SID327

AWS re:INVENT

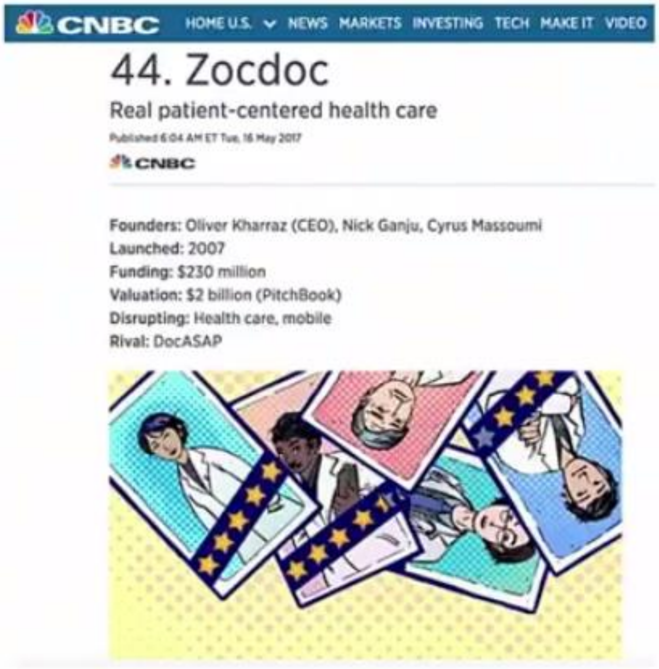
How Zocdoc Achieved Security and Compliance at Scale With Infrastructure as Code

Brian Lozada, CISO, Zocdoc, Inc
Zhen Wang, Head of Infrastructure, Zocdoc, Inc
Steve Boltuch, Sr Solutions Architect, AWS

November 30, 2017

re:Invent

aws



CNBC HOME U.S. NEWS MARKETS INVESTING TECH MAKE IT VIDEO

44. Zocdoc

Real patient-centered health care

Published 6:04 AM ET Tue, 16 May 2017

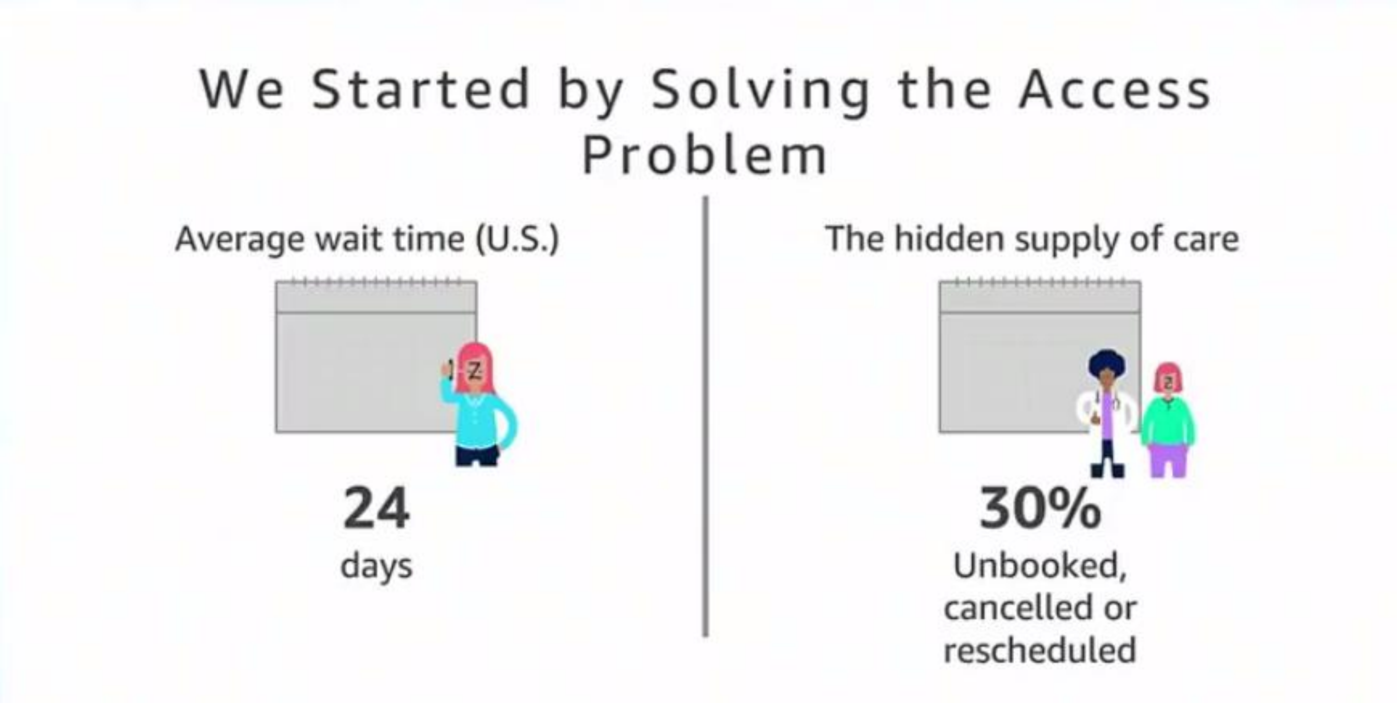
CNBC

Founders: Oliver Kharraz (CEO), Nick Ganju, Cyrus Massoumi
Launched: 2007
Funding: $230 million
Valuation: $2 billion (PitchBook)
Disrupting: Health care, mobile
Rival: DocASAP

*Courtesy CNBC

re:Invent

aws



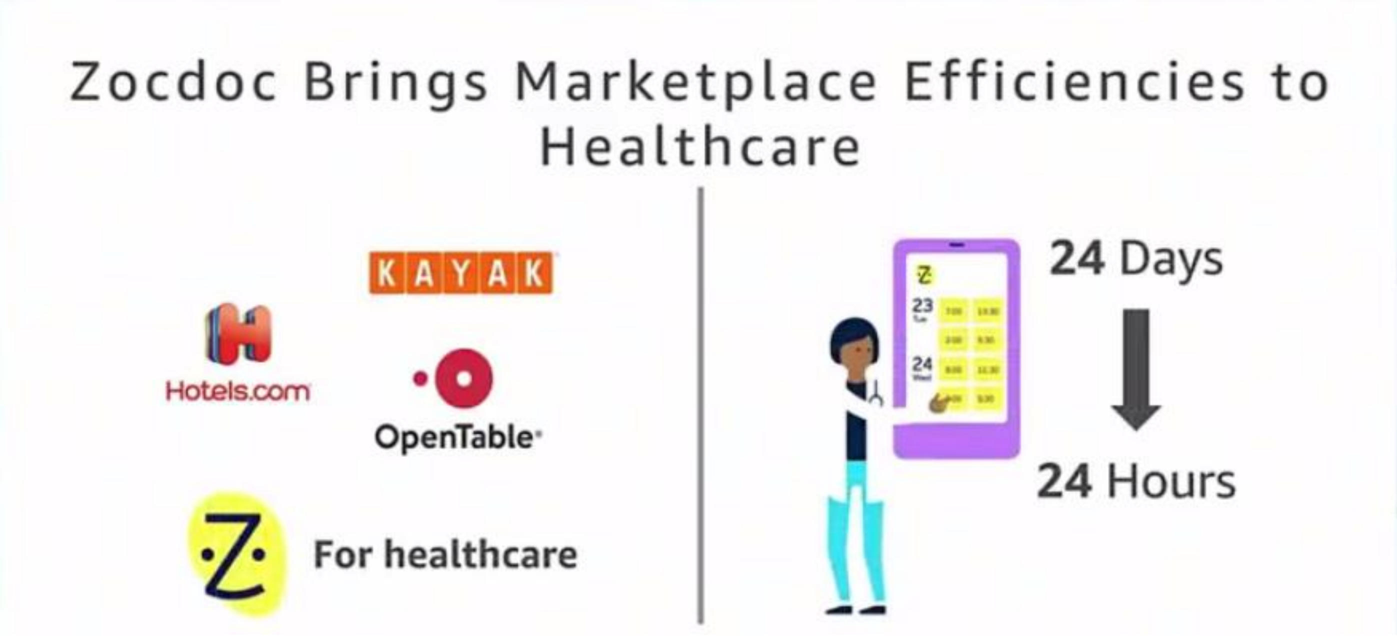
We Started by Solving the Access Problem

Average wait time (U.S.)

24
days

The hidden supply of care

30%
Unbooked, cancelled or rescheduled

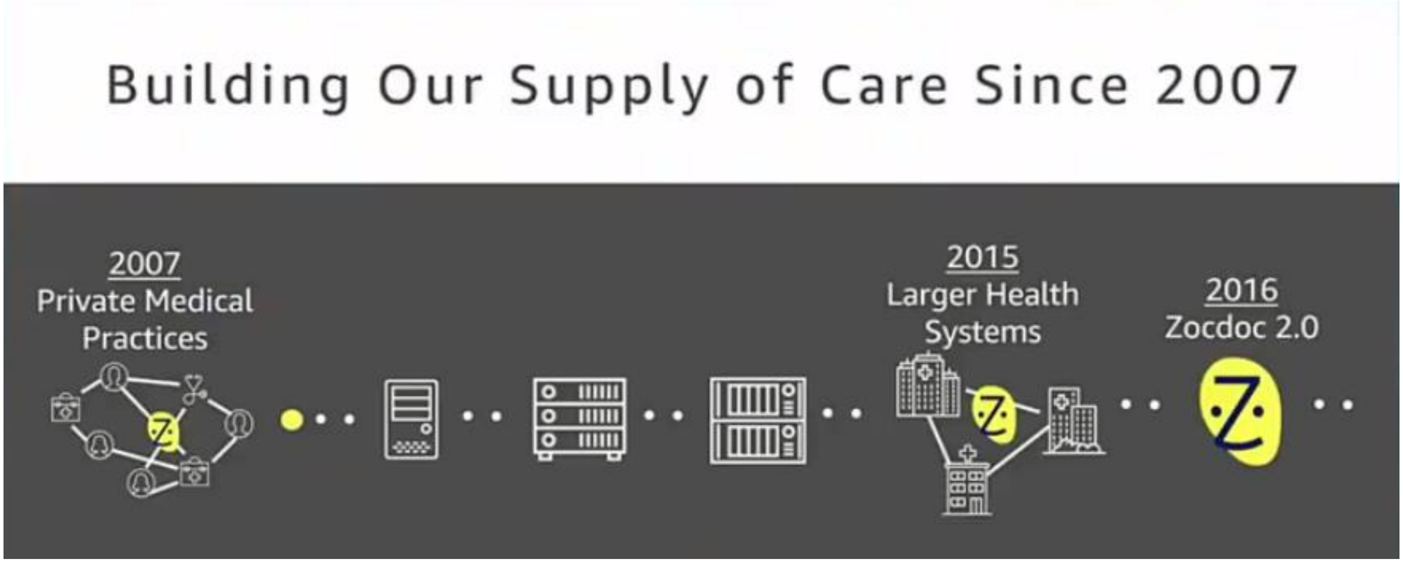


Zocdoc Brings Marketplace Efficiencies to Healthcare

For healthcare

24 Days

24 Hours



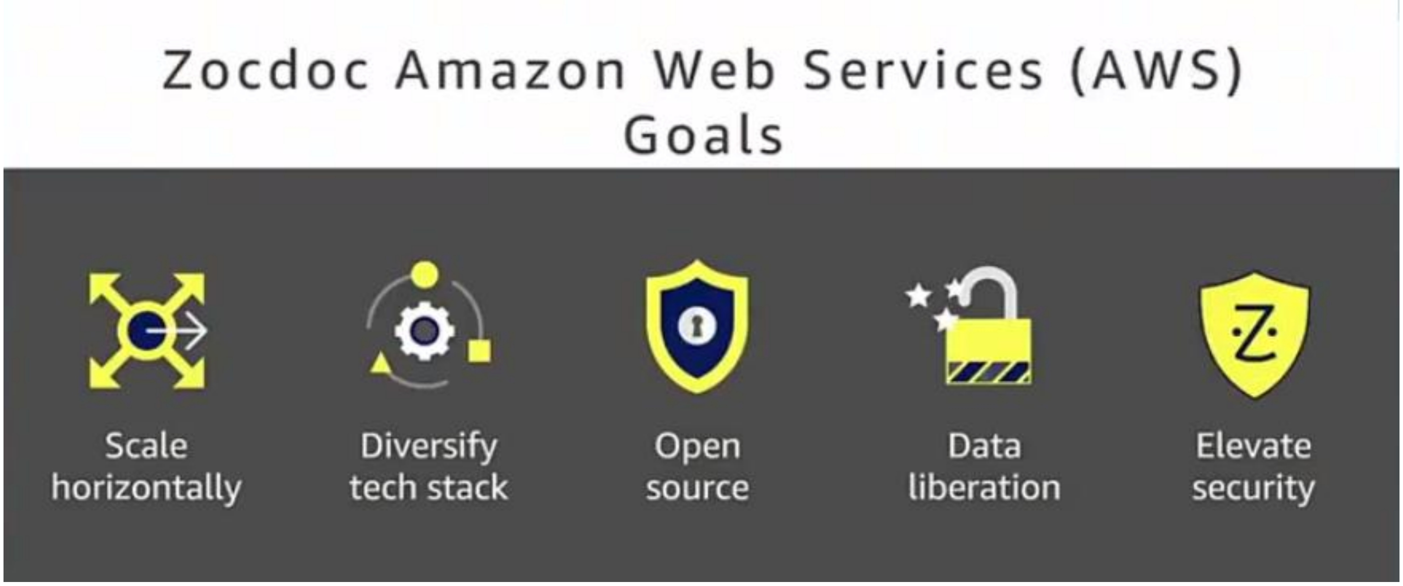
Building Our Supply of Care Since 2007

2007
Private Medical Practices

2015
Larger Health Systems

2016
Zocdoc 2.0

We started by going after local doctors and local practices, and we optimized our technology for that use case. But as we grew our architecture couldn’t handle all the load and we started partnering with large health systems that also wanted to bring more patients into the health systems.



Zocdoc Amazon Web Services (AWS) Goals

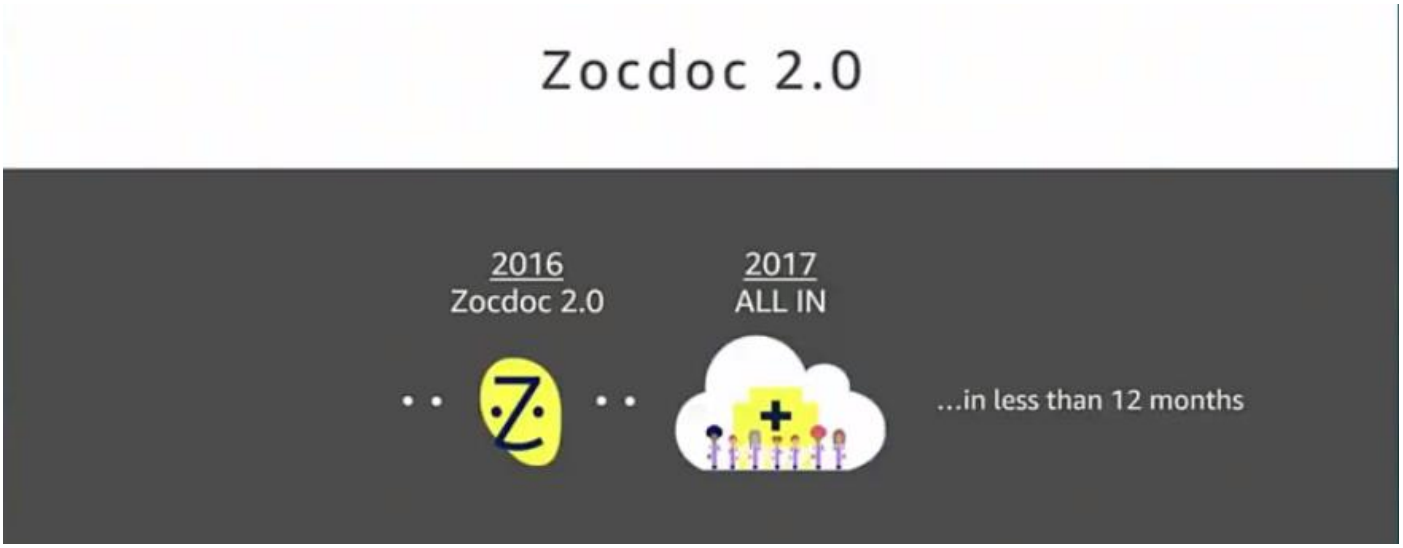
Scale horizontally

Diversify tech stack

Open source

Data liberation

Elevate security

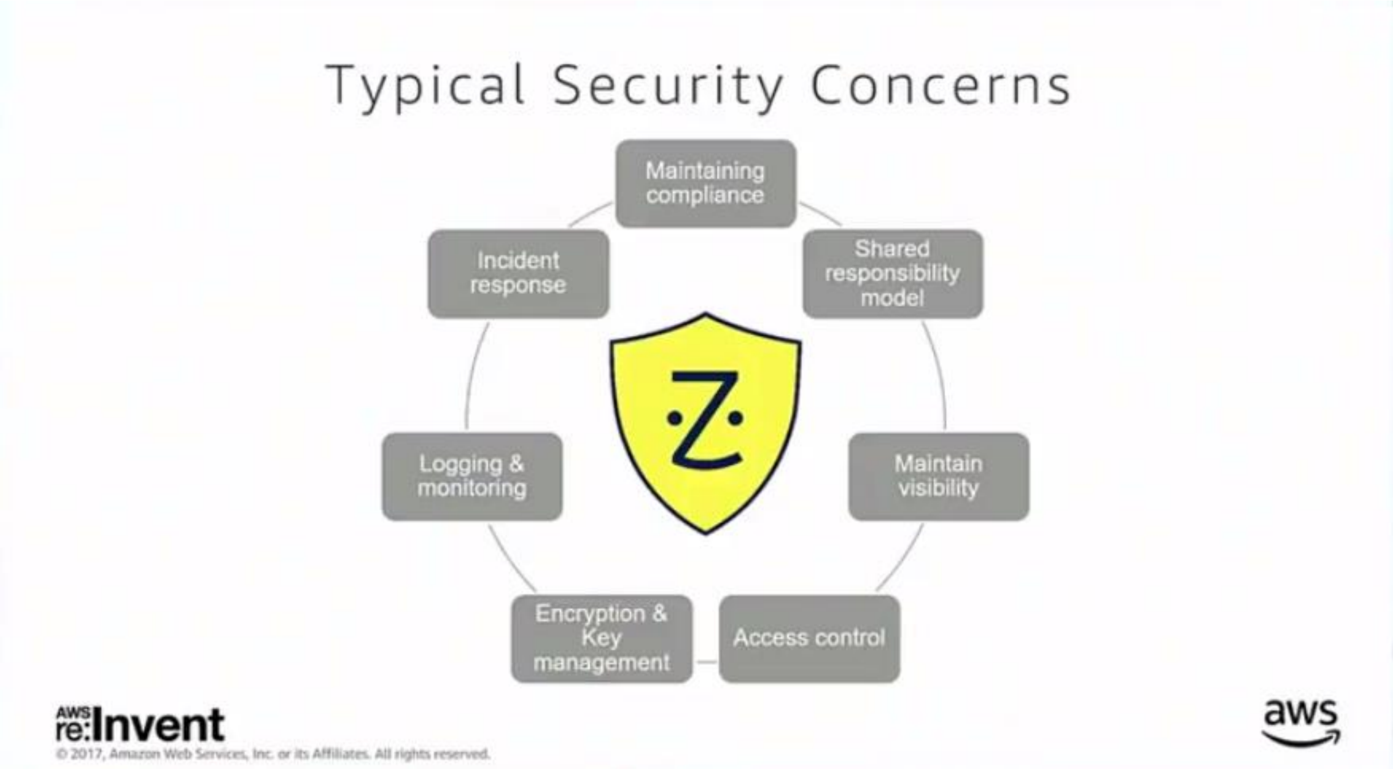


Zocdoc 2.0

2016
Zocdoc 2.0

2017
ALL IN

...in less than 12 months



Typical Security Concerns

Maintaining compliance

Shared responsibility model

Maintain visibility

Access control

Encryption & Key management

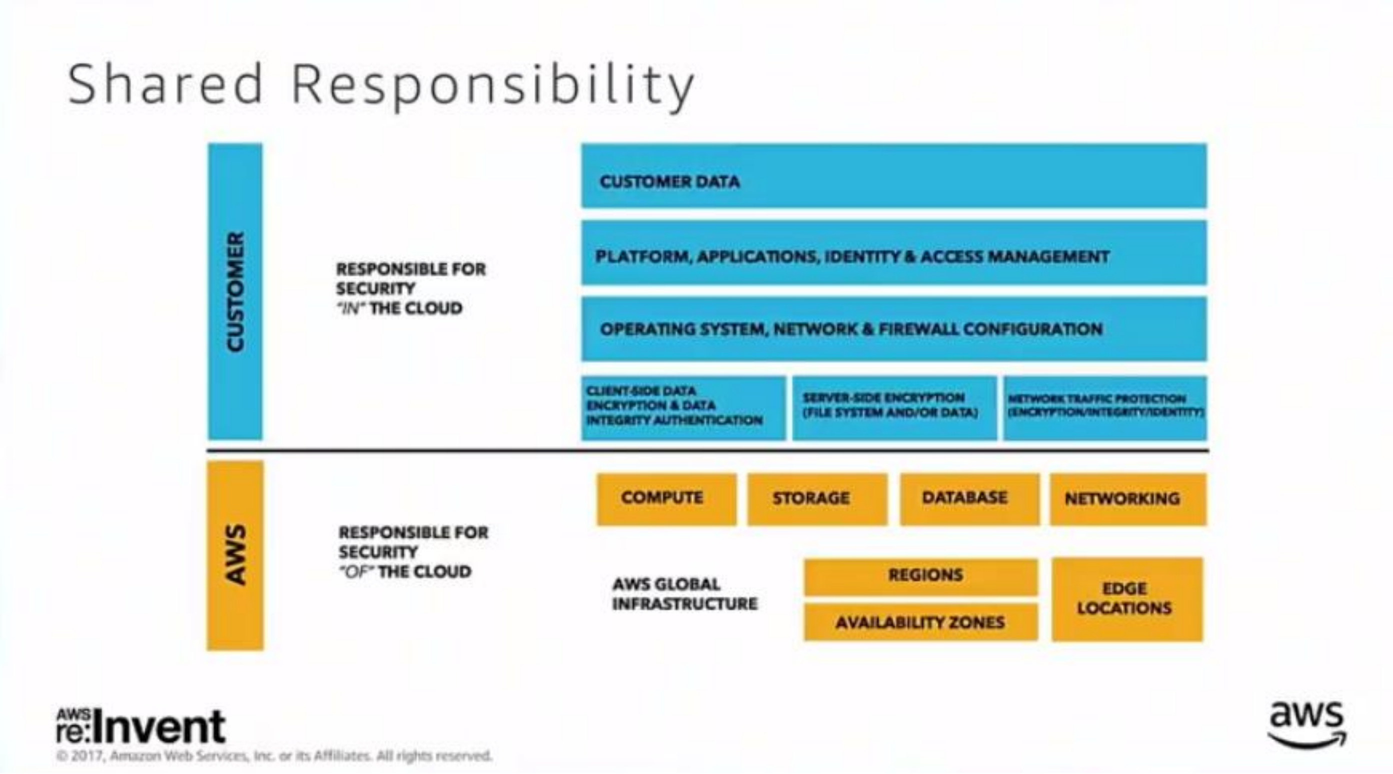
Logging & monitoring

Incident response

We currently have over 6 million patient visits every month and we need to be able to maintain our HIPAA compliance in the cloud. We also wanted end-to-end visibility of our data.

Maintaining Compliance

AICPA
SOC
HIPAA
ISO 27001
International Organization for Standardization
FedRAMP
cloud security alliance CSA
PCI Security Standards Council
PARTICIPATING ORGANIZATION
FISMA
NIST
AWS re:Invent
aws



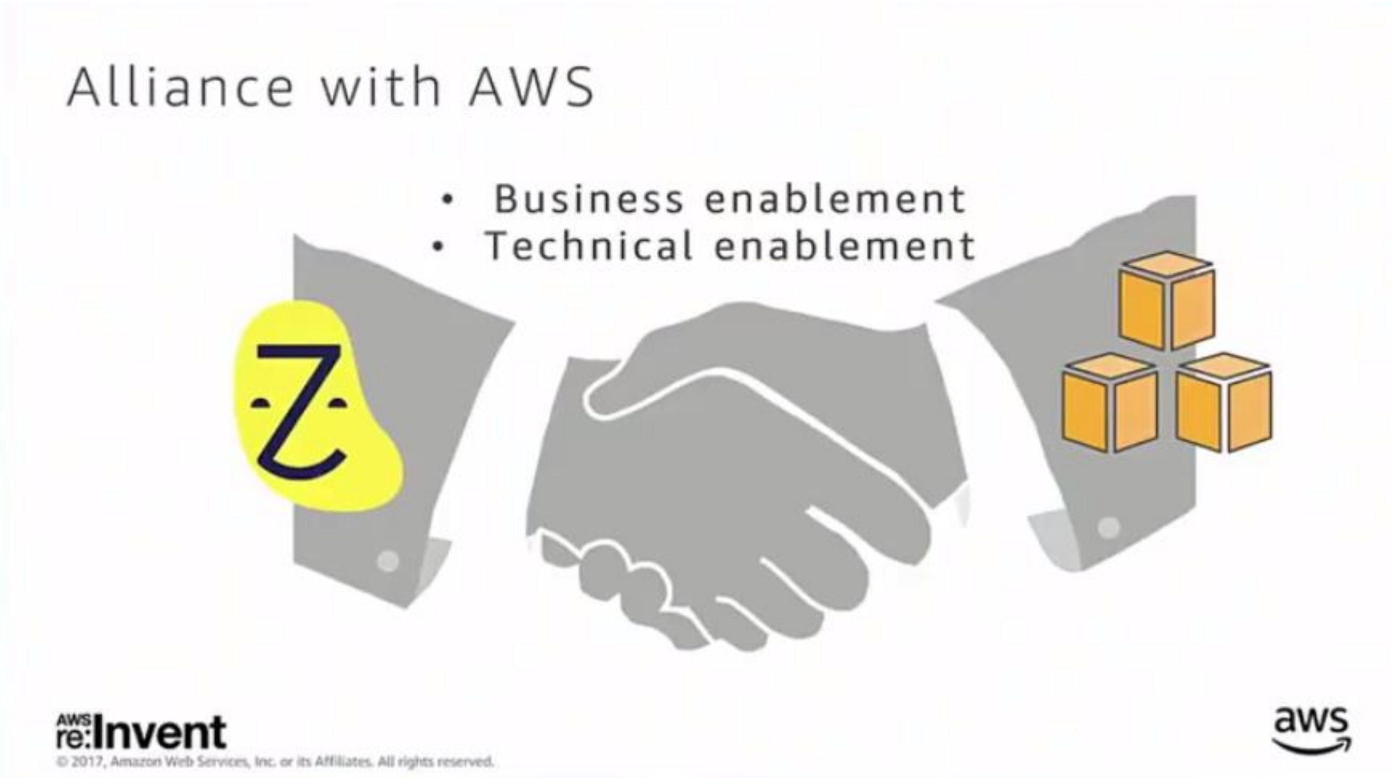
Shared Responsibility

CUSTOMER
RESPONSIBLE 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)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

AWS re:Invent

aws

Alliances



Alliance with AWS

- Business enablement
- Technical enablement

AWS re:Invent

aws

Alliance within Zocdoc

*image from gettyimages

Easier with AWS

Maintain visibility

Access control

Encryption & key management

Logging & monitoring

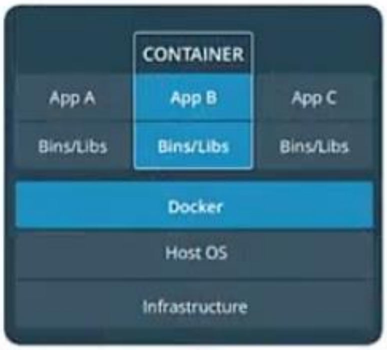
Incident response

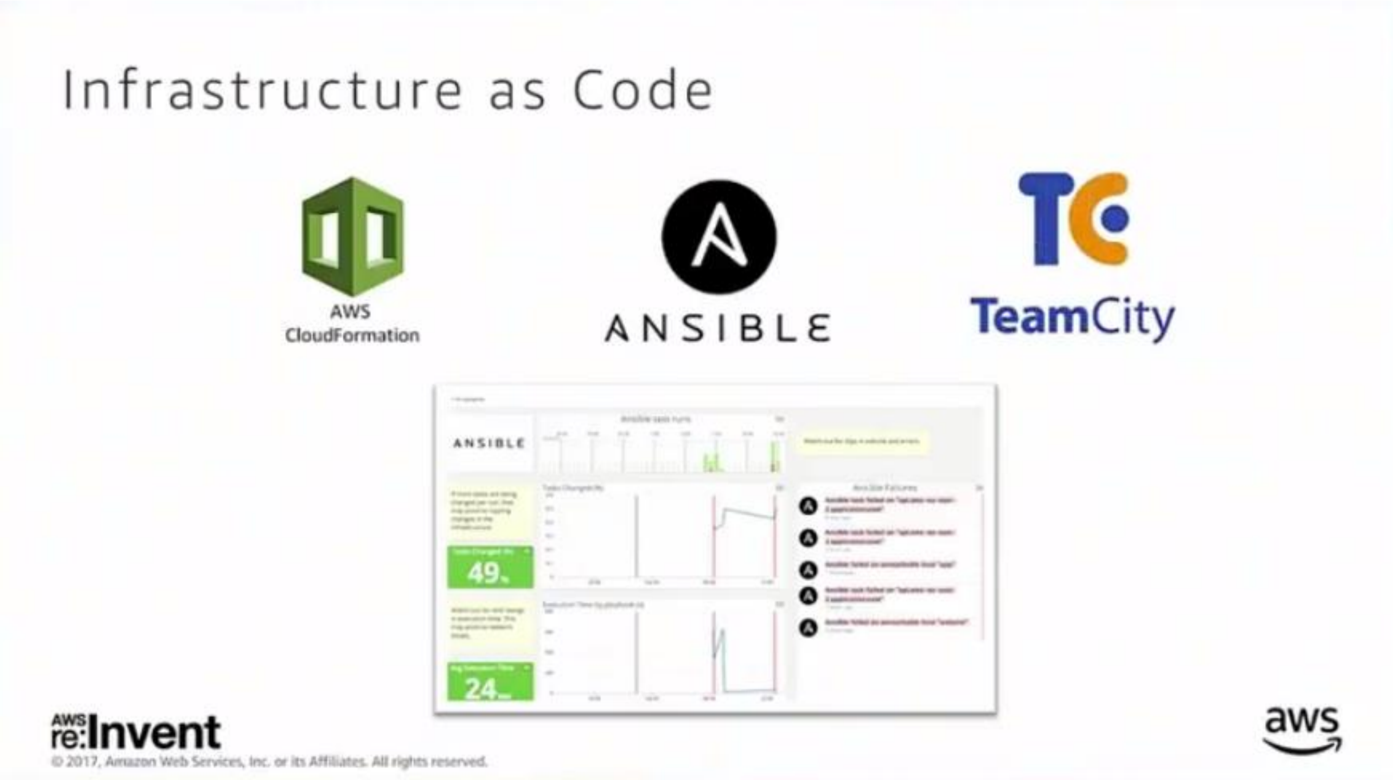
Maintaining Visibility & Control with Agility

- Visibility of critical data
- Scope reduction
- Enhanced alerting
- Standardized configurations

Infrastructure Hardening

- Hardened AMIs
  - Packer
  - Logging agents
  - Host based intrusion detection
  - Antivirus
- Hardened containers using Docker



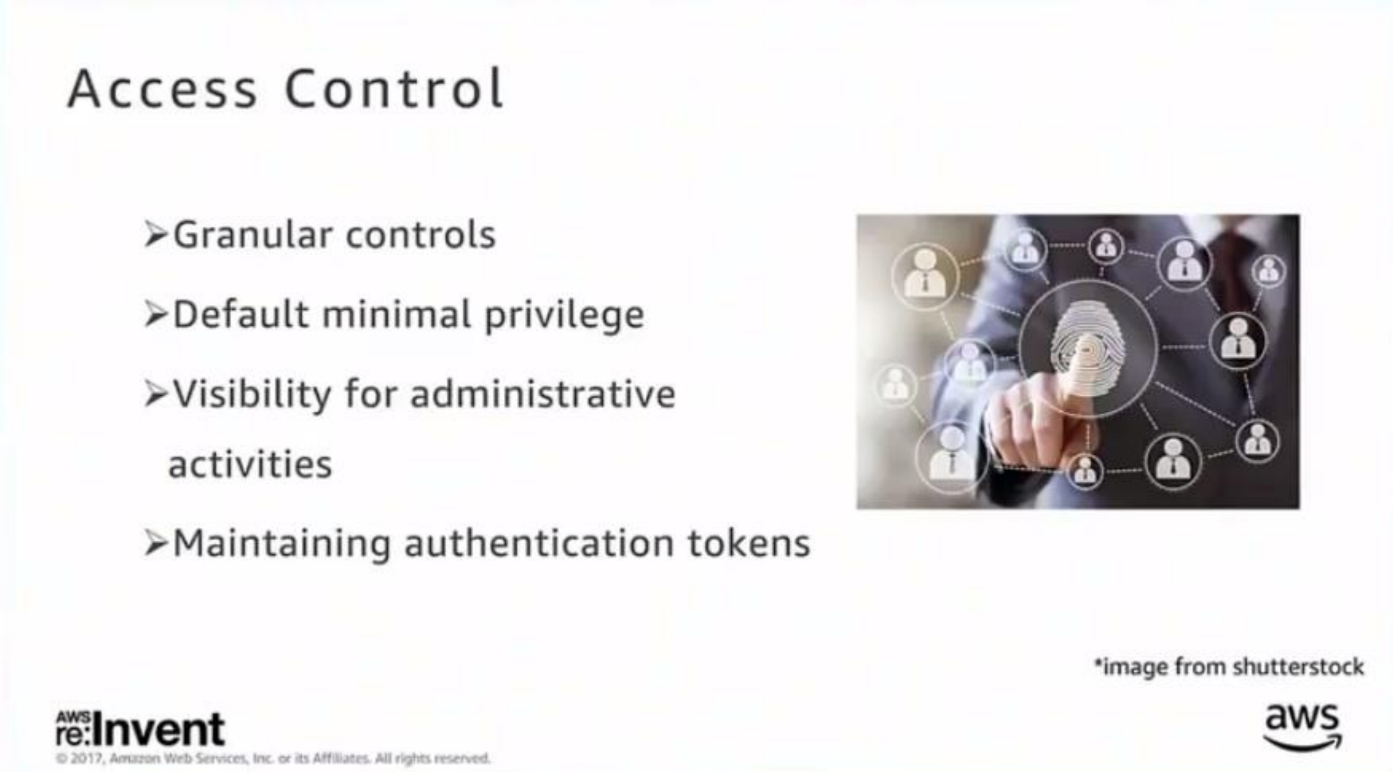


Infrastructure as Code

AWS re:Invent

aws

In CF, we templated the CF templates using Ansible by using variables for customization. TeamCity is our CI/CD tool instead of Jenkins.



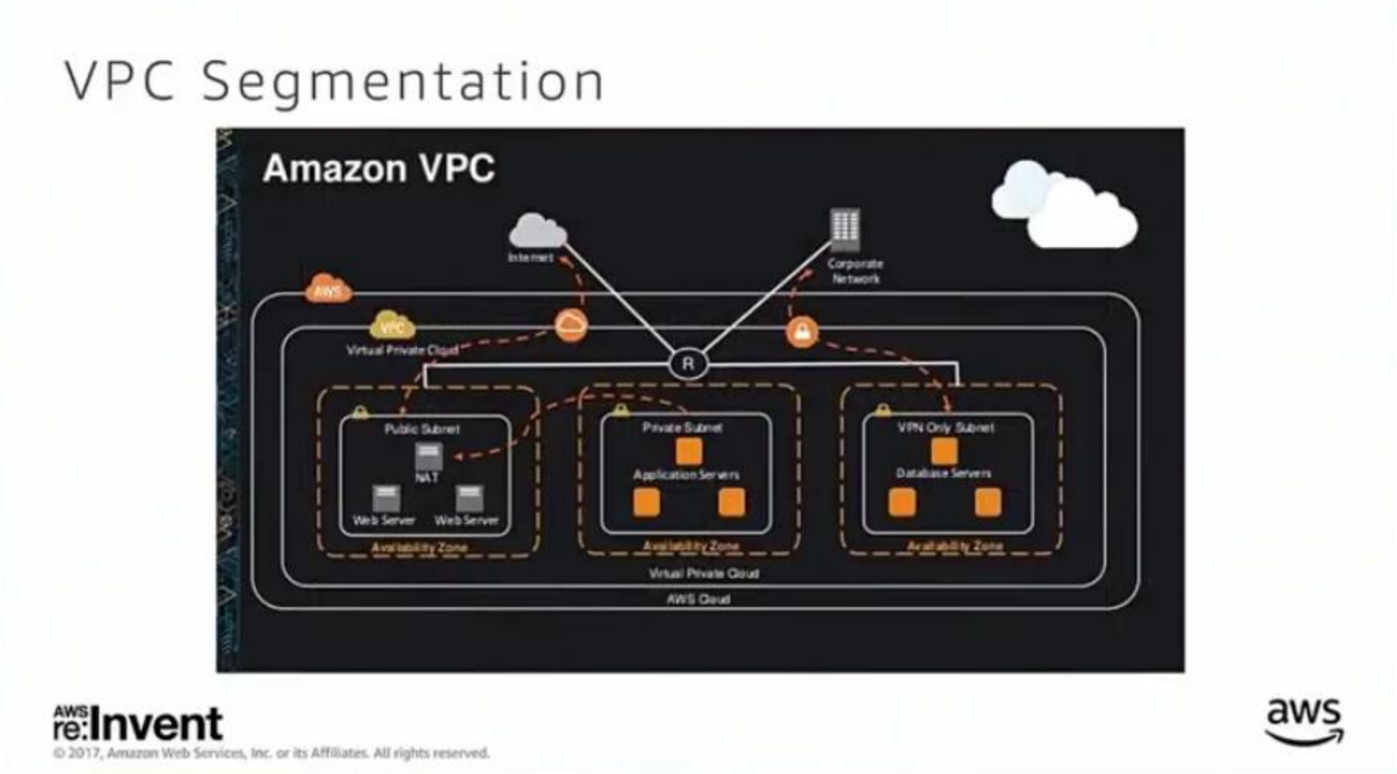
Access Control

- ➢Granular controls
- ➢Default minimal privilege
- ➢Visibility for administrative activities
- ➢Maintaining authentication tokens

*image from shutterstock

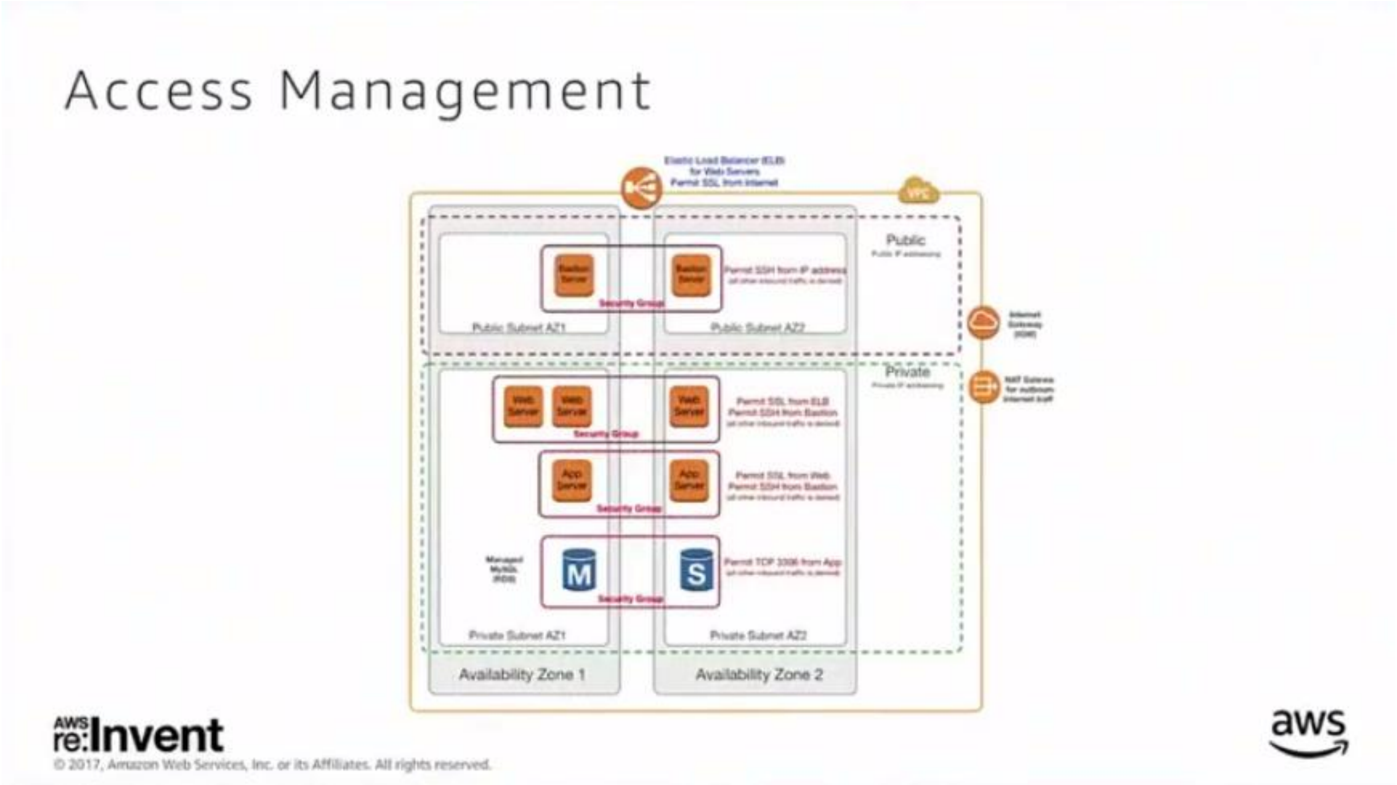
AWS re:Invent

aws



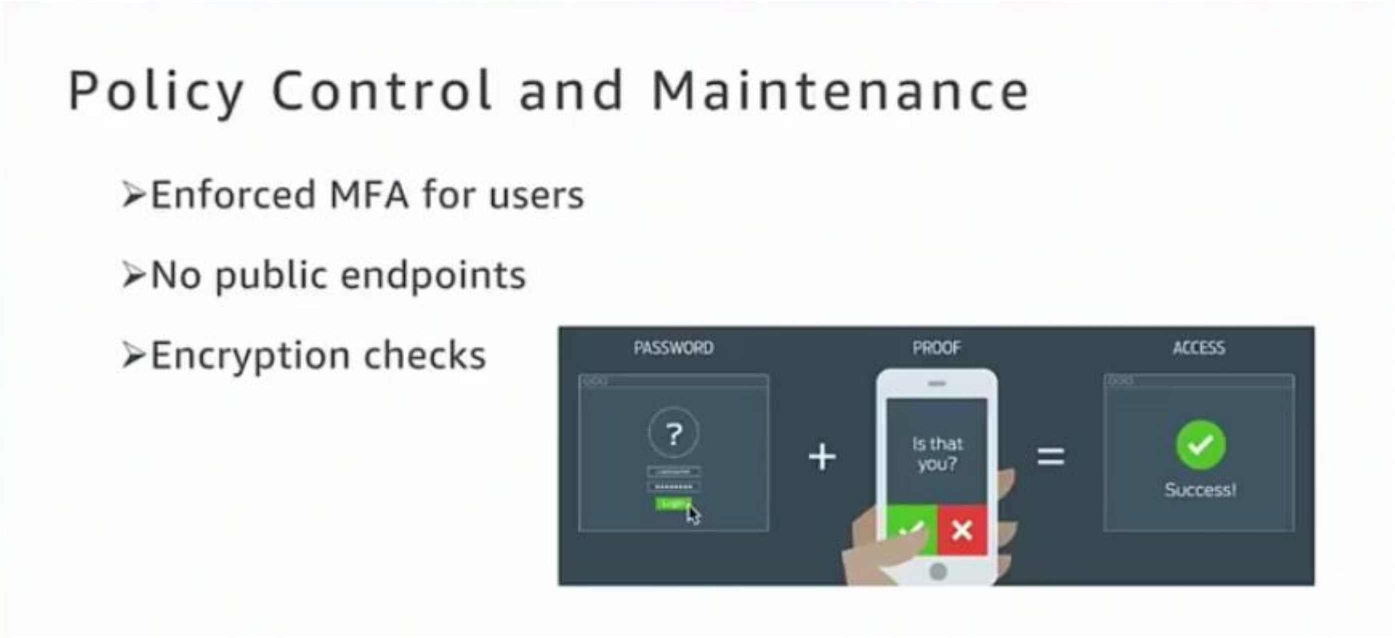
VPC Segmentation

We have many different VPCs for different groups of apps we run, this allows pure functionality segmentation and we restrict access between the VPCs.



Access Management

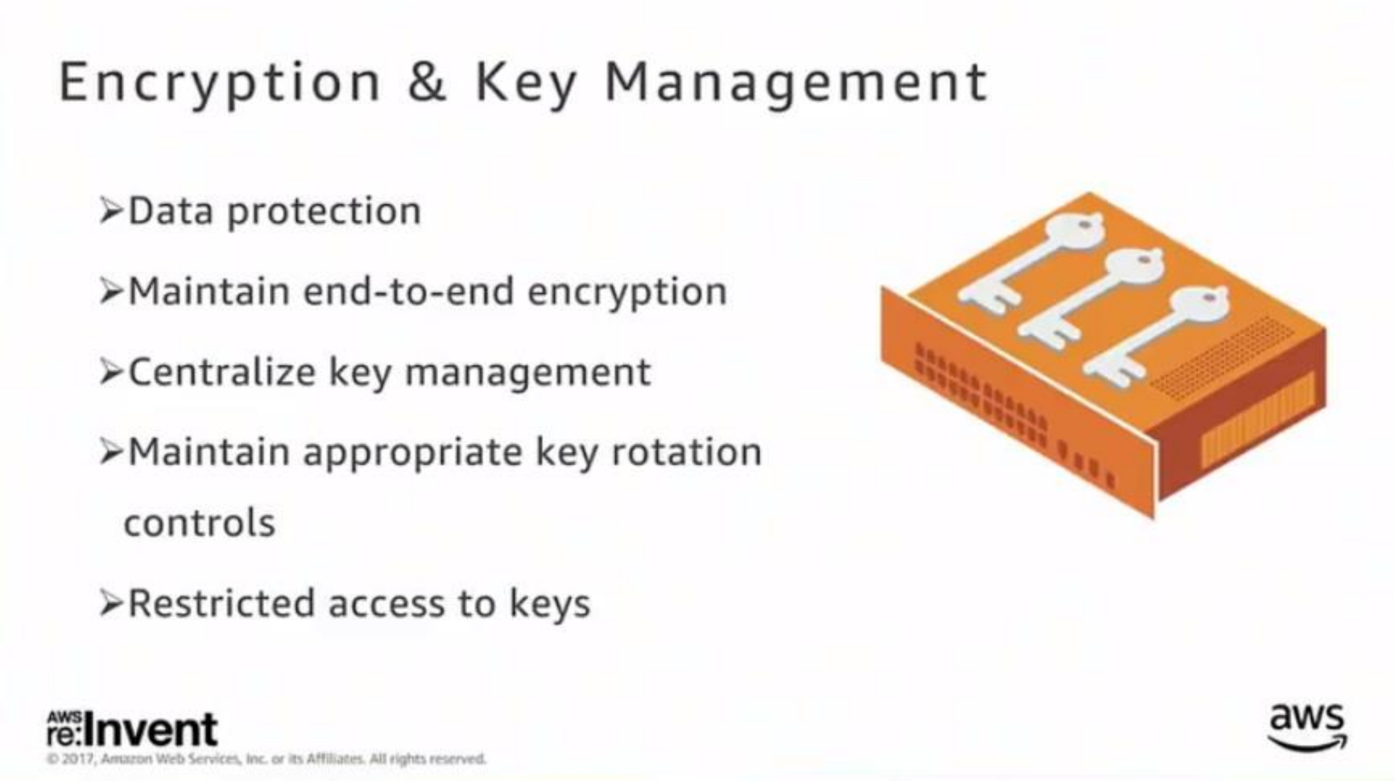
We are using Policies, IAM Roles, and Security Groups to restrict and grant access for our users and service accounts limited access based on what they are allowed to see and use within the whole infrastructure.



Policy Control and Maintenance

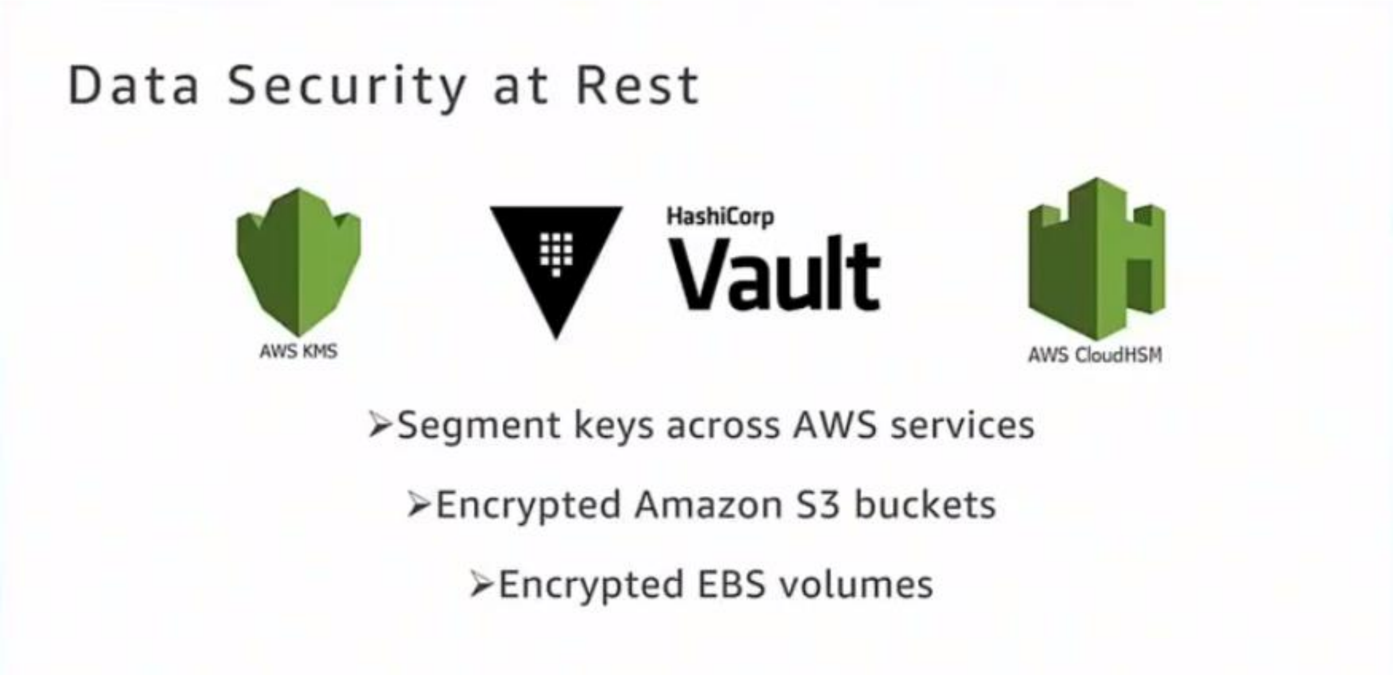
- Enforced MFA for users
- No public endpoints
- Encryption checks

Everything in transit is encrypted



Encryption & Key Management

- Data protection
- Maintain end-to-end encryption
- Centralize key management
- Maintain appropriate key rotation controls
- Restricted access to keys

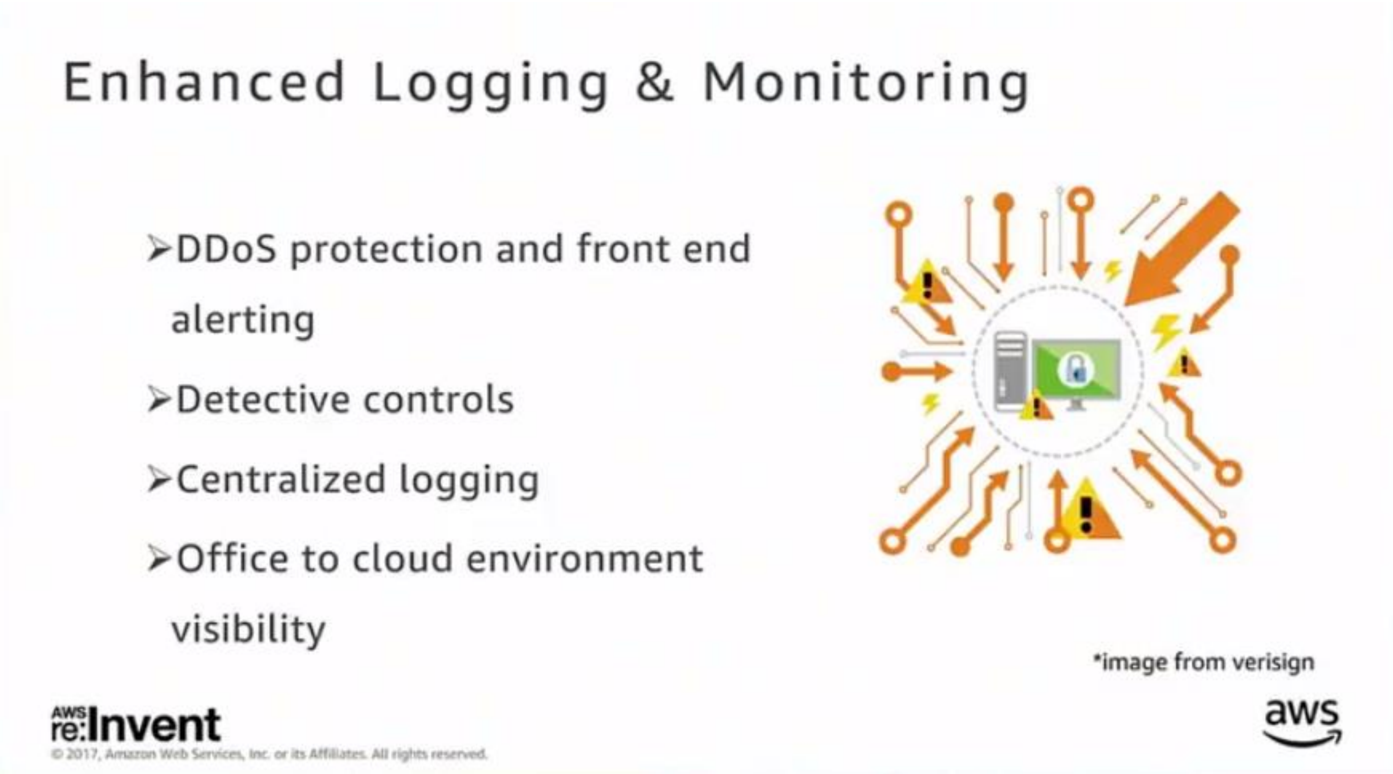


Data Security at Rest

AWS KMS
HashiCorp
Vault
AWS CloudHSM

- ➢Segment keys across AWS services
- ➢Encrypted Amazon S3 buckets
- ➢Encrypted EBS volumes

We use KMS to generate keys for us automatically and also to rotate those keys automatically.

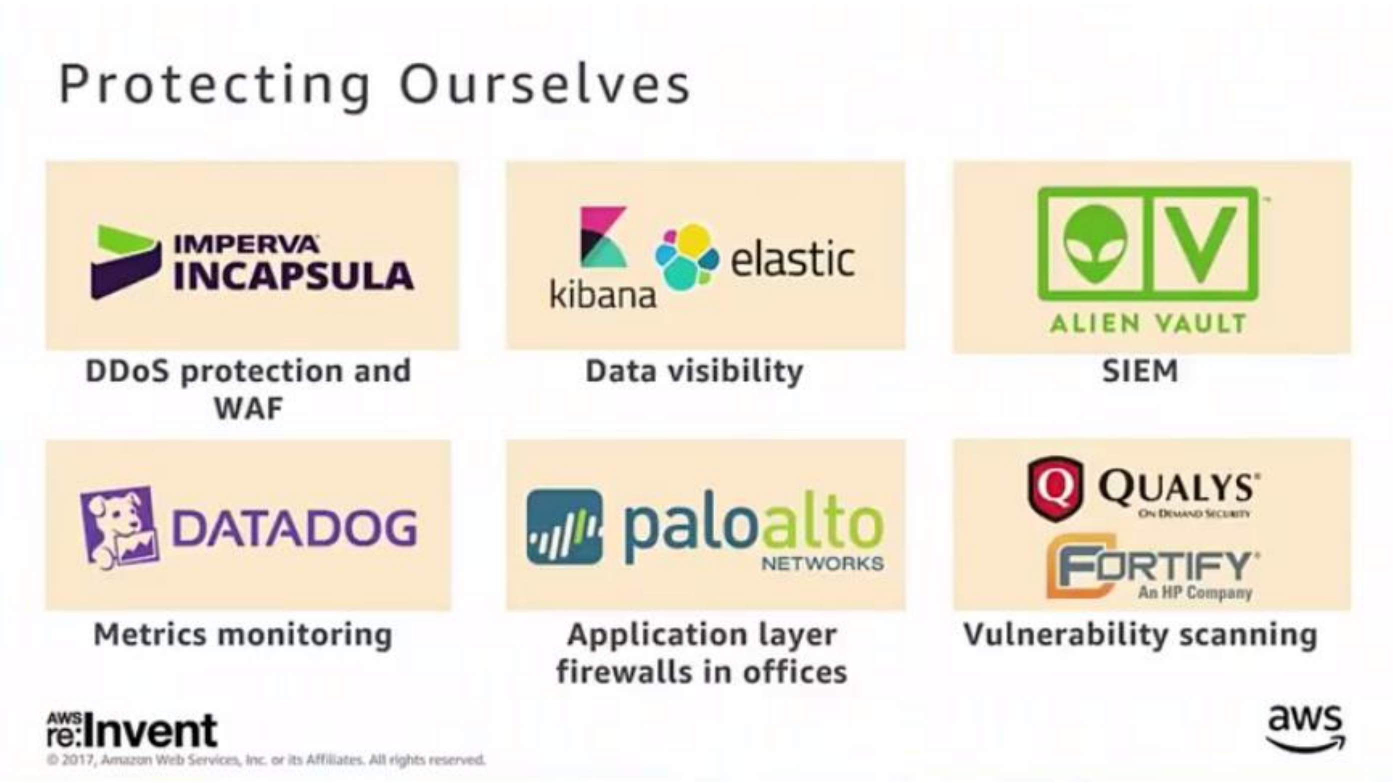


Enhanced Logging & Monitoring

- ➢DDoS protection and front end alerting
- ➢Detective controls
- ➢Centralized logging
- ➢Office to cloud environment visibility

*image from verisign

AWS re:Invent
aws



Protecting Ourselves

IMPERVA INCAPSULA

DDoS protection and WAF

kibana elastic

Data visibility

ALIEN VAULT

SIEM

DATADOG

Metrics monitoring

paloalto NETWORKS

Application layer firewalls in offices

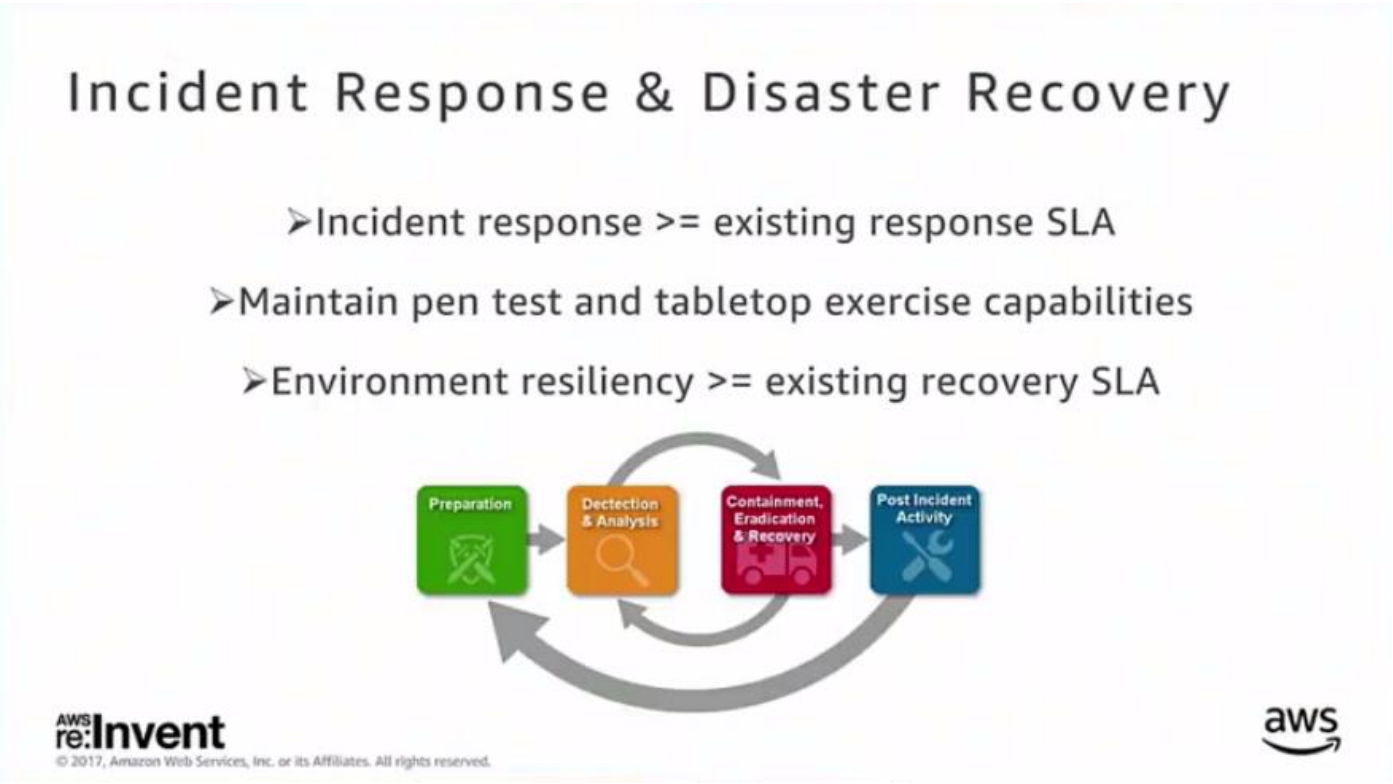
QUALYS ON DEMAND SECURITY

FORTIFY An HP Company

Vulnerability scanning

AWS re:Invent

aws



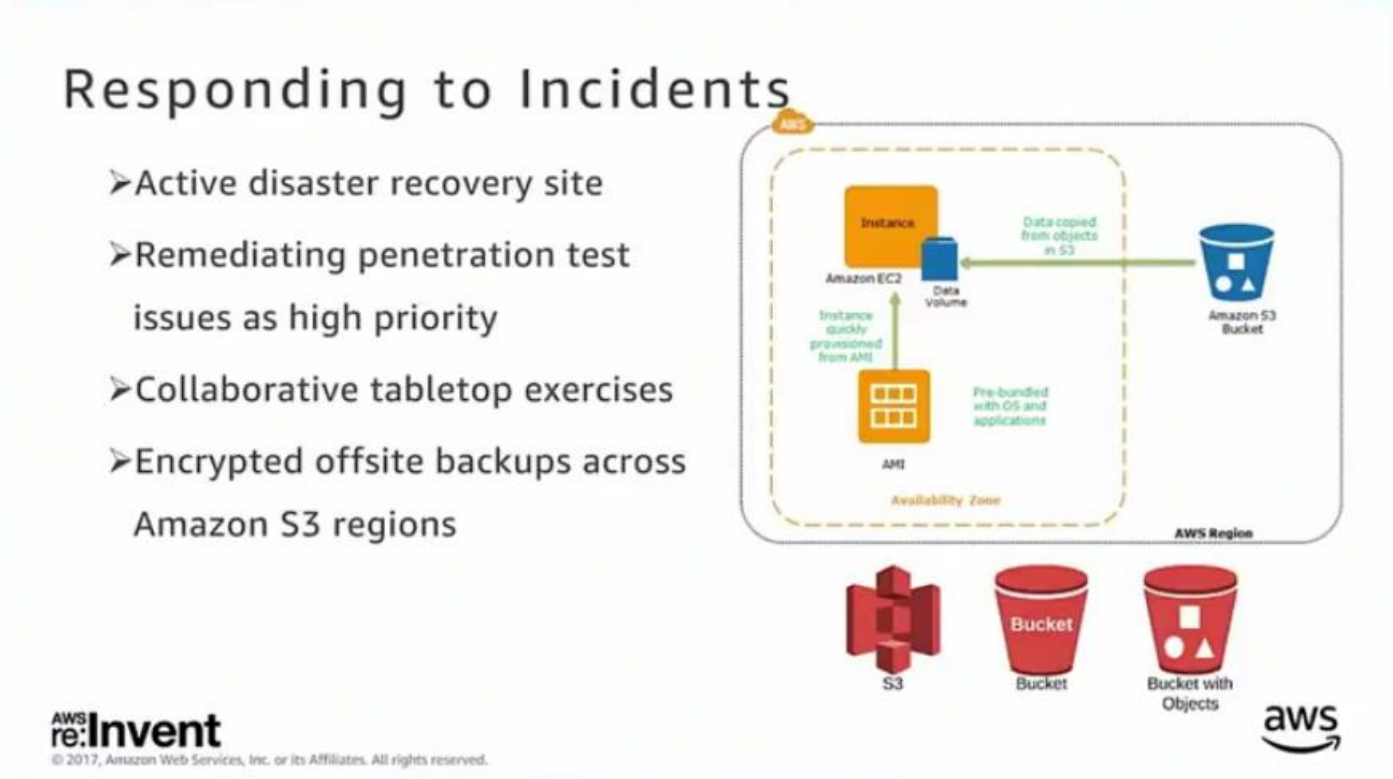
Incident Response & Disaster Recovery

- ➢Incident response >= existing response SLA
- ➢Maintain pen test and tabletop exercise capabilities
- ➢Environment resiliency >= existing recovery SLA

Preparation
Dectection & Analysis
Containment, Eradication & Recovery
Post Incident Activity

AWS re:Invent

aws

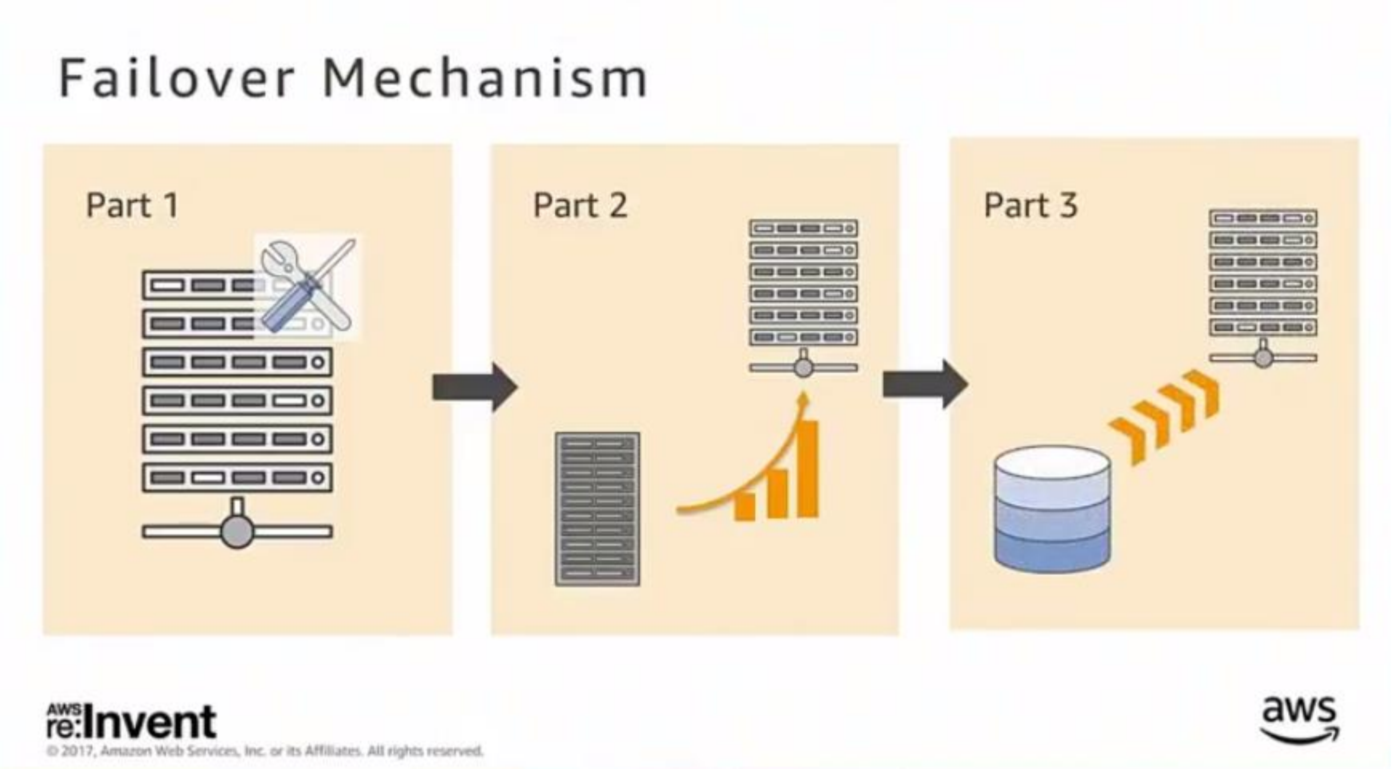


Responding to Incidents

- ➢Active disaster recovery site
- ➢Remediating penetration test issues as high priority
- ➢Collaborative tabletop exercises
- ➢Encrypted offsite backups across Amazon S3 regions

AWS re:Invent

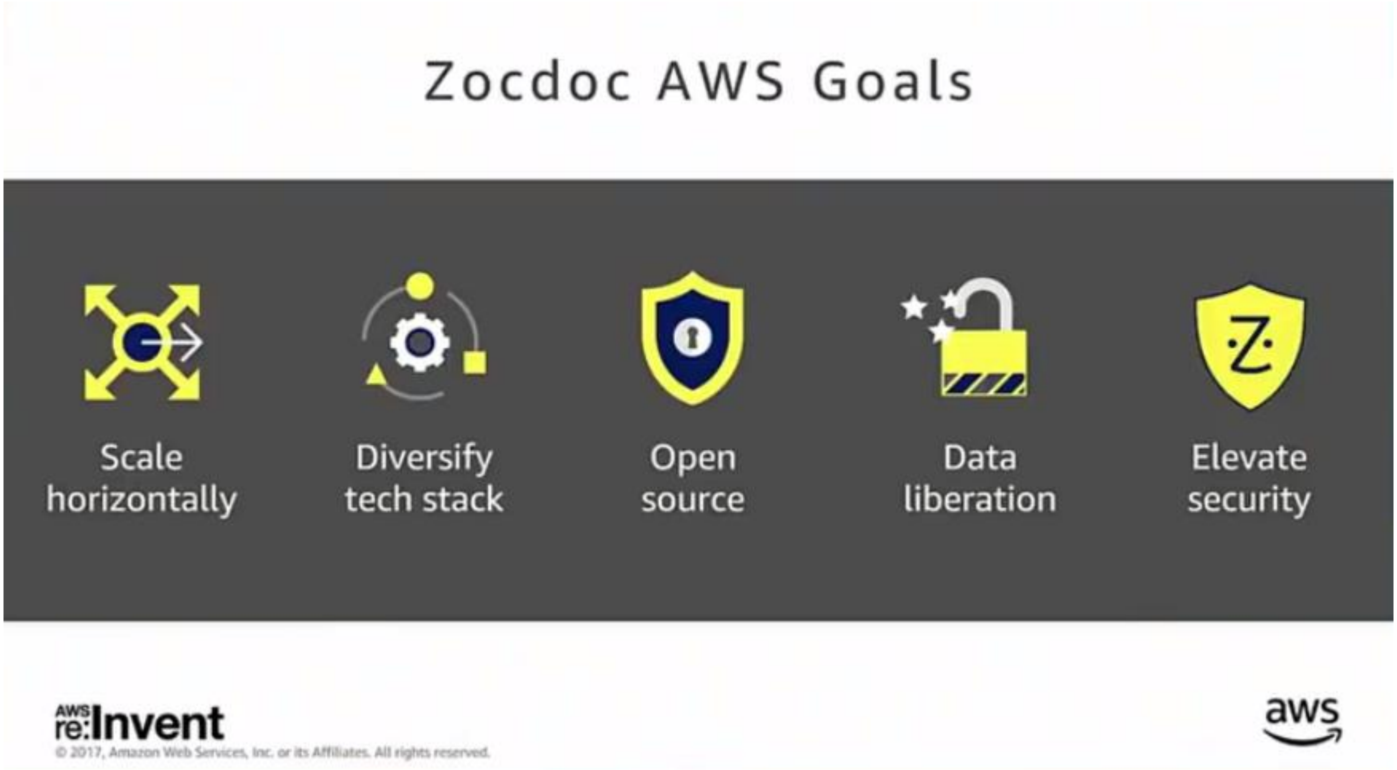
aws



Failover Mechanism

AWS re:Invent

aws

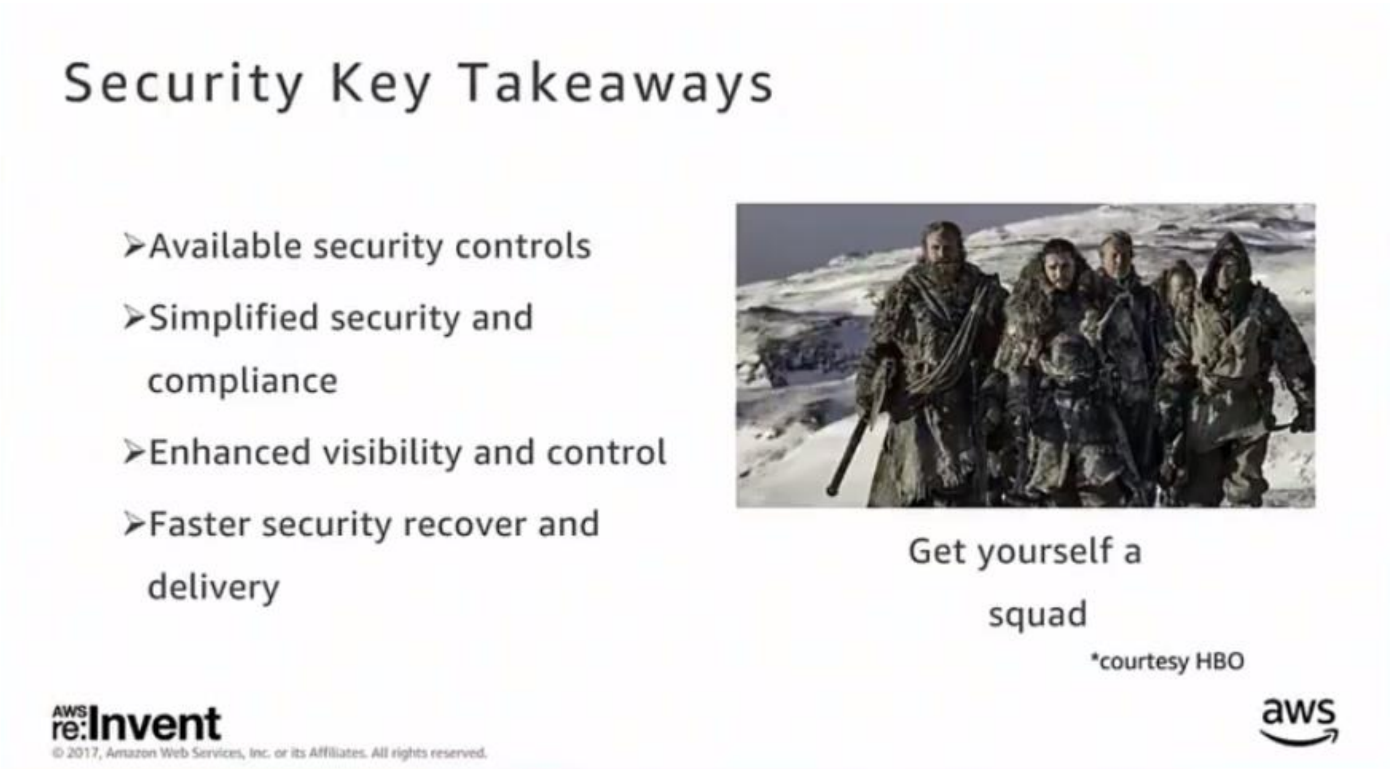


Zocdoc AWS Goals

- Scale horizontally
- Diversify tech stack
- Open source
- Data liberation
- Elevate security

AWS re:Invent

aws



Security Key Takeaways

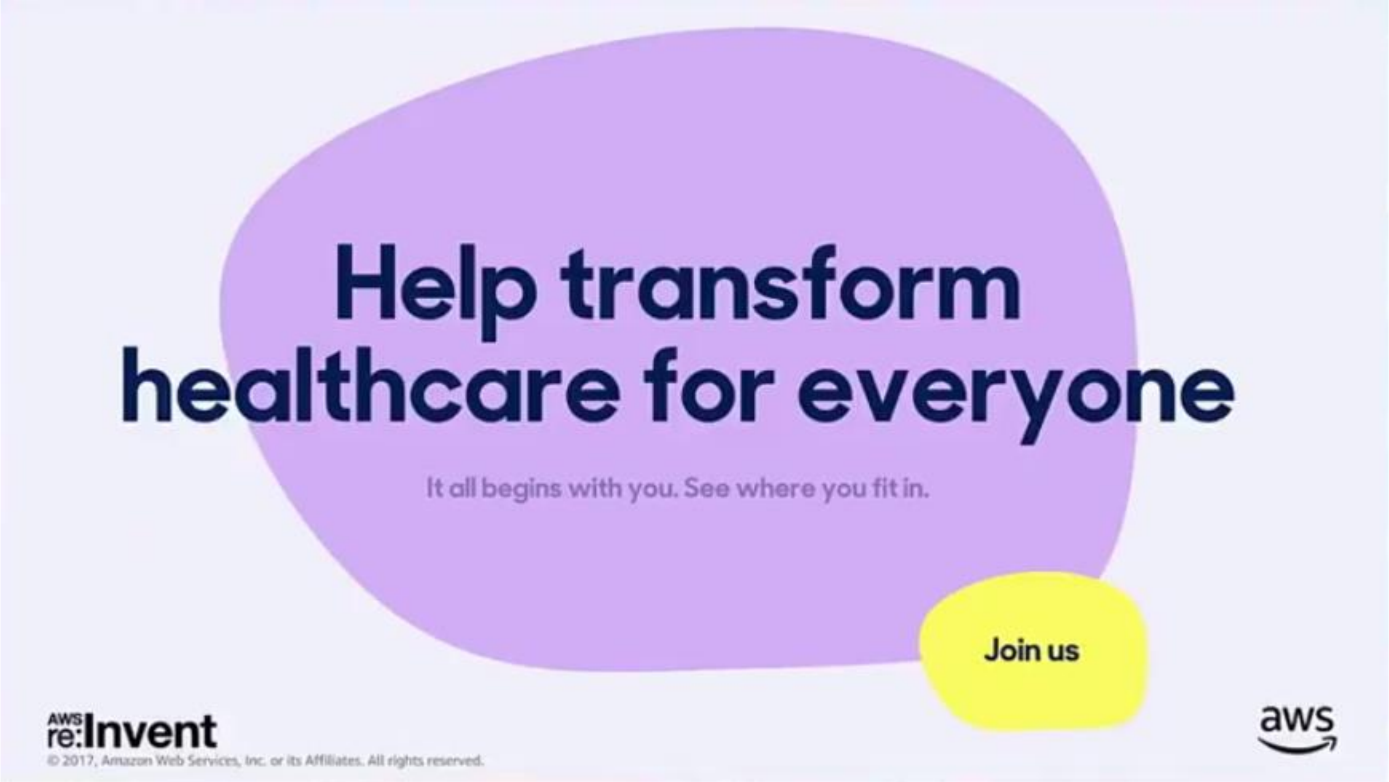
- ➢Available security controls
- ➢Simplified security and compliance
- ➢Enhanced visibility and control
- ➢Faster security recover and delivery

Get yourself a squad

*courtesy HBO

AWS re:Invent

aws



Help transform healthcare for everyone

It all begins with you. See where you fit in.

Join us

AWS re:Invent

aws