CyberCamp 2018

Cloud Security

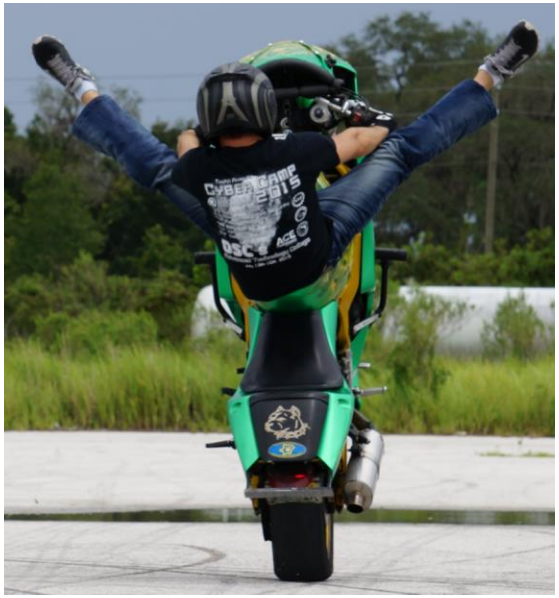
Ricky Payne CISSP, RHCE, RHCSA, Security+ , BS-IST, AS-CET

About Me

- Over 12 years of progressive DevSecOps experience from Intern to CSO
- Built "Gold Standard" federal security programs that produced 10+ federally certified systems.
- Expert generalist: from pre-sales proposal work, policy and reference architecture development, requirements decomposition into agile sprints, proof of concepts, implementation, operations, and technical training to incident response.

- Mentored/taught Windows and Linux security at CyberPatriot/CyberCamps since 2013. Accomplishments include 1st and 2nd in State and 1st in Regionals.

- As a CSO for a federal SaaS, leads end-to-end Security, Privacy, and Operations for a FedRAMP Moderate (325 NIST 800-53r4 security controls) authorized SaaS hosted in AWS GovCloud.

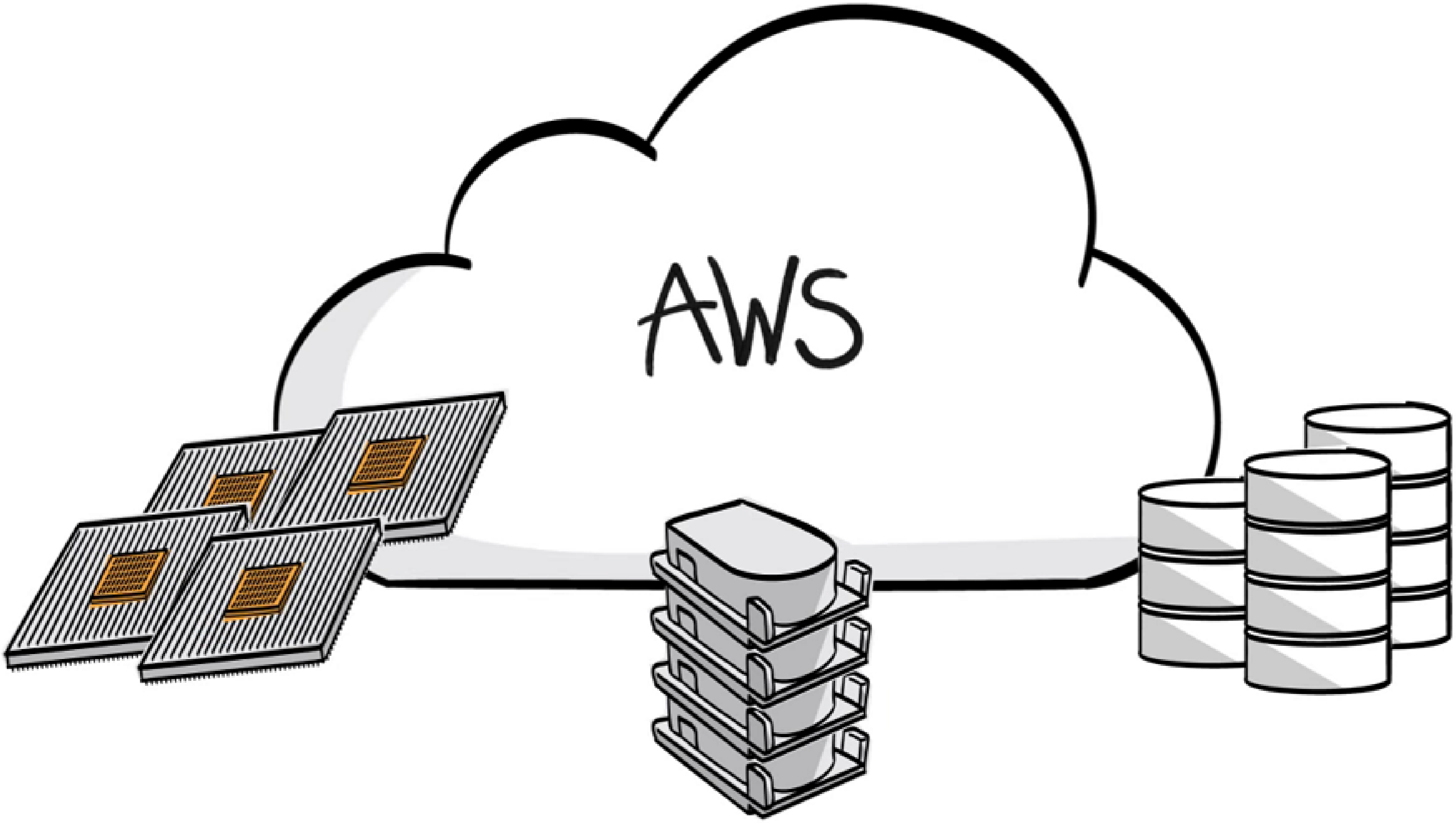


Ricky Payne
CISSP, RHCE, RHCSA
Security+, BS-IST, AS-CET
grep.rickp@gmail.com
@RickPayne929

Agenda

- What is the cloud?
- Who uses it?
- Who owns what? “Shared Responsibility Model”
- Cloud Breach - Uber
- Cloud Denial of Service (DoS) – AWS S3
- Cloud Insider Threat
- Cloud Security Framework parallels
- Demo?

What is “the cloud”?

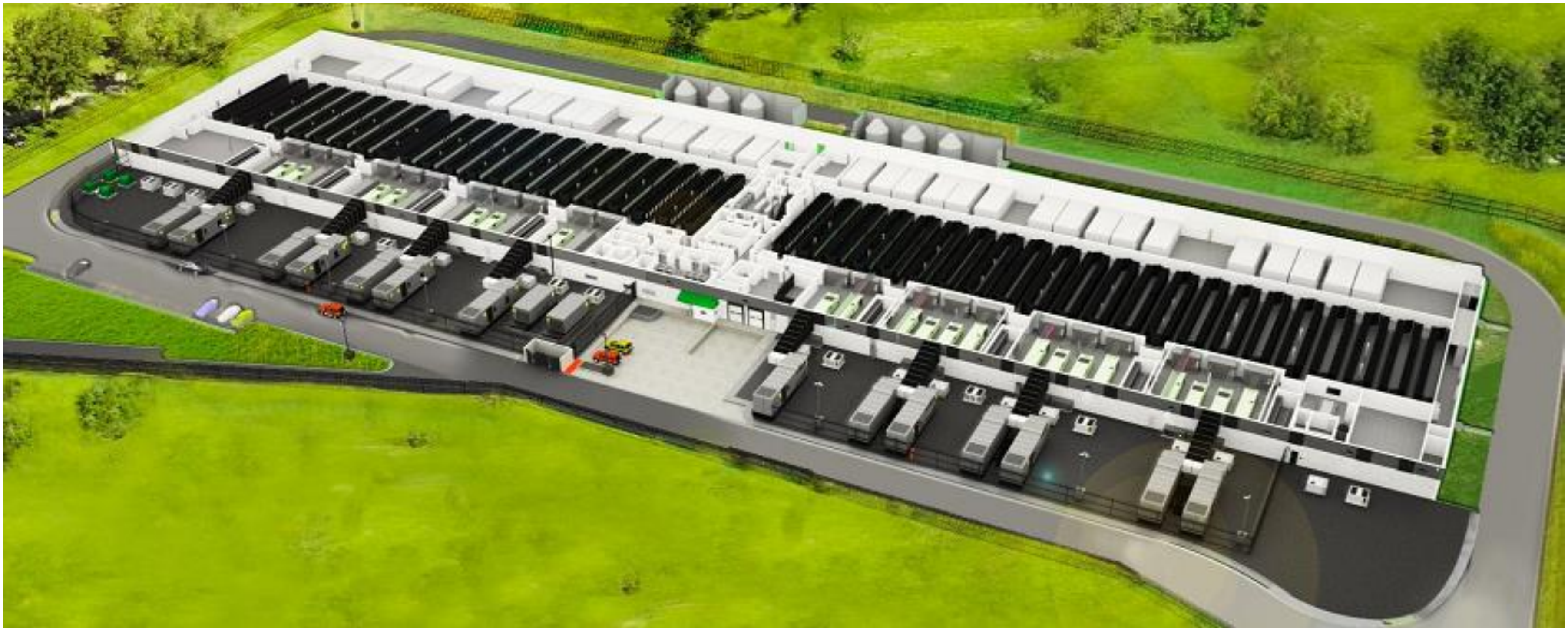


What is “the cloud”?

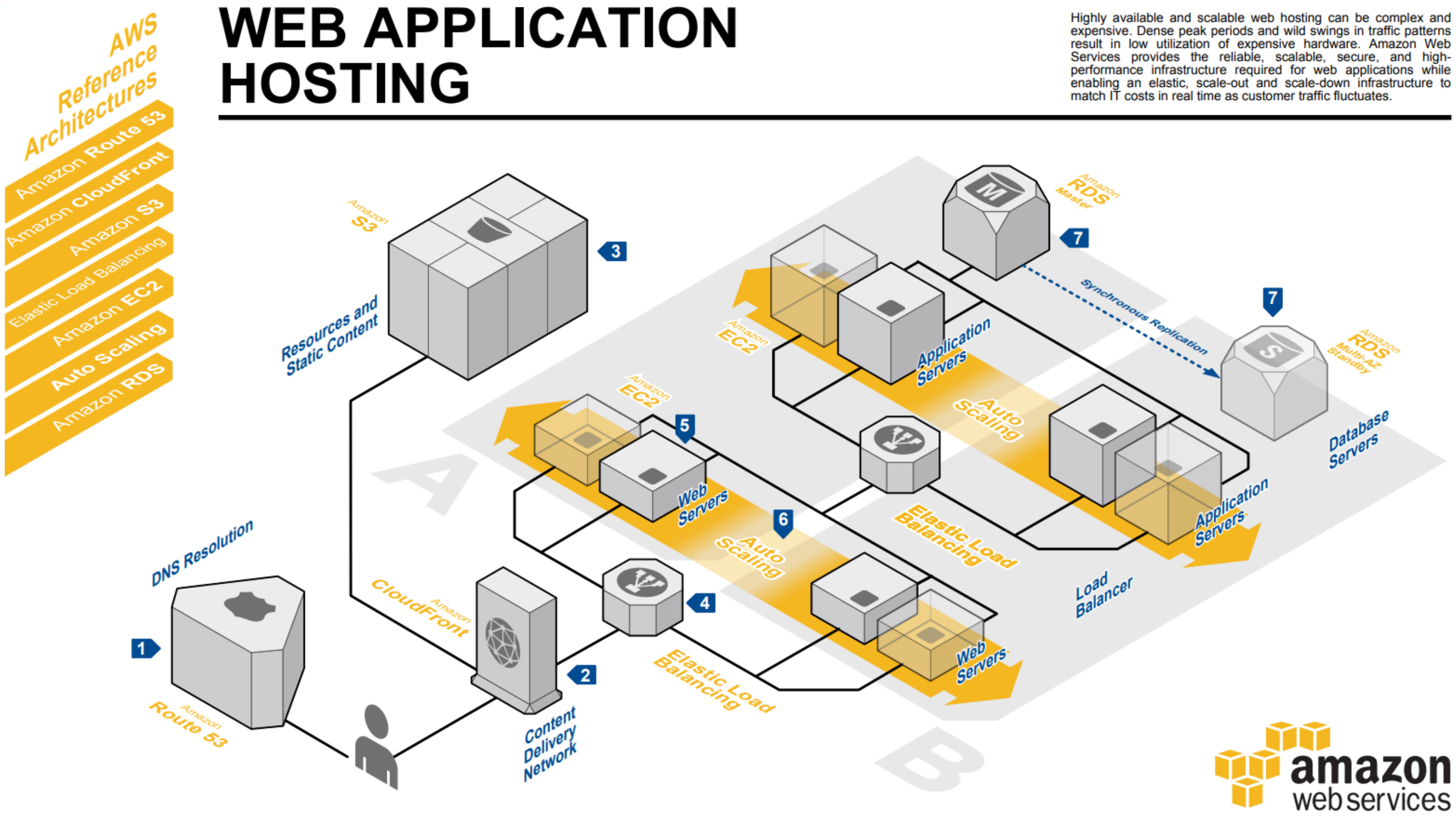
- Cloud computing is the on-demand delivery of compute power, database storage, applications, and other IT resources through a cloud services platform via the internet with pay-as-you-go pricing.[1]
- Cloud computing provides a simple way to access servers, storage, databases and a broad set of application services over the Internet.[1]

What is “the cloud”?

AWS Data Center[2]



What is “the cloud”?

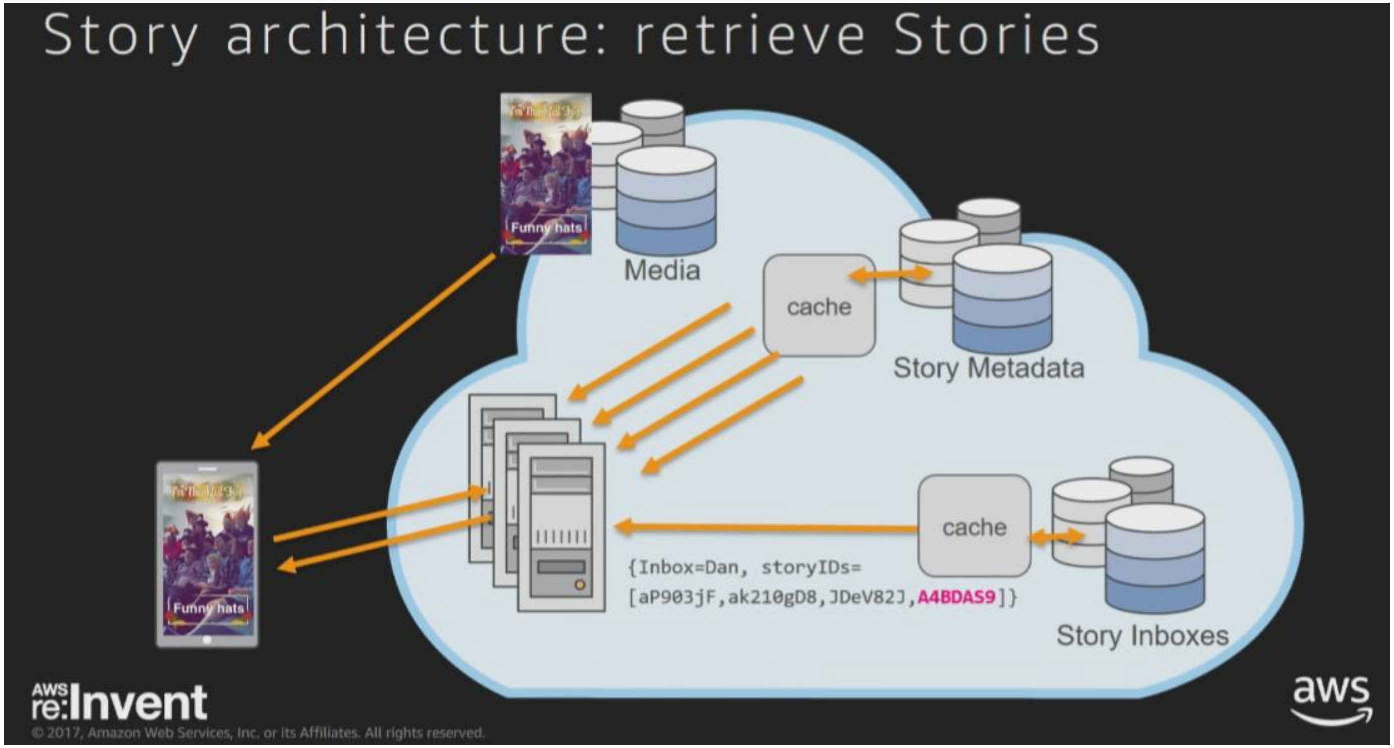


WEB APPLICATION HOSTING

Highly available and scalable web hosting can be complex and expensive. Dense peak periods and wild swings in traffic patterns result in low utilization of expensive hardware. Amazon Web Services provides the reliable, scalable, secure, and high-performance infrastructure required for web applications while enabling an elastic, scale-out and scale-down infrastructure to match IT costs in real time as customer traffic fluctuates.

Who uses it?

- Snapchat Stories[9]

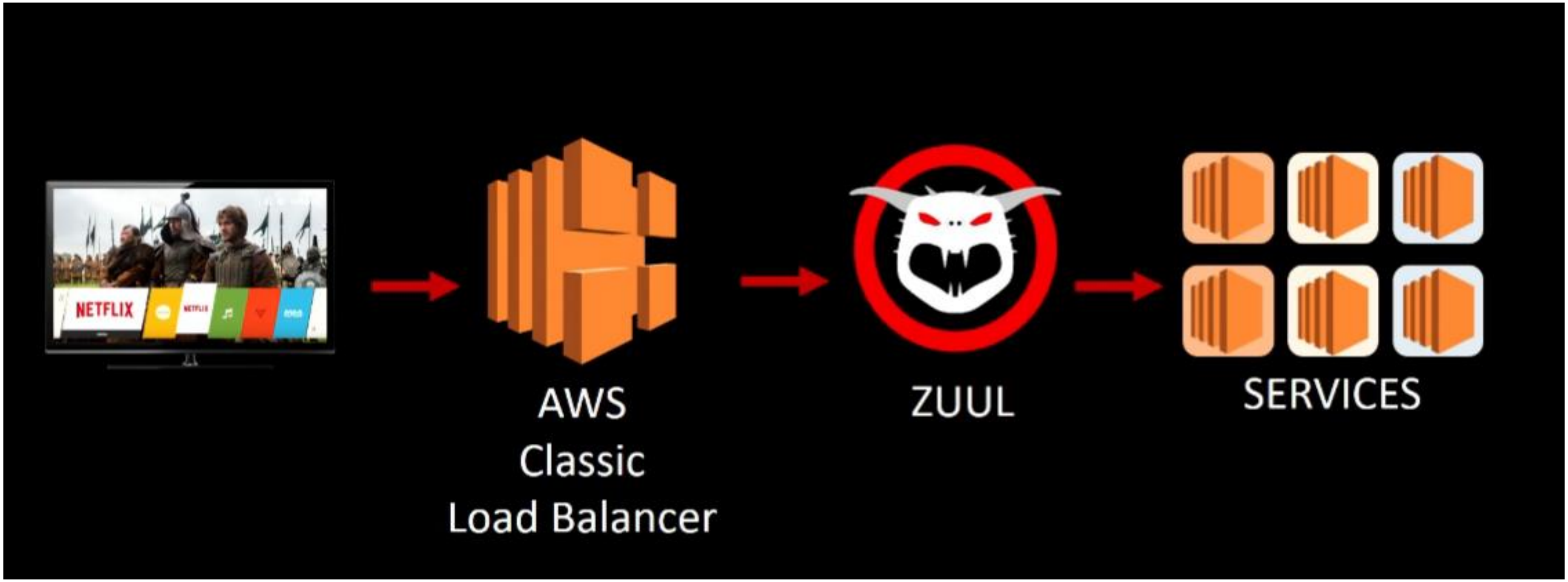


Story architecture: retrieve Stories

{Inbox=Dan, storyIDs=
[aP903jF,ak210gD8,JDeV82J,A4BDAS9]}

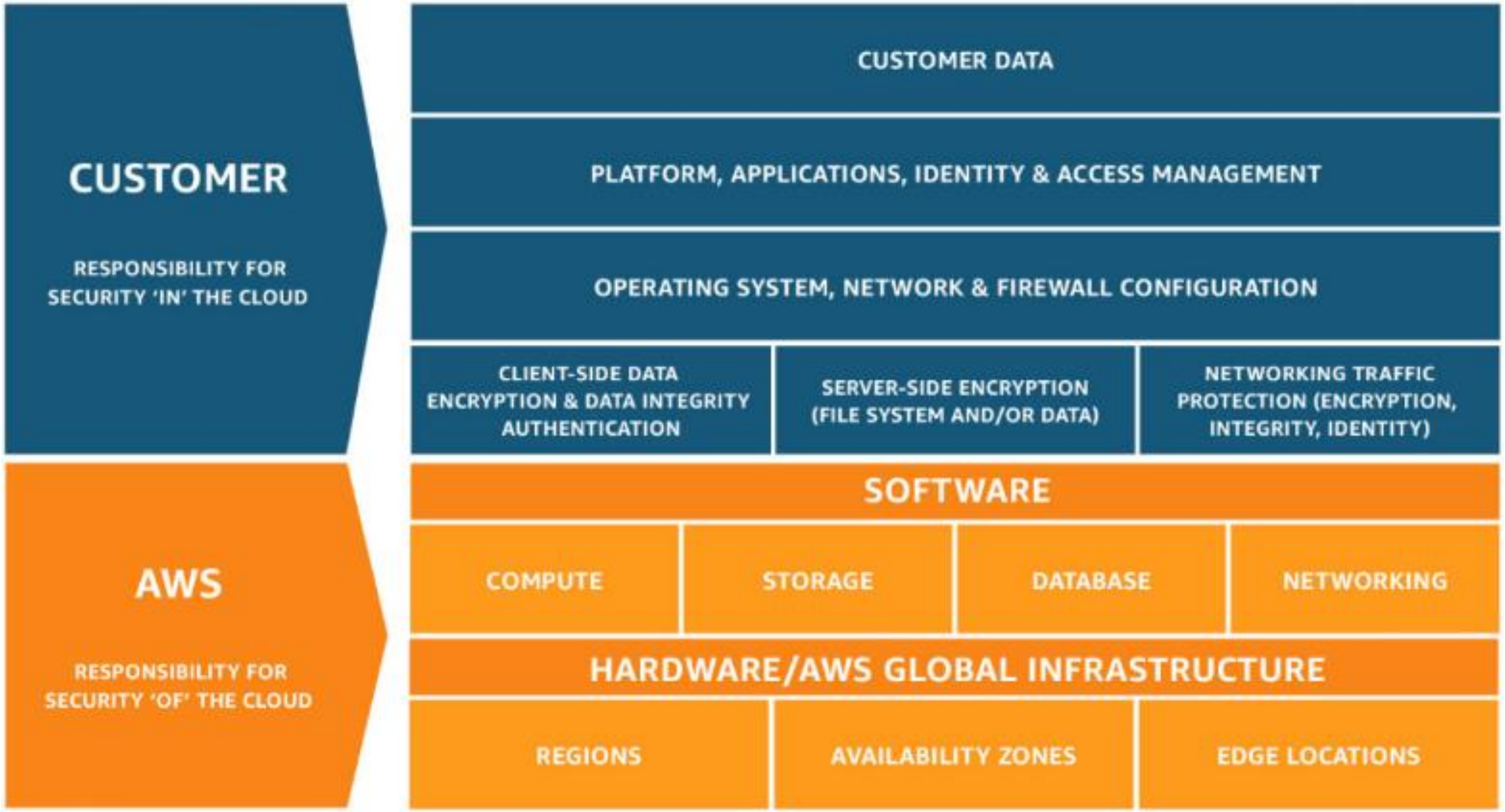
Who uses it?

- Netflix – 100,000 instances[3]



Who owns what?

- Cloud vs. Customer Shared Responsibility Model[4]



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

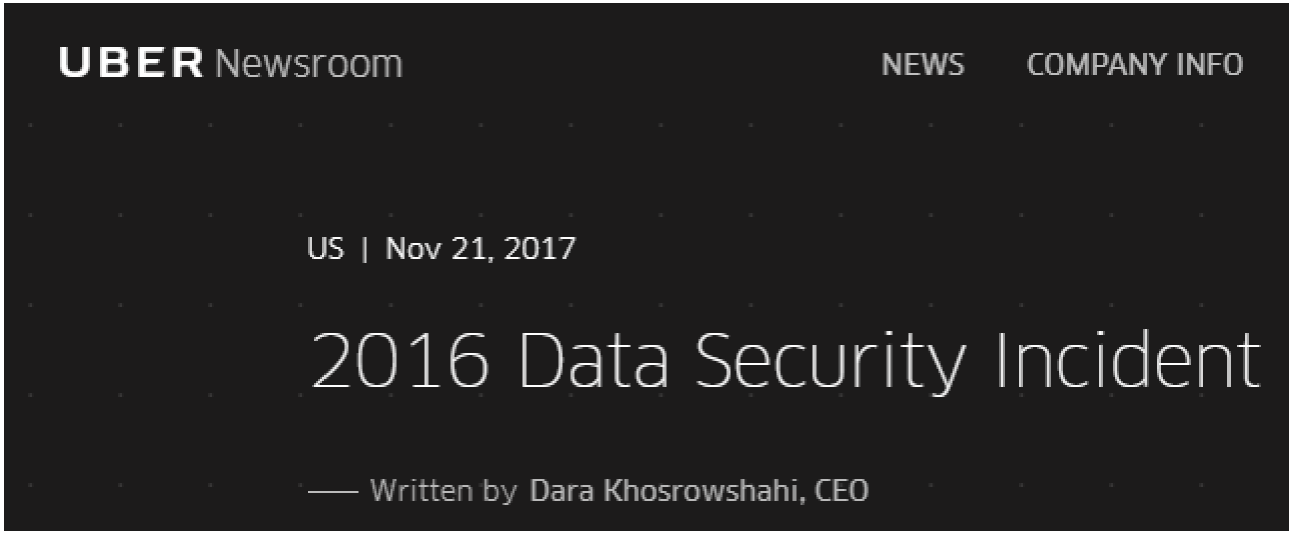
HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

EDGE LOCATIONS

Cloud Breach - Uber



UBER Newsroom

NEWS COMPANY INFO

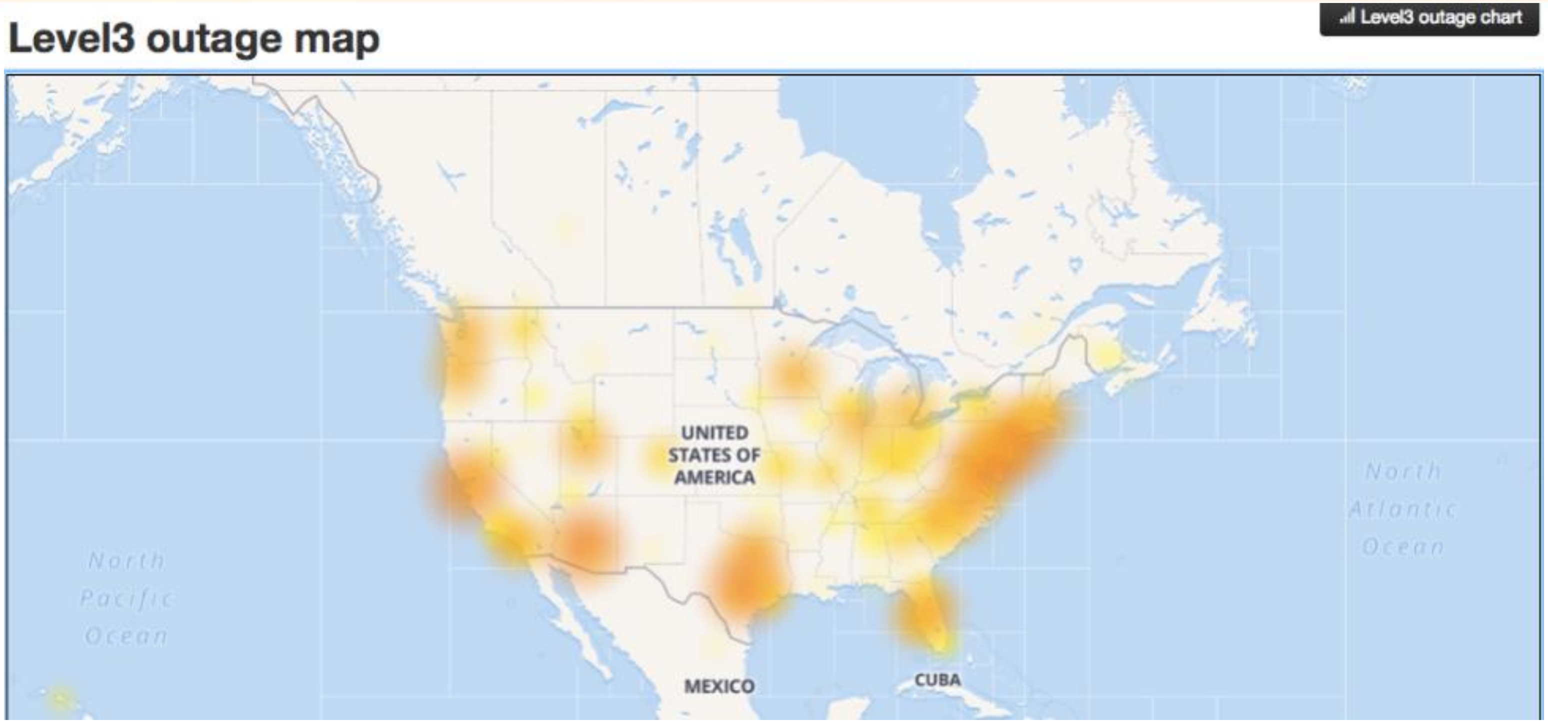
US | Nov 21, 2017

2016 Data Security Incident

—— Written by Dara Khosrowshahi, CEO

- Uber software engineers stored AWS login credentials in GitHub[5].

Cloud DoS – AWS S3



Level3 outage map

- Caused by AWS tech inputting a command parameter incorrectly.
- S3 outage disrupts many core AWS services.

Cloud Insider Threat

- Malicious vs. Unintentional?

Cloud Security Parallels

- Access Control - Account Management
- Auditing – Host vs Cloud
- Firewall – SG, NACL
- Identification and Authentication - Password Policy
- Least Functionality – Features, Services, Sharing
- Permissions – S3, IAM
- Patching – Application, System

Demo?

- Access Control - Account Management
- Auditing – Host vs Cloud
- Firewall – SG, NACL
- Identification and Authentication - Password Policy
- Least Functionality – Features, Services, Sharing
- Permissions – S3, IAM
- Patching – Application, System

What we learned…

- Cloud can take many shapes and sizes
- Ultimately renting computing resources
- Many large companies leverage cloud benefits
- You own security IN the cloud
- Unintentional insider threats
- Security IN the cloud conceptually parallels standard practices

References

1. What is Cloud Computing? AWS. Retrieved on July 17, 2018, from https://aws.amazon.com/what-is-cloud-computing/
2. Our Data Centers. AWS. Retrieved on July 17, 2018, from https://aws.amazon.com/compliance/data-center/controls/
3. A Day in the Life of a Netflix Engineer III (ARC209). https://www.youtube.com/watch?v=T_D1G42G0dE
4. Shared Responsibility Model. AWS. Retrieved on July 10, 2018, from https://aws.amazon.com/compliance/shared-responsibility-model/
5. Uber Paid Hackers to Delete Stolen Data on 57 Million People. Bloomberg. Retrieved on July 17, 2018, from https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

References

6. Summary of the Amazon S3 Service Disruption in the Northern Virginia (US-EAST-1) Region. AWS. Retrieved on July 17, 2018, from https://aws.amazon.com/message/41926/
7. Amazon Just Broke the Internet. Gizmodo. Retrieved on July 17, 2018, from https://gizmodo.com/amazon-just-broke-the-internet-1792827856
8. The Early Indicators of an Insider Threat. DigitalGuardian. Retrieved on July 17, 2018, from https://digitalguardian.com/blog/early-indicators-insider-threat
9. AWS re:Invent 2017: Snapchat Stories on Amazon DynamoDB (DAT325). Retrieved on July 17, 2018, from https://www.youtube.com/watch?v=WUleQzu9l_8