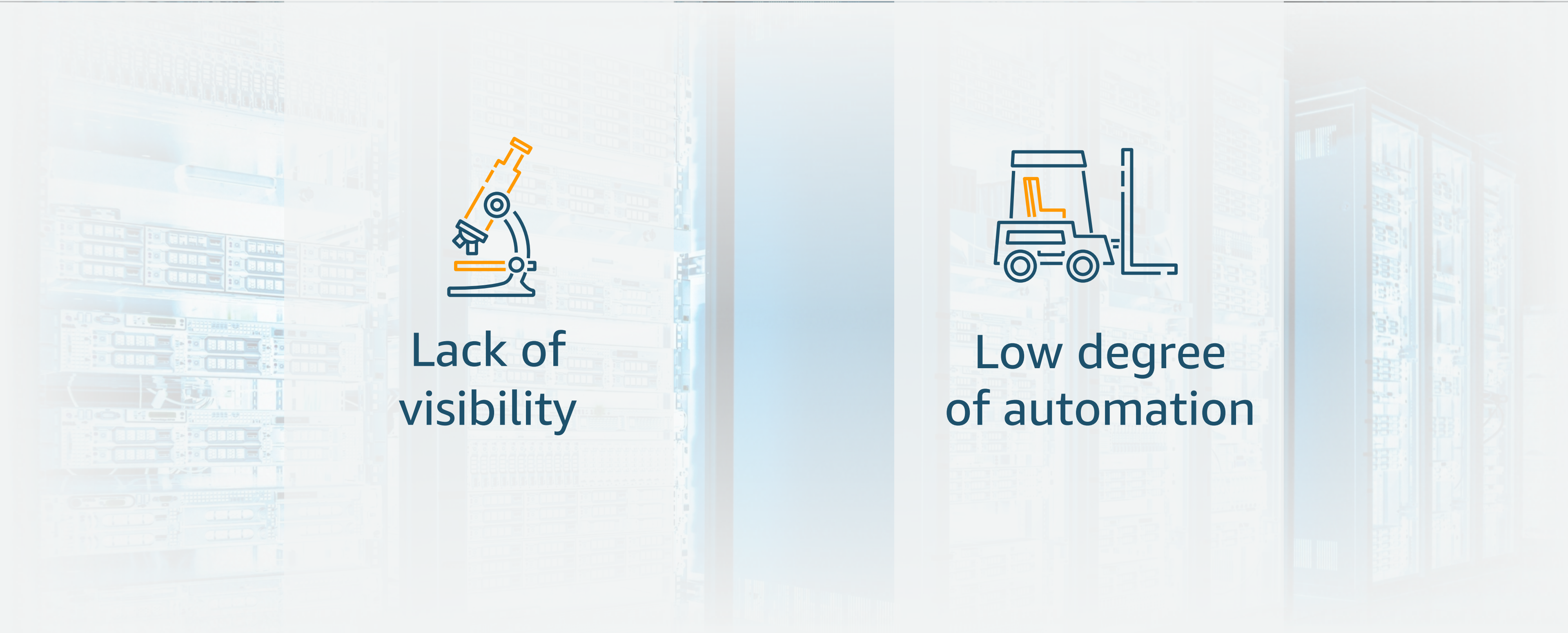
AWS Security, Identity, and Compliance

Elevate your security with the cloud

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

FINRA

"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)

Zocdoc

"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.

vodafone

"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

aws

Elevate your security with the AWS Cloud

Inherit global security and compliance controls

Scale with superior visibility and control

Highest standards for privacy and data security

Automate with comprehensive, integrated security services

Largest network of security partners and 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 FIPS CRYPTOGRAPHY

FISMA FEDERAL INFORMATION SECURITY MANAGEMENT ACT

DoD SRG

FR FedRAMP

FERPA

FFIEC Federal Financial Institutions Examination Council

NIST

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

G-Cloud

TISAX ENX ASSOCIATION

C5

CYBER ESSENTIALS PLUS

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010

aws

Scale with visibility and control

Control where your data is stored and who can access it

Fine-grain identity & access control so resources have the right access

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

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 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 solutions

Identity & access management

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

Detective controls

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

Infrastructure protection

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

Data protection

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

Incident response

- AWS Config Rules
- AWS Lambda

Largest ecosystem of security partners and solutions

Infrastructure security

- ALERT LOGIC
- ARMOR
- Barracuda
- Check Point
- CISCO
- CROWDSTRIKE
- Cyxtera
- FORTINET
- f5
- IMPERVA
- LACEWORK
- paloalto
- PROTECTWISE
- SOPHOS
- Symantec
- TREND MICRO
- zscaler

Identity & access control

- okta
- onelogin
- PingIdentity

Data protection

- gemalto
- HashiCorp
- Vormetric

Configuration & vulnerability analysis

- cavirin
- CloudCheckr
- Cloud Conformity
- CloudHealth by vmware
- CloudPassage
- Dome9
- evident.io
- Qualys
- RedLock
- SAVIYNT
- Telos
- tenable
- threat stack
- turbot

Logging & monitoring

- ALIEN VAULT
- splunk>
- sumologic

aws

Consulting competency partners with demonstrated expertise

Security engineering

- 8K Miles
- accenture High performance. Delivered.
- AllCloud
- [redacted]
- CLOUDZONE by matrix
- Deloitte.
- ECCO 华讯网络
- escala 24x7
- FOGHORN
- GuidePoint
- HELECLOUD
- Hewlett Packard Enterprise
- logicworks
- NRI Dream up the future
- REAN CLOUD
- rightCloud
- VERSENT

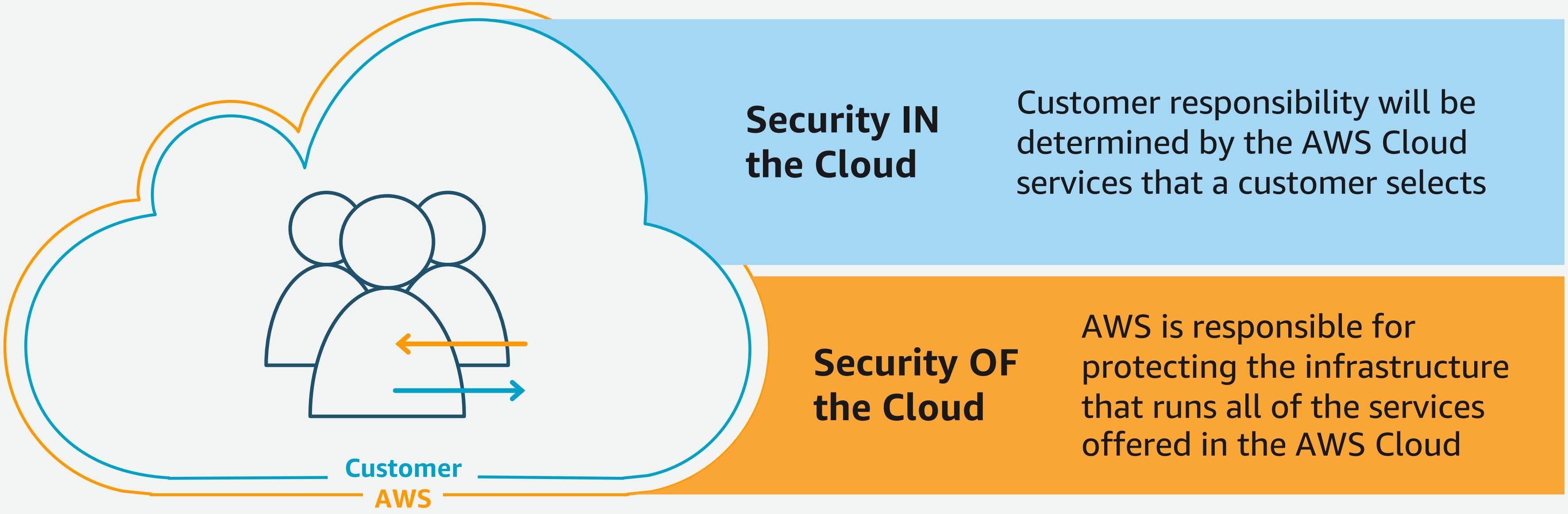
Governance, risk, & compliance

- Booz | Allen | Hamilton
- >CMD SOLUTIONS
- ECCO 华讯网络
- KindlyOps
- OPTIV
- REAN CLOUD
- stackArmor

Security operations & automation

- CLOUDREACH
- >CMD SOLUTIONS
- ECCO 华讯网络
- logicworks
- SAMSUNG SAMSUNG SDS

Shared responsibility model



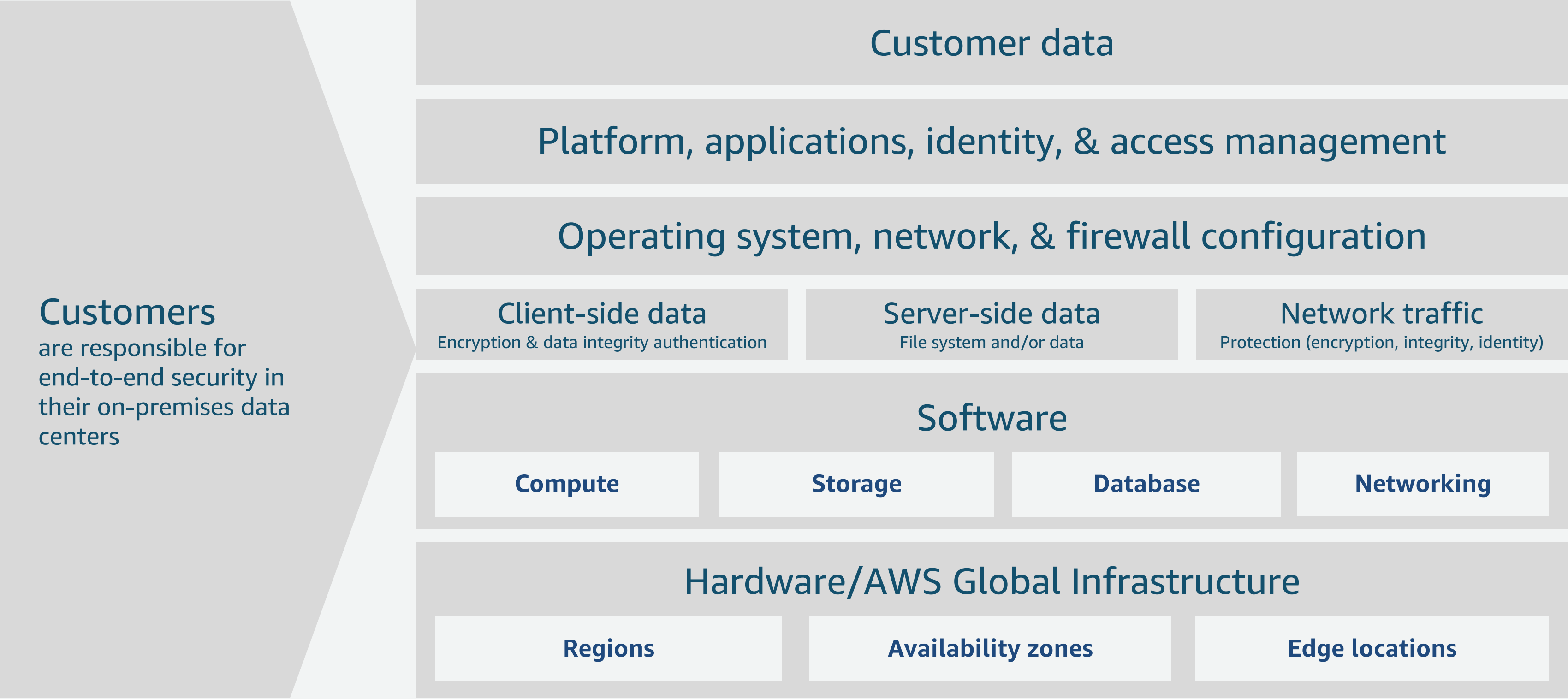
Security IN the Cloud

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

aws

Mobile top-up service

- Vodafone Italy is a prominent player in the Italian mobile phone market with over 30 million users.
- With a rise in SIM transactions, the company wanted to find a way to make it easier for customers to top up using a credit or debit card—and since each SIM card contains valuable personal information, that solution needed to be not only flexible, but also secure.
- With AWS Cloud, Vodafone Italy was able to users to purchase credits online with strong security and be compliant with the Payment Card Industry Data Security Standard (PCI DSS).
- With the muscle of the AWS cloud behind it, Vodafone easily managed top-up requests through the new service as it grew to several thousand daily and spread to multiple online channels, including social media platforms.

vodafone

> "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."
>
> "Using AWS, we were able to design and launch a security-compliant solution in three months while reducing our capital expenses by 30 percent."

—Stefano Harak, online senior product manager

aws

Thank you

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

Identity & access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM)

Securely control access to AWS services and resources

AWS Single Sign-On (SSO)

Centrally manage SSO access to multiple AWS accounts & business apps

AWS Directory Service

Managed Microsoft Active Directory in the AWS Cloud

Amazon Cognito

Add user sign-up, sign-in, and access control to your web/ mobile apps

AWS Organizations

Policy-based management for multiple AWS accounts

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

AWS Resource Access Manager

Simple, secure service to share AWS resources

Detective controls

Gain the visibility you need to spot issues before they impact the business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub

Centrally view & manage security alerts & automate compliance checks

Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads

AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, & security analysis

AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational/risk auditing of your AWS account

Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes

VPC Flow Logs

Capture info about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs

Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure operating systems

AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS

AWS WAF—Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security

AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications

Amazon Inspector

Automates security assessments to help improve the security and compliance of applications deployed on AWS

Amazon Virtual Private Cloud (VPC)

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define

Data protection

In addition to our automatic data encryption and management services, employ more features for data protection

(including data management, data security, and encryption key storage)

AWS Key Management Service (KMS)

Easily create and control the keys used to encrypt your data

AWS CloudHSM

Managed hardware security module (HSM) on the AWS Cloud

AWS Certificate Manager

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

Amazon Macie

Machine learning-powered security service to discover, classify, and protect sensitive data

Server-Side Encryption

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice

AWS Config Rules

Create rules that automatically take action in response to changes in your environment, such as isolating resources, enriching events with additional data, or restoring configuration to a known-good state

AWS Lambda

Use our serverless compute service to run code without provisioning or managing servers so you can scale your programmed, automated response to incidents