



<https://bit.ly/2zJJ3Fh>



Sponsors



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



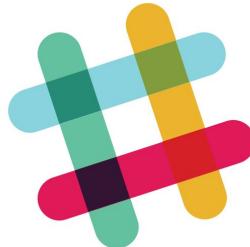
Doron Rogov



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

# 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

<b>Any Data Type</b>	<ul style="list-style-type: none"><li>· Block</li><li>· File</li><li>· Object</li></ul>	<b>Any Protocol</b>	<ul style="list-style-type: none"><li>· FC, iSCSI, iSER</li><li>· NFS, CIFS</li><li>· S3, Swift</li></ul>	<b>Any Location</b>	<ul style="list-style-type: none"><li>· On-Premises</li><li>· Public or Private Cloud</li><li>· Hybrid</li></ul>
----------------------	---	---------------------	---	---------------------	--

# 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



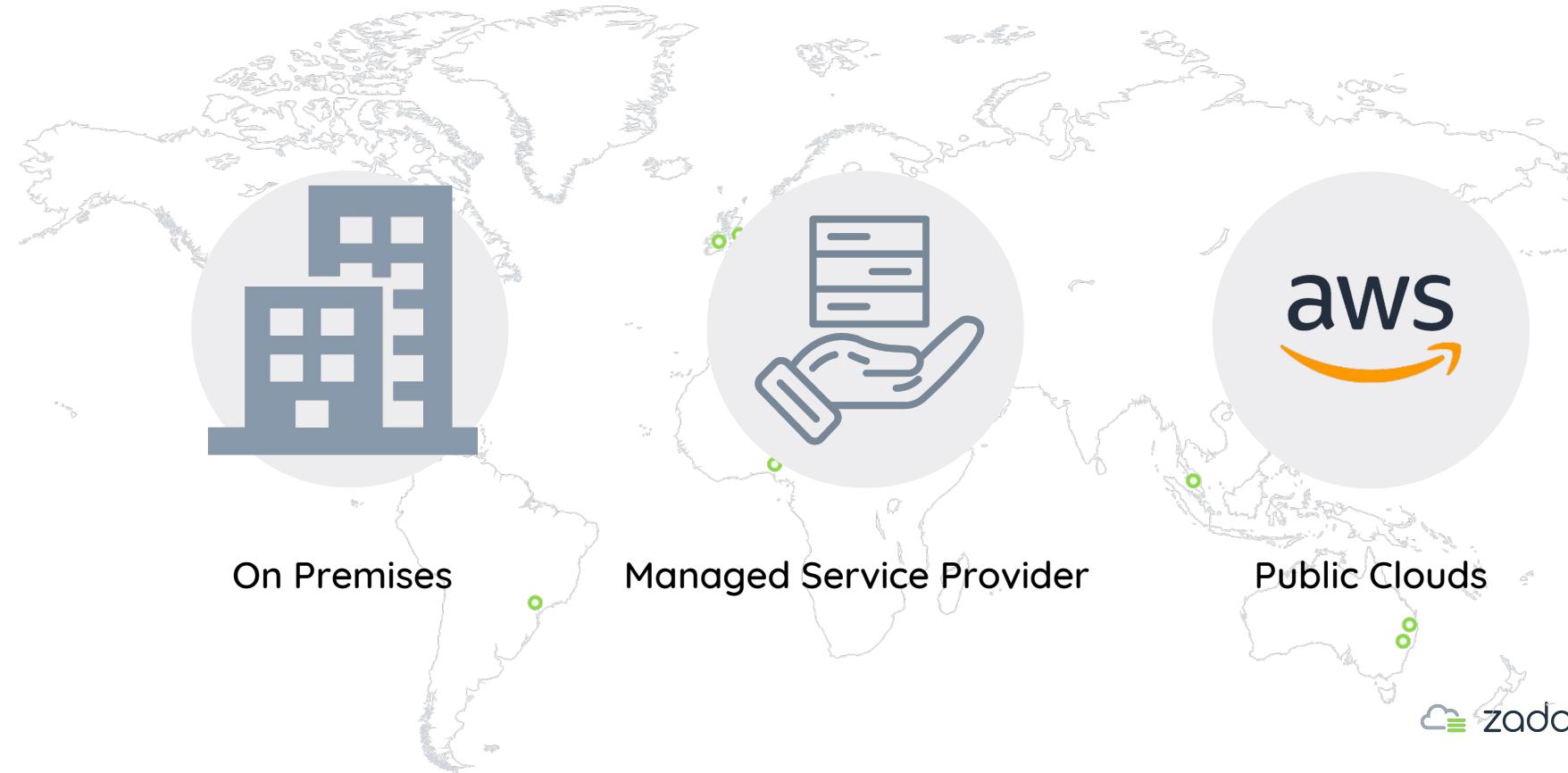
Cluster  
support



At-rest, in-flight  
data encryption

# Where?

---



When?

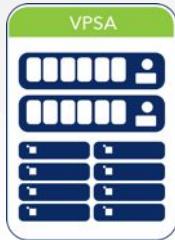
---

now!

[manage.zadarastorage.com](https://manage.zadarastorage.com)

# What is a VPSA Storage Array?

---



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



# Connectivity



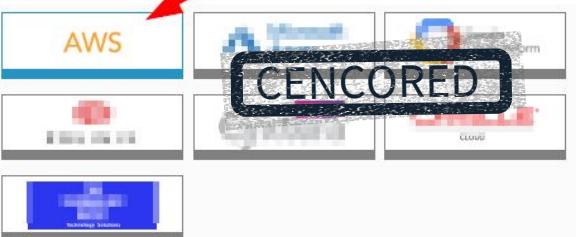
# Connectivity - AWS Direct Connect

### Create New VPSA® Storage Array

To create a new Virtual Private Storage Array (VPSA) takes just a few minutes. Please provide the information requested at each step, and watch as your VPSA takes shape in the right-hand column.

VPSA Name \*  
MY-CLOUD-STORAGE

VPSA Description  
AWS-STORAGE

Cloud Provider  
 CENSORED

Select Region  
AWS EU (London)

### Your Configuration

VPSA Name  
MY-CLOUD-STORAGE

Region  
AWS EU (London)

### AWS Connectivity Information

In order to establish a secure network connection between your VPC and Zadara, we require a bit of information. This information will be kept confidential and will be used solely for the purpose of establishing this connection.

AWS Account ID [?](#)

AWS ASN Information [?](#)  
64512

VPC CIDR Block [?](#)  
172.31.0.0/16

[Cancel](#) [Next](#)

# Connectivity - AWS Direct Connect - Closer look

The screenshot shows the AWS Direct Connect Virtual Interfaces page. The top navigation bar includes 'Services' (dropdown), 'Resource Groups' (dropdown), 'Direct Connect' (selected), 'S3' (icon), 'EC2' (icon), and user information 'shlomi @ zadarastorage' with dropdowns for 'London' and 'Support'.

The left sidebar has a 'Connections' section with 'Virtual Interfaces' selected, followed by 'LAGs' and 'Direct Connect Gateways'. A 'Create Virtual Interface' button is at the top of the main content area.

The main content area displays a table of 16 virtual interfaces, with 16 of 16 currently visible. The columns are: Name, ID, Connection, VLAN, Type, and State. Two entries are shown:

Name	ID	Connection	VLAN	Type	State
[REDACTED]_Zadara	dxvif-[REDACTED]	dxcon-[REDACTED]	2024	private	available
[REDACTED]_Zadara	dxvif-[REDACTED]	dxcon-[REDACTED]	1024	private	available

Below the table, a section titled 'Cloudzone\_Zadara' contains two tabs: 'Summary' (selected) and 'Peerings'. The 'Summary' tab displays the following details:

Name	dxvif-[REDACTED]	Location	[REDACTED]
ID	dxvif-[REDACTED]	AWS Device	[REDACTED]
AWS Account	[REDACTED]	Virtual Gateway	vgw-[REDACTED]
Type	private	VLAN Assigned	2024
State	available	Amazon side ASN	64512
Connection	dxcon-[REDACTED]	MTU	1500
		Jumbo Frame Capable	true

# Connectivity - AWS Direct Connect - VPC

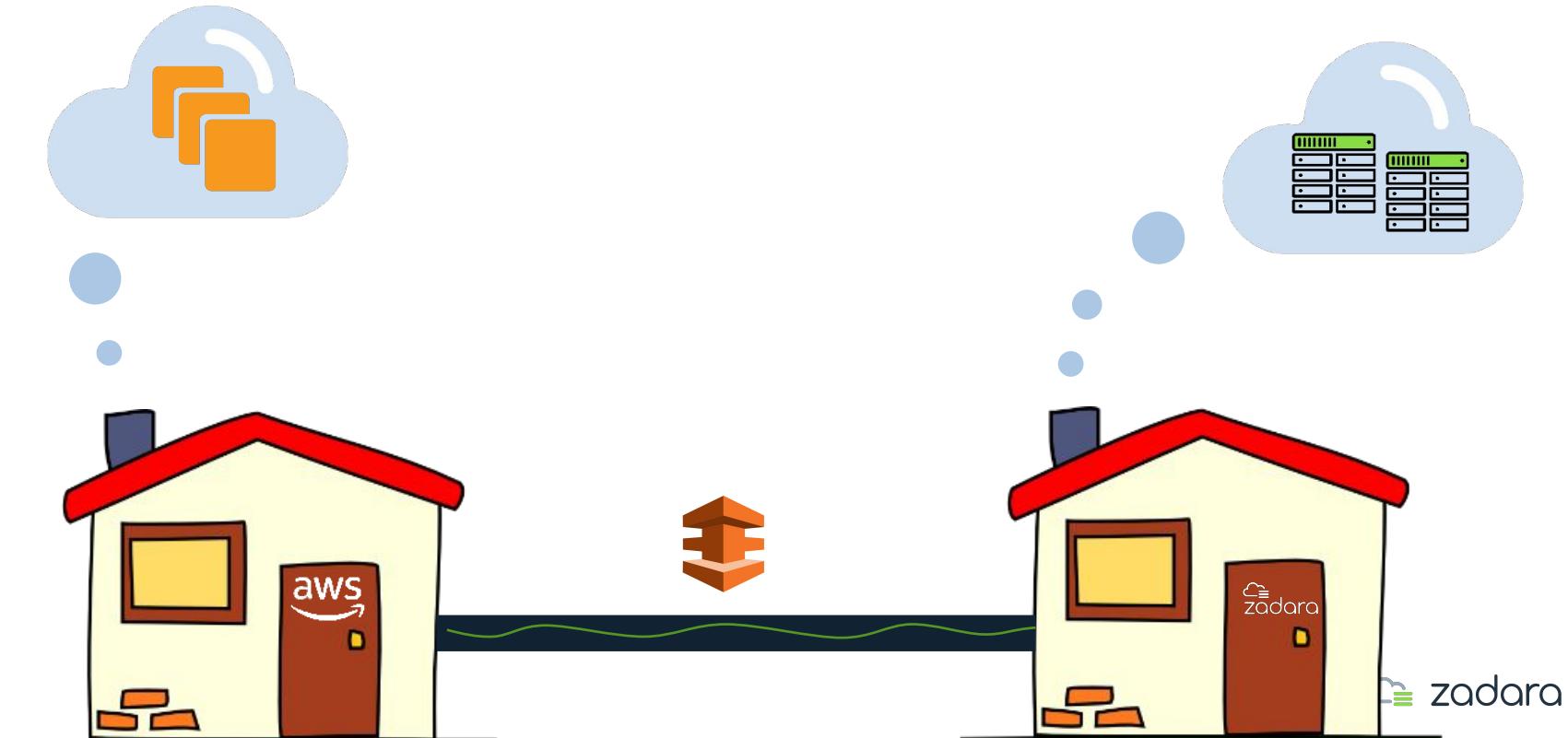
The screenshot shows the AWS VPC Dashboard with the 'Route Tables' section selected. A red box highlights the 'Route Tables' link in the left sidebar. Another red box highlights the 'Route Propagation' tab in the main content area. The table lists one route table:

Name	Route Table ID	Explicitly Associated with	Main	VPC ID	Owner
	rtb-1c59e776	-	Yes	vpc-e423278f	128231900384

Below the table, the 'Route Table: rtb-1c59e776' details are shown. The 'Route Propagation' tab is selected, indicated by a red box. The 'Edit route propagation' button is visible. Under the 'Virtual Private Gateway' section, the 'Propagate' dropdown is set to 'No', which is also highlighted with a red box.

# 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

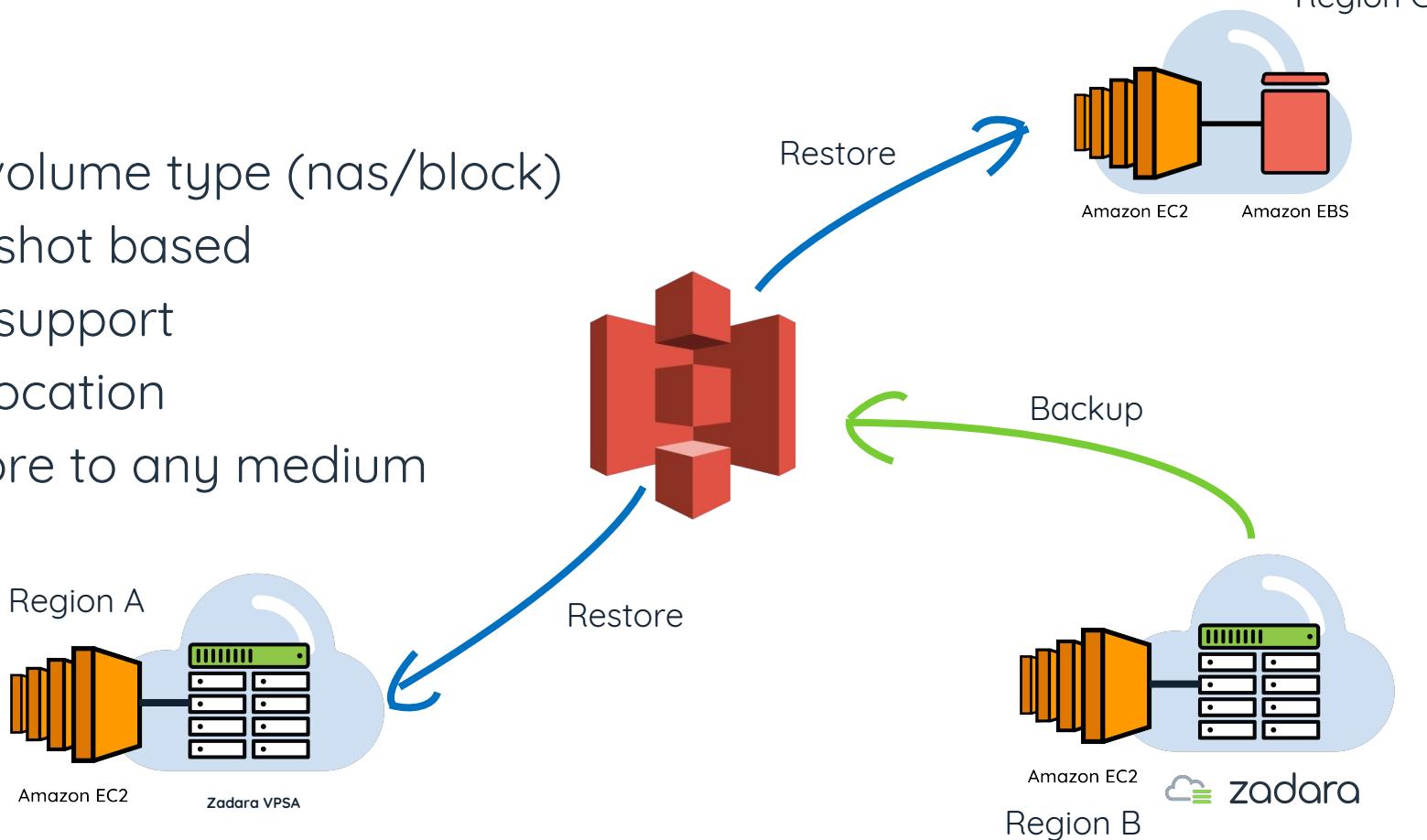
Backup to S3 (aka B2S3)



# 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

Connect Remote Object Storage

Interface:  S3

Type:  AWS  Google Cloud  VPSA Object Storage  Custom

Region: \* US East (N. Virginia)

Bucket: \* zadarastorage-demo

Access Key ID: \* MYACCESSKEYID

Secret Access Key: \*

Connect Via: \* Management IP ( [REDACTED] )

Ignore Lifecycle Policies:

Use KMS key id:

Use Proxy:

Proxy

Host: \* 172.31.240.150

Port: \* 3128

Use Authentication

User: \*

Password: \*

## #2 Set Policy

Create Backup Job

Job Name: \* HOME-BACKUP

Volume:

Name	Capacity	Status	Data Type
BLOCK-VOLUME-01	100 GB	Available	BLOCK
NFS-VOLUME-01	2 TB	Available	File-System
Jenkins_Logs	50 GB	In-use	File-System

Displaying 1 - 4 of 4

Remote Object Storage: \* AWS.s3.amazonaws.com-zadarastorage-demo

Snapshot Policy: \*

Name	Create Policy	Delete Policy	Dst. Delete Policy
Hourly Snapshots for a Day	Every hour	Keep latest 24 snapshots	Keep latest 24 snapshots
Daily Snapshots for a Week	Once per day after midnight	Keep latest 7 snapshots	Keep latest 7 snapshots
Weekly Snapshots for a Year	Every Sunday after midnight	Keep latest 53 snapshots	Keep latest 53 snapshots
Daily Backup for a Year	Once per day after midnight	Keep latest 7 snapshots	Keep latest 365 snapshots
on_demand	On Demand	Keep latest 10 snapshots	Keep latest 10 snapshots

SSE: \* AES256

Compress Data:

In-Flight:

## B2S3 – Restore a subset of a volume

# #3 Recover



# Thank you!



shlomi@zadara.com



The background image shows a vast expanse of white, fluffy clouds over a deep blue ocean. The perspective is from an airplane window, with the aircraft's white fuselage and wing visible on the right side.

# Compliance in the cloud

**And how it can prevent  
the next data breach**

**Offir Zigelman**



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



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



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



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



May 29, 2018 More Data Leaked from  
AWS Bucket Misconfigurations



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



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



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



# About me

## Offir Zigelman



[offir.zigelman@gmail.com](mailto: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”

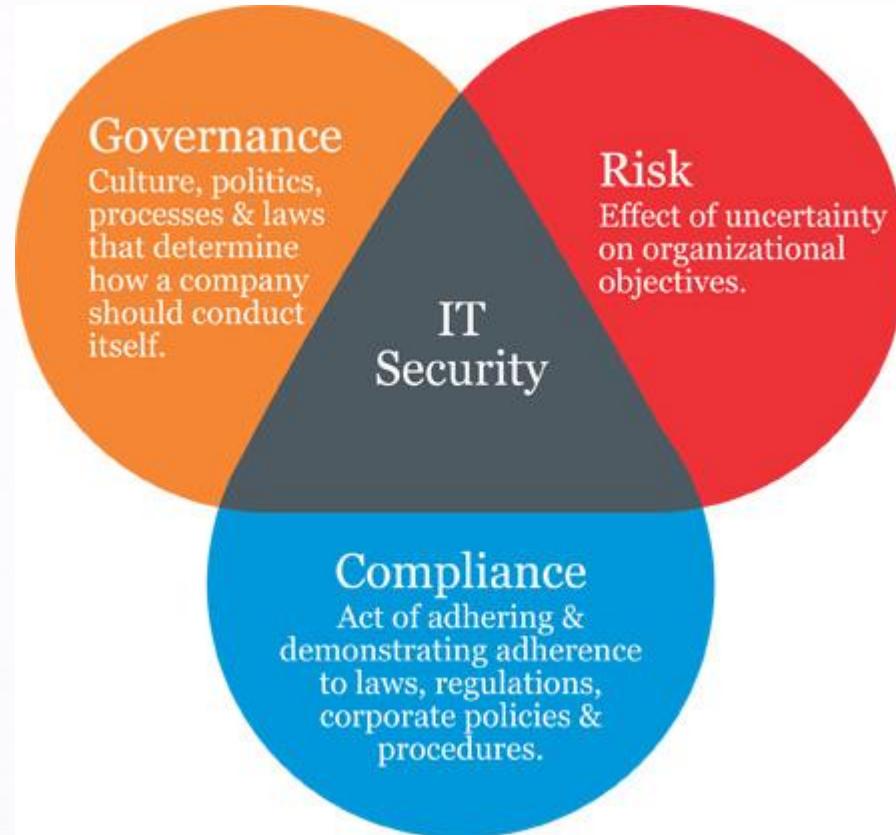
# AuditShark

# Security Compliance enforces information security standard





# GR C





# 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:**

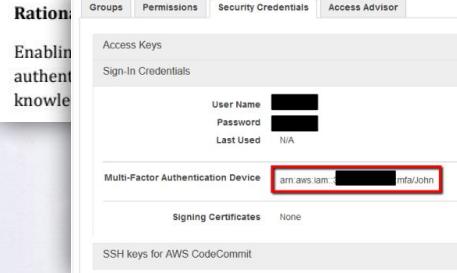
- Level 1

**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 Audit, prompted for their user name and password as well as for an authorized AWS MFA device. It is recommended that MFA be enabled for all IAM users having a console password.

**Rationale:**

Enabling MFA adds another layer of security to your AWS account.



The screenshot shows the 'Sign-In Credentials' section of the IAM console. It displays 'User Name' (redacted), 'Password' (redacted), and 'Last Used' (N/A). Below this is the 'Multi-Factor Authentication Device' section, which shows 'arn:aws:iam::[REDACTED]:mfa/john'. A red box highlights the 'arn:aws:iam::[REDACTED]:mfa/john' text. The 'Signing Certificates' and 'SSH keys for AWS CodeCommit' sections are also visible.

as it is now, it is not possible to determine if MFA 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.



A vertical strip on the left side of the slide shows an aerial view from an airplane window. It features a blue sky with white clouds above, and below is a vast expanse of blue ocean with small white waves. The edge of the airplane's window frame is visible on the left.

# 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

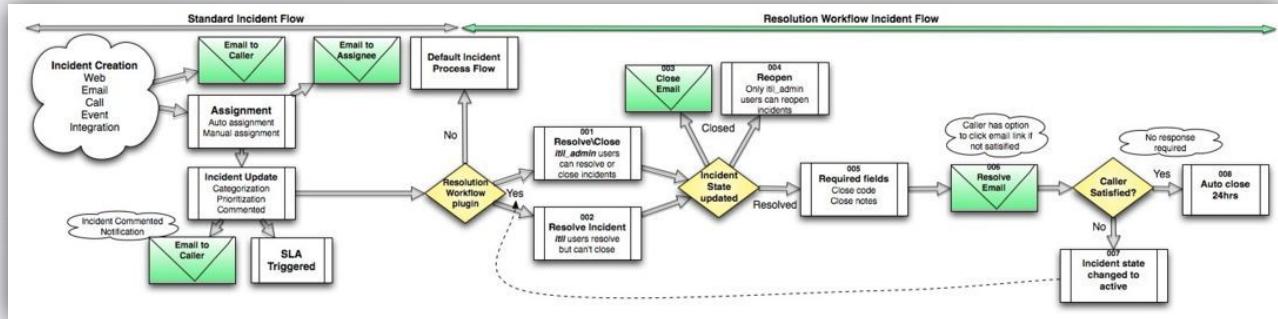
**AWS PCI-DSS 3.2, Sections 3.5.3, 3.6.3:**  
*“Use Encrypted RDS storage”*

Instance and IOPS		Encryption Details		Availability and Durability	
Instance Class	db.m3.medium <small>i</small>	Encryption Enabled	No	DB Instance Status	available
Storage Type	General Purpose (SSD)			Multi AZ	No
IOPS	disabled			Automated Backups	Enabled (7 Days)
Storage	5 GB			Latest Restore Time	April 30, 2016 at 6:50:00 PM UT
Maintenance Details					
Auto Minor Version Upgrade Yes					
Maintenance Window sat:07:59-sat:08:29					
Backup Window 03:48-04:18					
Pending Maintenance None					



# How Compliance people work(ed?)

A. Risk Assessment and Treatment				
Score Item	Question/Request	Response	Results	Additional Information
<small>The next question contains either Yes, No or N/A from this dropdown menu. If Yes or No, an explanation is mandatory. Use the additional information field in addition if applicable.</small>				
A.1	Has a risk management program that has been approved by management? If yes, is it available to employees and is an action to implement under review by the program? If yes, state it below.			A.1.1 Is a risk register that management can access.
A.2	Is there regular reporting of new incidents during the reporting period? If yes, state it below.			A.2.1 Incident Log.
A.3	Do business leaders have access to Request Systems and Data? (Actual business leaders, business unit managers, functional managers, departmental managers, business analysts, business intelligence managers, HR, IT, Legal, PR, etc.)			A.3.1 Business Risk Management Program.
A.4	Is there a vendor management program?			
A.5	Do external parties have access to Request Systems and Data? (including suppliers, partners, clients, etc.) If yes, state it below.			A.5.1 External Organization and Data Protection.
A.6	Is the reporting of all new management processes (e.g., internal audit, quality, risk, compliance, etc.) regular, timely and comprehensive? If yes, provide the frequency and reason. If no, explain reason.			A.6.1 Internal Audit and Quality Management.
A.7	Is the system used to manage incidents able to address the quality and accuracy of reported incidents effectively?			A.7.1 Quality Management and Program Maintenance.
A.8	Is there a comprehensive risk management system that addresses the aspects of identifying and characterizing the risks?			A.8.1 Risk Management and Program Maintenance.

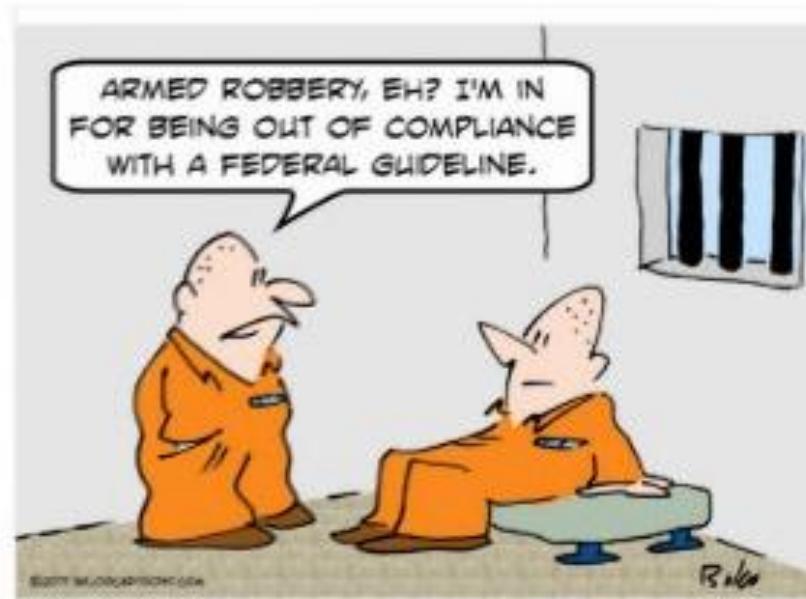




# Compliance may have legal implications



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





# 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

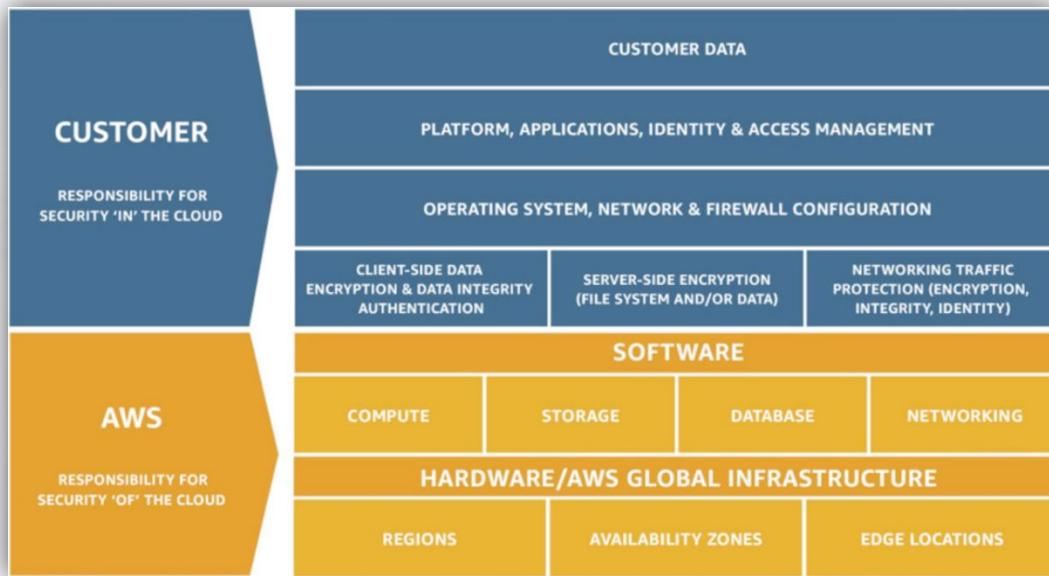


Compliance in AWS

# 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.

The image shows two side-by-side screenshots of the AWS Services catalog. The left screenshot, titled 'AWS Services, 2014', displays a list of approximately 100 services under various categories. The right screenshot, titled 'AWS Services, 2018', shows a significantly larger list of over 200 services, illustrating the rapid growth of AWS offerings over four years.

AWS Services, 2014

**Challenge:** Hard time for Compliance to keep up

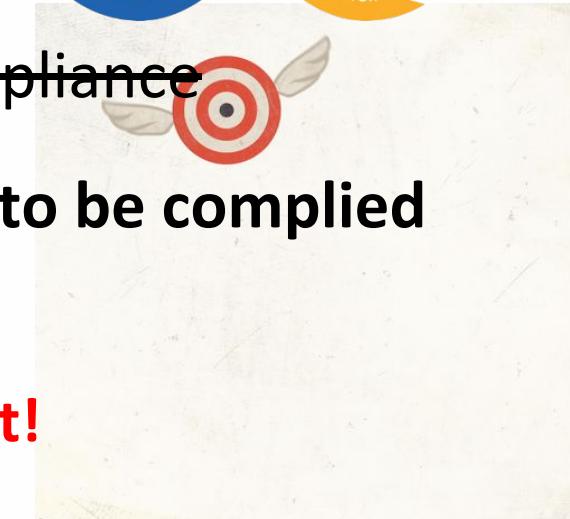
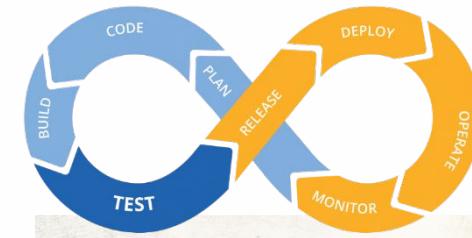


# Highly dynamic environments

- 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

- ~~100~~ Few years ago: every company had multiple cloud accounts
- ~~100~~ Today: multiple accounts for every team
- ~~100~~ 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

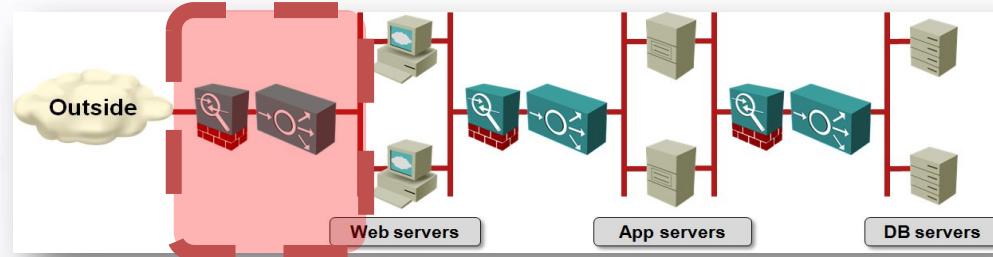
**Challenge:** multi-cloud compliance



A vertical strip on the left side of the slide showing an aerial view of white clouds over a blue ocean.

# The new “perimeter”

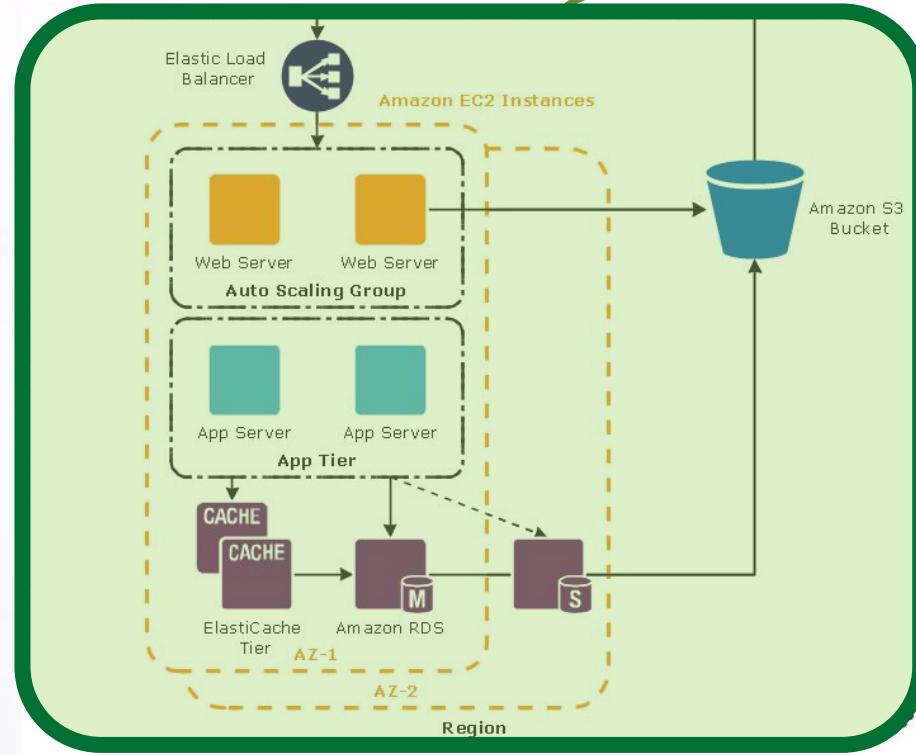
On the old datacenter, security team controlled the “perimeter”





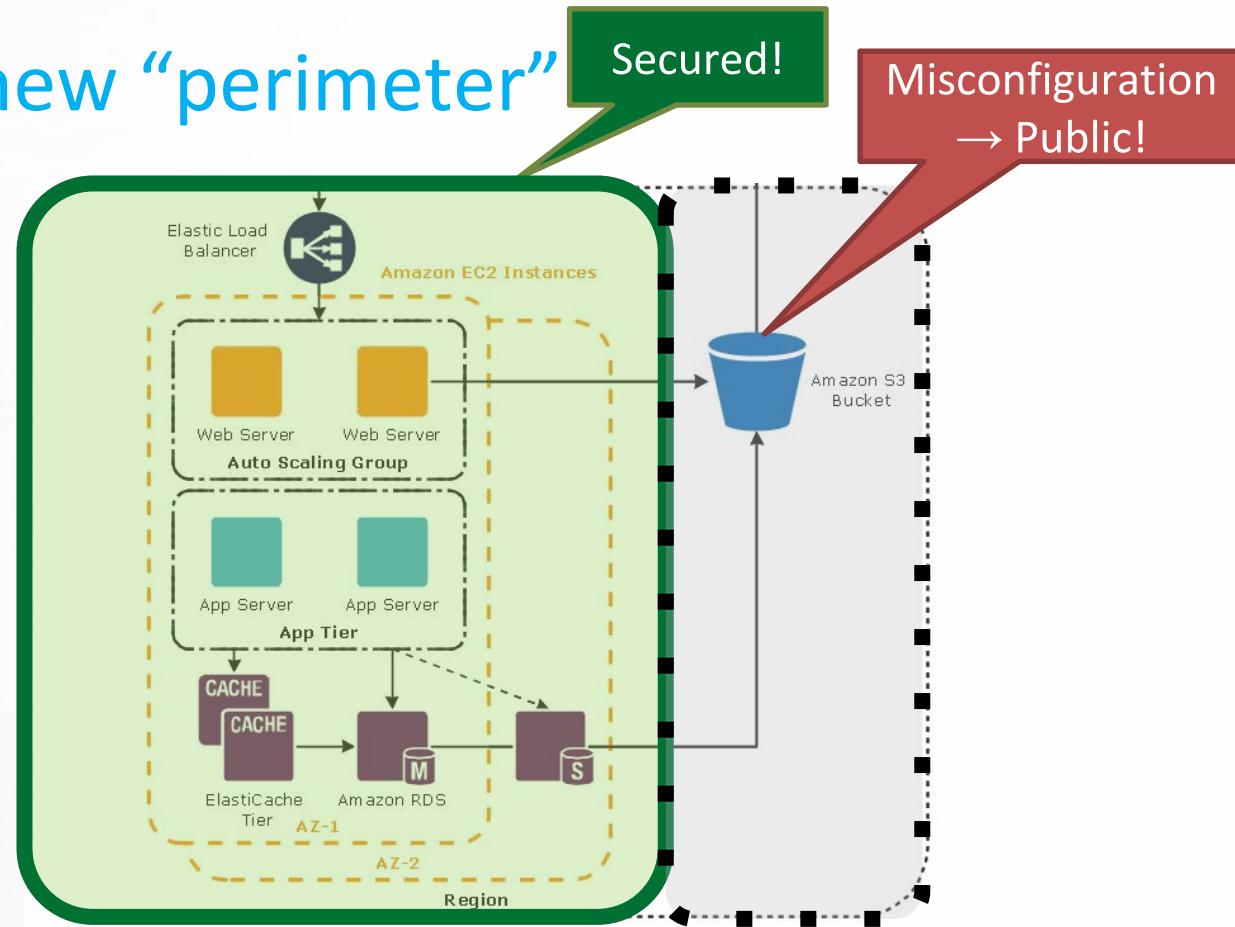
# The new “perimeter”

Secured!





# The new “perimeter”

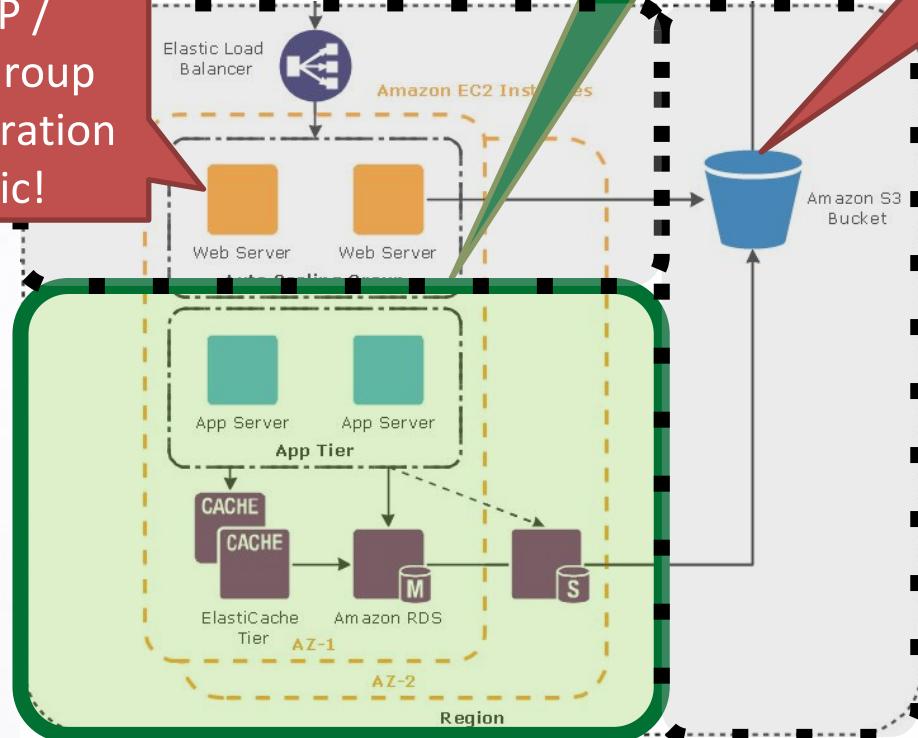


# The new “perimeter”

Elastic IP /  
Security Group  
Misconfiguration  
→ Public!

Secured!

Misconfiguration  
→ Public!

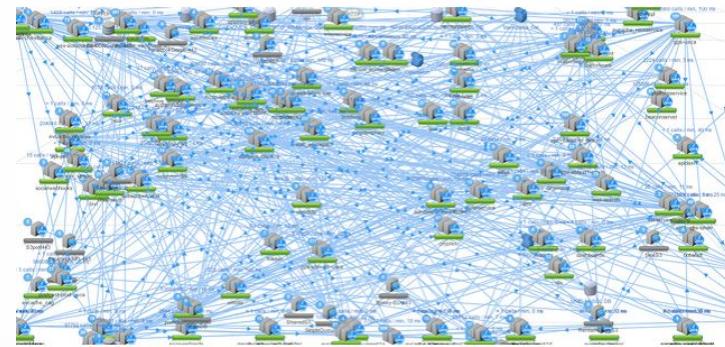




# The new “perimeter”

## 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

AWS Quick Starts    Amazon Connect integrations    FAQs    Resources

**REFERENCE DEPLOYMENT**

## Standardized Architecture for NIST on AWS

Deploy an AWS Cloud architecture for NIST-based assurance frameworks

[View deployment guide](#)    [View security controls matrix](#)

This Quick Start sets up a standardized AWS Cloud environment that helps support:

- NIST SP 800-53 (Rev. 4)
- NIST SP 800-122
- NIST SP 800-171
- FedRAMP TIC Overlay (pilot)
- DoD Cloud Computing SRG

The Quick Start template automatically configures the AWS resources and deploys a multi-tier, Linux-based web application in a few simple steps, in about 30 minutes. The [security controls matrix](#) (Microsoft Excel spreadsheet) shows how the Quick Start components map to NIST, TIC, and DoD Cloud SRG security requirements.

This Quick Start is part of a set of AWS compliance offerings, which provide security-focused architecture solutions to help Managed Service Providers (MSPs), cloud provisioning teams, developers, integrators, and information security teams follow strict security, compliance, and risk management controls. For additional Quick Starts in this category, see the [Quick Start catalog](#).

**REFERENCE DEPLOYMENT**

## Standardized Architecture for PCI DSS Compliance on AWS

Deploy an AWS architecture that helps support Payment Card Industry requirements

[View deployment guide](#)    [View security controls matrix](#)

This Quick Start was developed by AWS GovCloud (US) consultants and solution architects.

This Quick Start sets up an AWS Cloud environment that provides a standardized architecture for Payment Card Industry (PCI) Data Security Standard (DSS) compliance. PCI DSS helps ensure that companies maintain a secure environment for storing, processing, and transmitting credit card information. The Quick Start relies on the requirements of PCI DSS version 3.1.

The Quick Start template automatically configures the AWS resources and deploys a multi-tier, Linux-based web application in a few simple steps, in about 30 minutes.

The Quick Start also includes a security controls reference (Microsoft Excel spreadsheet), which shows how the Quick Start components and configuration map to PCI DSS controls.

This Quick Start is part of a set of AWS compliance offerings, which provide security-focused architecture solutions to help Managed Service Providers (MSPs), cloud provisioning teams, developers, integrators, and information security teams follow strict security, compliance, and risk management controls. For additional Quick Starts in this category, see the [Quick Start catalog](#).

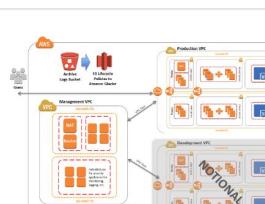
**What you'll build**    **How to deploy**    **Cost and licenses**

Watch this webinar

Quick Start

Use this Quick Start to build a cloud architecture that supports PCI DSS requirements. The deployment includes the following components and features:

- Basic AWS Identity and Access Management (IAM) configuration with custom IAM policies, with associated groups, roles, and instance profiles.
- Standard, external-facing Amazon Virtual Private Cloud (Amazon VPC) Multi-AZ architecture with separate subnets for different application tiers and private (back-end) subnets for application and database. The Multi-AZ architecture helps ensure high availability.
- Amazon Simple Storage Service (Amazon S3) buckets for encrypted web content, logs, and configuration files.
- Standard Amazon VPC security groups for Amazon Elastic Compute Cloud (Amazon EC2) instances and load balancers used in the sample application stack. The security group limit access to only necessary services.
- Three-tier Linux web application using Auto Scaling and Elastic Load Balancing, which can be modified or bootstrapped with customer applications.
- A secured bastion login host to facilitate command-line Secure Shell (SSH) access to EC2 instances for troubleshooting and systems administration activities.





# Use Compliance/Security tools

- ★ CloudGuard Dome9 (Check Point) 
- ★ RedLock (Palo Alto Networks) 
- ★ DivvyCloud  DivvyCloud
- ★ Threat Stack  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)

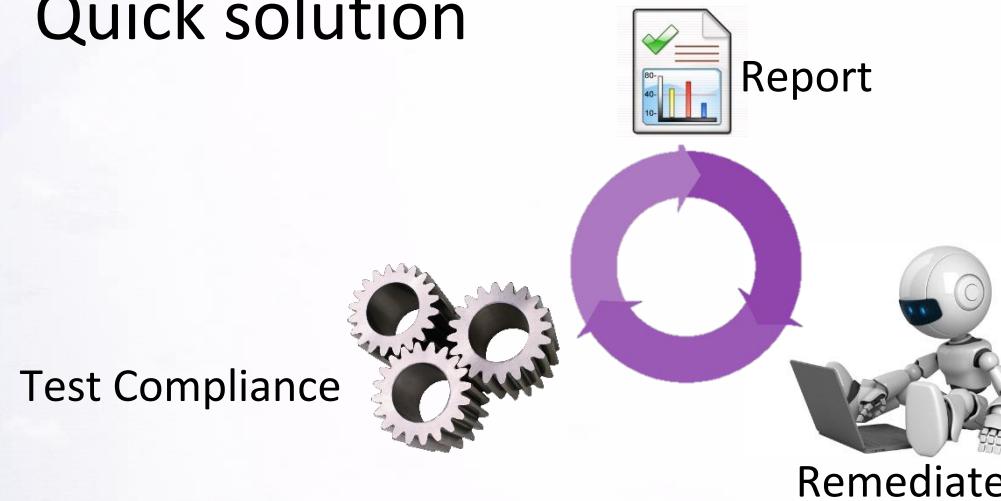




# Automatic Remediation

## Fix the failures automatically!

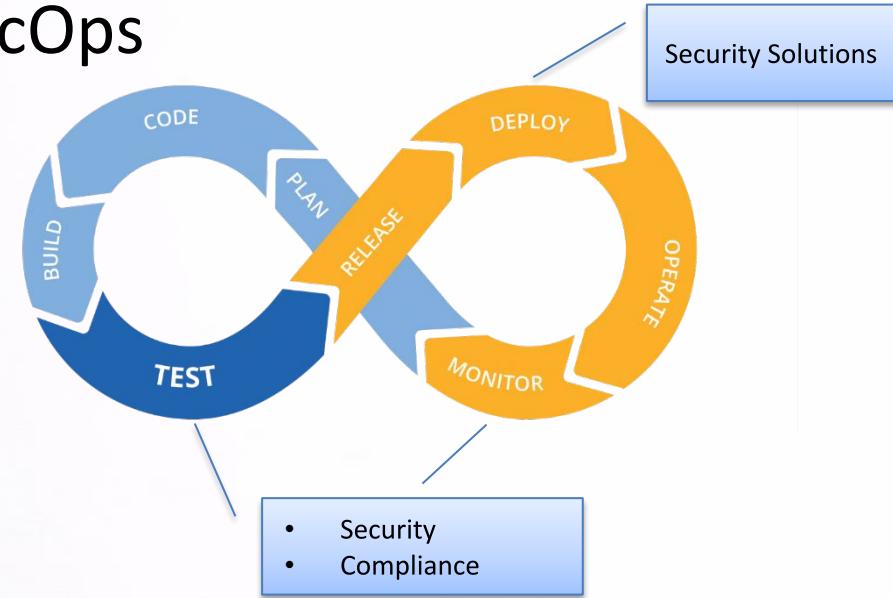
- ∞ Reduce manual effort
- ∞ Quick solution





# Bake everything into the CI/CD

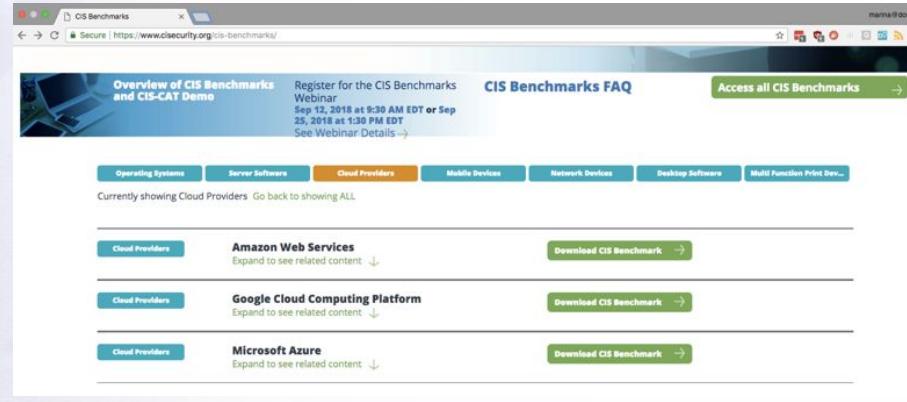
- ∞ Security/Compliance are INTEGRAL to the development and deployment
- ∞ DevSecOps





# 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](https://d0.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf)





# 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...



AWS Well-Architected

# 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



The background of the slide is a photograph taken from an airplane window, showing a vast expanse of white, fluffy clouds over a deep blue ocean. The perspective is looking down the length of the aircraft, with the windows visible on the right side.

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

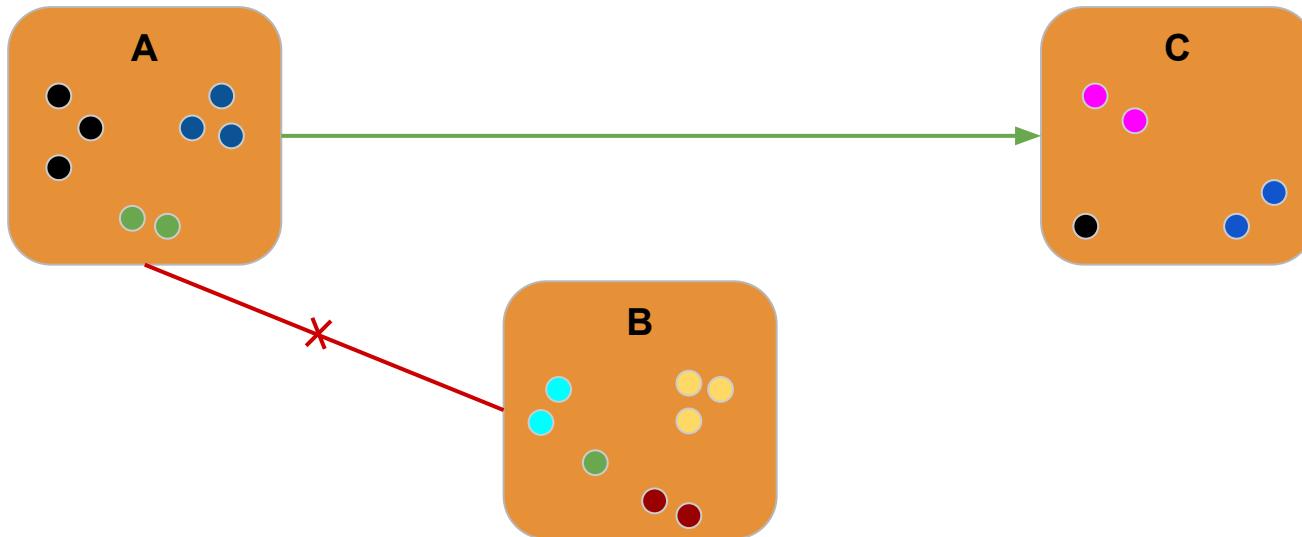
Share your experience in regards of security groups :)

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/>

