AWSome Day

Praha

Security and Compliance in AWS

Thursday, October 13, 2016
Clarion Congress Hotel

Vladimir Simek
Solutions Architect @AWS

Security is Job Zero

PEOPLE & PROCESS

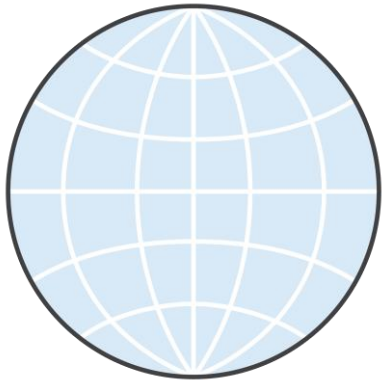
SYSTEM

NETWORK

PHYSICAL

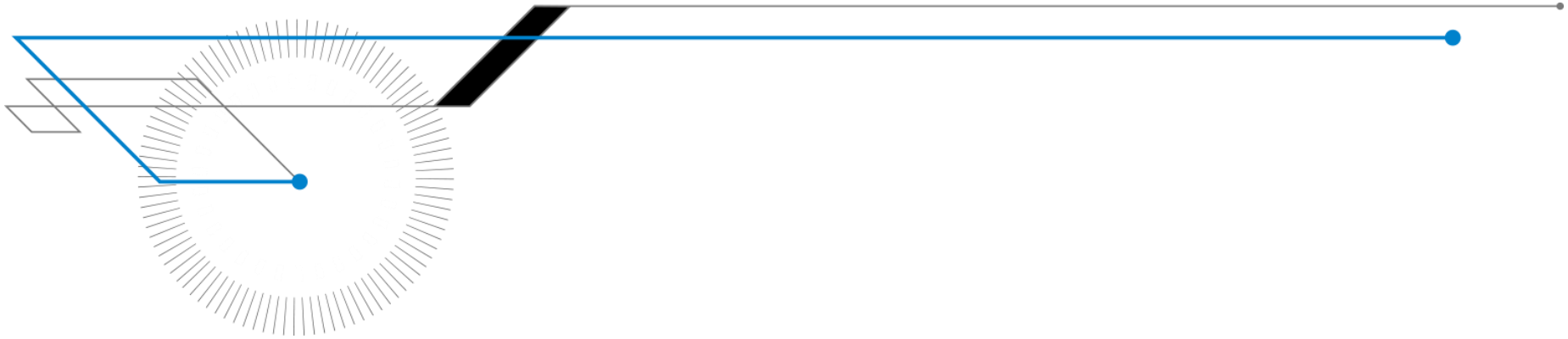
Familiar Security Model

Validated and driven by customers' security experts



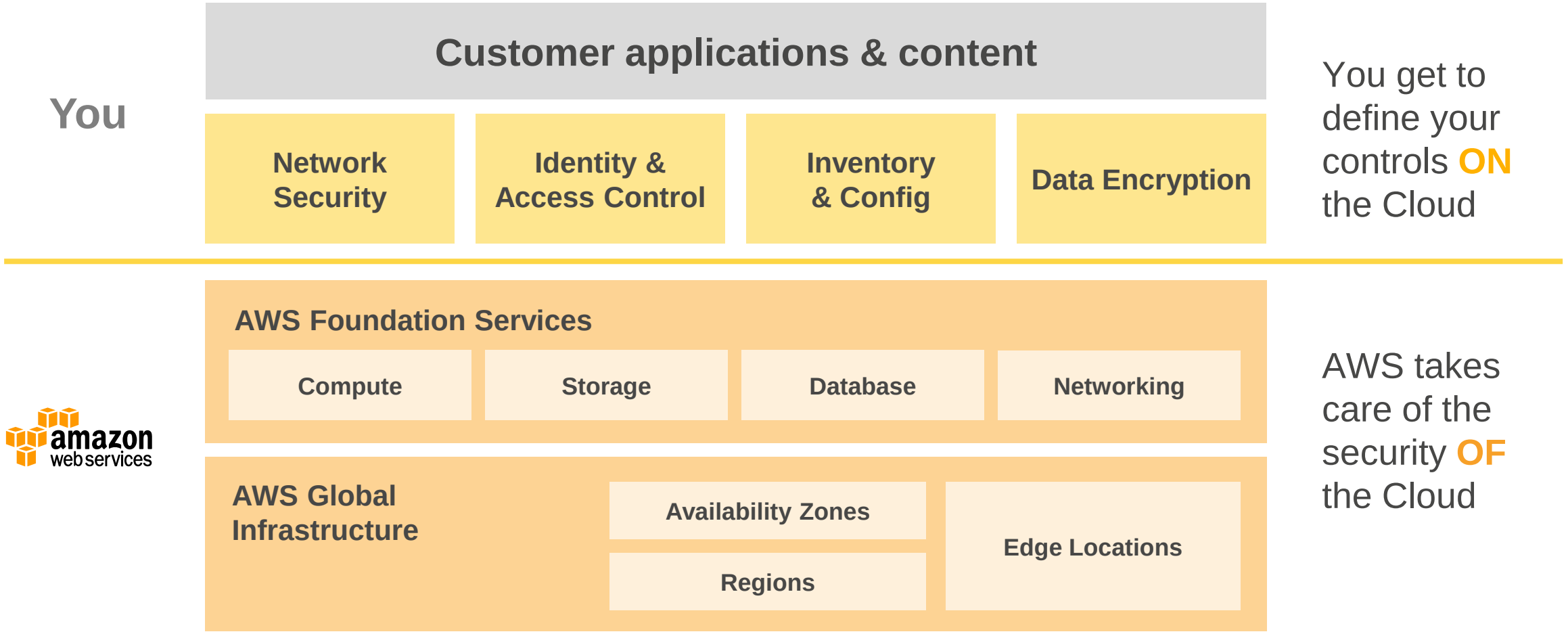
Benefits all customers

SECURITY IS SHARED



amazon web services

AWS and you share responsibility for security



amazon web services

AWS

- Facilities
- Physical Security
- Physical Infrastructure
- Network Infrastructure
- Virtualization Infrastructure

Physical

Logical

Operating System

Application

Security Groups

OS Firewalls

Network Configuration

Account Management

How does AWS get security?

Locations in nondescript, undisclosed facilities

Segregation of duties: staff with physical access versus staff with logical access

24/7 trained security guards

Physical access is recorded, videoed, stored, reviewed

Multi-factor authentication for physical access

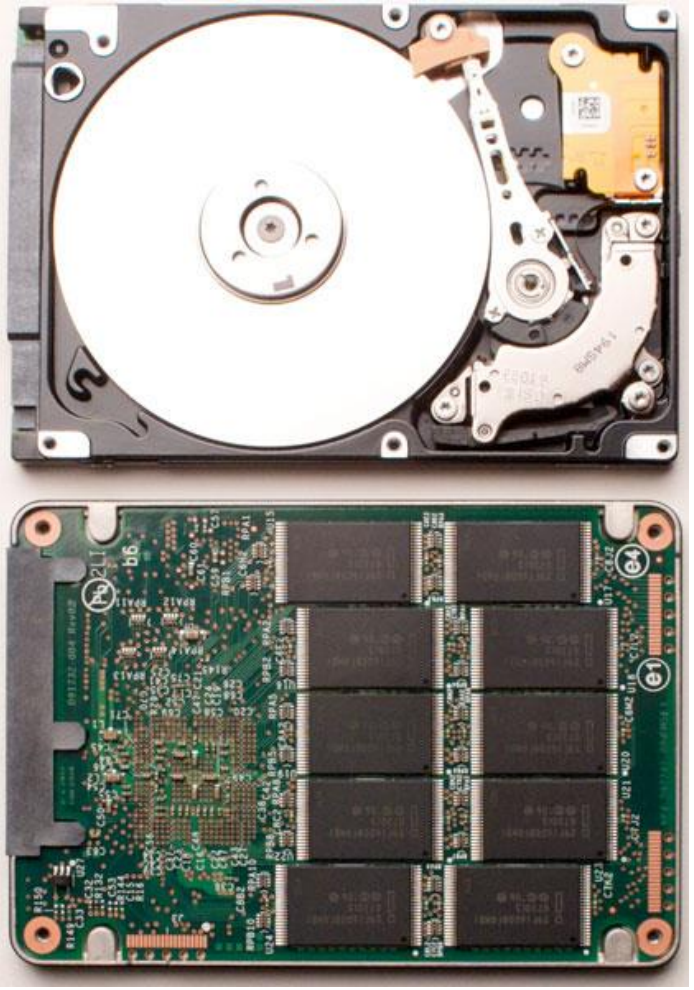
And every 90 days…

amazon web services

How does AWS get security?

amazon web services

How does AWS get security?



This

To This

amazon web services

Prove what AWS does!

Certifications

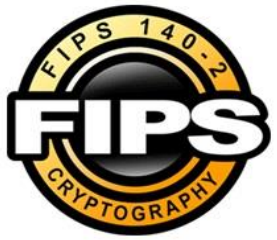
Audits & Attestations

- Independent 3rd parties
- Regularly refreshed
- Available to customers

https://aws.amazon.com/compliance/

amazon web services

Key AWS Certifications and Assurance Programs



amazon web services

AWS Data Processing Agreement EU Approved

EU Article 29 Working Party has approved AWS Data Processing Agreement

AWS DPA contains “model clauses” – standard provisions approved by the Working Party

Means you can sign the DPA without authorization from data protection authorities

Gives you additional options regarding which AWS Regions you use to process personal data

AWS is fully compliant with all applicable EU data protection laws

More: https://aws.amazon.com/compliance/eu-data-protection/

amazon web services

What about German regulations and laws?

ISO 27001, 27017, 27018	✓
ADV (DPA) (Auftragsdatenverarbeitungsvereinbarung)	✓
EU-Model Clauses	✓
BDSG Compliance	✓
IT-Grundschutz Zertifzierung	✓
External Audits	✓
I want to visit/see the datacenter!	✗

What this means

You benefit from an environment built for the most security sensitive organizations

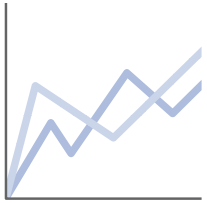
AWS manages 1800+ security controls **so you don't have to**

You get to define the right security controls for your workload sensitivity

You always have full ownership and control of your data

AWS can be more secure than your existing environment

In June 2015, IDC released a report which found that most customers can be more secure in AWS than their on-premises environment. **How?**



Automating logging and monitoring

Simplifying resource access

Making it easy to encrypt properly

Enforcing strong authentication

amazon web services

Capital One Will Reduce Datacenter Footprint from 8 to 3 by 2018

> The financial service industry attracts some of the worst cyber criminals. We work closely with AWS to develop a security model that we believe enables us to operate **more securely in the public cloud than we can in our own data centers.**
>
> **Rob Alexander**
> CIO, Capital One

Capital One is one of the nation's largest banks and offers credit cards, checking and savings accounts, auto loans, rewards, and online banking services for consumers and businesses.

- Capital One recognized that its customers are adopting mobile and digital platforms rapidly
- It is using AWS to develop, test, build, and run its most critical workloads, including its new flagship mobile-banking application
- As part of this strategy, Capital One looks to reduce its datacenter footprint from eight to three by 2018
- Capital One selected AWS for:
  - Its security model and pace of innovation
  - Elasticity to handle purchasing demands at peak times and high availability

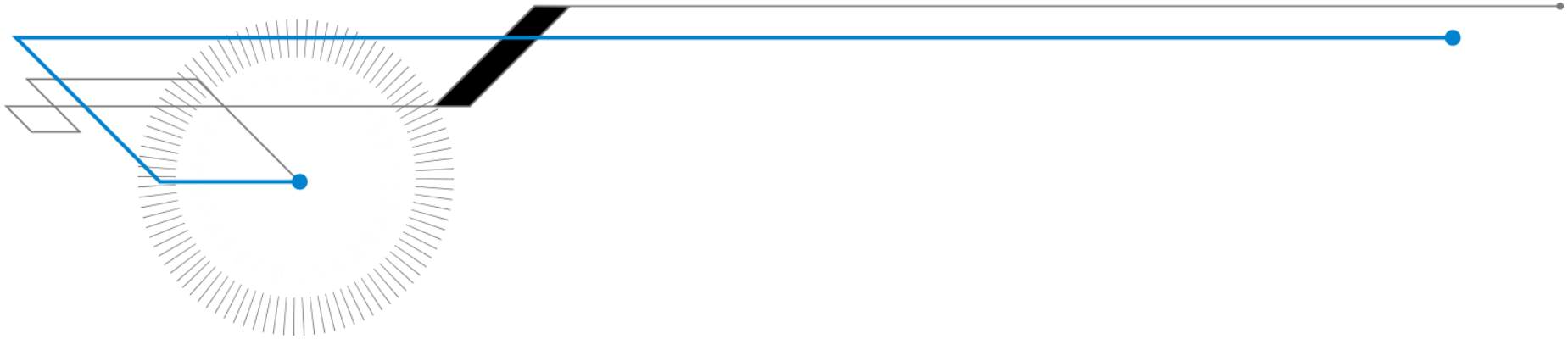
amazon web services

Security is Familiar

We strive to make security at AWS as familiar as what you are doing right now

- Visibility
- Auditability
- Controllability

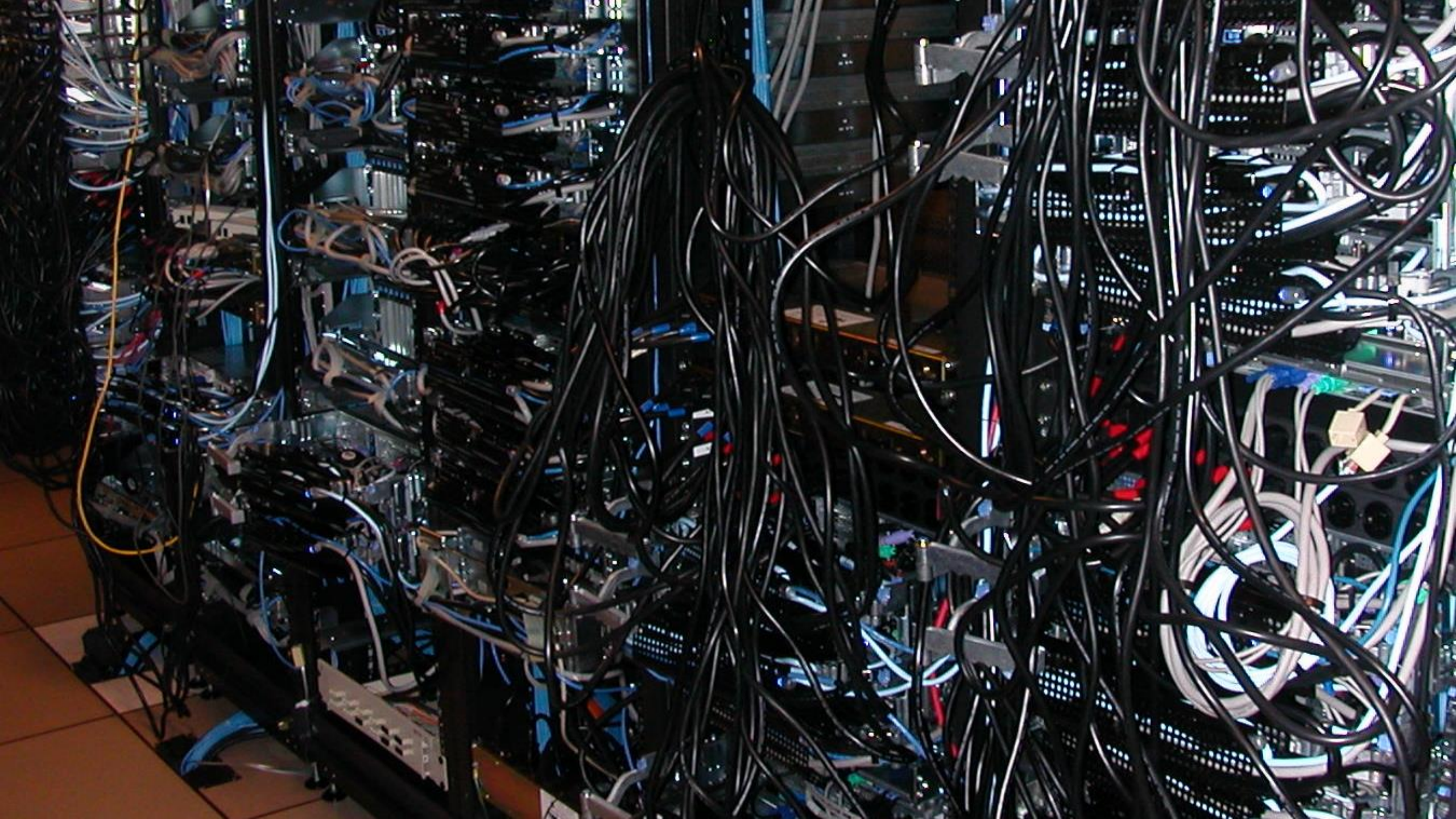
VISIBILITY

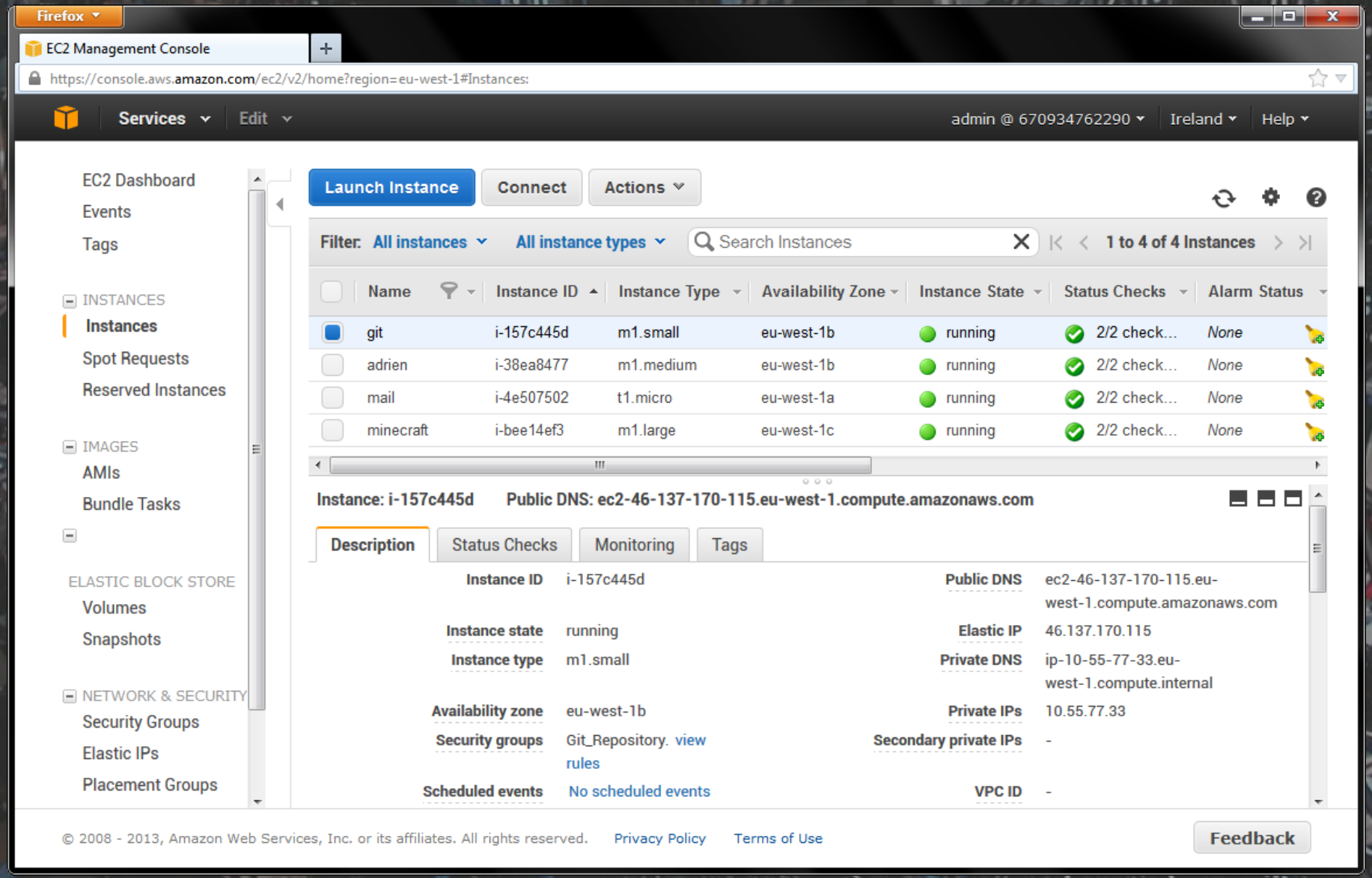


VISIBILITY

HOW OFTEN DO YOU MAP YOUR NETWORK?

WHAT'S IN YOUR ENVIRONMENT
RIGHT NOW?



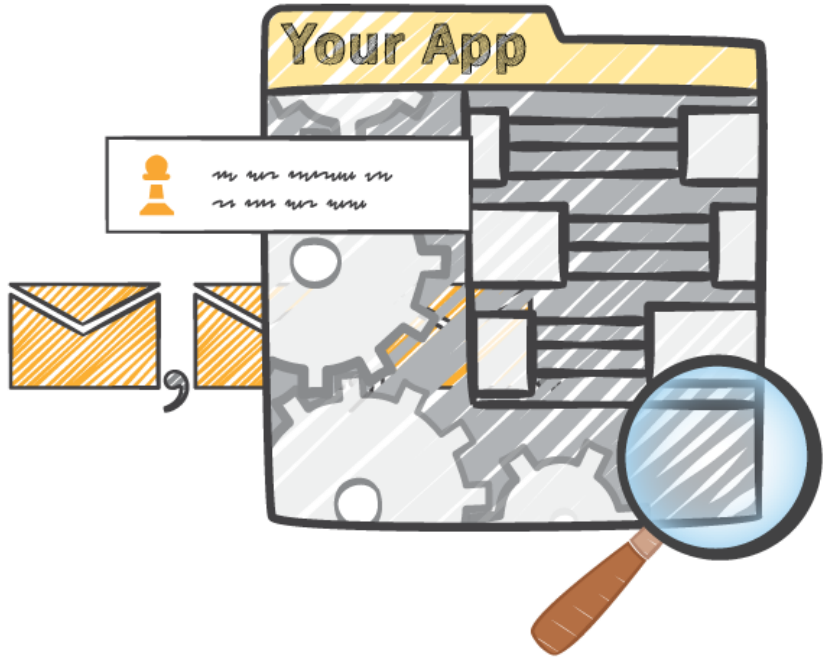

Firefox
EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=eu-west-1#Instances:
Services
Edit
admin @ 670934762290
Ireland
Help
EC2 Dashboard
Events
Tags
INSTANCES
Instances
Spot Requests
Reserved Instances
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
NETWORK & 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

Security is Visible

Who is accessing the resources?

Who took what action?

- When?
- From where?
- What did they do?
- Logs Logs Logs



CloudTrail

Your staff or scripts make calls…

on AWS API endpoints…

CloudTrail logs this to an S3 bucket…

so you can review this log

Use cases enabled by CloudTrail

Security Analysis

- Use log files as an input into log management and analysis solutions to perform security analysis and to detect user behavior patterns

Track Changes to AWS Resources

- Track creation, modification, and deletion of AWS resources such as Amazon EC2 instances, Amazon VPC security groups and Amazon EBS volumes

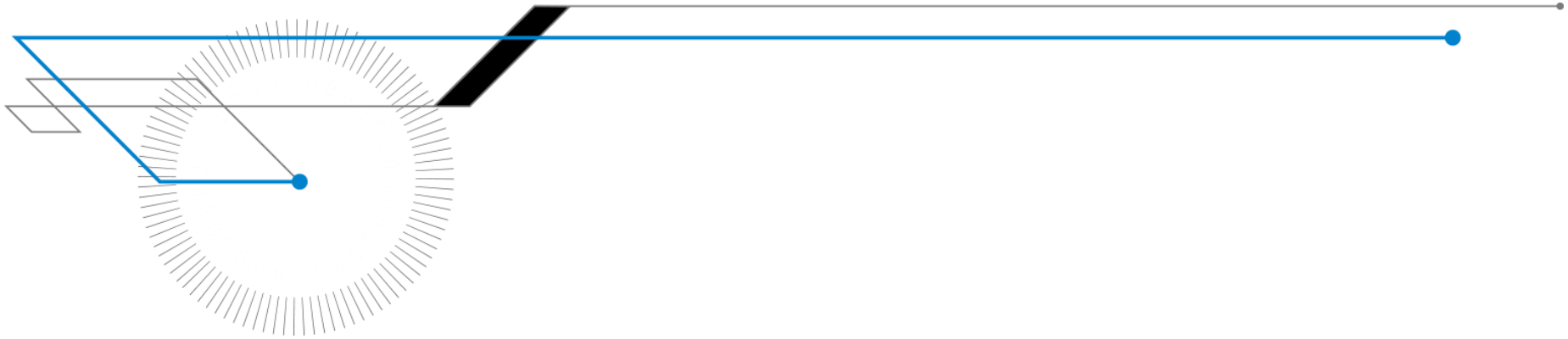
Troubleshoot Operational Issues

- Identify the most recent actions made to resources in your AWS account

Compliance Aid

- Easier to demonstrate compliance with internal policies and regulatory standards

AUDITABILITY

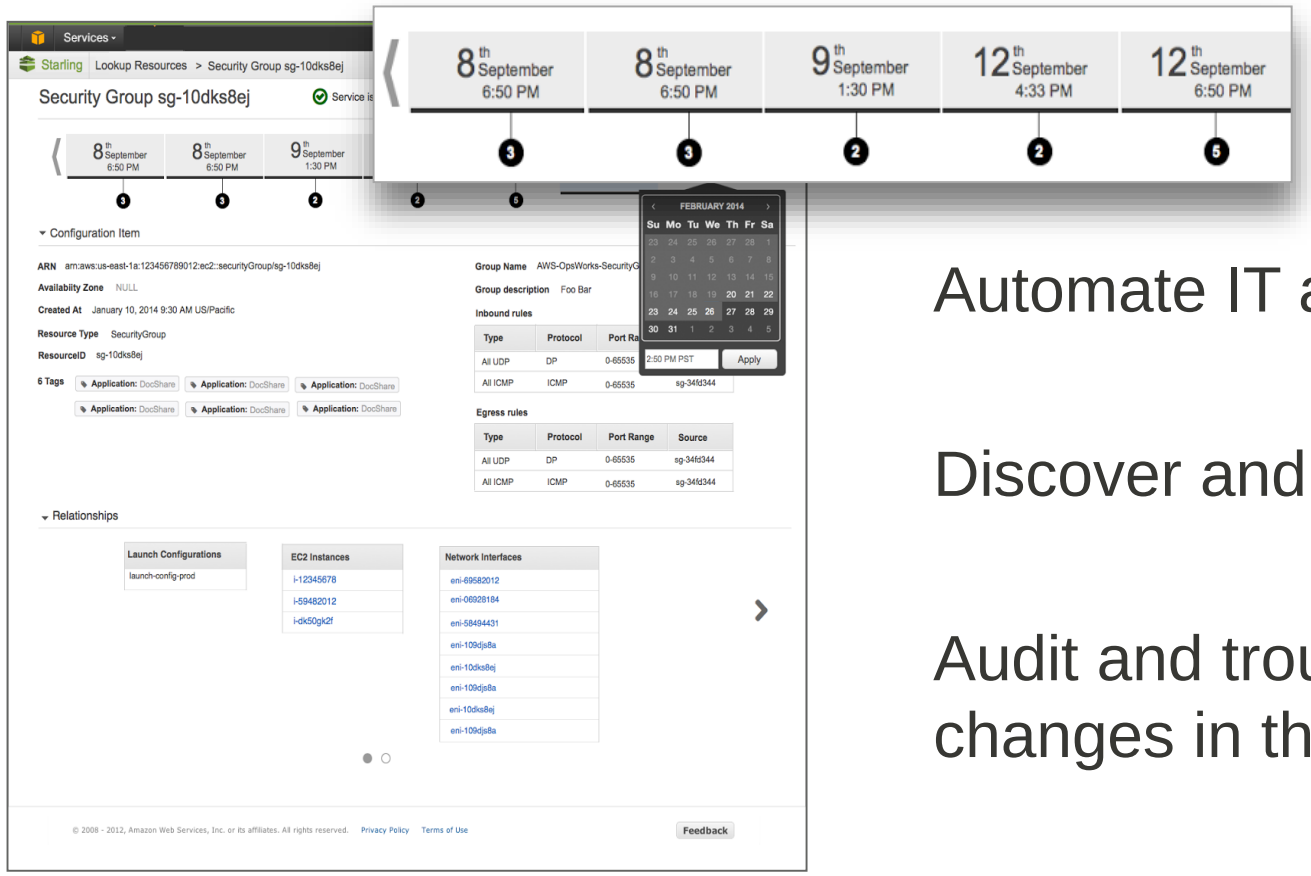


amazon web services

AWS Config

AWS Config is a fully managed service that provides you with an inventory of your AWS resources, lets you audit the resource configuration history and notifies you of resource configuration changes.

Understand Configuration Changes



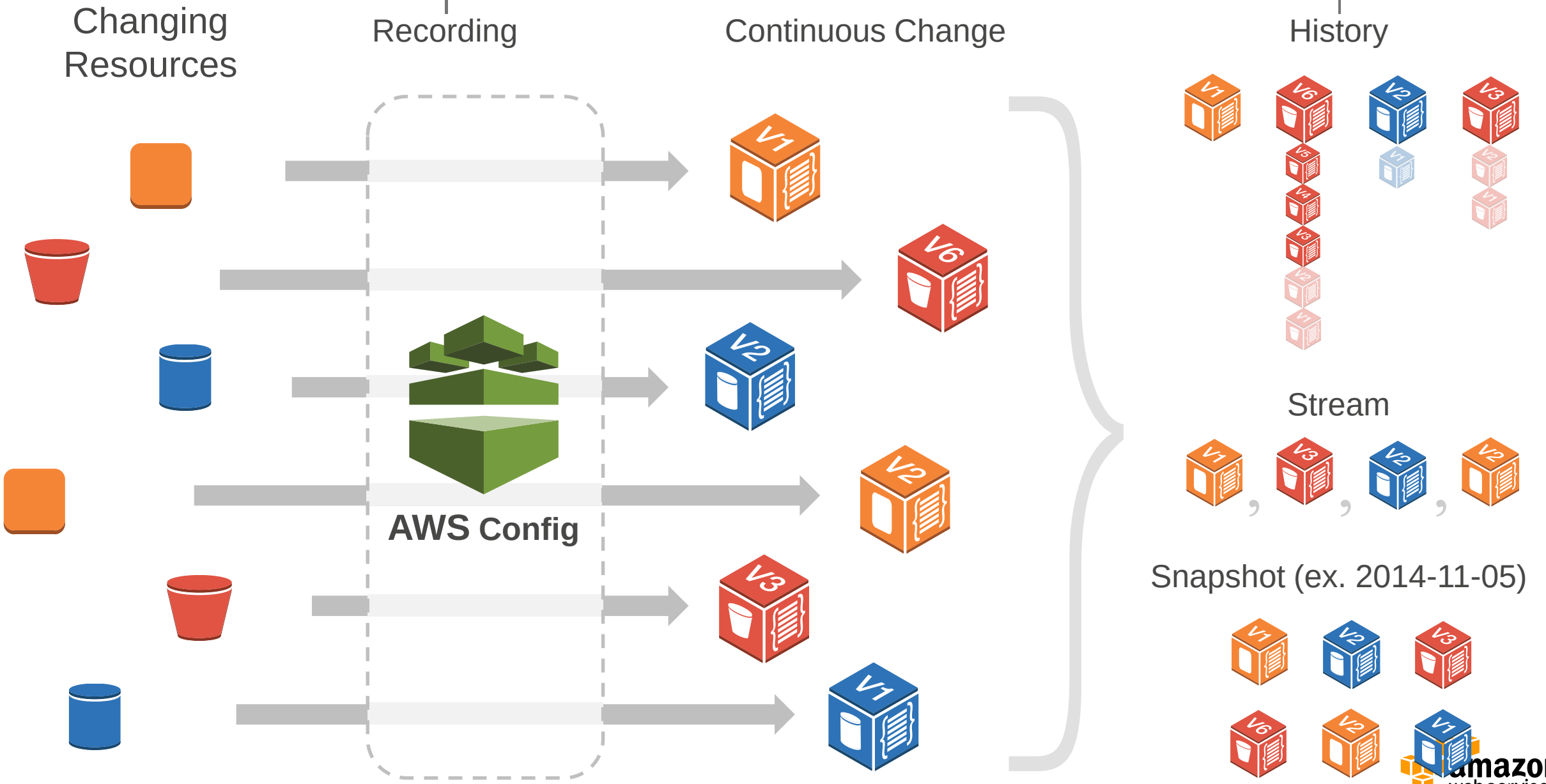
Automate IT asset inventory

Discover and provision cloud services

Audit and troubleshoot configuration changes in the cloud

amazon web services

AWS Config


Changing Resources
Recording
Continuous Change
History
AWS Config
Stream
Snapshot (ex. 2014-11-05)

Use cases enabled by AWS Config

Security Analysis

Audit Compliance

Change Management

Troubleshooting

Security Analysis: Am I safe?

Properly configured resources are critical to security

Config enables you to continuously monitor the configurations of your resources and evaluate these configurations for potential security weaknesses

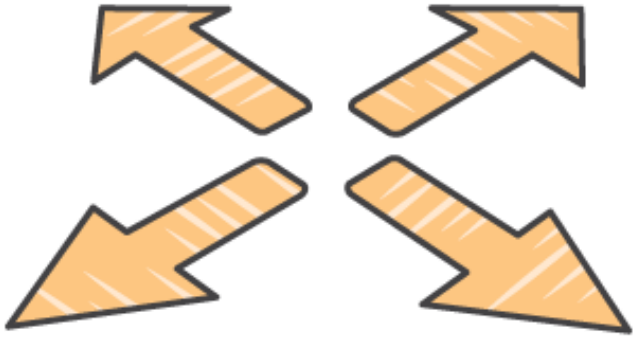
Audit Compliance - Where is the evidence?

Many compliance audits require access to the state of your systems at arbitrary times (i.e. PCI, HIPAA)

A complete inventory of all resources and their configuration attributes is available for any point in time

Change Management - What will this change affect?

When your resources are created, updated, or deleted, these configuration changes are streamed to Amazon SNS



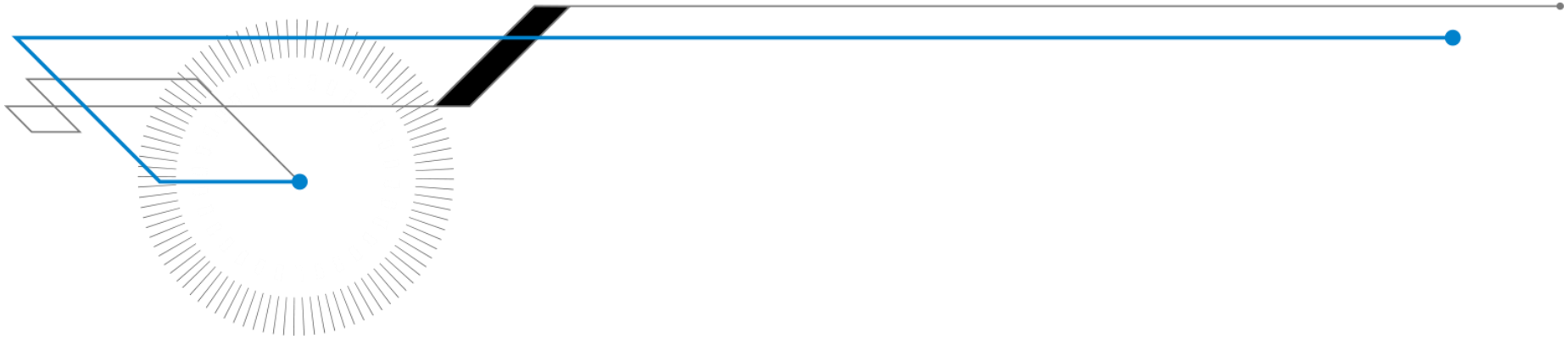
Relationships between resources are understood, so that you can proactively assess change impact

Toubleshooting - What changed?

It is critical to be able to quickly answer “What has changed?”

You can quickly identify the recent configuration changes to your resources by using the console or by building custom integrations with the regularly exported resource history files

CONTROL



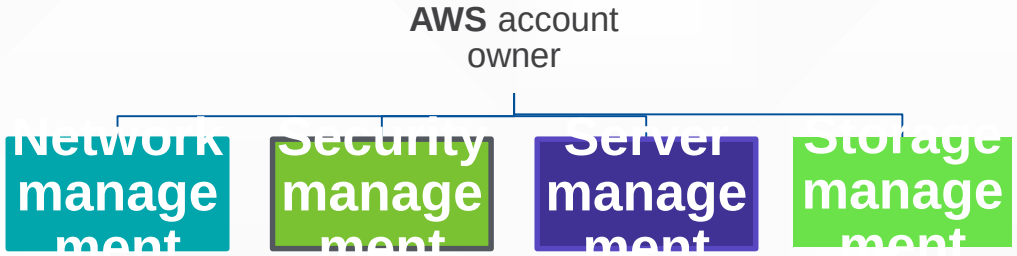
amazon web services

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

Enforce consistent security on servers

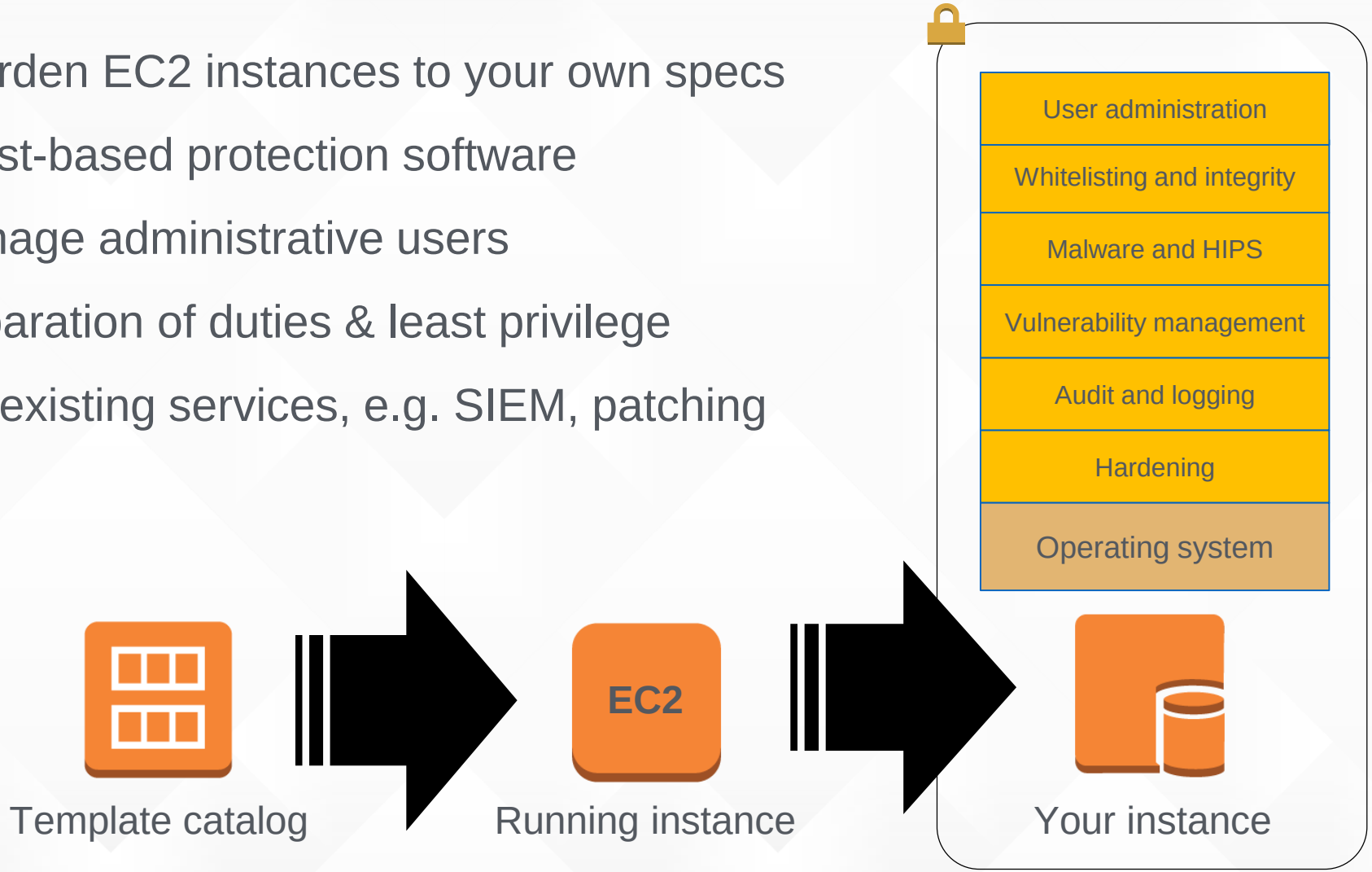
Configure and harden EC2 instances to your own specs

Use host-based protection software

Manage administrative users

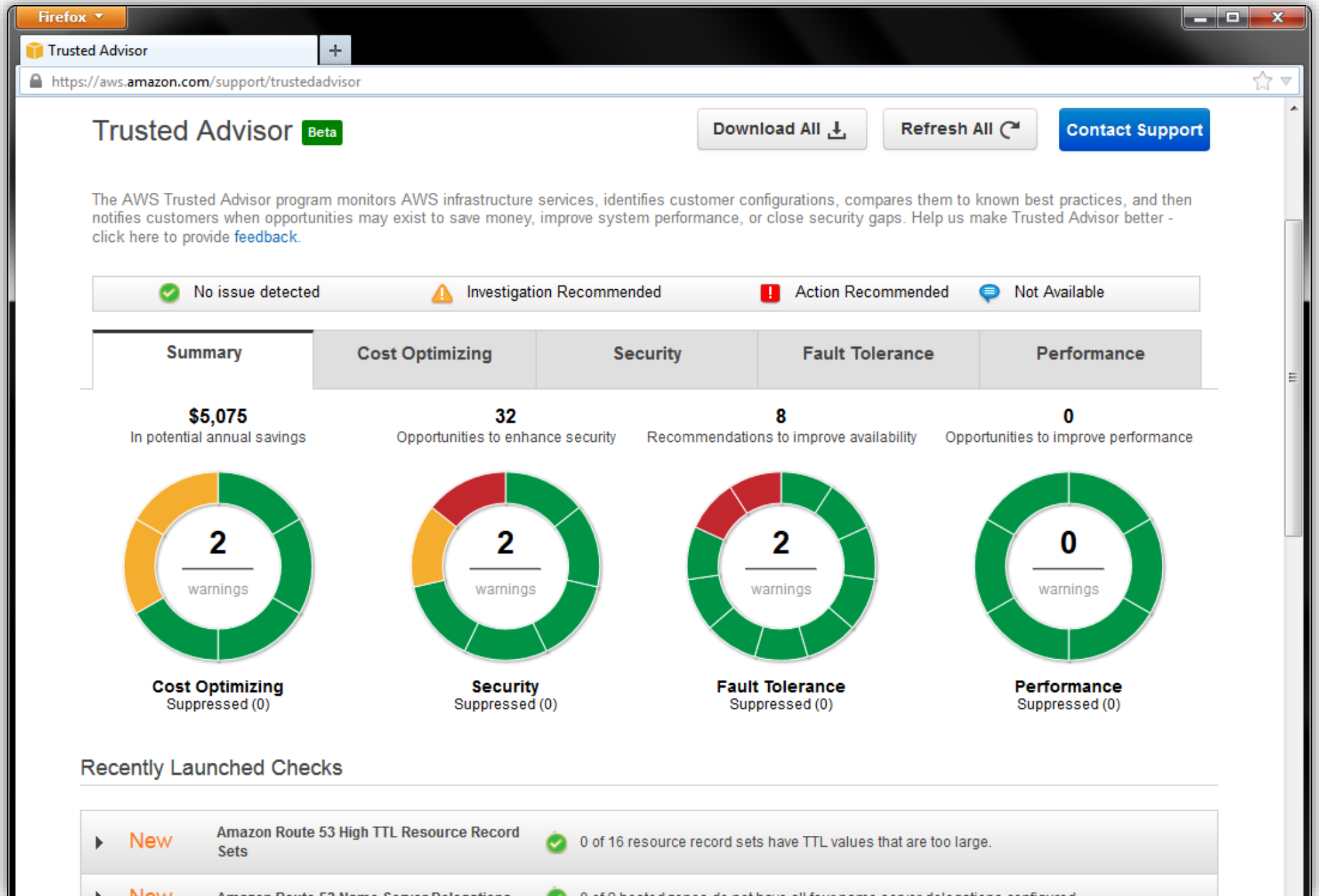
Enforce separation of duties & least privilege

Connect to your existing services, e.g. SIEM, patching



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.


Firefox
Trusted Advisor
https://aws.amazon.com/support/trustedadvisor
Trusted Advisor
Beta
Download All
Refresh All
Contact Support
The AWS Trusted Advisor program monitors AWS infrastructure services, identifies customer configurations, compares them to known best practices, and then notifies customers when opportunities may exist to save money, improve system performance, or close security gaps. Help us make Trusted Advisor better - click here to provide feedback.
No issue detected
Investigation Recommended
Action Recommended
Not Available
Summary
Cost Optimizing
Security
Fault Tolerance
Performance
$5,075
In potential annual savings
32
Opportunities to enhance security
8
Recommendations to improve availability
0
Opportunities to improve performance
2
warnings
Cost Optimizing
Suppressed (0)
2
warnings
Security
Suppressed (0)
2
warnings
Fault Tolerance
Suppressed (0)
0
warnings
Performance
Suppressed (0)
Recently Launched Checks
New
Amazon Route 53 High TTL Resource Record Sets
0 of 16 resource record sets have TTL values that are too large.

Well Architected Program

Assesses Security, Reliability, Performance and Cost Optimization

Recommending best practices

Performed by AWS

AWS Well-Architected Framework

October 2015

amazon web services

Integrated Support from Our Partner Ecosystem

amazon web services

AWS Marketplace: One-stop shop for security tools

35 categories +
2.700+ product listings from more than 925 ISVs

Advanced Threat Analytics	Application Security	Identity and Access Mgmt	Server & Endpoint Protection	Network Security	Encryption & Key Mgmt	Vulnerability & Pen Testing
ALERTLOGIC	IMPERVA	CIPHERGRAPH networks	TREND MICRO	FORTINET	SafeNet	tenable network security
ALIEN VAULT	FORTINET	SECUREAUTH	intel Security	SOPHOS	Vormetric	QUALYSGUARD
	Barracuda	M-Pin SSO Authentication for Enterprises		Check Point We Secure the Internet.	HYTRUST	
				paloalto networks.		

amazon web services

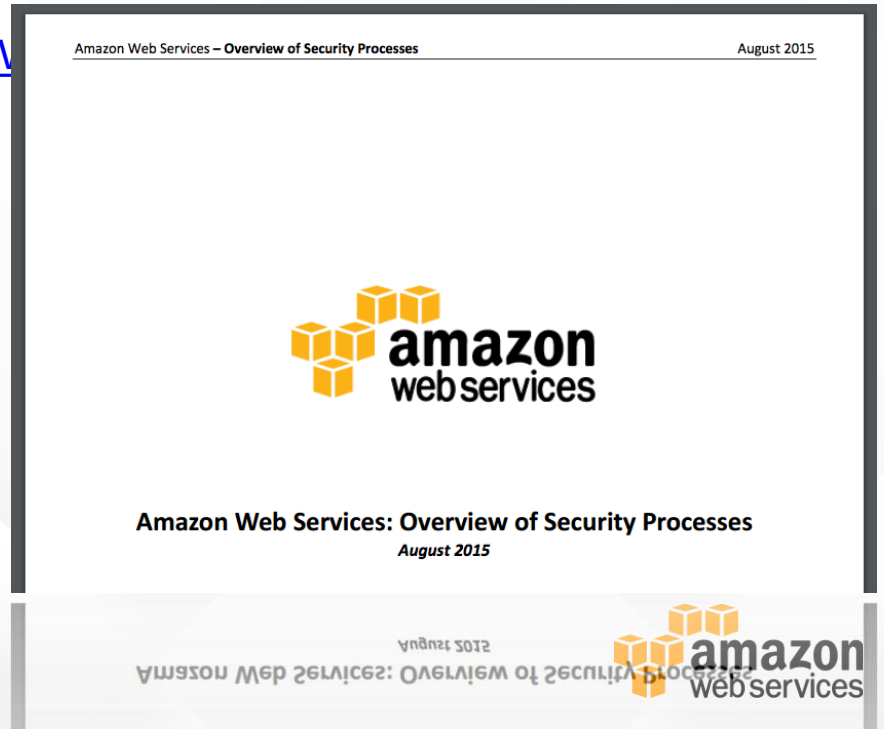
Documentation

- AWS Security Whitepaper

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

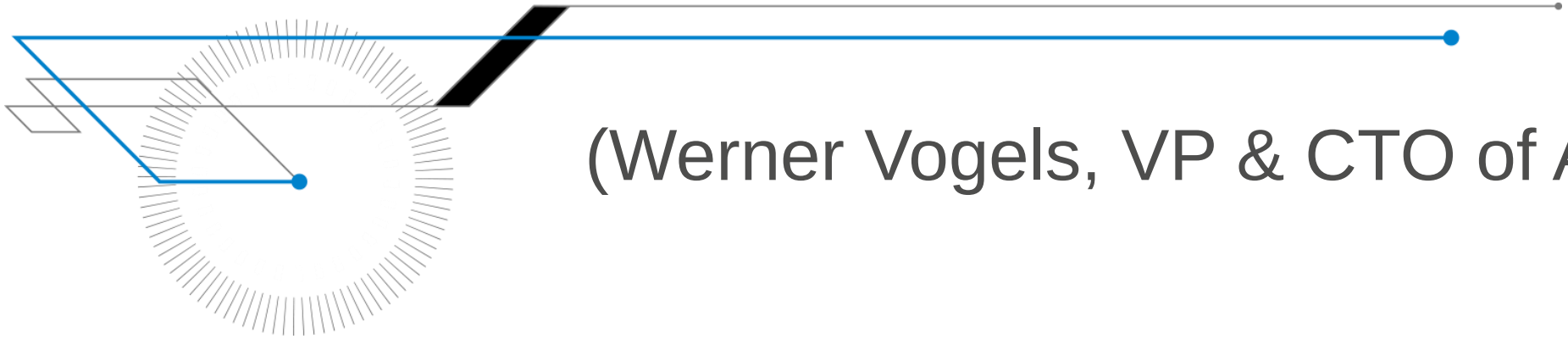
  http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_W
aper.pdf
- AWS Security Best Practices

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



High Availability

“Everything fails all the time”



(Werner Vogels, VP & CTO of Amazon.com)

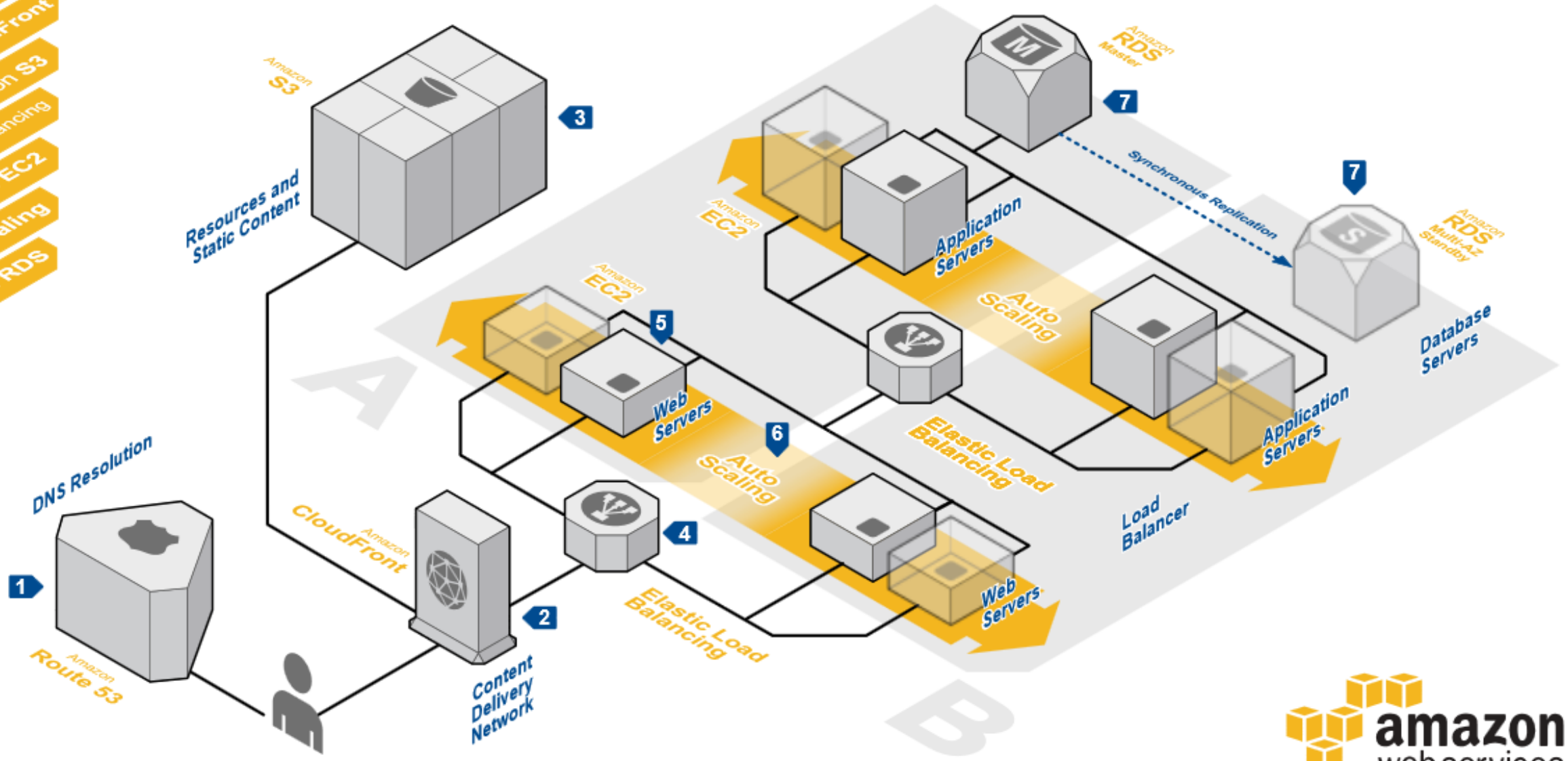
amazon web services

AWS Reference Architectures

- Amazon Route 53
- Amazon CloudFront
- Amazon S3
- Elastic Load Balancing
- Amazon EC2
- Auto Scaling
- Amazon RDS

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.



amazon web services

Summary

- Security is job zero for AWS
- AWS takes care of the security **OF** the Cloud
- You define your controls **IN** the Cloud
- Compliance is more cost effective in AWS – you got more visibility, auditability and controllability
- “Everything fails all the time” – so be prepared for it by architecting with redundancy in mind

Q & A

Thank you