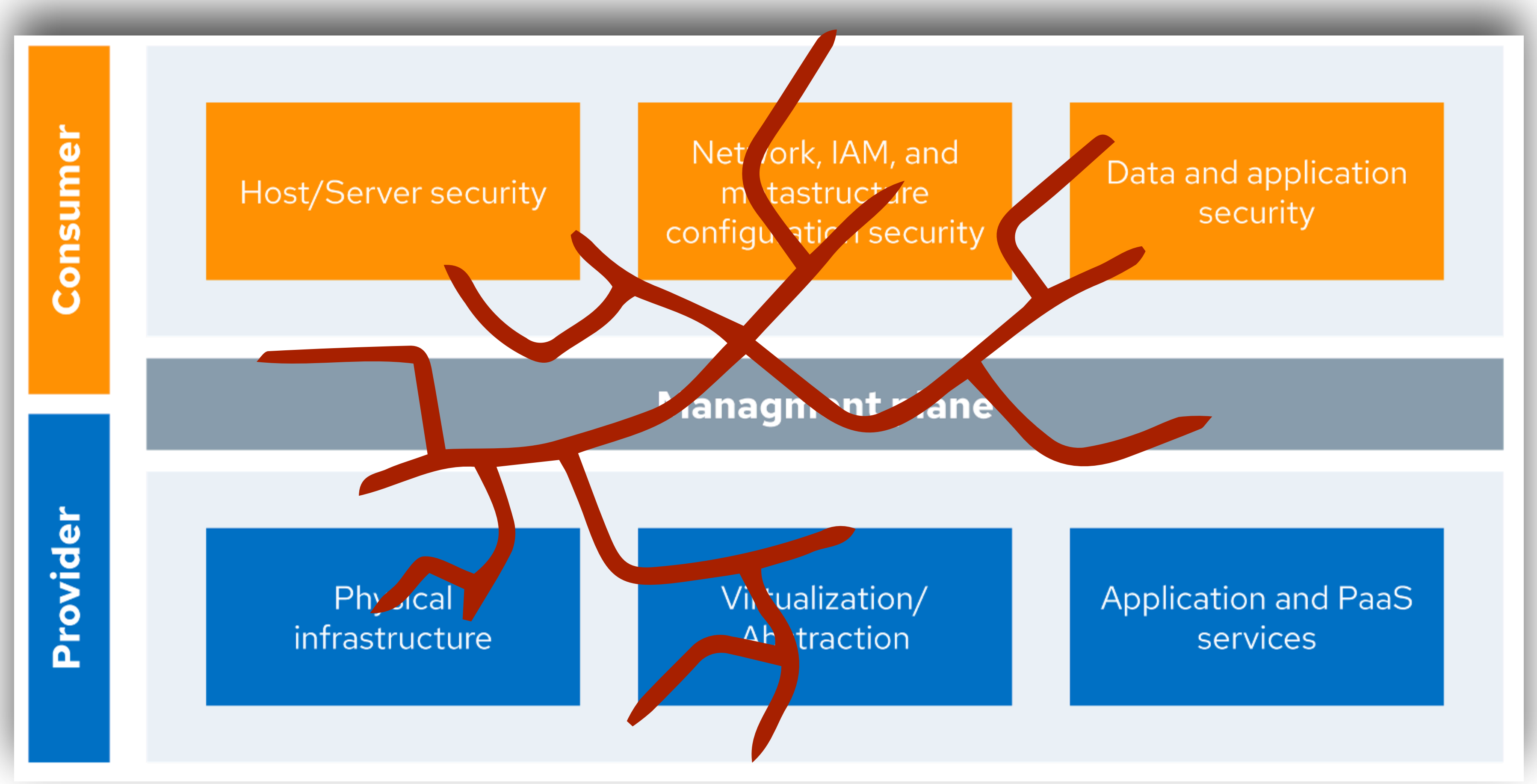
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

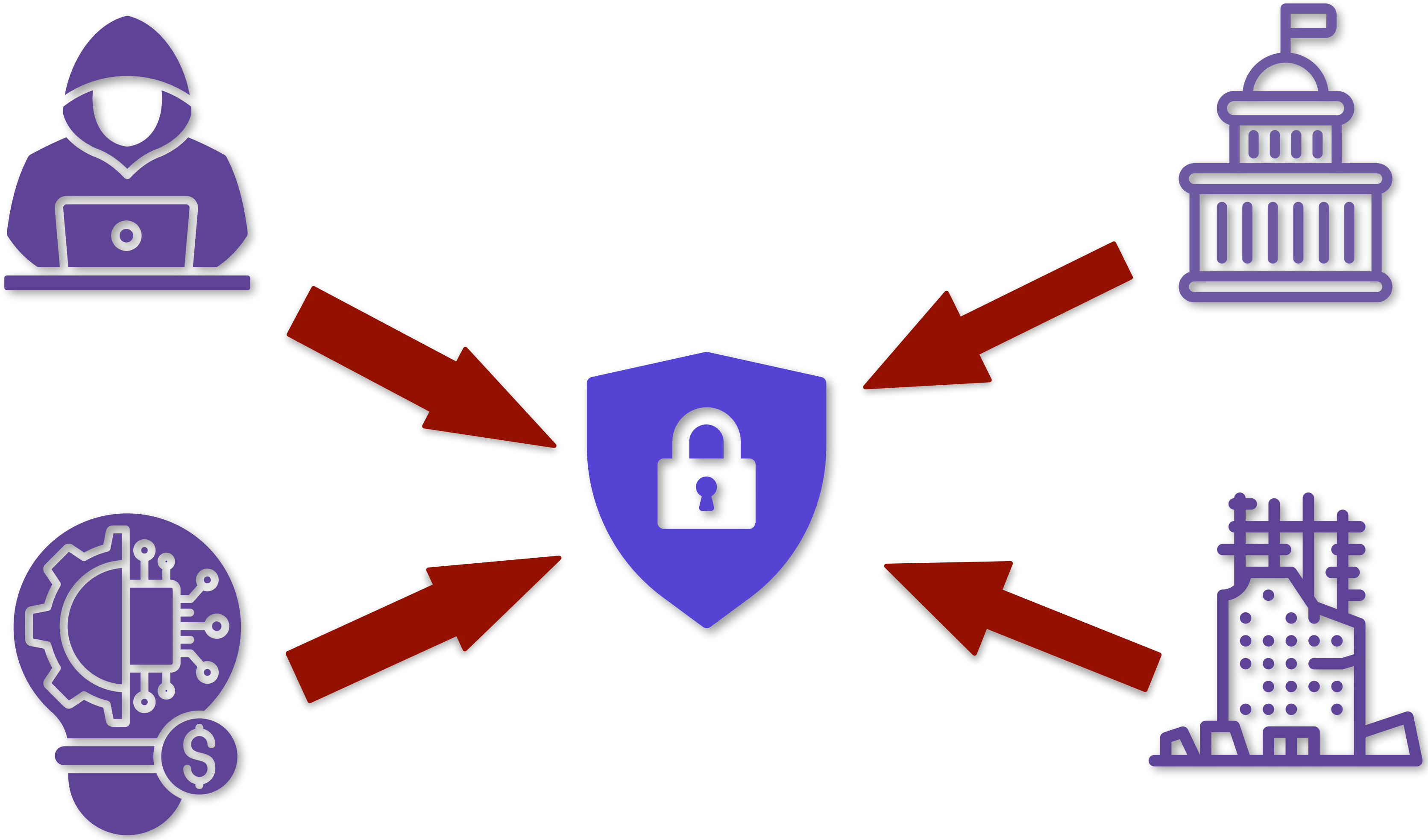
A Brief and Select History of Clouds

It’s about governance and mindset more than technology

Shared Responsibilities Under Attack


Consumer
Host/Server security
Network, IAM, and metastructure configuration security
Data and application security
Managment plane
Provider
Physical infrastructure
Virtualization/ Abstraction
Application and PaaS services

Disrupting Security



Shared Responsibilities Disruptions

What **other CSPs** are doing

What **governments** are doing

What **adversaries** are doing

How **customers** use cloud

A story in 3 acts… with 4 characters…

The Dawn of Cloud

The Adversaries Strike

The Rise of the Resistance

Cloud Service Customers (CSC)

Cloud Service Providers (CSP)

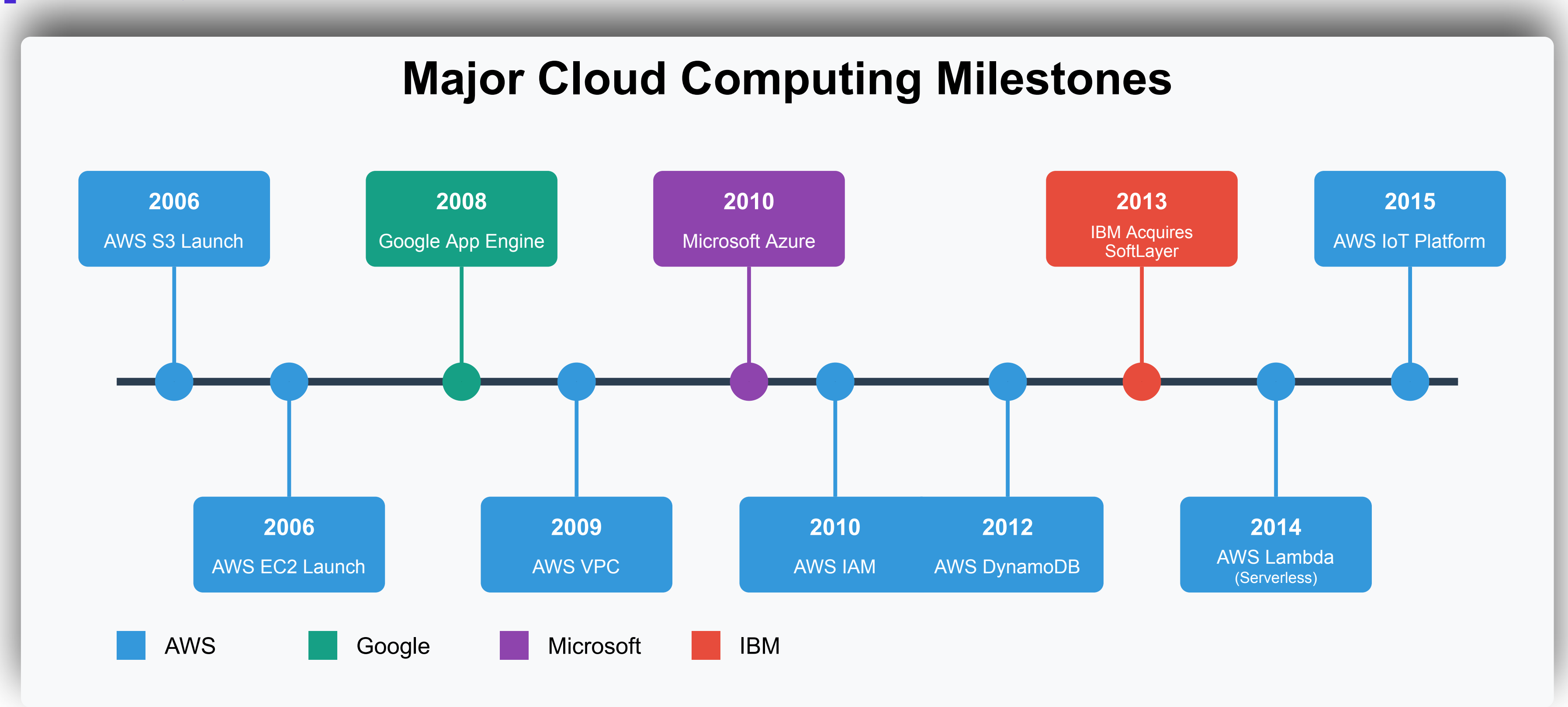
Threat Actors

Governments
(The other threat actors)

Cloud’s First Decade

Building the Shared Foundation: 2009-2019

Rampant, Unfettered Innovation



Major Cloud Computing Milestones

2006 AWS S3 Launch

2006 AWS EC2 Launch

2008 Google App Engine

2009 AWS VPC

2010 Microsoft Azure

2010 AWS IAM

2012 AWS DynamoDB

2013 IBM Acquires SoftLayer

2014 AWS Lambda (Serverless)

2015 AWS IoT Platform

🟦 AWS 🟩 Google 🟪 Microsoft 🟥 IBM

Experimentation

Shadow IT

You did what?!?

Priority: Get Security Buy-In/Remove Security Friction

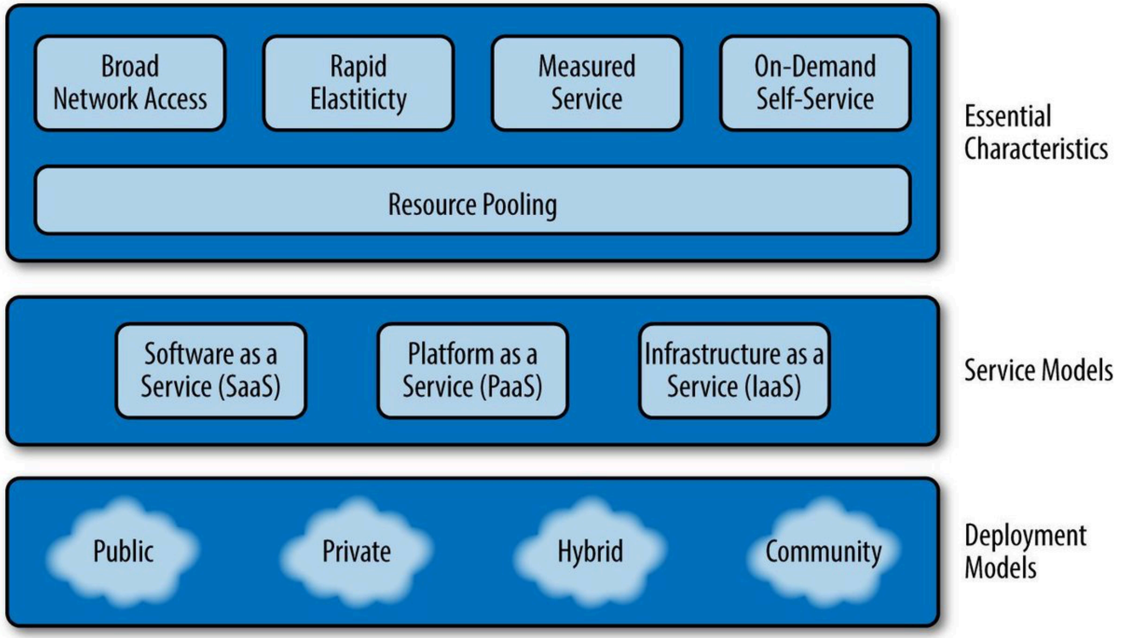
- Appease security server huggers
  - Eliminate Vetos
- Appease security auditors
  - Minimum compliance requirements, audits/ attestations, etc.

- Feature examples
  - Very small/point foundations
    - security groups, VPCs, IAM
  - Add ons for the banks/F500- “we’ll go if you give us this one control”
    - NACLs/KMS
  - Add-on Security Services:
    - GuardDuty
    - Macie

CSP

What Gov was (not) doing

- Early NIST model
- Origins of GovCloud
- YOLO regs
  - Europe- ENISA, not fully regulated, trying to keep it local
  - Data privacy was the focus, and not necessarily cloud specific



Cloud Adoption Models

Developer Tethering

Snap Migration

Datacenter Transformation

Native New Build

Higher Risk
Dominant 2009-2019

Cloud Adoption Models

Developer Tethering

Snap Migration

Datacenter Transformation

Native New Build

What we did

What we thought we were doing

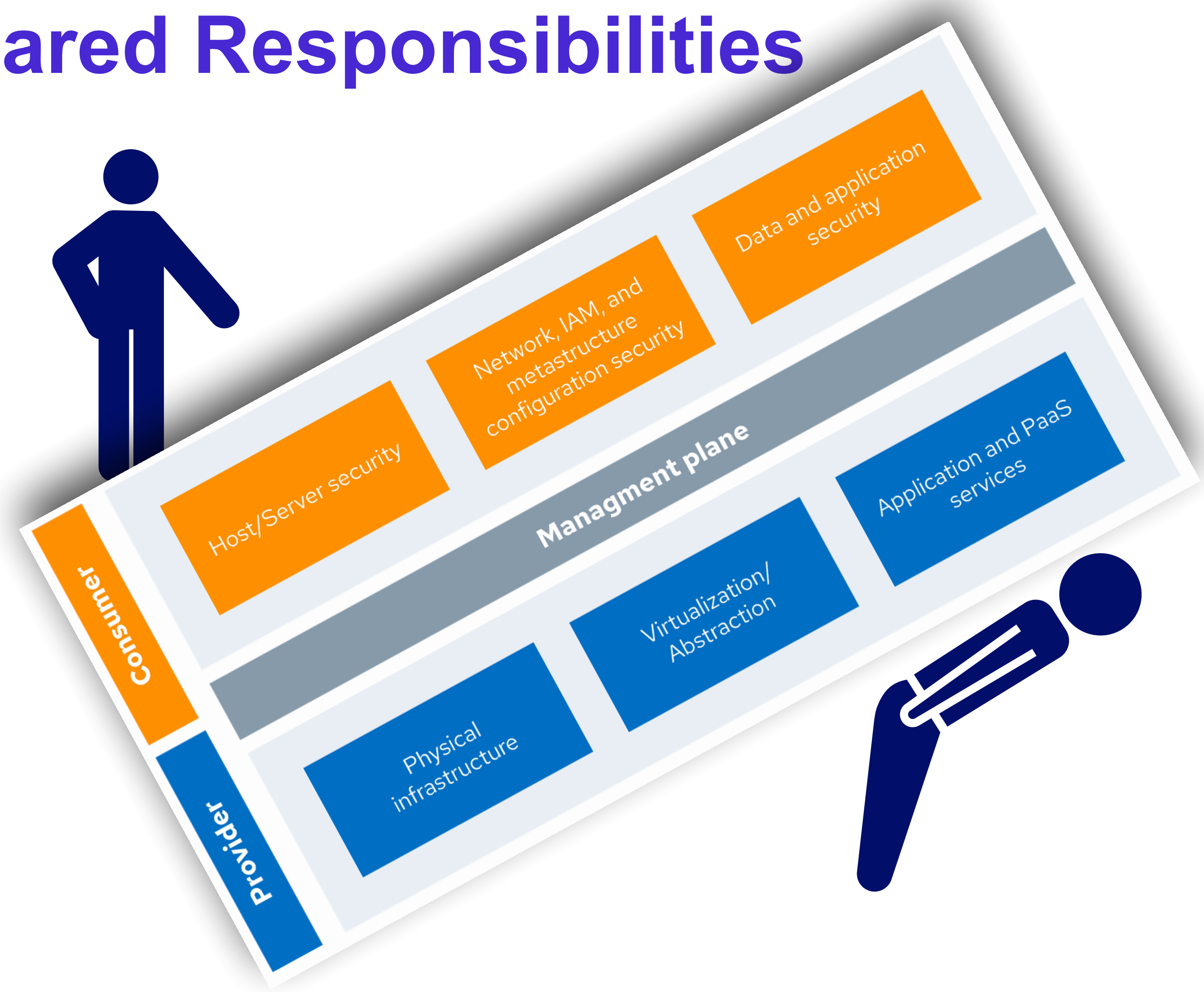
What we hoped to be able to do someday

Random Threats

- Threat actors don't know cloud yet
- Happy accidental incidents
- First early successes, but not organized
- DEMO MODE

TA

Shared Responsibilities


Consumer
Provider
Host/Server security
Network, IAM, and metastructure configuration security
Data and application security
Managment plane
Physical infrastructure
Virtualization/ Abstraction
Application and PaaS services

CSPs could lean on the Shared Responsibilities Model to blame customers for security incidents

RSAC 2025 Conference

The Adversaries Strike (Fudge Around Phase)

From Capital One to Snowflake: 2019-2024

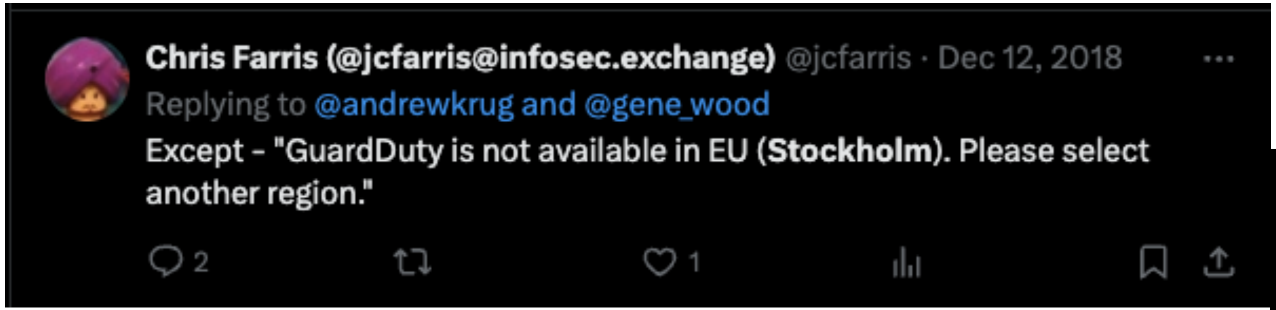
Many Voices.
One Community.

Everything Changed when the Fire Nation Attacked

Not financially motivated, but it was the attack that made headlines when threat actors started figuring out their financial models.

The Inflection Event

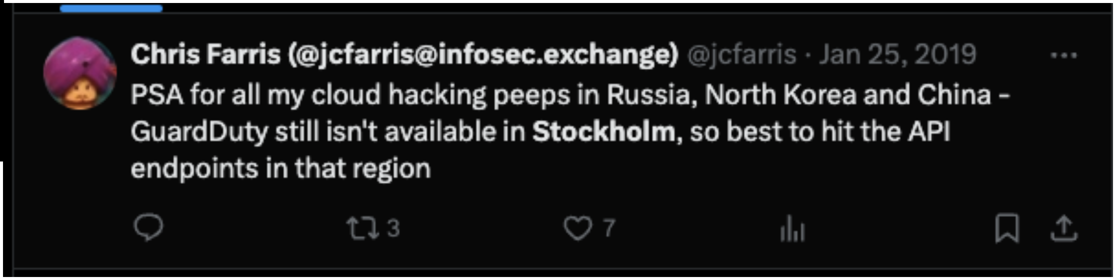
- The customer engineers didn't fully understand the technologies in question
- The provider ignored warnings from the cloud sec community
- The customer failed to adhere to least privilege
- The provider failed to deploy critical security services in all regions.



Chris Farris (@jcfarris@infosec.exchange) @jcfarris · Dec 12, 2018

Replying to @andrewkrug and @gene_wood

Except - "GuardDuty is not available in EU (**Stockholm**). Please select another region."



Chris Farris (@jcfarris@infosec.exchange) @jcfarris · Jan 25, 2019

PSA for all my cloud hacking peeps in Russia, North Korea and China - GuardDuty still isn't available in **Stockholm**, so best to hit the API endpoints in that region

What changed for threat actors

- They learned how to use cloud
- They learned how to make money using the cloud
- Nation states entered the game

Cryptomining

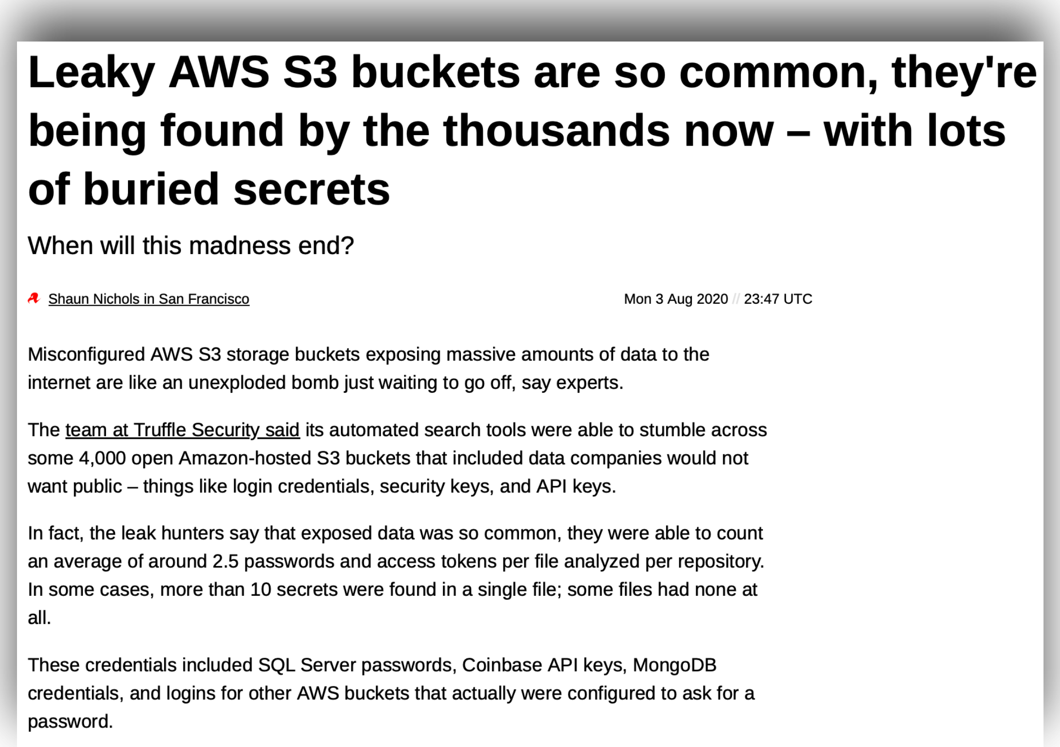
Spam/Phishing

Espionage

Ransomware

TA

What changed for customers



Leaky AWS S3 buckets are so common, they're being found by the thousands now – with lots of buried secrets

When will this madness end?

Shaun Nichols in San Francisco Mon 3 Aug 2020 // 23:47 UTC

Misconfigured AWS S3 storage buckets exposing massive amounts of data to the internet are like an unexploded bomb just waiting to go off, say experts.

The team at Truffle Security said its automated search tools were able to stumble across some 4,000 open Amazon-hosted S3 buckets that included data companies would not want public – things like login credentials, security keys, and API keys.

In fact, the leak hunters say that exposed data was so common, they were able to count an average of around 2.5 passwords and access tokens per file analyzed per repository. In some cases, more than 10 secrets were found in a single file; some files had none at all.

These credentials included SQL Server passwords, Coinbase API keys, MongoDB credentials, and logins for other AWS buckets that actually were configured to ask for a password.

- More cloud and more clouds
- Production workloads
- Better defensive tooling
- Compliance, standards, and models
- Islands of expertise
- Headlines

Threat actors use which initial access method most often?

Lost/leaked access keys/credentials

#4

66%

valid IAM credentials

↑

1/3

of those are **root credentials**

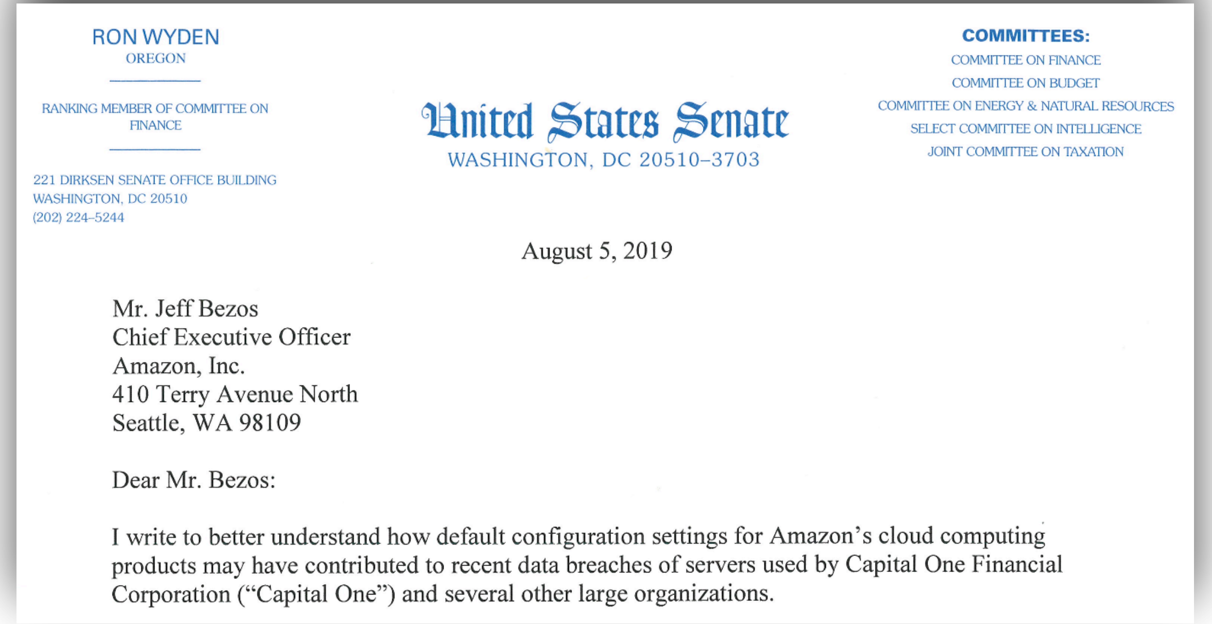
[20% of all initial access method use]

13%

Public-facing EC2 instance

What changed for governments… the first spark

- Cloud became critical infrastructure
- Ergo, more breaches
- Hearings (but little action)
- Standards, but little regulation outside of gov use itself



RON WYDEN
OREGON

RANKING MEMBER OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

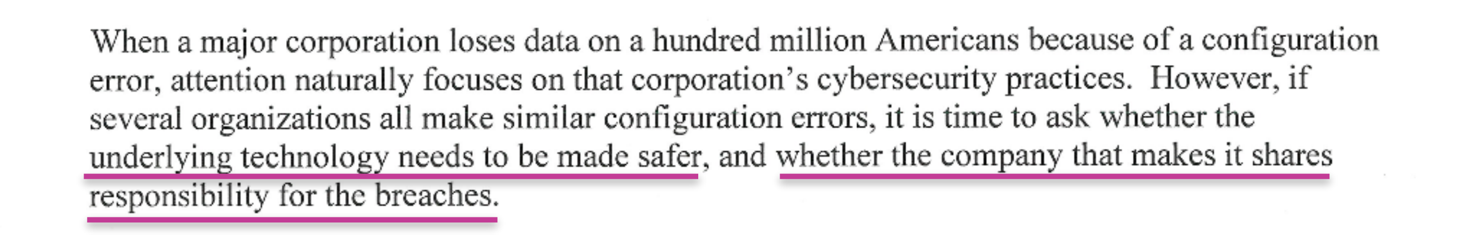
COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON BUDGET
COMMITTEE ON ENERGY & NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

August 5, 2019

Mr. Jeff Bezos
Chief Executive Officer
Amazon, Inc.
410 Terry Avenue North
Seattle, WA 98109

Dear Mr. Bezos:

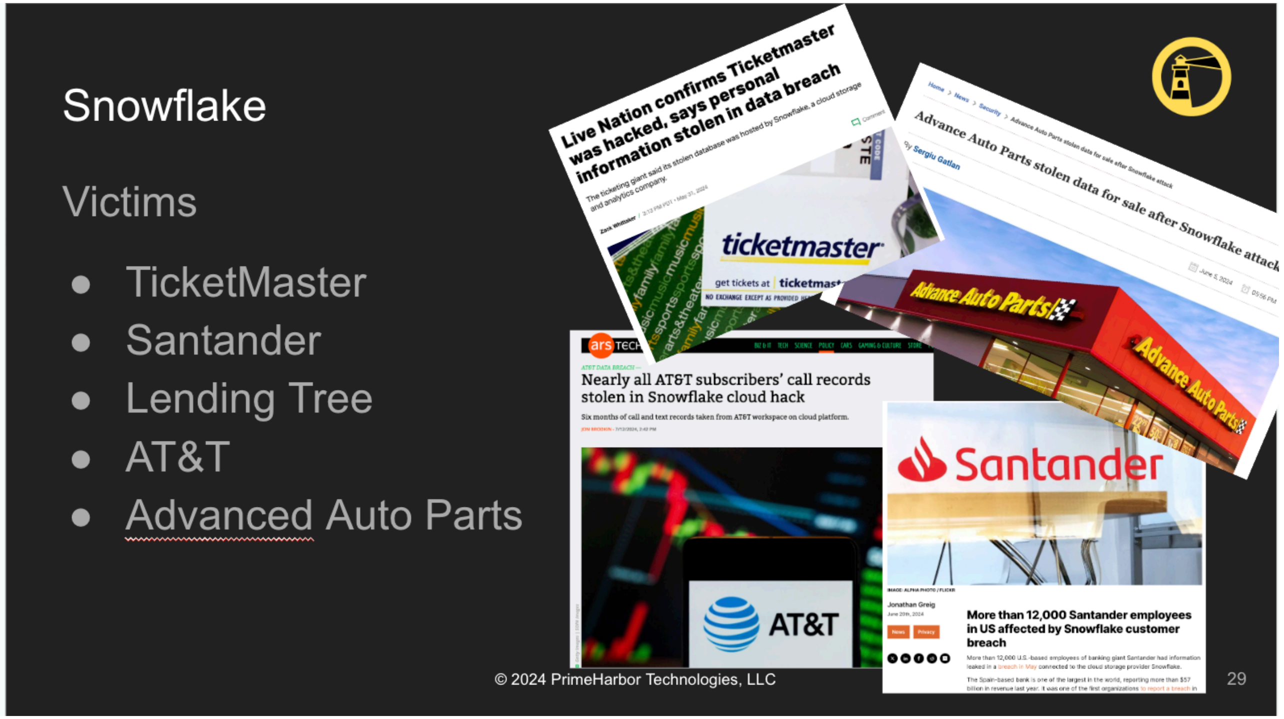
I write to better understand how default configuration settings for Amazon's cloud computing products may have contributed to recent data breaches of servers used by Capital One Financial Corporation ("Capital One") and several other large organizations.



When a major corporation loses data on a hundred million Americans because of a configuration error, attention naturally focuses on that corporation's cybersecurity practices. However, if several organizations all make similar configuration errors, it is time to ask whether the underlying technology needs to be made safer, and whether the company that makes it shares responsibility for the breaches.

GOV

Dawn of the Shared Irresponsibilities Model



Snowflake

Victims

- TicketMaster
- Santander
- Lending Tree
- AT&T
- Advanced Auto Parts

Live Nation confirms Ticketmaster was hacked, says personal information stolen in data breach

The ticketing giant said its stolen database was hosted by Snowflake, a cloud storage and analytics company.

Zack Whittaker / 3:13 PM PDT • May 31, 2024

Home > News > Security > Advance Auto Parts stolen data for sale after Snowflake attack

Advance Auto Parts stolen data for sale after Snowflake attack

By Sergiu Gatlan

June 5, 2024 05:56 PM

AT&T DATA BREACH —

Nearly all AT&T subscribers' call records stolen in Snowflake cloud hack

Six months of call and text records taken from AT&T workspace on cloud platform.

JON BRODKIN - 7/12/2024, 2:42 PM

IMAGE: ALPHA PHOTO / FLICKR

Jonathan Greig

June 20th, 2024

More than 12,000 Santander employees in US affected by Snowflake customer breach

More than 12,000 U.S.-based employees of banking giant Santander had information leaked in a breach in May connected to the cloud storage provider Snowflake.

The Spain-based bank is one of the largest in the world, reporting more than $57 billion in revenue last year. It was one of the first organizations to report a breach in

29

> Cloud providers will be considered partially responsible for any customer breach involving their services, even if the breach was due to customer misconfiguration.
>
> - Rich Mogull, Securosis

https://securosis.com/cloud/the-cloud-shared-irresponsibilities-model/

What changed for cloud providers

CYBER SAFETY REVIEW BOARD

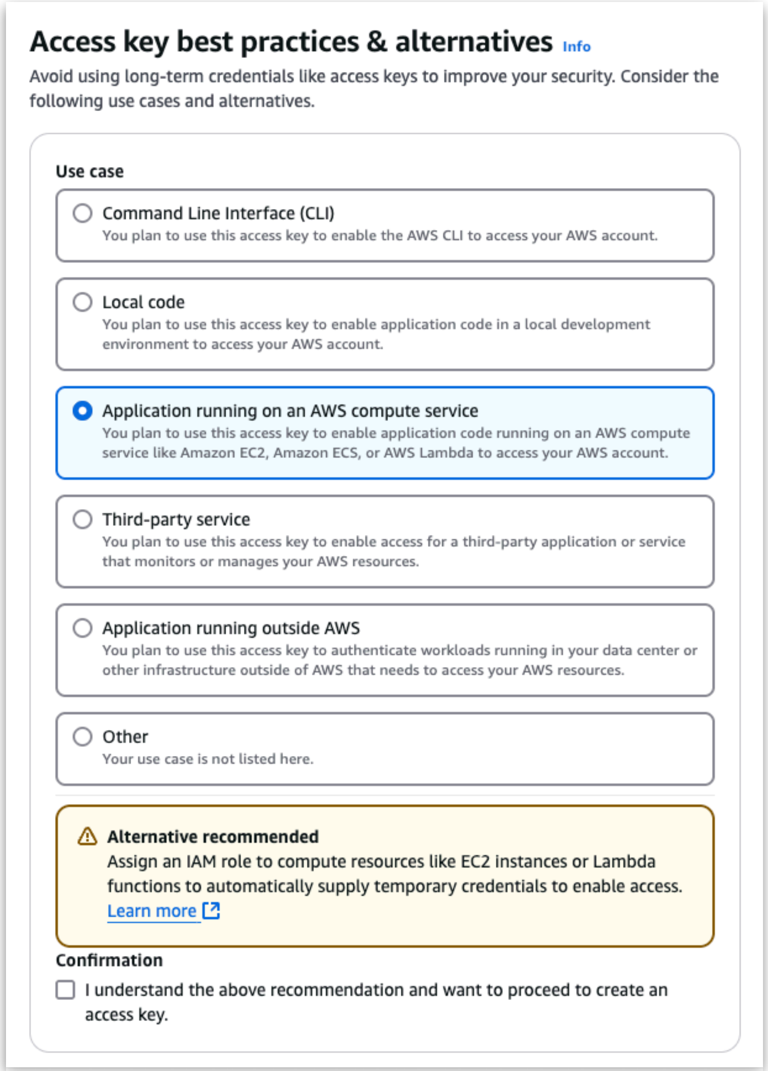
"The Board identified a series of Microsoft operational and strategic decisions that collectively point to a corporate culture that deprioritized both enterprise security investments and rigorous risk management."

– Cyber Safety Review Board
March, 2024

CSP

Attempts were made

- Cloud Providers started to realize they were getting blamed for their customers
  - Also increasing support costs
  - Also increasing fraud credits
- Some attempts were made to solve this for the lowest common denominator.
- *Customers migrated to IaC, where these warnings **don't exist**.*



Access key best practices & alternatives

Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

○ Command Line Interface (CLI)
You plan to use this access key to enable the AWS CLI to access your AWS account.

○ Local code
You plan to use this access key to enable application code in a local development environment to access your AWS account.

● Application running on an AWS compute service
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

○ Third-party service
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

○ Application running outside AWS
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

○ Other
Your use case is not listed here.

⚠ **Alternative recommended**
Assign an IAM role to compute resources like EC2 instances or Lambda functions to automatically supply temporary credentials to enable access.
Learn more

Confirmation

□ I understand the above recommendation and want to proceed to create an access key.

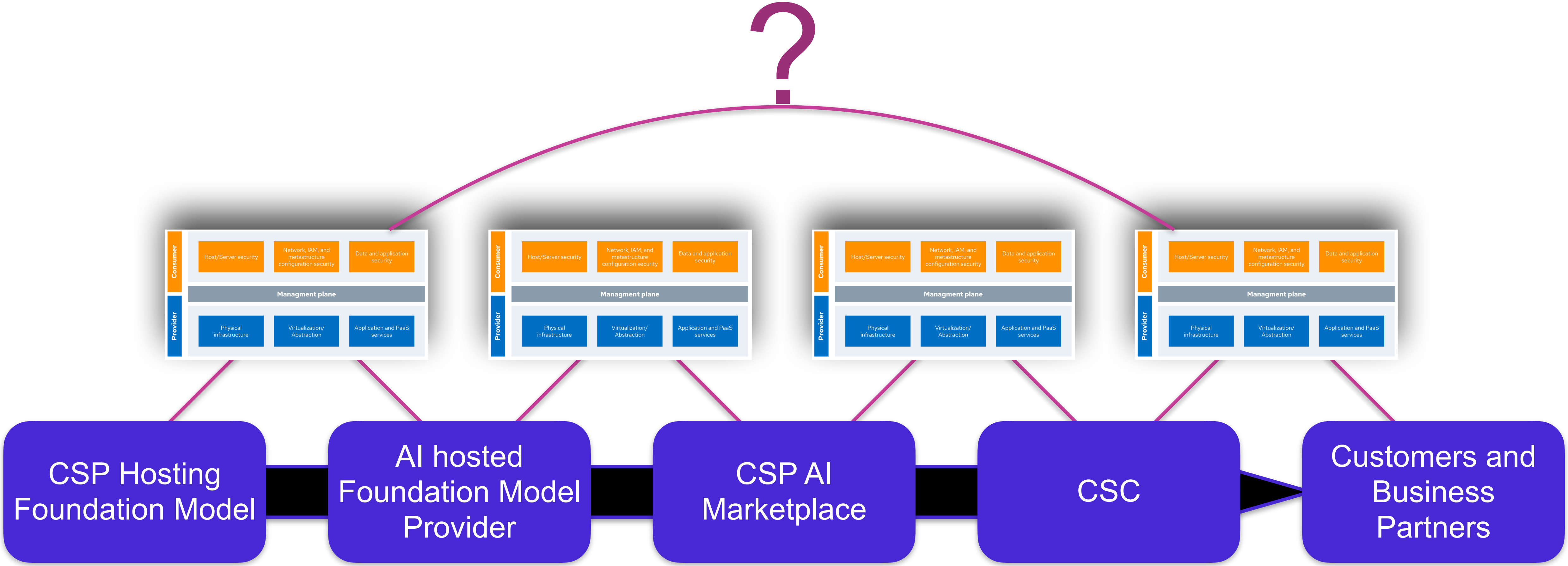
RSAC 2025 Conference

Late Stage Cloud (The Find Out Phase)

2025 and Beyond (Okay, until Thursday)

Many Voices.
One Community.

Shared Responsibilities now extends across the Software Supply Chain: AI and Marketplaces


?
Consumer
Host/Server security
Network, IAM, and metastructure configuration security
Data and application security
Managment plane
Provider
Physical infrastructure
Virtualization/ Abstraction
Application and PaaS services
Consumer
Host/Server security
Network, IAM, and metastructure configuration security
Data and application security
Managment plane
Provider
Physical infrastructure
Virtualization/ Abstraction
Application and PaaS services
Consumer
Host/Server security
Network, IAM, and metastructure configuration security
Data and application security
Managment plane
Provider
Physical infrastructure
Virtualization/ Abstraction
Application and PaaS services
Consumer
Host/Server security
Network, IAM, and metastructure configuration security
Data and application security
Managment plane
Provider
Physical infrastructure
Virtualization/ Abstraction
Application and PaaS services

CSP Hosting Foundation Model

AI hosted Foundation Model Provider

CSP AI Marketplace

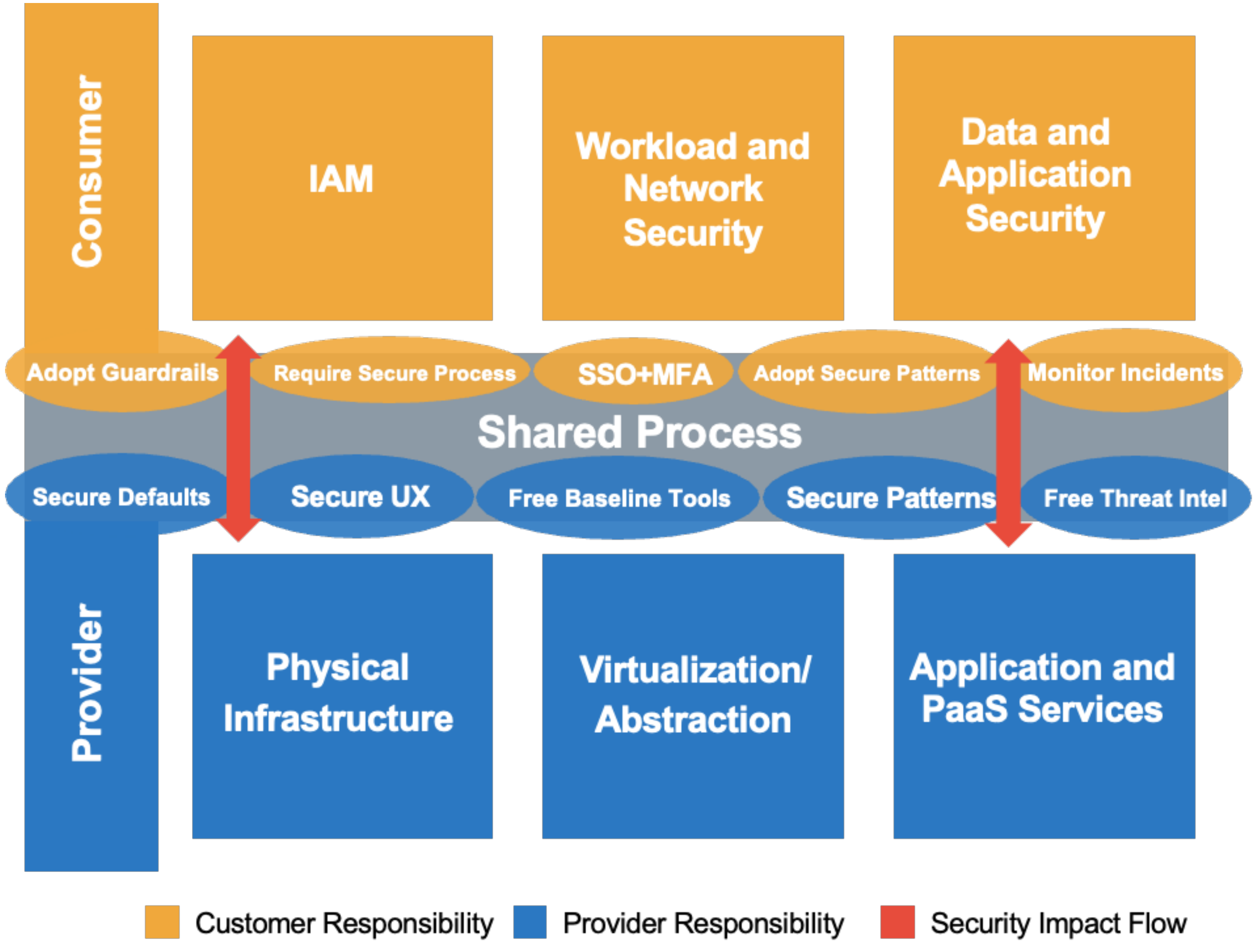
CSC

Customers and Business Partners

Shared Fate

- Shared responsibilities defines who in the relationship is responsible for which aspects of security based on technology.
  - SRM draws a dividing line
- Shared fate defines an evolving, bidirectional relationship for security success based on *process*.
  - Both sides have responsibilities
  - But it is a relationship of security processes, not lines drawn around technology
  - (Google is the first to publish on Shared Fate… our work is a different/related perspective using the same term: https://cloud.google.com/architecture/framework/security/shared-responsibility-shared-fate)

The Shared Fate Model (Shared Responsibilities 2.0)



Consumer

IAM

Workload and Network Security

Data and Application Security

Adopt Guardrails

Require Secure Process

SSO+MFA

Adopt Secure Patterns

Monitor Incidents

Shared Process

Secure Defaults

Secure UX

Free Baseline Tools

Secure Patterns

Free Threat Intel

Provider

Physical Infrastructure

Virtualization/ Abstraction

Application and PaaS Services

🟧 Customer Responsibility 🟦 Provider Responsibility 🟥 Security Impact Flow

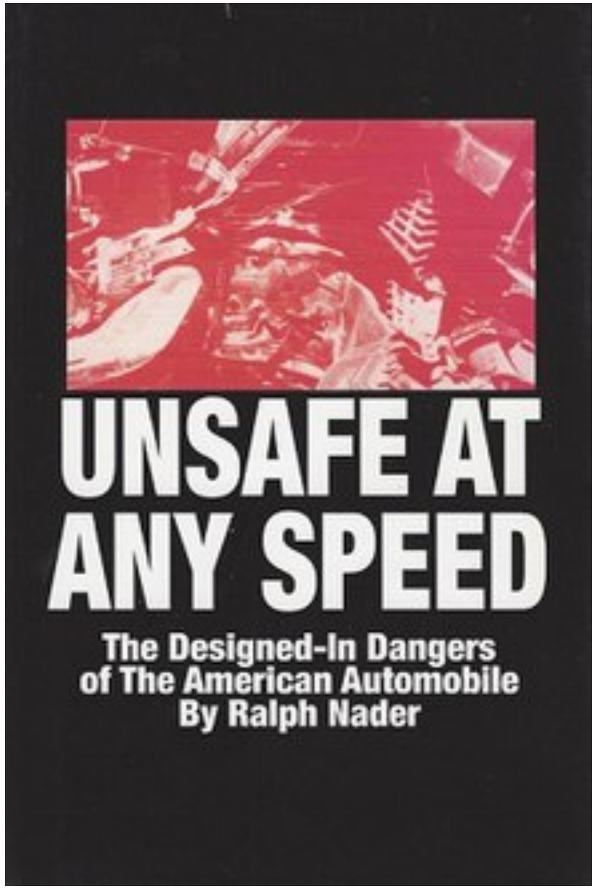
- **Secure process support, not just secure services**
- Services and UX secure by default
- Baseline security the simple path
  - Supported with patterns
  - CSPs are opinionated
- Required flags for risky API calls
  - Clearer warnings logged by default
- Free security tooling automatically enabled for the most common actively exploited issues
  - Adapted over time

What Threat Actors need to do

- Customer's are getting better at this - even if some providers aren't
- Traditional methods of monetization aren't there
  - Extortion is pretty much the main one
- It's harder to hide in the cloud plane
  - Unless your targets can't afford E5 licenses
- More customers are using cloud to control ICS/OT

What Government needs to do

- Public Cloud is more entwined in core functions than ever before.
- Government *should* put pressure on the CSPs
  - DORA is a start, but only for a specific industry
- Government should pressure on CSCs
  - NIS2 in Europe is a good example. *Requires MFA and maturity assessments!*
  - *The FTC was starting to hold companies accountable for ignoring security, but now…*
- Digital Sovereignty becoming more important
  - Invest in your own destiny

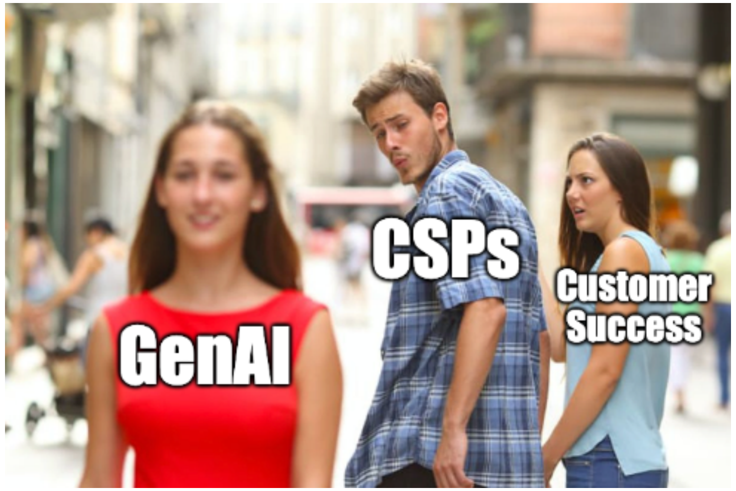


What CSPs need to do

- The CSRB Report on STORM-0558 highlighted some of them
  - Stop hiding security behind paywalls
  - CSPs should report all incidents, and commit to disclosing CVEs
- CSPs need to help their customers
  - Concise documentation
  - Implement **safeguards** in Console and APIs
  - Consider how customers (of all sizes) will use or misuse features

What Customers need to do

- You have the power
  - Government won't help you
  - Cyberinsurance may force you
- CSPs are focused on bottom line, lost the plot
- You can vote with your dollars and feet
  - 85% of workloads are still on-prem
  - Even without government pressure, the internet is not getting safer
- You are responsible for your half of Shared Fate



Either we all Win

Or we all lose

RSAC 2025 Conference

Many Voices.
One Community.

Rich Mogull
@rmogull@defcon.social
@rmogull.com
https://securosis.com

Chris Farris
@jcfarris@infosec.exchange
jcfarris.bsky.social
https://primeharbor.com