https://bit.ly/2zJJ3Fh

AWS Israel Community

Sponsors

datree.io

aws

Overcoming messy things on AWS

AWS Israel Community

- Founded - Feb **2013**
- **86** meetups with **~6000** Members
- Monthly meetups
- No Marketing, No bullshit
- All AWS: AI, BigData, Serverless, Containers, etc

MEET THE TEAM

Shimon Tolts

Arthur Schmunk

Tal Hibner

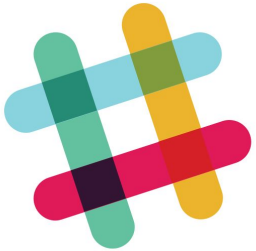
Niv Yungelson

Eitan Sela

Doron Rogov

Boaz Ziniman

Join the Community!



https://bit.ly/2zJJ3Fh

https://www.meetup.com/AWS-IL/

https://www.meetup.com/AWS-IL/

Upcoming Meetups

13/03 - AWS Summit Tel Aviv

April meetup - Deep Dive into newly announced services

Overcoming messy things on AWS

- Super charge your AWS Storage by Shlomi Avihou
- Compliance in the Cloud and how it can prevent the next data breach by Offir Zigelman, Product Manager at Dome9.
- Replacing network rules with application identity by Ran Marom, Director of Product Management at Portshift.

Supercharge your AWS storage

AWS Israel Community

Nice to meet you!

Shlomi Avihou
Operations > PdM
Zadara

zadara

Agenda

- Quick (very!) Zadara introduction
- Connectivity – AWS Direct Connect
- Glimpse of data protection
- Q&A

Quick introduction

5 slides :)

What?

Enterprise Storage-as-a-Service

Any Data Type
- Block
- File
- Object

Any Protocol
- FC, iSCSI, iSER
- NFS, CIFS
- S3, Swift

Any Location
- On-Premises
- Public or Private Cloud
- Hybrid

zadara

Why?

Block, file and object storage

All-Flash + dedupe; SSD cache options

Thin provisioned volumes

Large volume sizes

NFS, CIFS (AD), FC, iSCSI, iSER

Multi-zone high-availability

Non-disruptive upgrades

Remote mirroring

Cluster support

At-rest, in-flight data encryption

zadara

Where?

On Premises

Managed Service Provider

Public Clouds

zadara

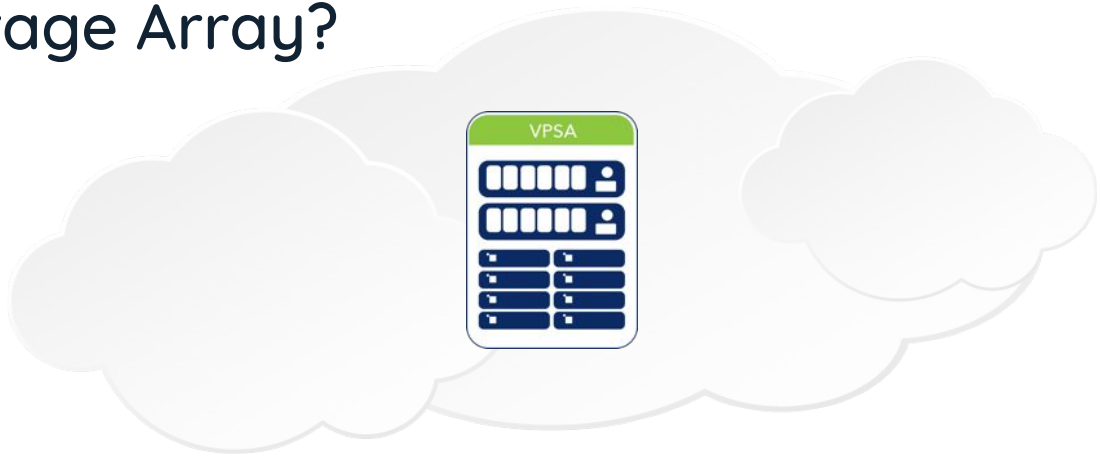
When?

now!

manage.zadarastorage.com

zadara

What is a VPSA Storage Array?

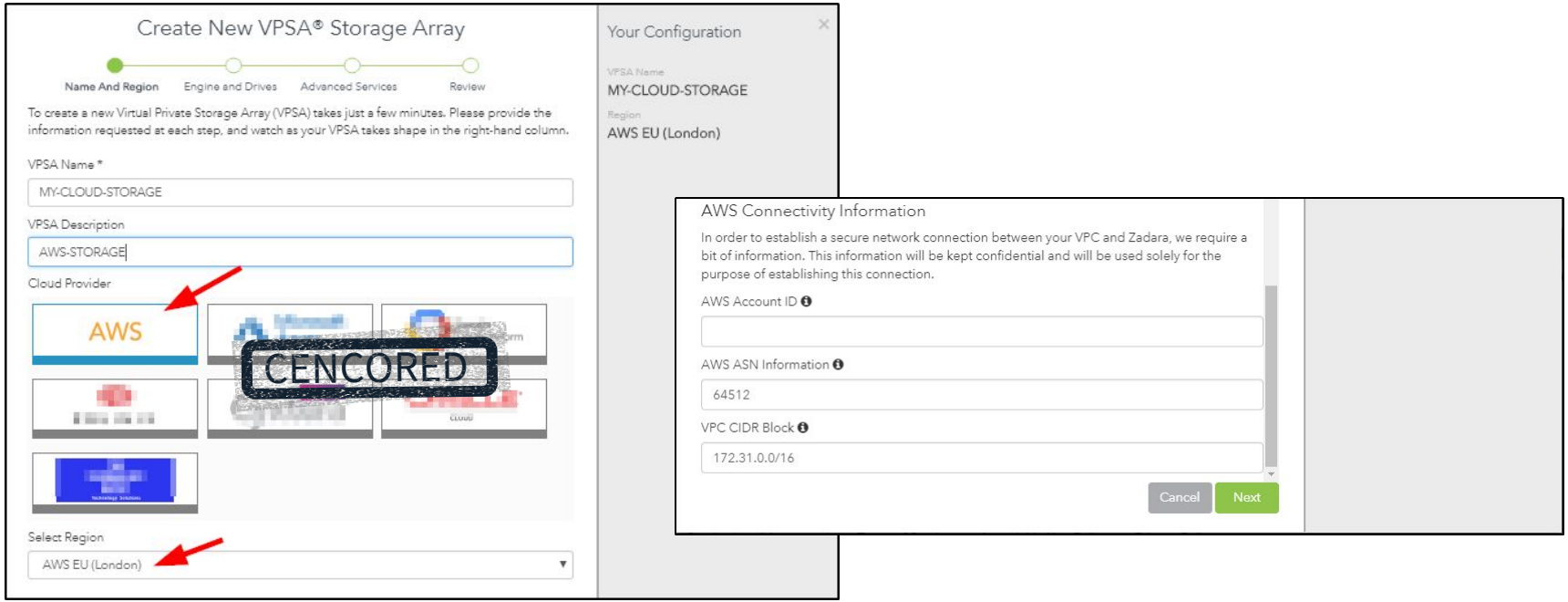


- Block and File Storage
- NFS, CIFS (Active Directory), Fibre Channel, iSCSI, iSER
- Large Volume Sizes (200TB)
- At-Rest and In-flight Data Encryption (user owns keys) SMB Encrypt
- Cluster Support
- Thin Provisioned Volumes
- Large SSD cache options
- Non-Disruptive Upgrades
- 100% RESTful API coverage

zadara

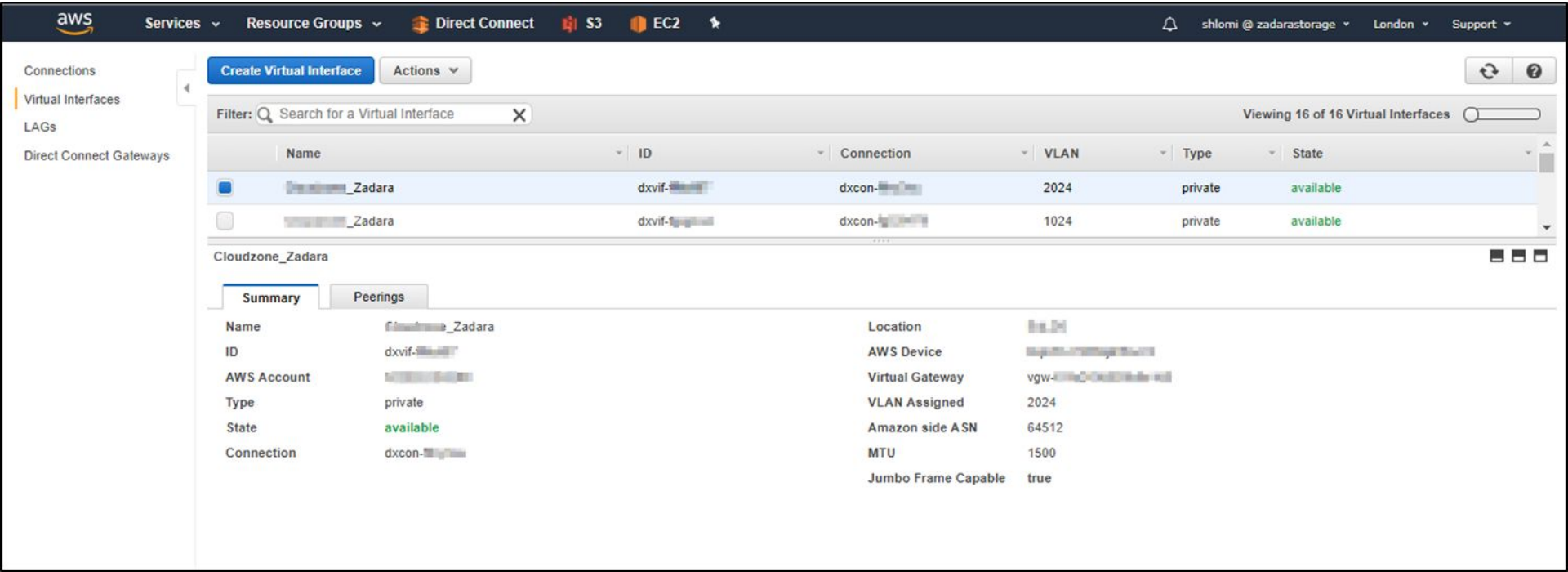
Connectivity

Connectivity – AWS Direct Connect

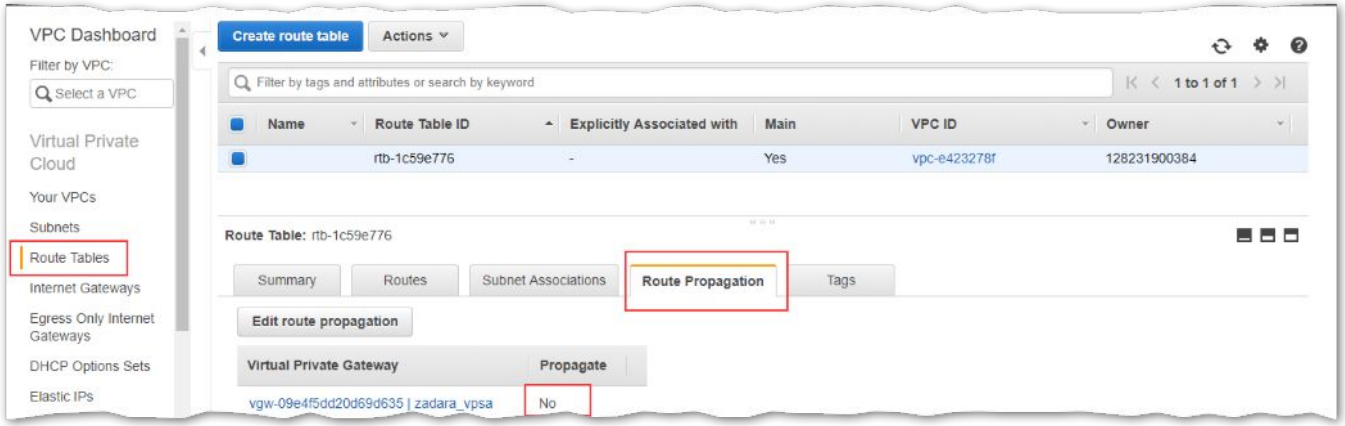


zadara

Connectivity – AWS Direct Connect – Closer look

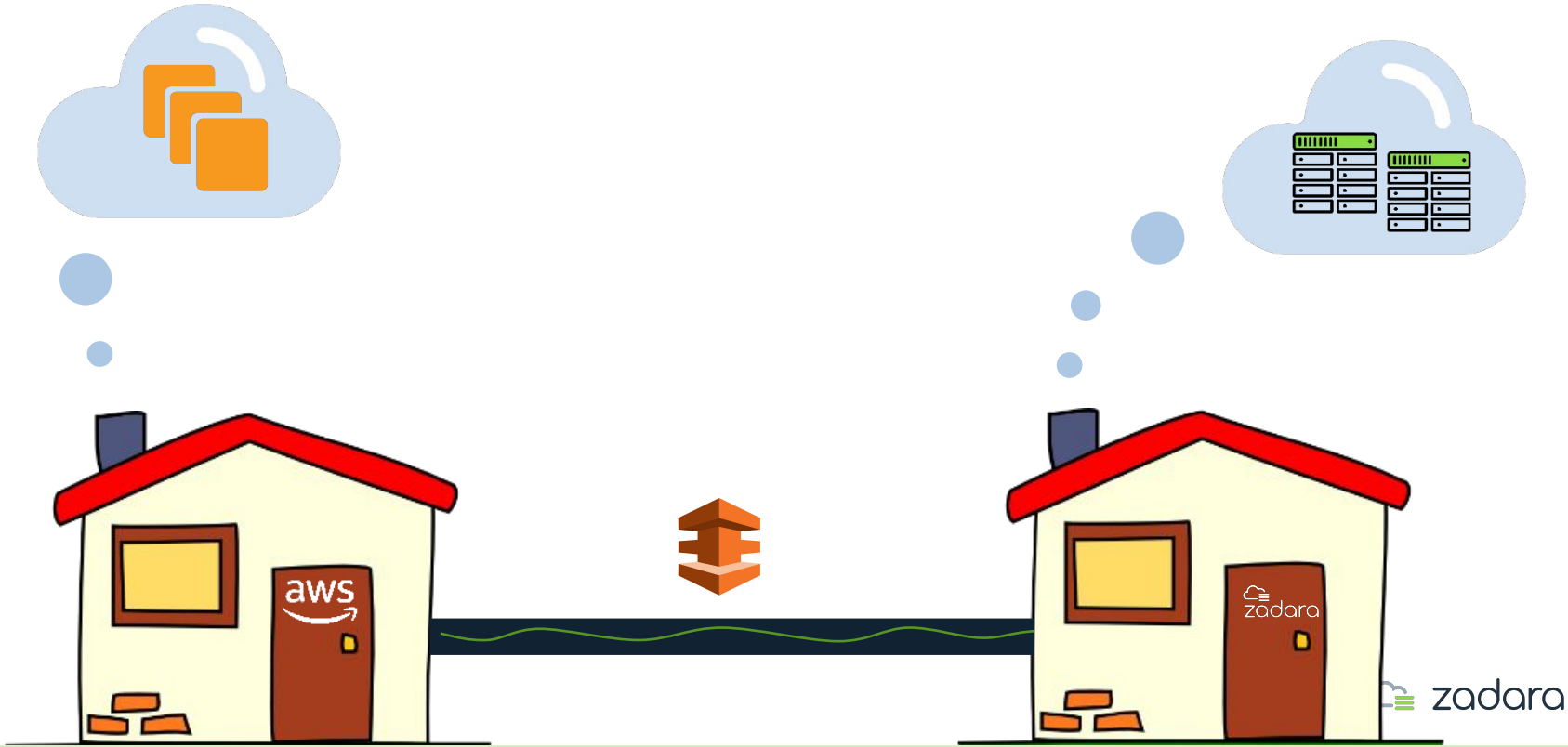


Connectivity – AWS Direct Connect – VPC



zadara

Connectivity – AWS Direct Connect



Connectivity – AWS Direct Connect – main benefits

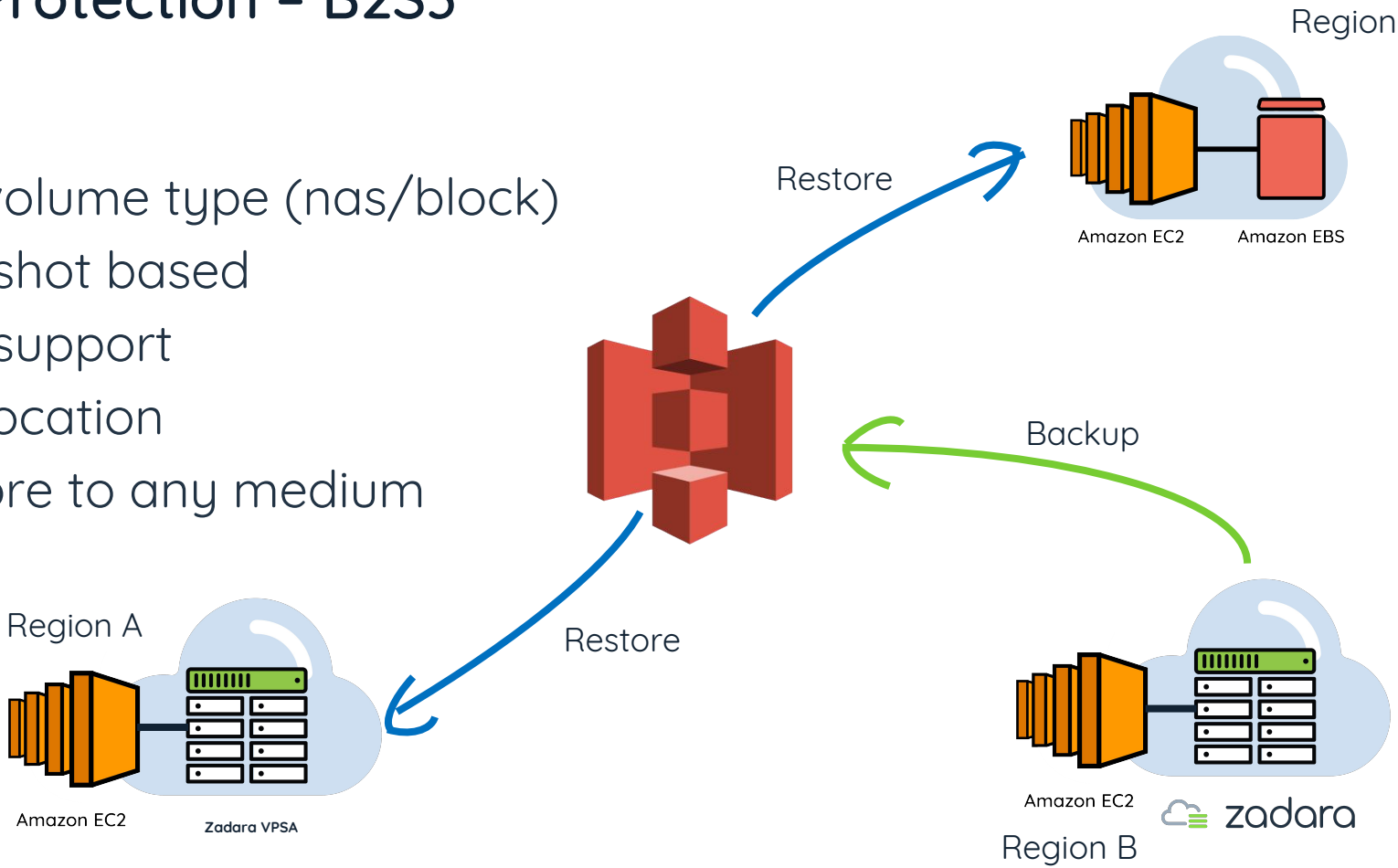
- Secured and private – tenant networking separation
- Consistent performance (up-to 10Gb)
- Low latency (< 2ms rt)
- HA – dual VIFs
- Access from multiple AZs

Data Protection

Backup to S3 (aka B2S3)

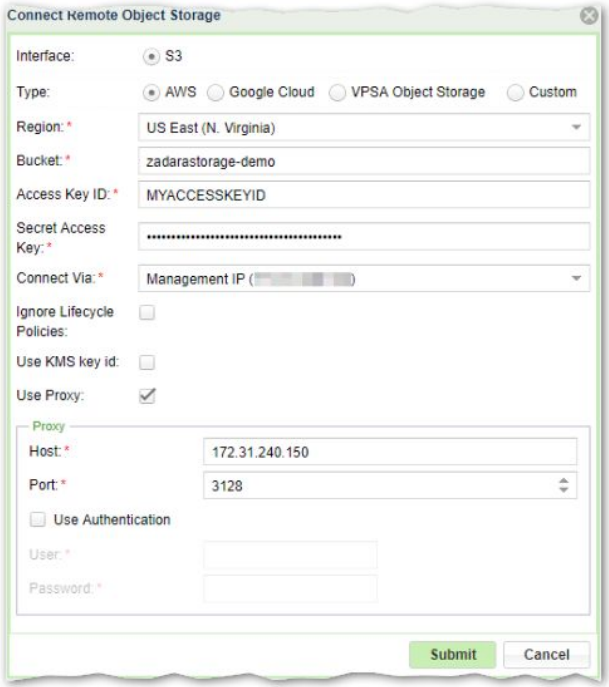
Data Protection – B2S3

- Any volume type (nas/block)
- Snapshot based
- KMS support
- Any location
- Restore to any medium

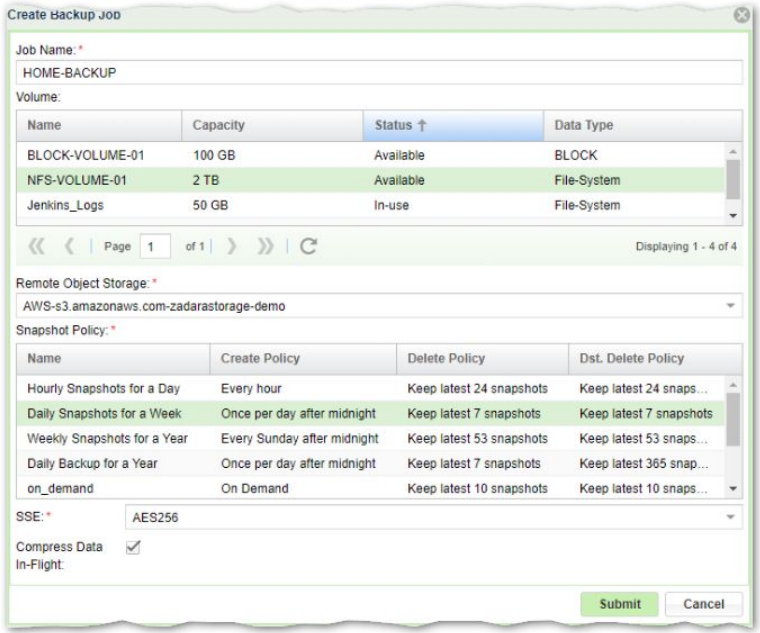


B2S3 – Restore a subset of a volume

#1 Set Remote S3 Target

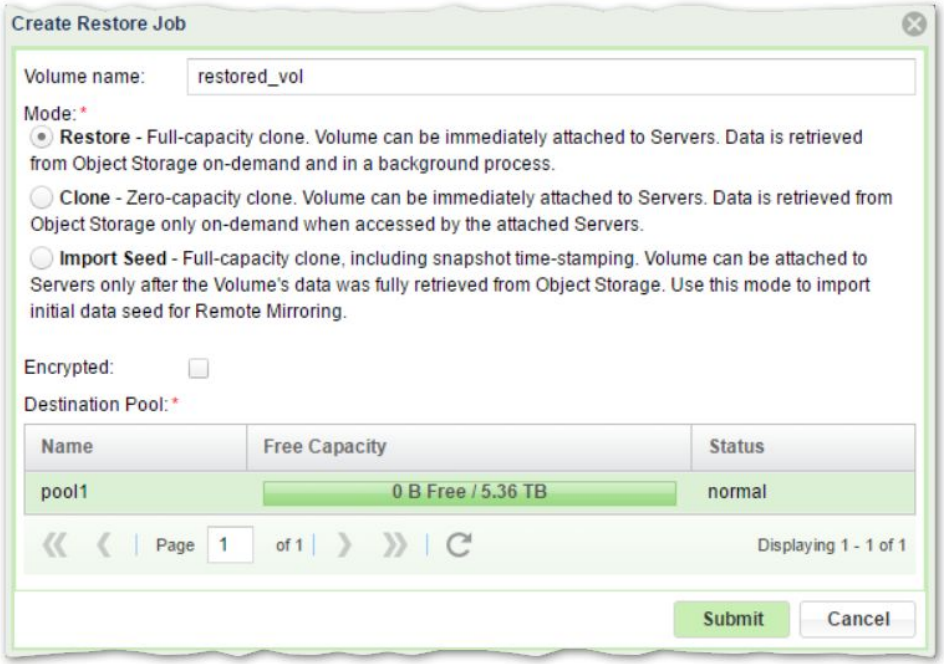


#2 Set Policy



B2S3 – Restore a subset of a volume

#3 Recover



zadara

Thank you!

shlomi@zadara.com


Compliance in the cloud
And how it can prevent the next data breach
Offir Zigelman

engadget

Aug 8, 2018 **Amazon AWS error exposes info on 31,000 GoDaddy servers**

SC MAGAZINE FOR IT SECURITY PROFESSIONALS

Jun 1, 2017 **Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS server**

eSecurity Planet

Jul 12, 2017 **Cloud Security Failure: Millions of Wrestling Fans' Personal Data Exposed**

threatpost

Jul 12, 2017 **Misconfigured Amazon Storage Exposes 14 Million Verizon Customer Records**

info security STRATEGY | INSIGHT | TECHNOLOGY

May 29, 2018 **More Data Leaked from AWS Bucket Misconfigurations**

siliconANGLE

Apr 3, 2018 **37M Panera Bread customer records found to be exposed to all and sundry in the cloud**

BUSINESS INSIDER

Jul 9, 2018 **Social media memories app Timehop got hit by a data breach affecting 21 million users**

UpGuard

Dec 18, 2018 **Cloud Leak: How A Verizon Partner Exposed Millions of Customer Accounts**

About me

Offir Zigelman

offir.zigelman@gmail.com


https://www.linkedin.com/in/offir-zigelman

- Product Manager – Dome9 (acq. by Check Point)
- System Architect – Imperva (previous)
- Work in the cloud since 2010

What's in this session for me?!

- Compliance is relevant for everyone
- Education: understand the compliance challenges in the cloud
- Replace "Compliance" with "Security": practically the same issues!

WHAT IS COMPLIANCE?

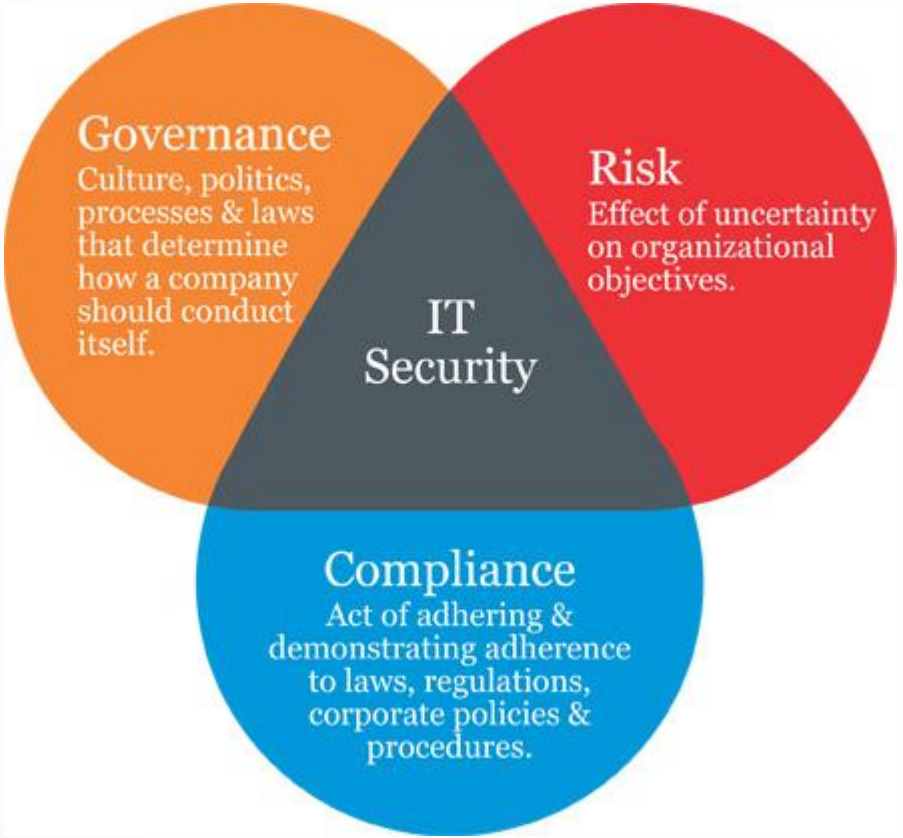
Compliance

"Computer system compliance is the state of meeting system settings which have been mandated"

AuditShark

Security Compliance enforces information security standard

GRC


Governance
Culture, politics, processes & laws that determine how a company should conduct itself.
Risk
Effect of uncertainty on organizational objectives.
IT Security
Compliance
Act of adhering & demonstrating adherence to laws, regulations, corporate policies & procedures.

Types of Compliance

- **Regulatory** (Law/Act)

  Examples:
  - GDPR (General Data Protection Regulation)
  - HIPAA (Health Insurance Portability and Accountability Act)

- **Information Security Risk Management and Compliance**

  Examples:
  - NIST (National Institute of Standards and Technology)

- **Industry Specific standards**

  Examples:
  - PCI-DSS (Payment Card Industry Data Security Standard)

Example of a Control

CIS Foundations for AWS v1.1.0

1.2 Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)

Profile Applicability:

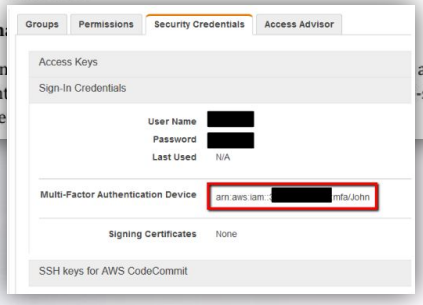
- Level 1

Description:

Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a user name and password. With MFA enabled, when a user signs in to an AWS prompted for their user name and password as well as for an auth their AWS MFA device. It is recommended that MFA be enabled fo console password.

Rationa

Enablin as it authent -sen knowle



Audit:

Perform the following to determine if a MFA device is enabled for all IAM users having a console password:
Via Management Console

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the left pane, select `Users`
3. If the `MFA Device` or `Password` columns are not visible in the table, click the gear icon at the upper right corner of the table and ensure a checkmark is next to both, then click `Close` .
4. Ensure each user having a `MFA Device` column.

Remediation:

Perform the following to enable MFA:

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Users.
3. In the User Name list, choose the name of the intended MFA user.
4. Choose the Security Credentials tab, and then choose Manage MFA Device.
5. In the Manage MFA Device wizard, choose A virtual MFA device, and then choose Next Step.

CIS Center for Internet Security®

Other frameworks, similar controls

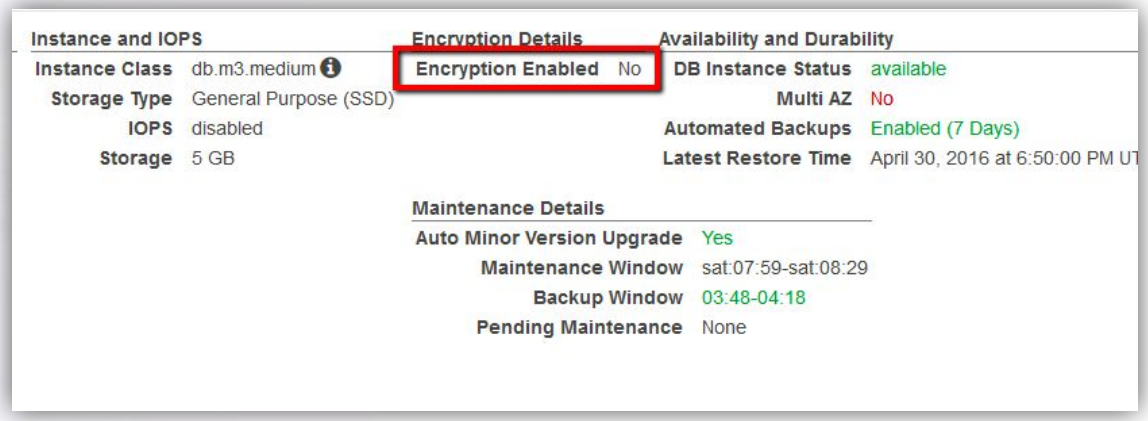
Enable MFA on “root”

- **AWS CIS Foundations** v1.1.0, Section 1.2
- **GDPR** Compliance on AWS, Article 25
- **PCI-DSS** v3.2, Sections 8.3.1, 8.3.2
- **ISO 27001:2013**, Sections A.6.2.2, A.9.1.2, A.9.2.3, A.9.3.1
- **HIPAA**, Article 164.312(e)(1)

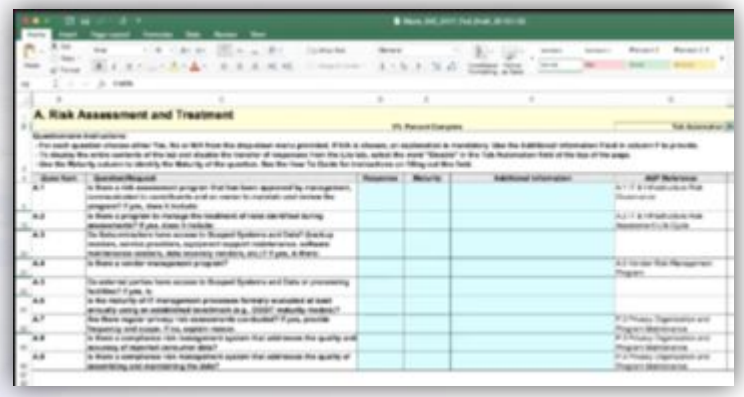
(Another) Example of a Control

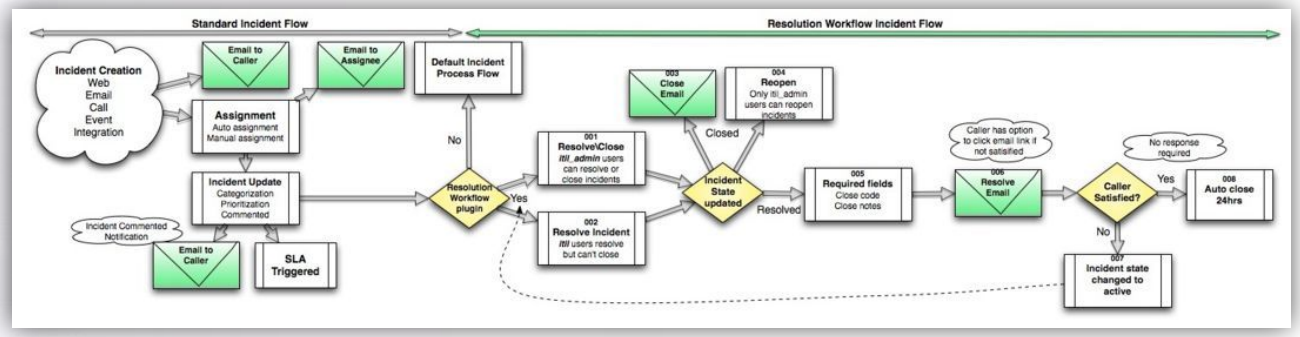
AWS PCI-DSS 3.2, Sections 3.5.3, 3.6.3:

"Use Encrypted RDS storage"



How Compliance people work(ed?)





Compliance may have legal implications

Jan 21, 2019 **GDPR: Google hit with €50 million fine by French data protection watchdog**

The “regular” compliance challenges

Speed vs. Security

Many required compliance frameworks

Information Security Management ISO 27001 Certified

PCI DSS COMPLIANT

HIPAA Health Insurance Portability and Accountability Act

GDPR

CCM™ Cloud Controls Matrix

FedRAMP

NIST National Institute of Standards and Technology U.S. Department of Commerce

AICPA Service Organization Control Reports SOC 2 Formerly SAS 70 Reports

Types of Compliance (Cont.)

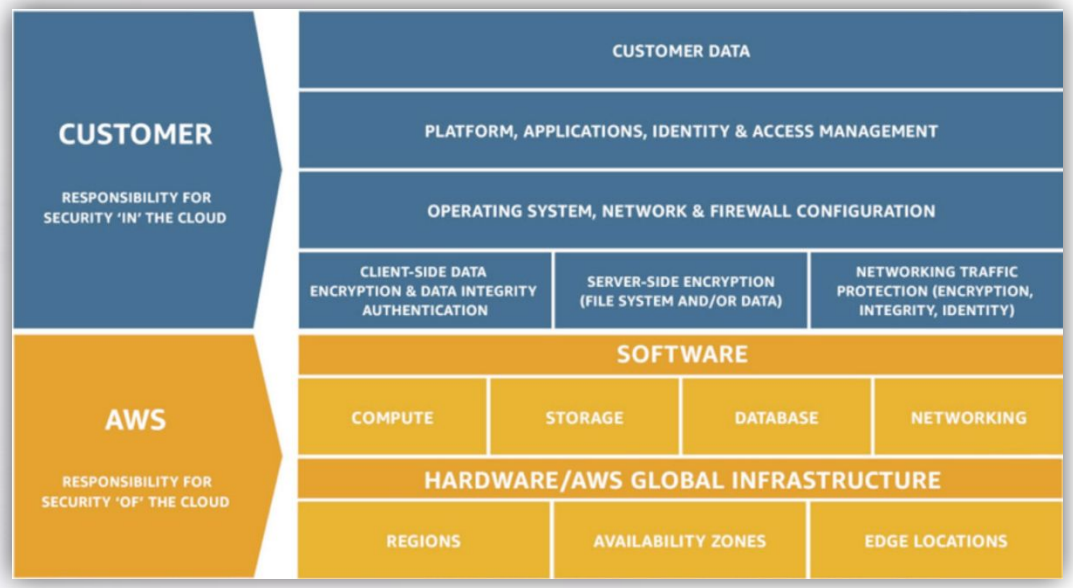
- **Regulatory** (Law/Act)
  Examples:
  - GDPR (General Data Protection Regulation)
  - HIPAA (Health Insurance Portability and Accountability Act)
- **Information Security Risk Management and Compliance**
  Examples:
  - NIST (National Institute of Standards and Technology)
- **Industry Specific standards**
  Examples:
  - PCI (Payment Card Industry Data Security Standard)
- **Organizational Policy**
  Examples:
  - All security groups need to be whitelisted to the office IP
  - Every element needs to have “owner” tag

Compliance in AWS

THE CHALLENGES

Shared Responsibility Model

It means that compliance (just like security) is your responsibility…



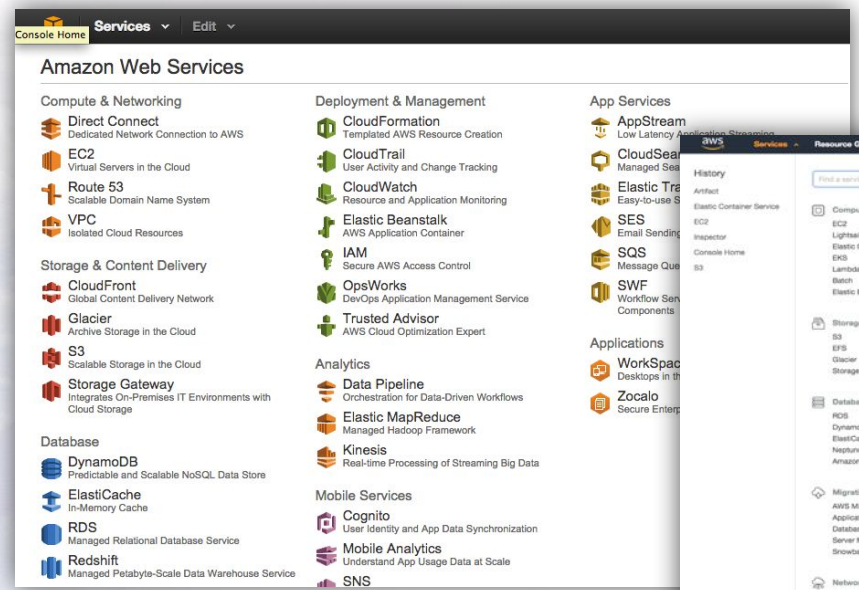
Knowledge. The lack of it…

- Cloud is relatively new (to some orgs)
- Many compliance people are not very technical

Challenge: Gaps in

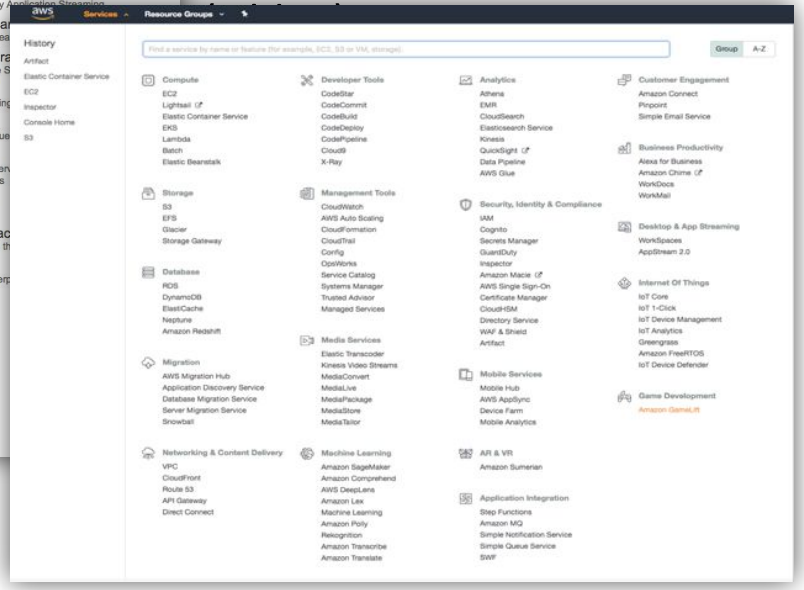
- ⚠ Understand risks
- ⚠ Governance
- ⚠ More…

Many Changes. At a fast Pace.



AWS Services, 2014

AWS Services, 2018



Challenge: Hard time for Compliance to keep up

Highly dynamic environments

- CI/CD age – new services may be used in any time
- Element scale up/down

Challenges:

⚠ No place for ~~manual compliance~~
- And for security in general…

⚠ Hard to find **what needs to be complied**

Compliance is a moving target!

of services/environments/elements

- 💯 Few years ago: every company had multiple cloud accounts
- 💯 Today: multiple accounts for every team
- 💯 Huge number of elements

Challenge: scale is a major issue

We're now in the era of enterprises managing **1000s** cloud accounts

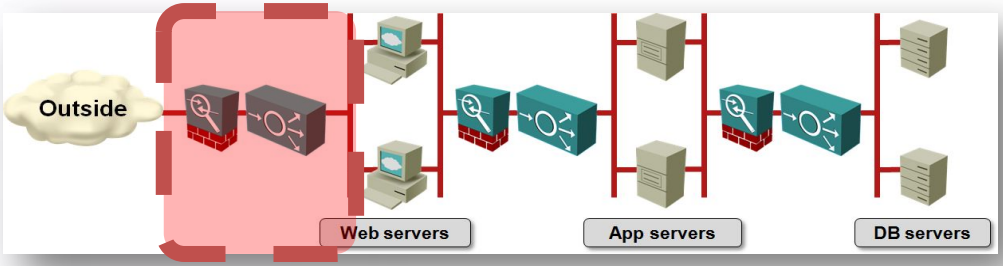
Multi Cloud

- More organizations are choosing multiple cloud platforms

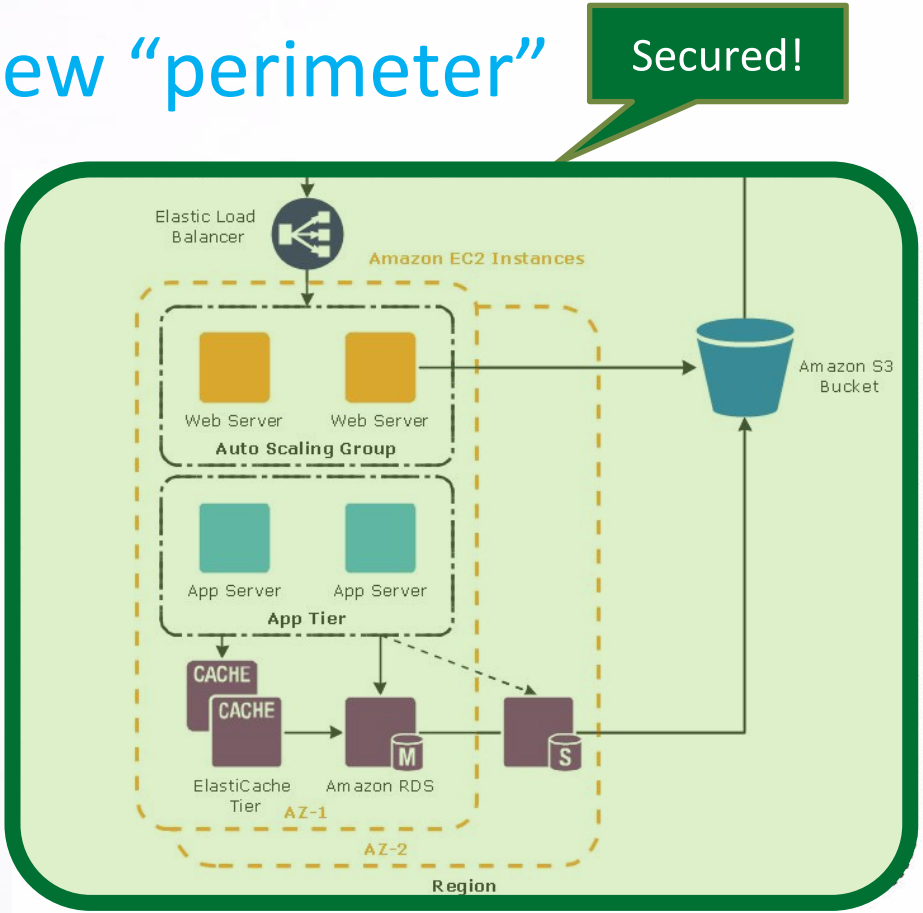
Challenge: multi-cloud compliance

The new “perimeter”

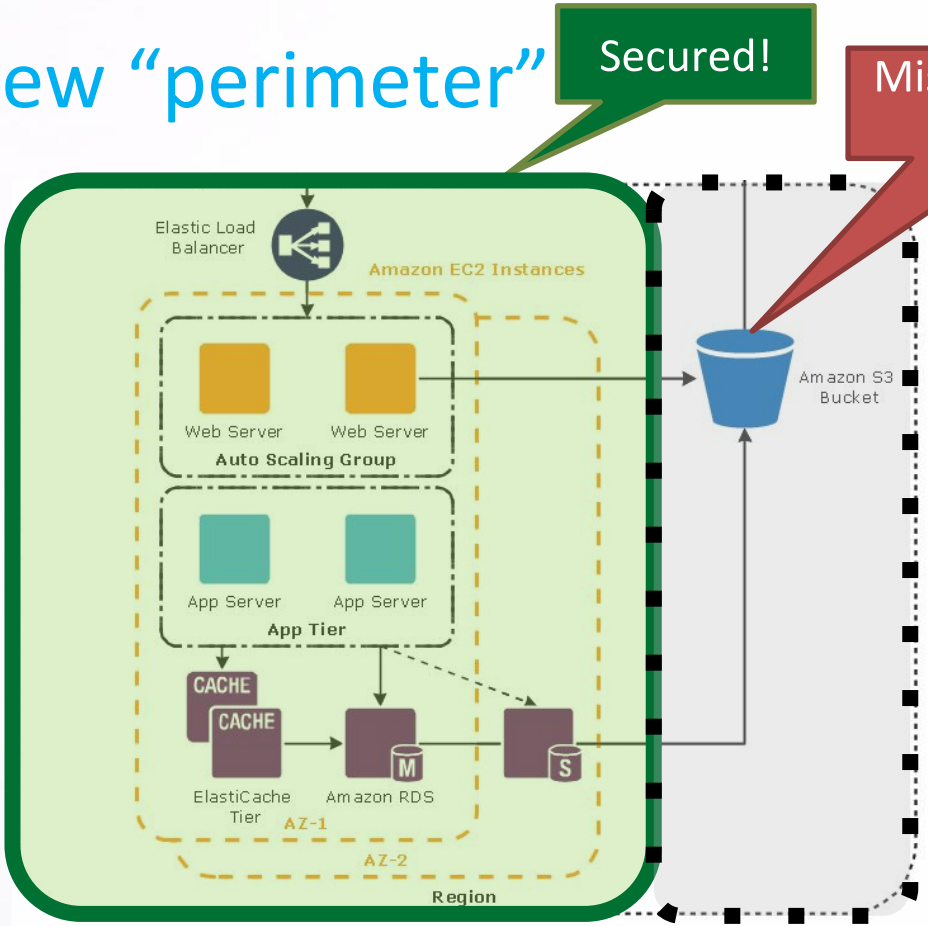
On the old datacenter, security team controlled the “perimeter”



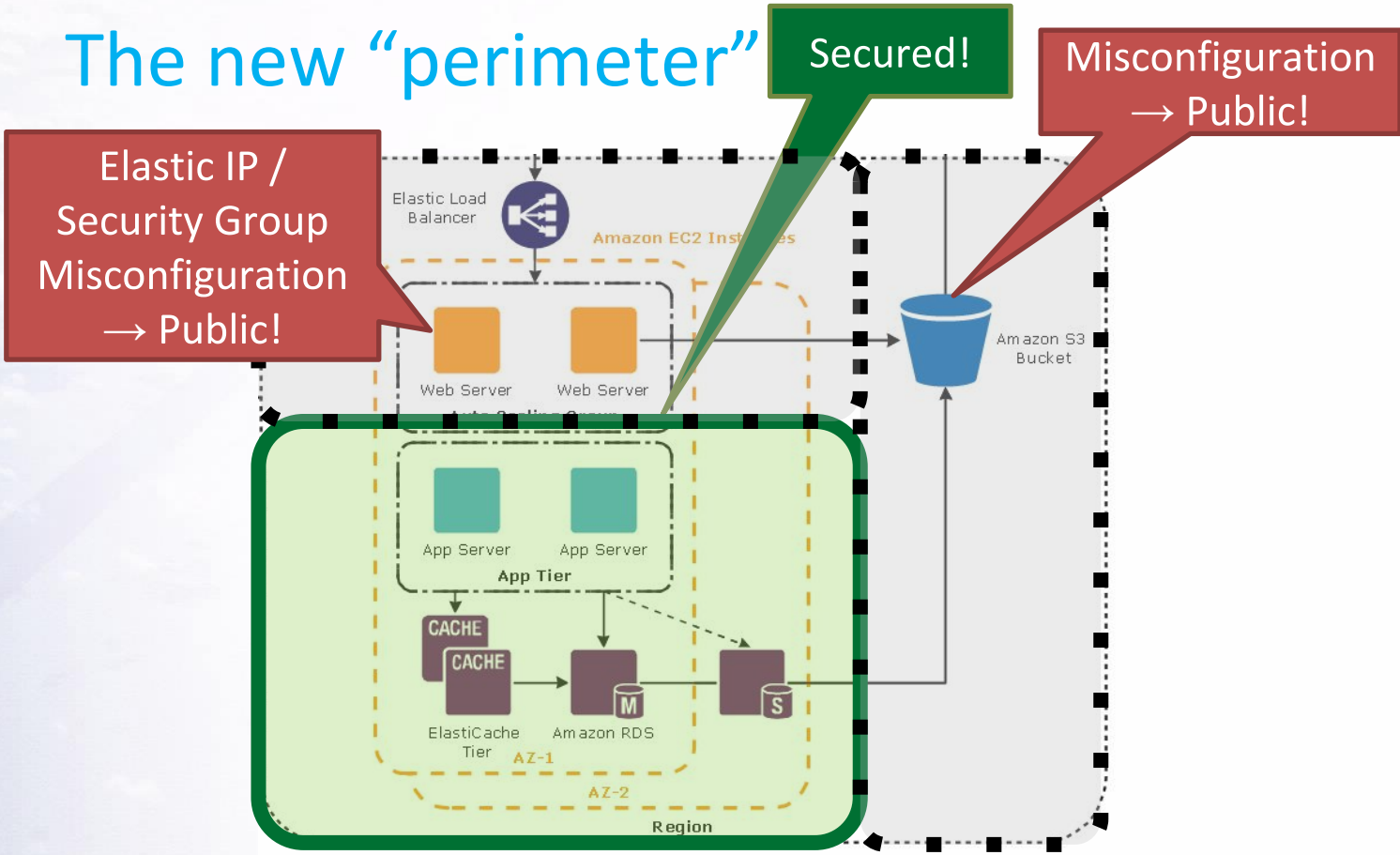
The new “perimeter”



The new “perimeter”



The new “perimeter”



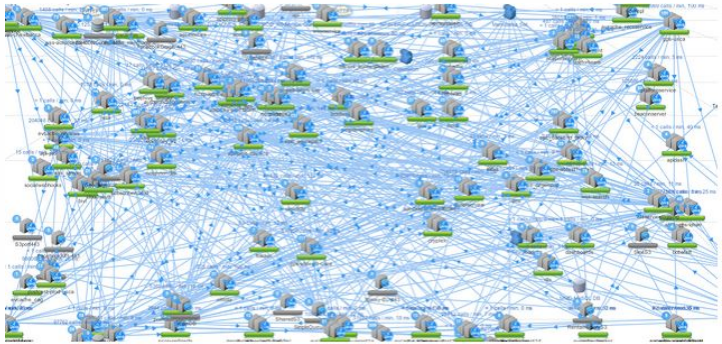
The new “perimeter”

Challenges:

⚠ Every mistake can be critical
Lead to data leakage!

⚠ Infinite points of security failures

⚠ Different OWNERS



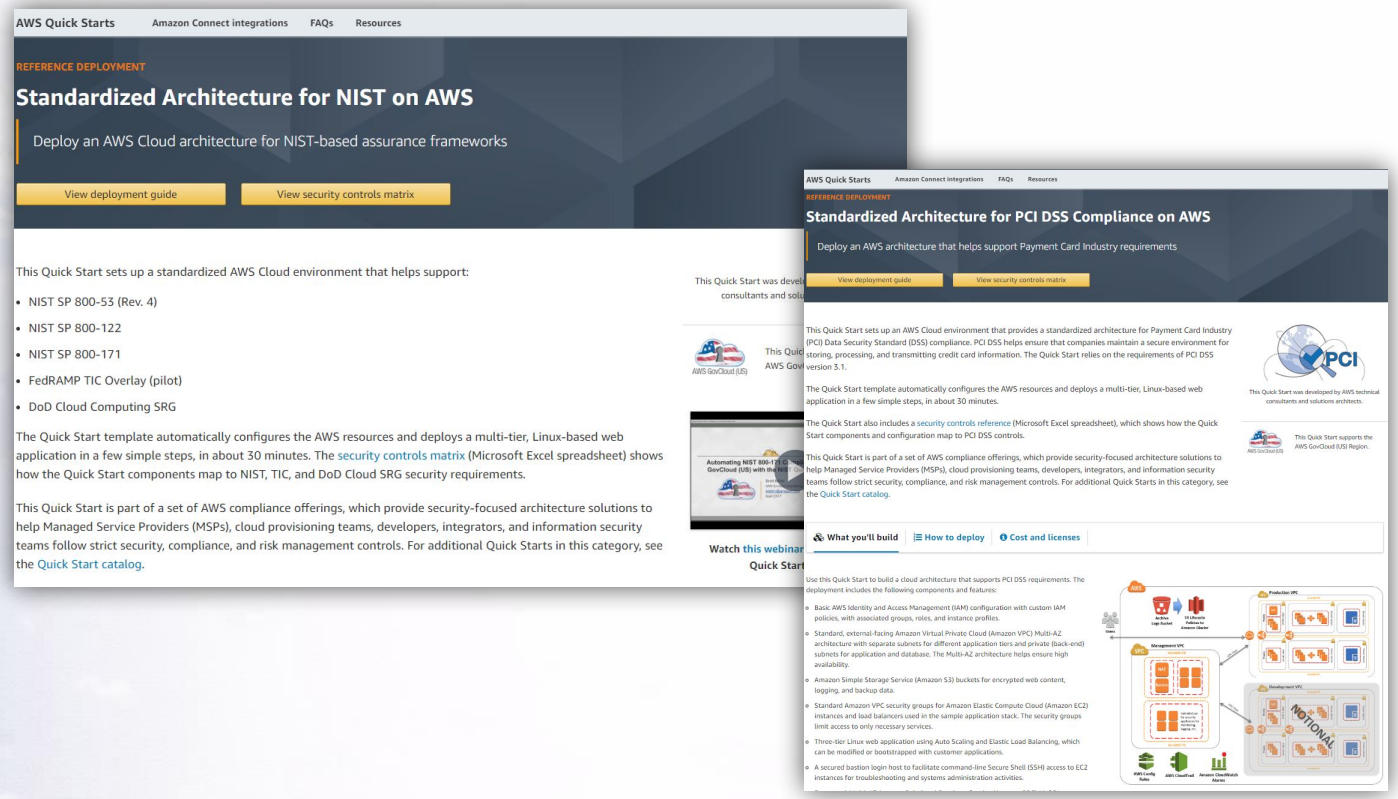
Netflix micro-service architecture (Outdated ☺)

Challenges – Summary

- Architecture can be more challenging than in the traditional datacenter
- More points of failure
- The scale is huge
- More automation
- Environments more dynamic
- Fast pace of new services
- More owners
- Multi Cloud
- Knowledge gap
- More…

RECOMMENDATIONS!

AWS Standardized Architecture



Use Compliance/Security tools

- CloudGuard Dome9 (Check Point)
- RedLock (Palo Alto Networks)
- DivvyCloud
- Threat Stack
- Cloud Custodian (Open Source)
- Others…

Use automatic tools

Automate everything!

- Can be debugged
- Less error prone (well… except bugs)
- Everything is documented
- More scalable

No manual operations in production

Continuous Compliance

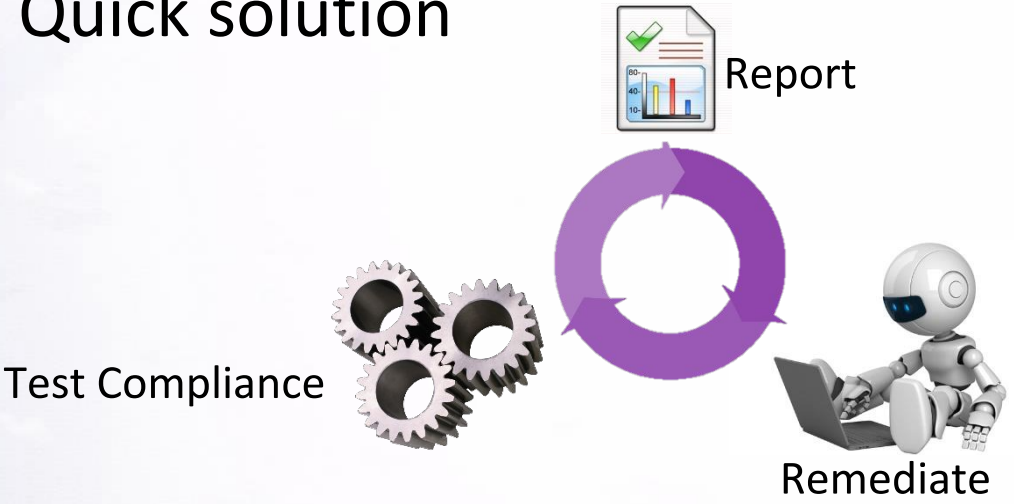
Try to be complied all the time!

- Find gaps and mitigate continuously
- Send the results to the owner
  (rather through mediators)

Automatic Remediation

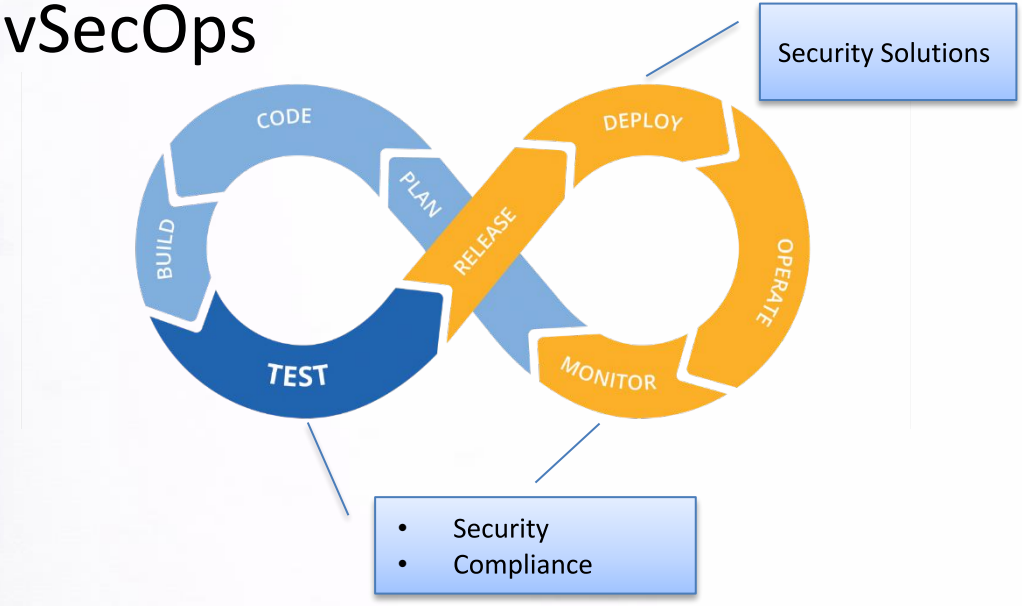
Fix the failures automatically!

- Reduce manual effort
- Quick solution



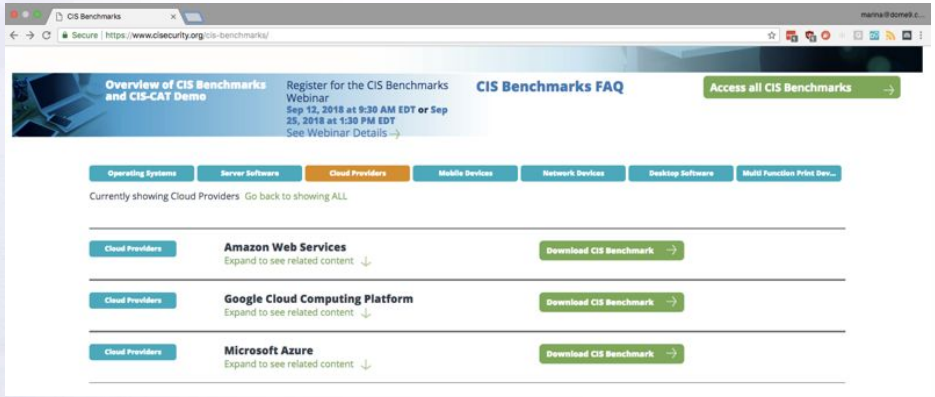
Bake everything into the CI/CD

- Security/Compliance are INTEGRAL to the development and deployment
- DevSecOps



Consult with CIS

- Center for Internet Security
  https://www.cisecurity.org
- "CIS Amazon Web Services Benchmarks"
  https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf



CIS Center for Internet Security®

Check out AWS Best Practices

- “AWS Well-Architected” portal
  https://aws.amazon.com/architecture/well-architected
- AWS Security Blog
  https://aws.amazon.com/blogs/security
- Many more…


SUMMARY

Compliance ⇔ Security

- Compliance aims to enforce security standards
- The cloud is massive and dynamic
- Follow various best practices
- Use automation and dedicated tools for
  - Security
  - Compliance
  - Remediation


Thank You!
offir.zigelman@gmail.com
https://www.linkedin.com/in/offir-zigelman

Security groups vs. Identity based segmentation

Director Product Management,
Ran Marom

Agenda

- Cloud network best practices
- Security groups - share your experience
- Security groups and microservices
- Security groups the reality
- Portshift

Cloud network best practices

- Segment your environments
  - PROD / DEV / Pii / PCI
- Micro-segment your services
  - Service to service communication
- Encryption where its needed
- Visibility
  - Real time visibility to your network communication
- Response
  - Take action if anomaly/malicious activity happened

Security groups - your experience

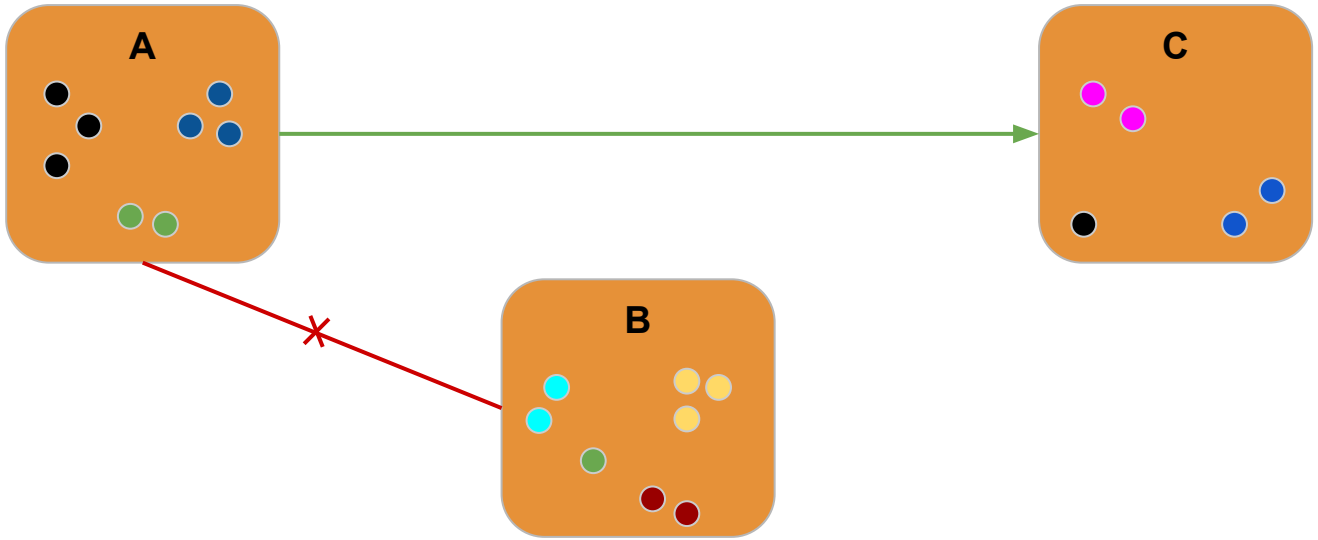
Share your experience in regards of security groups :)

Good and bad

Security groups & microservices

- Hard to manage in a microservice environment

- Does not meet the security requirements of a microservice environment



Security groups - reality

- Flat network
- Wide IP range exposed
- Wide port range exposed
- Mismatching rules
- Rule with no instances/subnet

Portshift answer

Portshift:

Identity-based workload security from code to runtime

- Prevent unauthorized workload from running in your environment
- Identity-based Micro-Segmentation: preventing unauthorized communication

Demo

- Cloud analysis tool

- Portshift network policies and runtime map

We are hiring !!!!

https://www.portshift.io/careers/