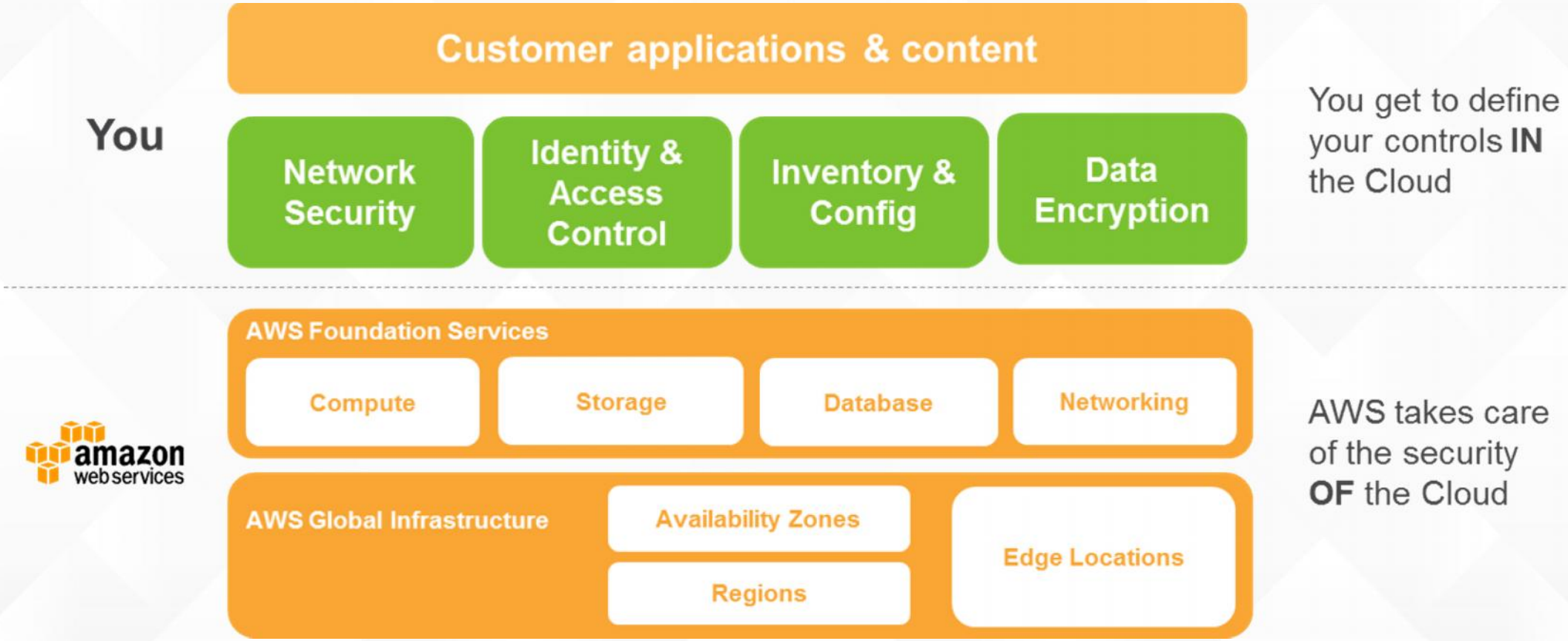
Security and Compliance in AWS

Zubin Chagpar
Head of Middle East and Africa, AWS

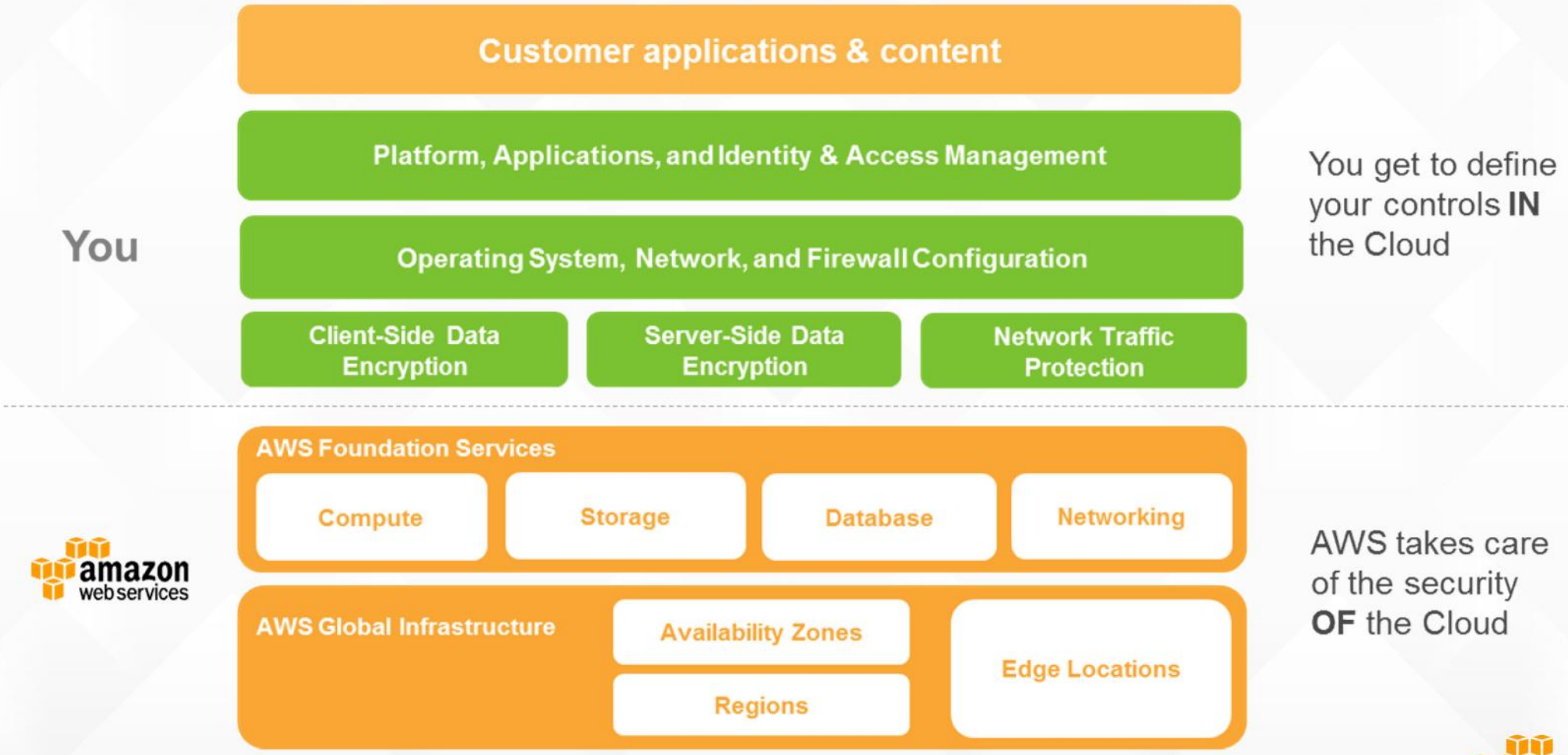
@phylosopher
chagparz@amazon.com

Shared Responsibility Model

AWS and you share responsibility for security



AWS and you share responsibility for security



An Example: EC2

AWS	Customer
•Facilities •Physical Security •Physical Infrastructure •Network Infrastructure •Virtualization Infrastructure	•Operating System •Application •Security Groups •Network ACLs •Network Configuration •Account Management

amazon web services

Key AWS Certifications and Assurance Programs

Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
• ISO 9001 • ISO 27001 • ISO 27017 • ISO 27018 • MLPS Level 3 • MTCS • PCI DSS Level 1 • SEC Rule 17-a-4(f) • SOC 1 • SOC 2 • SOC 3 • DoD CSM • FedRAMP • FIPS • IRAP	• EU Data Protection Directive • EU Model Clauses • U.K. DPA - 1988 • CS Mark [Japan] • EAR • FERPA • GLBA • HIPAA • HITECH • IRS 1075 • ITAR • My Number Act [Japan] • VPAT / Section 508 • Privacy Act [Australia] • Privacy Act [New Zealand] • PDPA - 2010 [Malaysia] • PDPA - 2012 [Singapore]	• CJIS • CLIA • CMS EDGE • CMSR • CSA • FDA • FedRAMP TIC • FISC • FISMA • G-Cloud • GxP (FDA CFR 21 Part 11) • IT Grundschutz • MITA 3.0 • MPAA • NERC • NIST • PHR • UK Cyber Essentials

Vodafone Italy Migrates to AWS and Creates a Secure Environment for Customer Transactions While Reducing Capital Costs by 30%

> Since migrating to AWS, we created a secure solution for our customers that can handle thousands of daily transactions, while reducing our costs by 30%
>
> **Stefano Harak**
> Online Senior Product Manager, Vodafone

Vodafone Italy, based in Milan, provides mobile services for more than 30 million customers

Customers can buy additional for SIM cards using a credit or debit card.

Key requirement was to build a PCI DSS-compliant solution

amazon web services

Security Control Objectives

1. Security Organization
2. Amazon Employee Access
3. Logical Security
4. Secure Data Handling
5. Physical Security and Environment Safeguards
6. Change Management
7. Data Integrity, Availability and Redundancy
8. Incident Handling

Your data stays where you put it

13 regions

35 Availability Zones

Announced:
4 AWS regions (Canada, China, Ohio, and the United Kingdom)
9 Availability Zones

amazon web services

1st key point: Security is Job Zero

PEOPLE & PROCESS

SYSTEM

NETWORK

PHYSICAL

Familiar Security Model

Validated and driven by customers' security experts

Benefits all customers

2st Key point: Protect the cloud with the cloud

- Use the tools AWS provide to protect Cloud Assets
- Architect for End-to-End Security

Patterns adopted by highly successful security programs

Ubiquitous encryption

Just-in-time access

Ubiquitous logging

DevSecOps

Security services and API

Security programme

Security as code

Minimum security baseline

Asset management

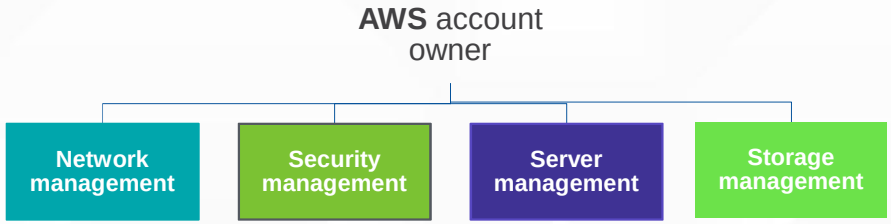
Security management layer

Control access and segregate duties everywhere

You get to control **who** can do **what** in your AWS environment **when** and from **where**

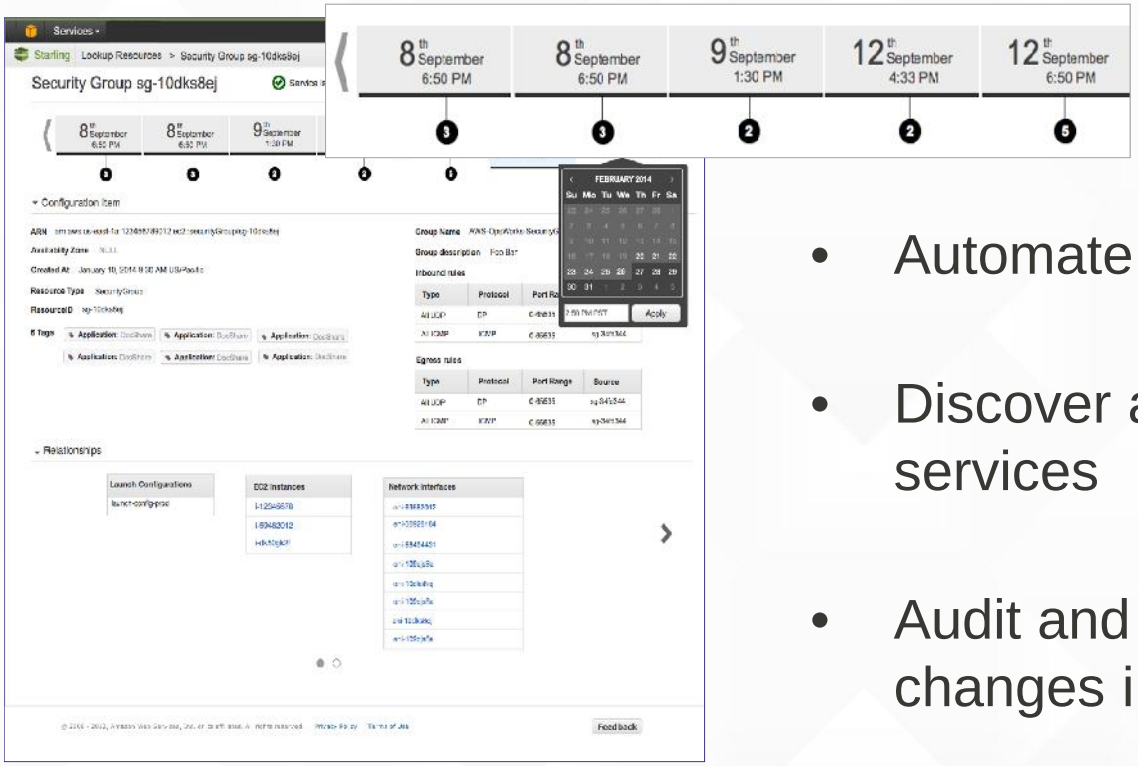
Fine-grained control of your AWS cloud with **multi-factor authentication**

Integrate with your existing Active directory using federation and single sign-on



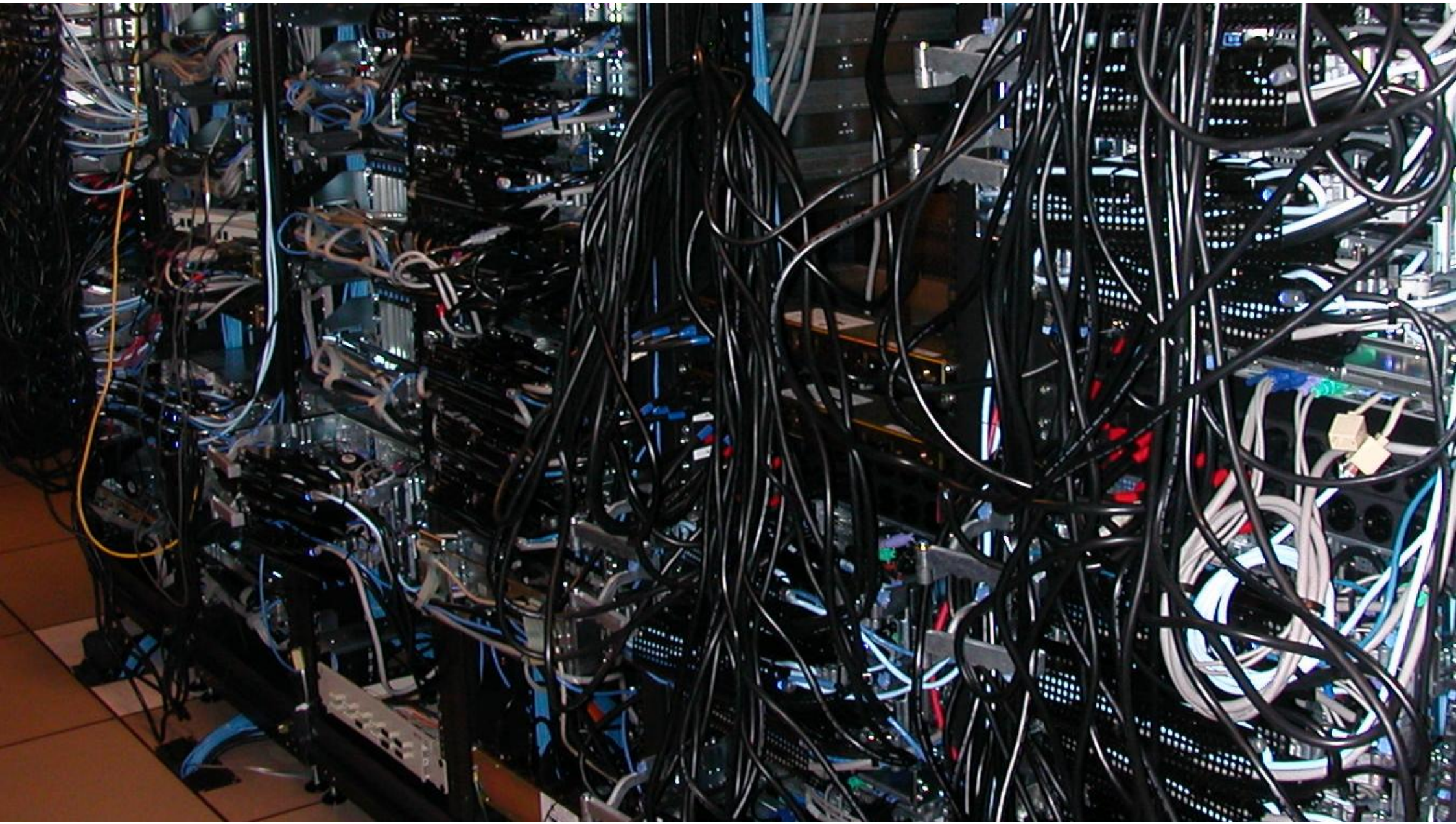
amazon web services

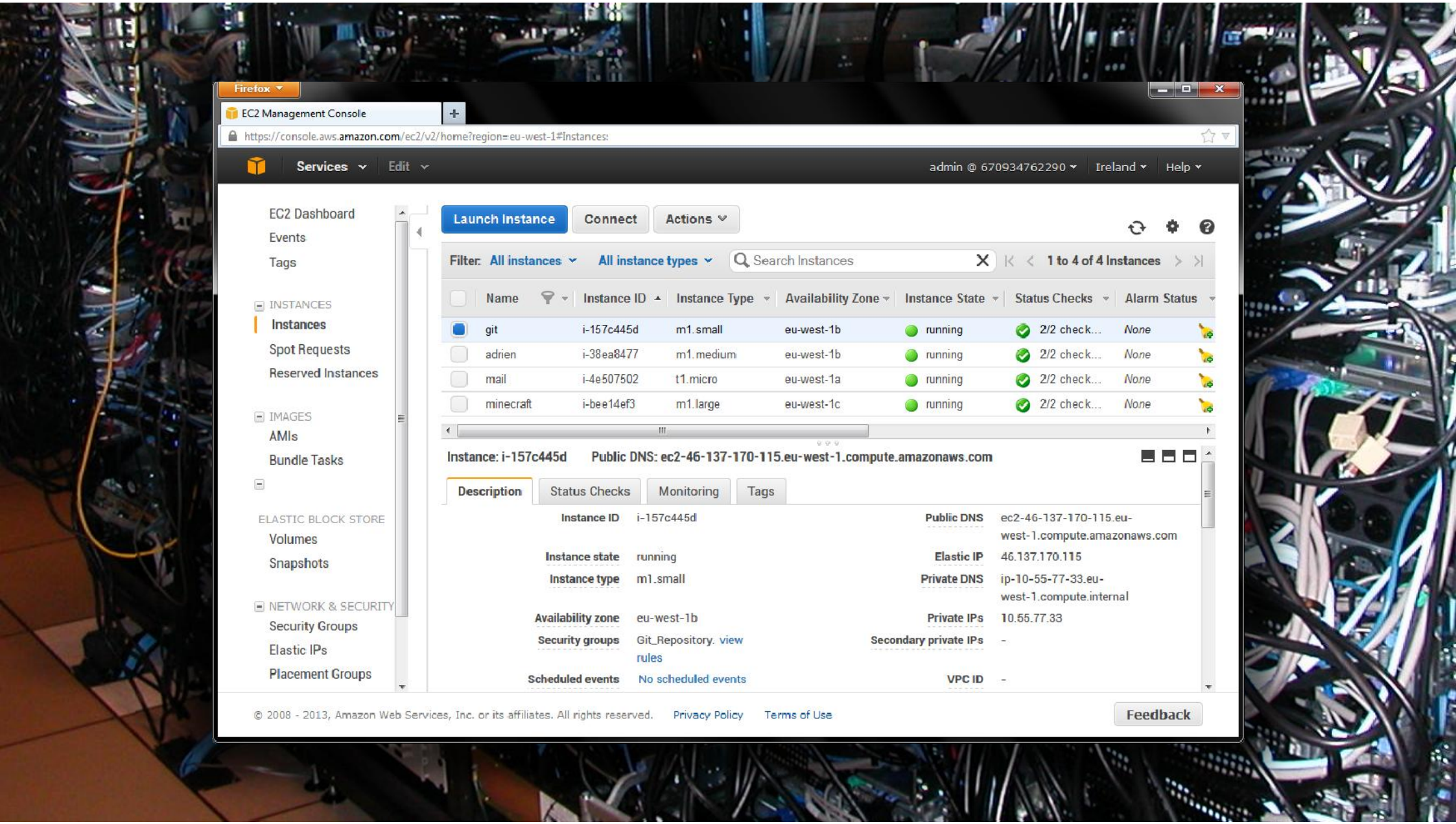
Understand Configuration Changes



- Automate IT asset inventory
- Discover and provision cloud services
- Audit and troubleshoot configuration changes in the cloud

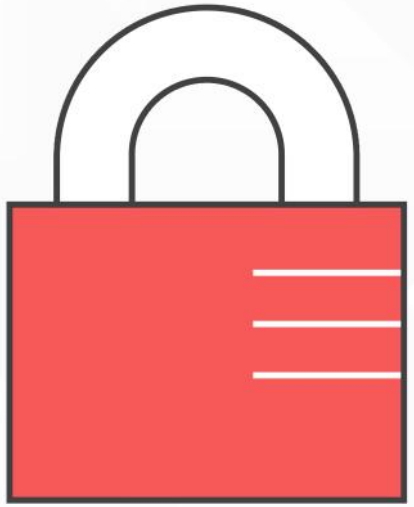
amazon web services




Firefox
EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Instances:
Services
Edit
admin @ 670934762290
Ireland
Help
EC2 Dashboard
Events
Tags
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Launch Instance
Connect
Actions
Filter: All instances
All instance types
Search Instances
1 to 4 of 4 Instances
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
git i-157c445d m1.small eu-west-1b running 2/2 check... None
adrien i-38ea8477 m1.medium eu-west-1b running 2/2 check... None
mail i-4e507502 t1.micro eu-west-1a running 2/2 check... None
minecraft i-bee14ef3 m1.large eu-west-1c running 2/2 check... None
Instance: i-157c445d
Public DNS: ec2-46-137-170-115.eu-west-1.compute.amazonaws.com
Description
Status Checks
Monitoring
Tags
Instance ID i-157c445d
Instance state running
Instance type m1.small
Availability zone eu-west-1b
Security groups Git_Repository. view rules
Scheduled events No scheduled events
Public DNS ec2-46-137-170-115.eu-west-1.compute.amazonaws.com
Elastic IP 46.137.170.115
Private DNS ip-10-55-77-33.eu-west-1.compute.internal
Private IPs 10.55.77.33
Secondary private IPs -
VPC ID -
© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use
Feedback

Encrypt your sensitive information

- Native encryption across services for free
  - S3, EBS, RDS, RedShift
  - End to end SSL/TLS
- Scalable Key Management
  - AWS Key Management Services provides scalable, low cost key management
  - CloudHSM provides hardware-based, high assurance key generation, storage and management
- Third Party Encryption options
  - Trend Micro, SafeNet, Vormetric, Hytrust, Sophos etc.



Monitoring: Get consistent visibility of logs

Full **visibility** of your AWS environment

- CloudTrail will record access to API calls and save logs in your S3 buckets, no matter how those API calls were made

Who did **what** and **when** and from **where** (IP address)

- CloudTrail support for many AWS services and growing - includes EC2, EBS, VPC, RDS, IAM and RedShift
- Easily Aggregate all log information

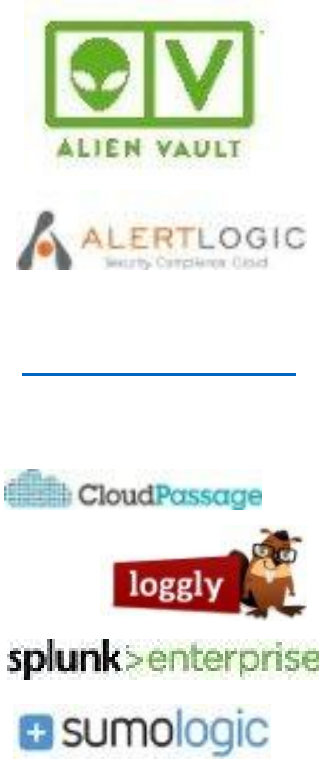
Out of the box **integration** with log analysis tools from AWS partners including Splunk, AlertLogic and SumoLogic

amazon web services

Marketplace

Infrastructure Security

Logging and Monitoring



Identity and Access Control

Configuration and Vulnerability Analysis

Data Protection

amazon web services

Documentation

- AWS Security Whitepaper

  https://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf
- AWS Risk and Compliance Whitepaper

  http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf
- AWS Security Best Practices

  http://media.amazonwebservices.com/AWS_Security_Best_Practices.pdf

Thank You

@phylosopher
chagparz@amazon.com