AWS Security, Identity, and Compliance

Infrastructure and services to elevate your security in the cloud

Mukhtar Kabir, CISSP

08-26-2021

Agenda

9:00AM - 10:00AM CDT

Intro to AWS Security:
Introduction to security on AWS and what services are available to help you keep your applications and data secure.

10:00AM - 11:00AM CDT

Presentation: Threat Detection

Deep dive into AWS Security Hub, Amazon GuardDuty, and AWS Config.

11:00AM - 11:30AM CDT

Presentation: Incident Response

Deep dive into Amazon Detective, EventBridge, and AWS Lambda.

11:30AM - 12:00PM CDT

Threat Detection & Incident Response: Workshop Overview

Overview of the workshop architecture and scenario walk-throughs.

12:00PM - 12:30PM CDT

Break

12:30PM - 2:30PM CDT

Threat Detection & Incident Response Workshop:

We'll walk through how to use AWS Security Hub, Config, GuardDuty, Lambda, EventBridge, and Detective to detect, investigate, and response to potential issues in your environment.

2:30PM - 3:00PM CDT

Presentation: Data Protection:

Deep dive into Amazon Macie.

3:00PM - 5:00PM CDT

Workshop: Data Discovery and Classification with Amazon Macie

This workshop is designed to help you get familiar with Amazon Macie and learn how to scan and classify data in your S3 buckets.

Why is security traditionally so hard?

Lack of visibility

Low degree of automation

Before…

Move fast OR Stay secure

Now...

Move fast **AND** Stay secure

The most sensitive workloads run on AWS

"We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance."

—John Brady, CISO, FINRA (Financial Industry Regulatory Authority)

"AWS allowed us to scale our business to handle 6 million patients a month and elevate our security—all while maintaining HIPAA compliance--as we migrated 100% to cloud in less than 12 months"

—Brian Lozada, CISO, Zocdoc.

"Amazon Web Services was the clear choice in terms of security and PCI DSS Level 1 compliance compared to an on-premises or co-location data center solution."

—Stefano Harak, online senior product manager for Vodafone Italy

Infrastructure and services to elevate your security in the cloud

Inherit global security & compliance controls

Scale with superior visibility & control

Highest standards for privacy & data security

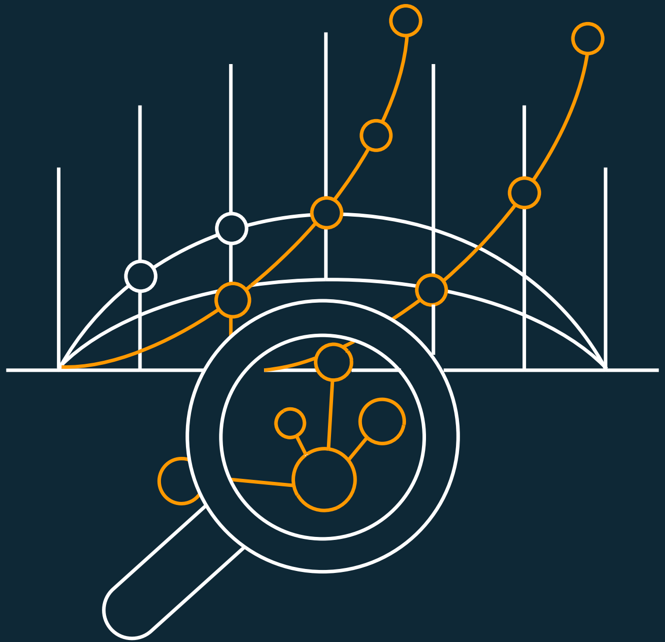
Automate & reduce risk with deeply integrated services

Largest ecosystem of security partners & solutions

Inherit global security and compliance controls

- CSA cloud security alliance℠
- ISO 9001 International Organization for Standardization
- ISO 27001 International Organization for Standardization
- ISO 27017 International Organization for Standardization
- ISO 27018 International Organization for Standardization
- PCI Security Standards Council PARTICIPATING ORGANIZATION™
- AICPA SOC — SOC 1
- AICPA SOC — SOC 2
- AICPA SOC — SOC 3
- CJIS
- FIPS 140-2 CRYPTOGRAPHY
- FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT
- DoD SRG
- FR FedRAMP
- FERPA
- FFIEC Federal Financial Institutions Examination Council
- C5
- SEC Rule 17a-4(f)
- GxP
- HIPAA
- ITAR International Traffic in Arms Regulations Compliant
- MPAA
- iDA SINGAPORE
- マイナンバー My Number Act
- VPAT Section 508
- FISC
- irap
- ISMS
- G-Cloud
- TISAX ENX ASSOCIATION
- CYBER ESSENTIALS PLUS
- CERTIFICACIÓN DE CONFORMIDAD CON EL ens

Scale with superior visibility and control



Control where your data is stored and who can access it

Fine-grain identity & access controls so users and groups have the right access to resources

Reduce risk via security automation and continuous monitoring

Integrate AWS services with your solutions to support existing workflows, streamline ops, and simplify compliance reporting

Highest standards for privacy and data security

Meet data residency requirements
Choose an AWS Region and AWS will not replicate it elsewhere unless you choose to do so

Encryption at scale
with keys managed by our AWS Key Management Service (KMS) or managing your own encryption keys with AWS CloudHSM using FIPS 140-2 Level 3 validated HSMs

Comply with local data privacy laws
by controlling who can access content, its lifecycle, and disposal

Access services and tools that enable you to **build compliant infrastructure** on top of AWS

Automate and reduce risk with integrated services

Comprehensive set of APIs and security tools

Continuous monitoring and protection

Threat remediation and response

Operational efficiencies to focus on critical issues

Securely deploy business critical applications

AWS security, identity, and compliance solutions

Identity & access management

- AWS Identity & Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

Detection

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs

Infrastructure protection

- AWS Firewall Manager
- AWS Shield
- AWS WAF – Web application firewall
- Amazon Virtual Private Cloud (VPC)
- AWS PrivateLink
- AWS Systems Manager

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Amazon Detective
- CloudEndure DR
- AWS Config Rules
- AWS Lambda

Largest ecosystem of security partners and solutions

Network & infrastructure security

- ALERT LOGIC Security. Compliance. Cloud.
- APPGATE
- ARMOR
- Barracuda
- Check Point SOFTWARE TECHNOLOGIES LTD.
- CISCO
- FORTINET
- Guardicore
- paloalto NETWORKS
- PROTECTWISE
- SKinfosec co.,ltd.
- SOPHOS
- zscaler

Host & endpoint security

- CROWDSTRIKE
- Symantec
- TREND MICRO

Application security

- Barracuda
- Checkmarx
- f5

Identity & access control

- CLOUDKNOX
- okta
- onelogin
- Ping Identity
- SAVIYNT

Vulnerability & configuration analysis

- Qualys
- RAPID7
- tenable
- threat stack

Data protection & encryption

- CYBERARK
- DataSunrise Data & Database Security
- gemalto security to be free
- HashiCorp
- PRIVITAR
- THALES

Logging, monitoring, SIEM, threat detection, & analytics

- ALIEN VAULT
- LACEWORK
- McAfee Together is power.
- SECURONIX Security Analytics. Delivered.
- splunk>
- sumo logic

aws

Consulting and technology competency partners

Security engineering

- 8K Miles
- accenture High performance. Delivered.
- AllCloud
- CMD SOLUTIONS
- CLOUDZONE by matrix
- cloudten
- Deloitte.
- ECCOM 华 讯 网 络
- escala 24x7
- FOGHORN
- GuidePoint SECURITY
- HELECLOUD
- Hewlett Packard Enterprise
- Itoc
- lightstream
- logicworks
- NRI
- pwc
- Smartronix CLOUD ASSURED
- Eleven Paths Telefonica CYBER SECURITY COMPANY
- VERSENT
- direktgruppe

Governance, risk, & compliance

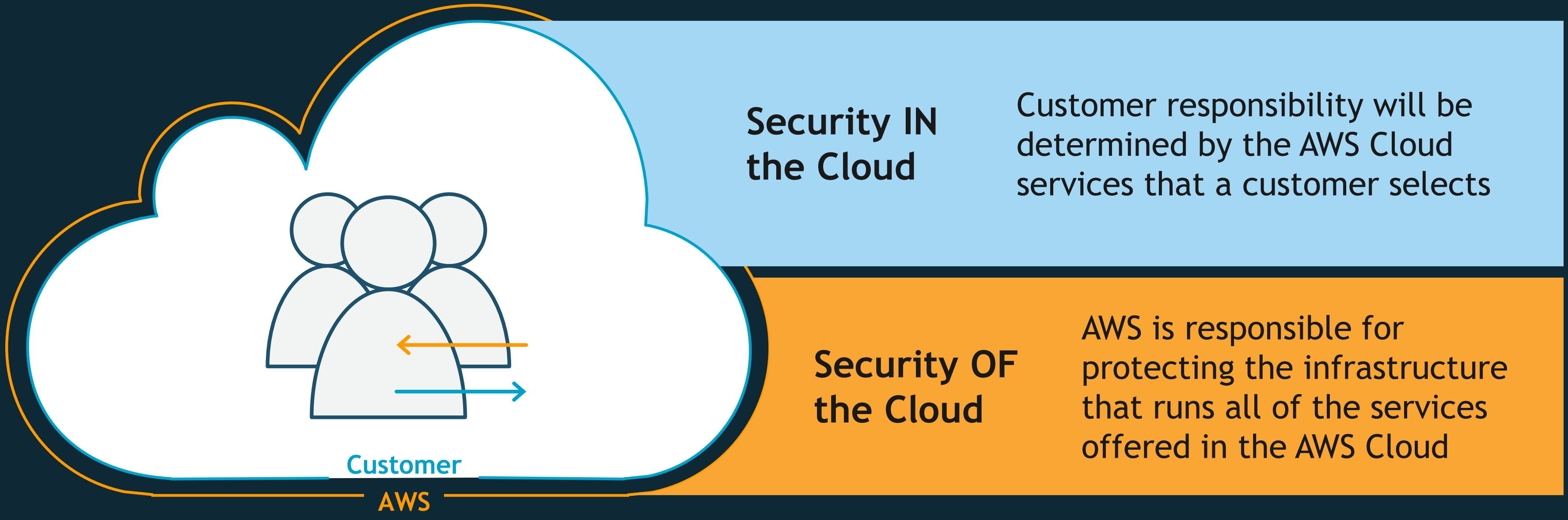
- Booz | Allen | Hamilton
- Cloudgotech
- cavirin
- CloudCheckr
- CloudHealth by vmware
- CloudPassage
- COALFIRE
- DivvyCloud Cloud Automation Reimagined
- ECCOM 华 讯 网 络
- Flux7 an NTT DATA Company
- KindlyOps
- OPTIV
- pwc
- Telos
- TREND MICRO
- turbot
- wirewheel
- direktgruppe
- stackArmor

Security operations & automation

- Cloudreach
- ECCOM 华 讯 网 络
- eCloud valley
- Mphasis stelligent The Next Applied
- pwc
- SAMSUNG SAMSUNG SDS

aws

Shared responsibility model



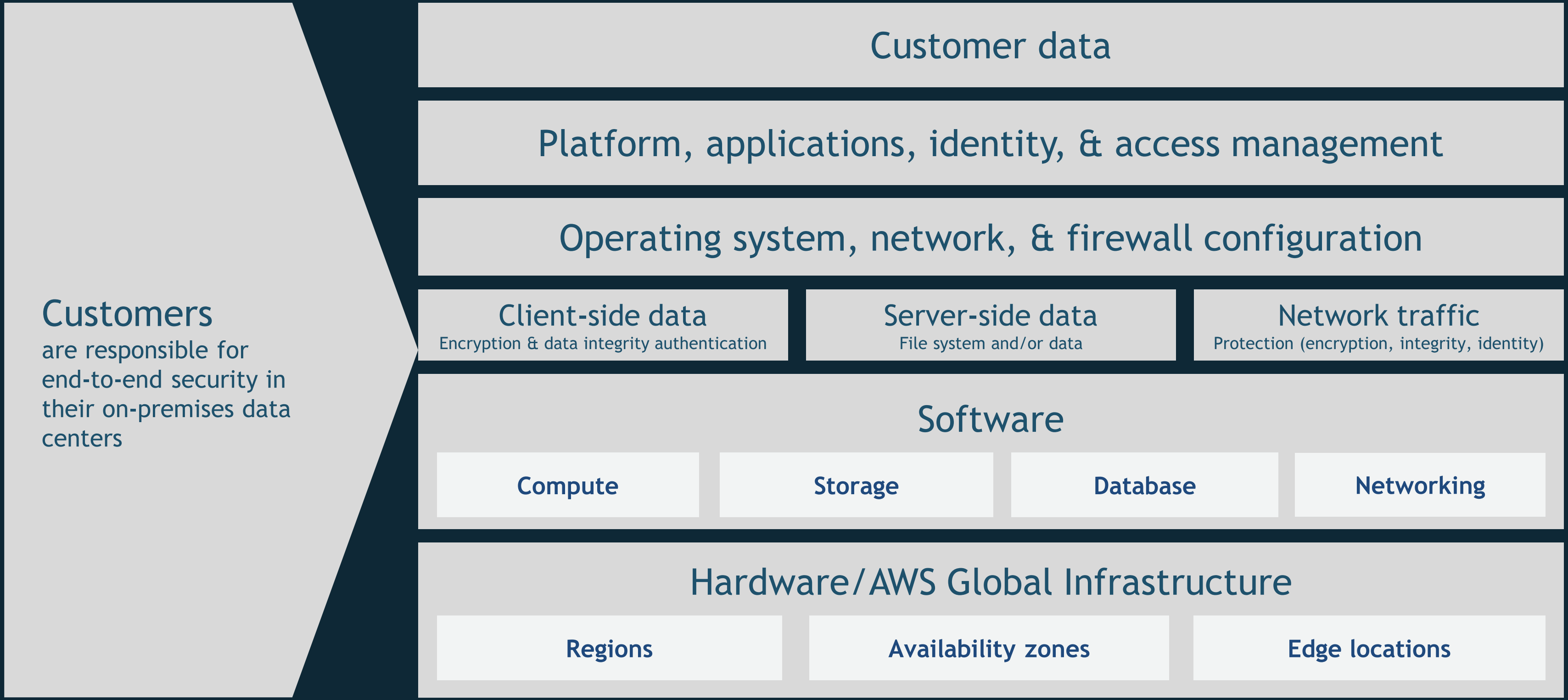
Security IN the Cloud

Customer responsibility will be determined by the AWS Cloud services that a customer selects

Security OF the Cloud

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud

Traditional on-premises security model



Customers are responsible for end-to-end security in their on-premises data centers

Customer data

Platform, applications, identity, & access management

Operating system, network, & firewall configuration

Client-side data
Encryption & data integrity authentication

Server-side data
File system and/or data

Network traffic
Protection (encryption, integrity, identity)

Software

Compute

Storage

Database

Networking

Hardware/AWS Global Infrastructure

Regions

Availability zones

Edge locations

Financial industry regulatory authority

- Looks for fraud, abuse, and insider trading over nearly 6 billion shares traded in U.S. equities markets every day
- Processes approximately 6 terabytes of data and 37 billion records on an average day
- Went from 3-4 weeks for server hardening to 3-4 minutes
- DevOps teams focus on automation and tools to raise the compliance bar and simplify controls
- Achieved incredible levels of assurance for consistencies of builds and patching via rebooting with automated deployment scripts

> “I have come to realize that as a relatively small organization, we can be far more secure in the cloud and achieve a higher level of assurance at a much lower cost, in terms of effort and dollars invested. We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance.”

—John Brady, CISO FINRA

Online medical care scheduling

Zocdoc

- Migrated all-in on AWS in under 12 months, becoming a HIPAA compliant cloud-first organization
- New York based startup leveraged infrastructure as code to securely scale to 6 million patients per month
- Data liberation—use data to innovate and drive more solutions for patients, reducing patient wait times from 24 days to 24 hours
- Maintain end to end visibility of patient data using AWS

"Previously all our servers were configured and updated by hand or through limited automation, we didn't take full advantage of a configuration management…All our new services are built as stateless docker containers, allowing us to deploy and scale them easily using Amazon's ECS."

"AWS allowed us to scale our business to handle 6 million patients a month and elevate our security—all while maintaining HIPAA compliance--as we migrated 100% to cloud in less than 12 months"

—Brian Lozada, chief information security officer

Thank you

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

@AWSSecurityInfo
@AWSIdentity