

Immersion Day

Cibersegurança e Conformidade na nuvem **AWS**

Fernando Gebara

Security Assurance, Public Sector, Brazil

fgebara@amazon.com



AWS Cloud Computing Introduction



Technical & Business Support

Marketplace

Analytics



DevOps



IoT



Machine Learning



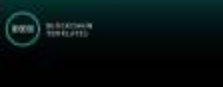
Mobile Services



App Services



Blockchain



Enterprise Apps



Infrastructure



Migration



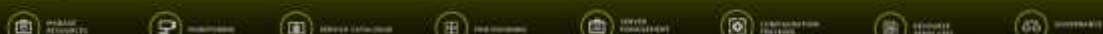
Security & Compliance



Core Services



Management Tools



AWS security solutions



Identity

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



Detective control

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



Infrastructure security

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



Identity & access control



Data protection



Configuration & vulnerability analysis



Logging & monitoring



AWS Cloud Computing Security Overview



AWS – Security is Job Zero

PEOPLE & PROCESS

SYSTEM

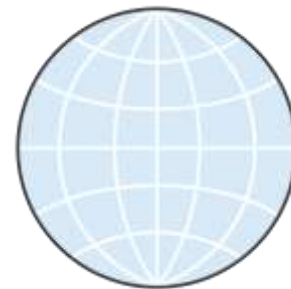
NETWORK

PHYSICAL



Familiar Security
Model

Validated and driven by
customers' security experts



Benefits
all customers

Security is a Shared Responsibility

Security expertise is a scarce resource; AWS oversees the big picture, letting your security team focus on a subset of overall security needs.



- Facilities
- Physical security
- Compute infrastructure
- Storage infrastructure
- Network infrastructure
- Virtualization layer (EC2)
- Hardened service endpoints
- Rich IAM capabilities

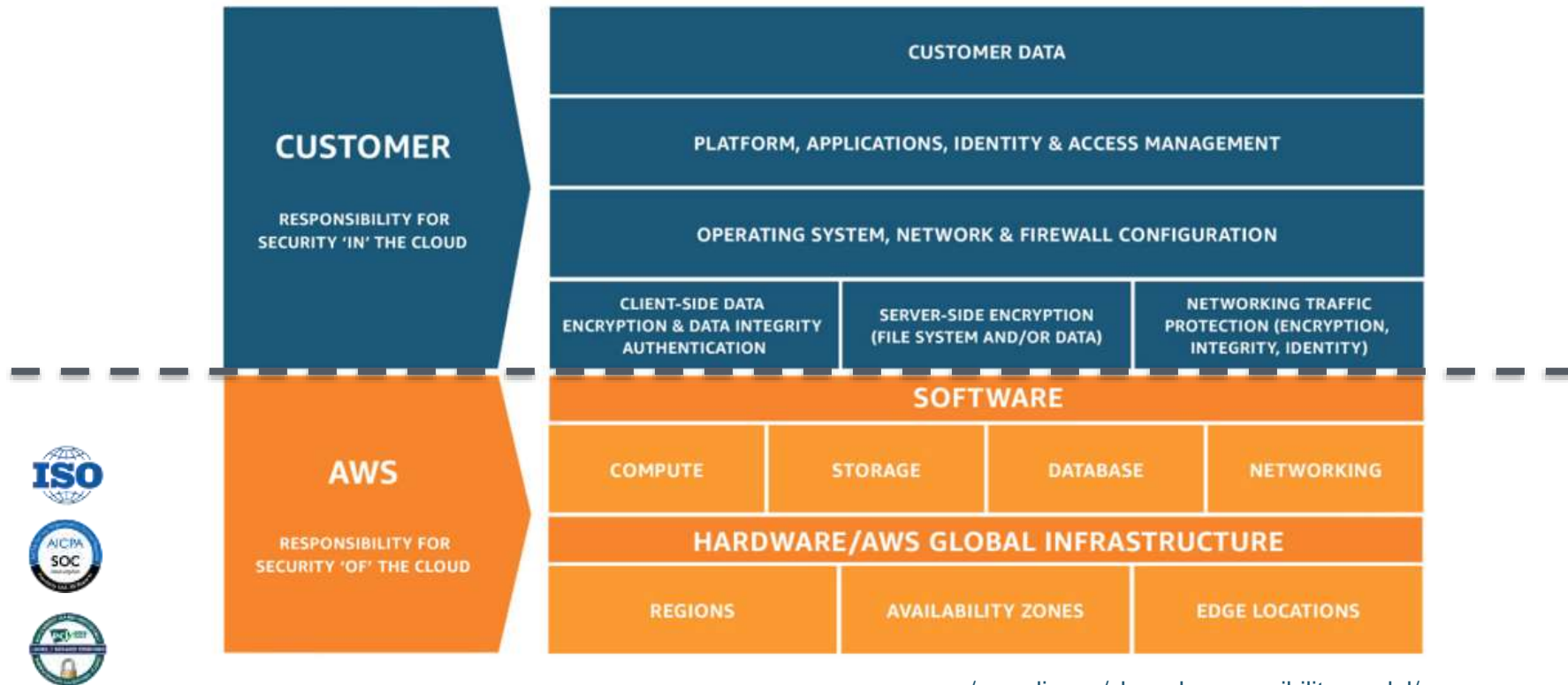


- Network configuration
- Security groups
- OS firewalls
- Operating systems
- Application security
- Proper service configuration
- AuthN and account management
- Authorization policies



More secure and compliant systems than any single entity could normally achieve on its own

AWS – Shared Responsibility Model



aws.amazon.com/compliance/shared-responsibility-model/

Encryption Data at Transit and Rest

Volume Encryption

EBS Encryption

Filesystem Tools

AWS
Marketplace/Partner

Object Encryption

S3 Server Side
Encryption (SSE)

S3 SSE w/ Customer
Provided Keys

Client-Side Encryption

Database Encryption

RDS
MSSQL
TDE

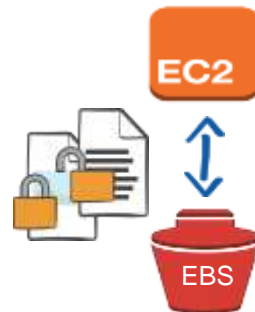
RDS
ORACLE
TDE/HSM

RDS MYSQL
KMS

RDS
PostgreSQL
KMS

Redshift
Encryption

End-to-end SSL/TLS



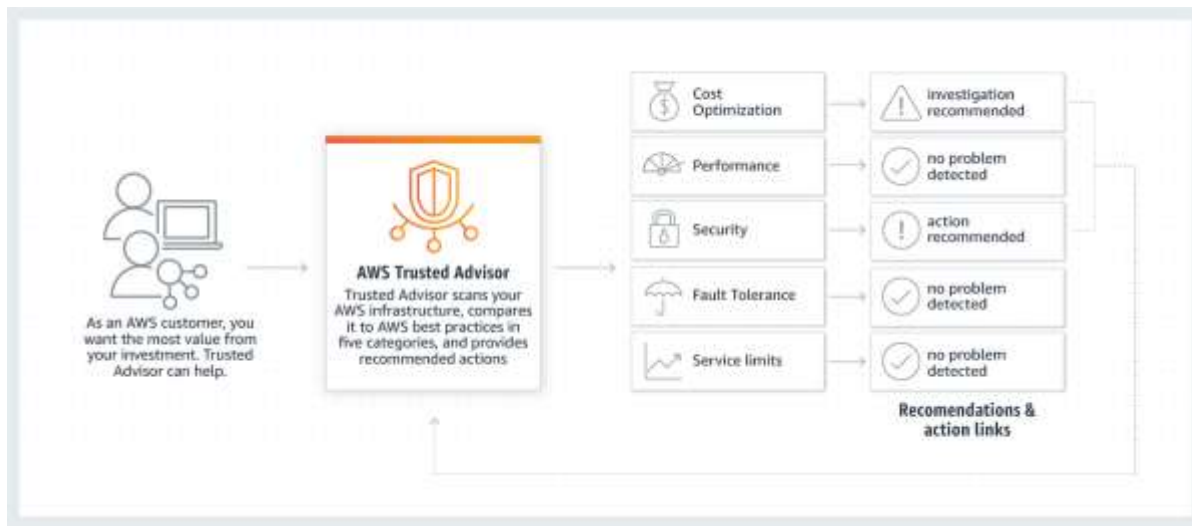
[AWS Whitepaper Securing Data at Rest with Encryption](#)

AWS Trusted Advisor – Real time guidance






Security configuration checks of your AWS environment:


- Open ports
- Unrestricted access
- CloudTrail Logging
- S3 Bucket Permissions
- Multi-factor auth
- Password Policy
- DB Access Risk
- DNS Records
- Load Balancer config






AWS Trusted Advisor


Security

Download   





4  1  4 
1 excluded items

View



All checks 

Security Checks



Security Groups - Specific Ports Unrestricted

Updated: Dec 22, 2014 6:32 AM



Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

44 of 124 security group rules allow unrestricted access to a specific port.



Security Groups - Unrestricted Access

Updated: Dec 22, 2014 6:24 AM



Checks security groups for rules that allow unrestricted access to a resource.

47 of 124 security group rules have a source IP address with a /0 suffix. 1 items have been excluded.

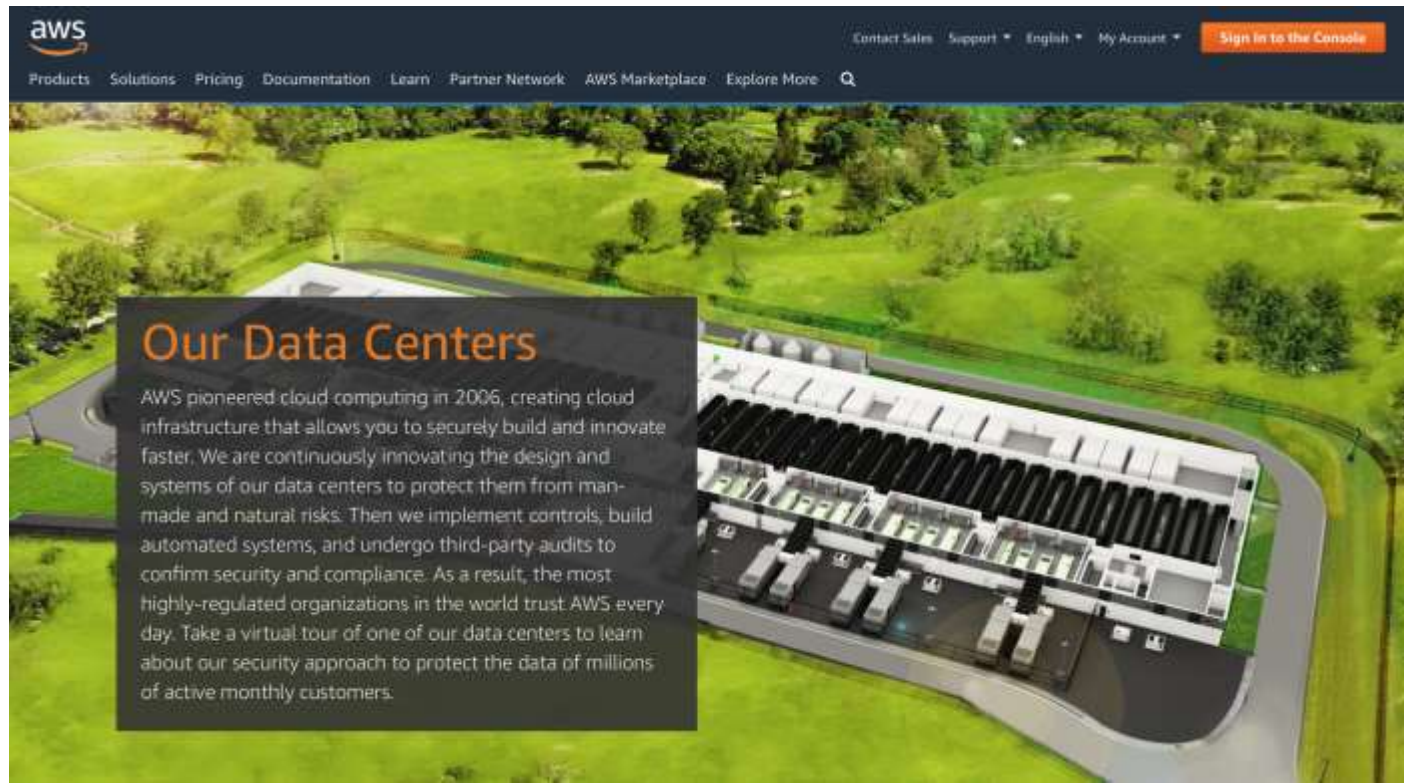
Amazon S3 Bucket Permissions

Updated: Dec 22, 2014 6:24 AM

Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions.

AWS – Datacenter Virtual Tour



<https://aws.amazon.com/compliance/data-center/>

Global compute platform for compute everywhere

- Regions
- CloudFront PoPs
- Direct Connect locations

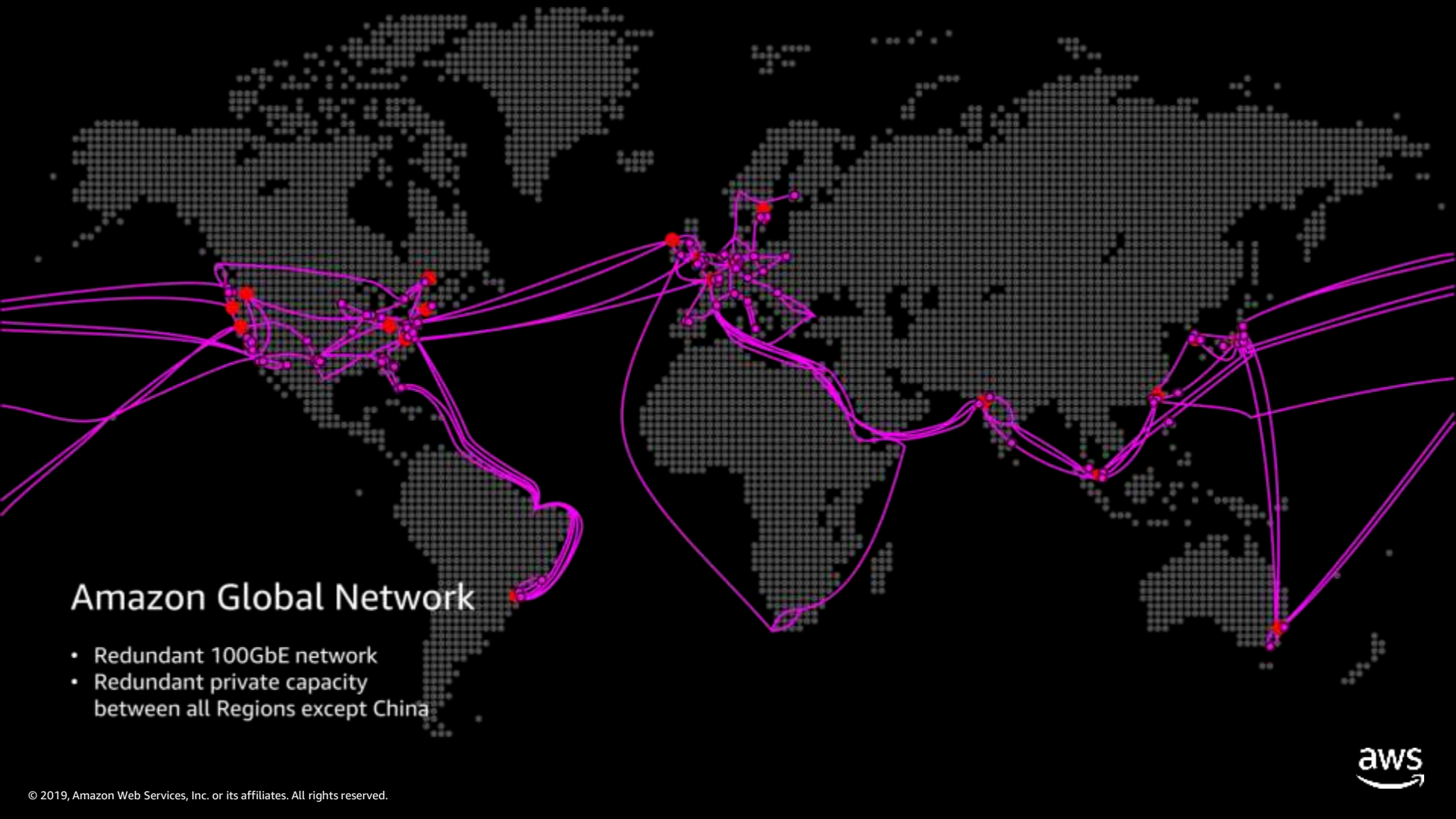
Global Availability

21 Regions
66 Availability Zones

Global Edge Network

166 Points of Presence
110 Direct Connect Locations





Amazon Global Network

- Redundant 100GbE network
- Redundant private capacity between all Regions except China



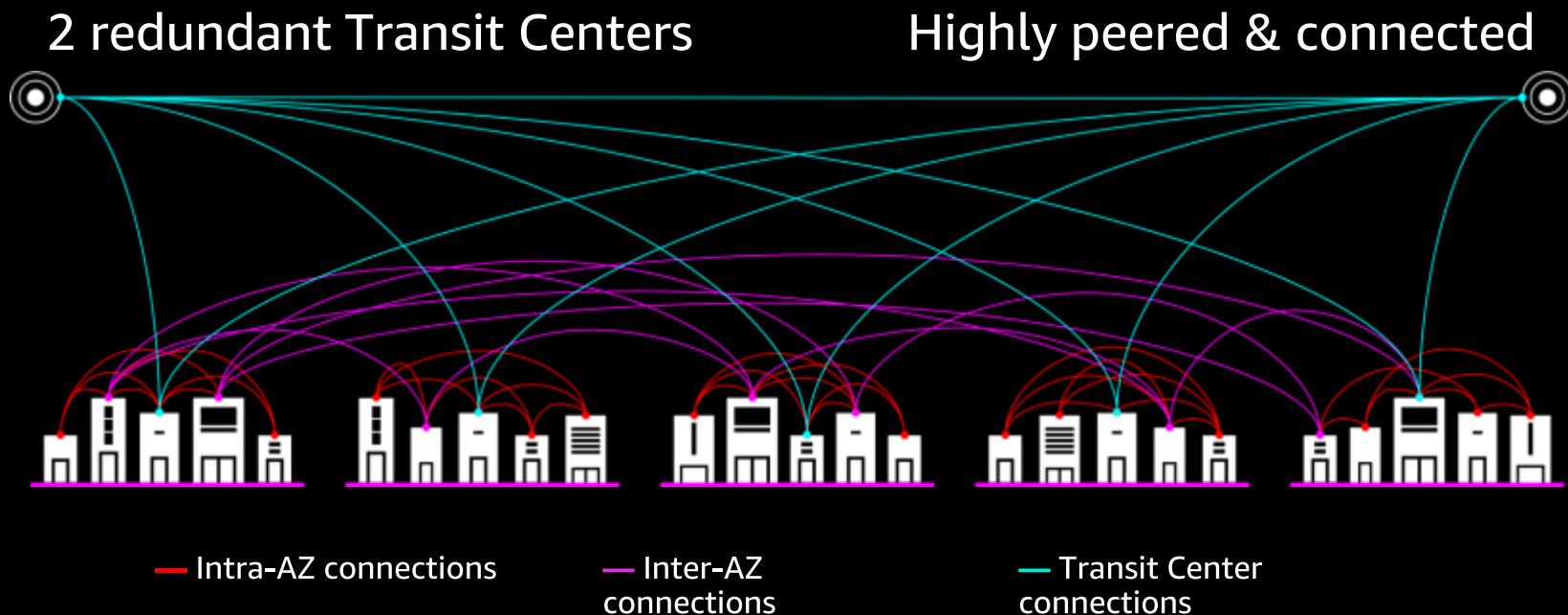
Availability Zones

- Fully isolated infrastructure with one or more datacenters
- Meaningful distance of separation
- Unique power infrastructure
- Many 100Ks of servers at scale
- Data centers connected via fully redundant and isolated metro fiber



Anatomy of an AWS Region

Redundant transit centers



One last thing, data sanitization



From this

To This



AWS Cloud Computing Assurance Program Compliance



AWS Compliance Program



CSA
Cloud Security
Alliance Controls



ISO 9001
Global Quality
Standard



ISO 27001
Security
Management
Controls



ISO 27017
Cloud Specific
Controls



ISO 27018
Personal Data
Protection



PCI DSS Level 1
Payment Card
Standards



SOC 1
Audit Controls
Report






SOC 2
Security, Availability,
& Confidentiality
Report



SOC 3
General Controls
Report

AWS Compliance Program



 Certifications / Attestations	 Laws, Regulations, and Privacy	 Alignments / Frameworks
C5 [Germany]	CISPE	CIS
Cyber Essentials Plus [UK]	DNB [Netherlands]	CJIS
DoD SRG	EU Model Clauses	CSA
FedRAMP	FERPA	ENS [Spain]
FIPS	GLBA	EU-US Privacy Shield
IRAP [Australia]	HIPAA	FISC
ISO 9001	HITECH	FISMA
ISO 27001	IRS 1075	G-Cloud [UK]
ISO 27017	ITAR	GxP (FDA CFR 21 Part 11)
ISO 27018	My Number Act [Japan]	ICREA
MLPS Level 3 [China]	U.K. DPA - 1988	IT Grundschutz [Germany]
MTCS [Singapore]	VPAT / Section 508	MITA 3.0
PCI DSS Level 1	EU Data Protection Directive	MPAA
SEC Rule 17-a-4(f)	Privacy Act [Australia]	NIST
SOC 1	Privacy Act [New Zealand]	PHR
SOC 2	PDPA - 2010 [Malaysia]	Uptime Institute Tiers
SOC 3	PDPA - 2012 [Singapore]	UK Cloud Security Principles
	PIPEDA [Canada]	
	Spanish DPA Authorization	

AWS Services in Scope by Compliance Program

SOC	PCI	ISO	FedRAMP	DoD CC SRG	HIPAA BAA	IRAP	MTCS	C5	K-ISMS	ENS High
SERVICES / PROGRAMS										SOC 1,2,3
Amazon API Gateway										✓
Amazon Athena										✓
Amazon Cloud Directory										✓
Amazon CloudFront										✓
Amazon CloudWatch Logs										✓
Amazon Cognito										✓
Amazon Connect										✓
Amazon DynamoDB										✓
Amazon Elastic Container Registry (ECR)										✓
Amazon Elastic Container Service (ECS) [both Fargate and EC2 launch types]										✓
Amazon ElastiCache										✓
Amazon Elastic Block Store (EBS)										✓
Amazon Elastic Compute Cloud (EC2)										✓

<https://aws.amazon.com/compliance/services-in-scope/>

SLA

[Products](#) [Solutions](#) [Pricing](#) [Documentation](#) [Learn](#) [Partner Network](#) [AWS Marketplace](#) [Explore More](#) 

[Contact Sales](#) [Support](#) [English](#) [My Account](#) [Sign in to the Console](#)

LEGAL

[AWS Service Level Agreements](#)

RELATED LINKS

[What is AWS?](#)

[AWS Products & Services](#)

[AWS Solutions](#)

AWS Service Level Agreements

- [Amazon API Gateway Service Level Agreement](#)
- [Amazon CloudFront Service Level Agreement](#)
- [AWS CloudHSM Service Level Agreement](#)
- [Amazon Cognito Service Level Agreement](#)
- [Amazon Database Migration Service Level Agreement](#)
- [AWS Direct Connect Service Level Agreement](#)
- [AWS Directory Service Service Level Agreement](#)
- [Amazon DocumentDB \(with MongoDB compatibility\) Service Level Agreement](#)
- [Amazon DynamoDB Service Level Agreement](#)
- [Amazon EC2 Service Level Agreement](#)
- [Amazon EFS Service Level Agreement](#)
- [Amazon EKS Service Level Agreement](#)
- [Amazon Elastic Container Registry Service Level Agreement](#)
- [Amazon Elastic Load Balancing Service Level Agreement](#)
- [Amazon ElastiCache Service Level Agreement](#)
- [Amazon EMR Service Level Agreement](#)
- [Amazon FSx Service Level Agreement](#)
- [AWS Glue Service Level Agreement](#)
- [AWS Hybrid Storage and Data Transfer Service Level Agreement](#)

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 Cloud HSM 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

Customers are in **control of privacy**

- Retain ownership and control of content
- Control which end users have **access** to content.
- Customer always **own their data, the ability to encrypt it, move it, and delete it**
- **Choose the specific AWS Region** where content will be hosted
- Control content **lifecycle**.



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 an existing Active Directory using federation and single sign-on



AWS Cloud Computing



Services Health Dashboard

 **SERVICE HEALTH DASHBOARD**

Amazon Web Services • Service Health Dashboard











Get a personalized view of AWS service health

Open the Personal Health Dashboard

Current Status - Mar 26, 2019 PDT

Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time, operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

North AmericaSouth AmericaEuropeAsia PacificContact Us

Recent Events	Details	RSS
✓ No recent events.		
Remaining Services	Details	RSS
✓ Alexa for Business (N. Virginia)	Service is operating normally	
✓ Amazon API Gateway (Montreal)	Service is operating normally	
✓ Amazon API Gateway (N. California)	Service is operating normally	
✓ Amazon API Gateway (N. Virginia)	Service is operating normally	
✓ Amazon API Gateway (Ohio)	Service is operating normally	
✓ Amazon API Gateway (Oregon)	Service is operating normally	
✓ Amazon AppStream 2.0 (N. Virginia)	Service is operating normally	
✓ Amazon AppStream 2.0 (Oregon)	Service is operating normally	
✓ Amazon Athena (Montreal)	Service is operating normally	
✓ Amazon Athena (N. Virginia)	Service is operating normally	

<https://status.aws.amazon.com/>

Subcontractors



Acesso de subcontratados

Informamos proativamente os nossos clientes caso algum subcontratado tenha acesso a dados de propriedade do cliente carregados para a AWS, incluindo dados que podem conter informações pessoais.

Data de entrada em vigor: 15 de maio de 2019

Os subcontratados autorizados pela AWS a acessar todos os dados de propriedade do cliente que você carregou na AWS são os seguintes:

-Nenhum

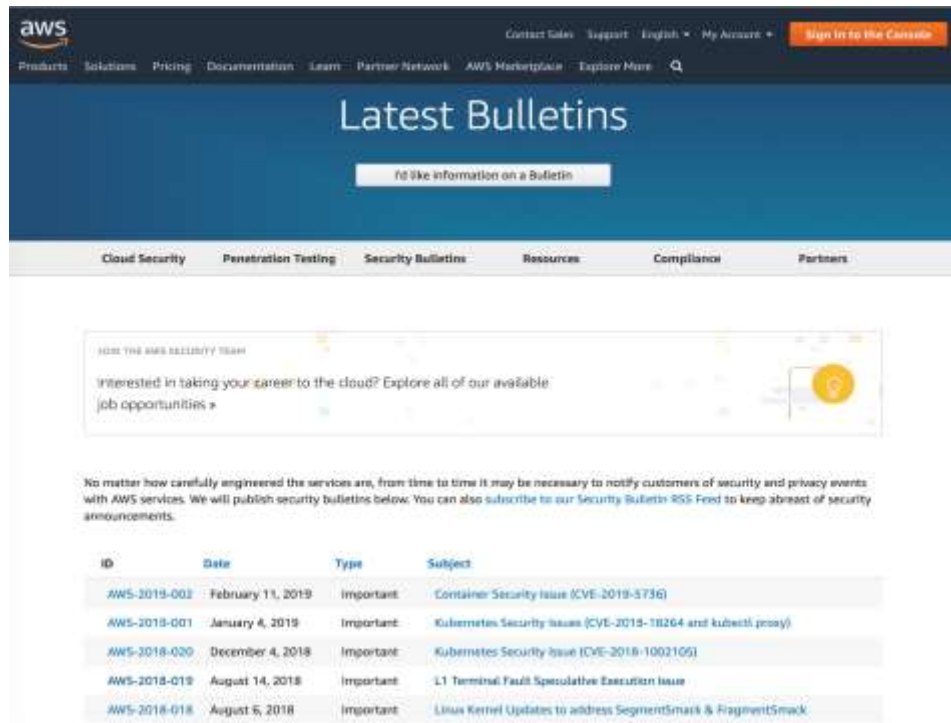
Porém, menos 30 dias antes de autorizarmos e permitirmos que qualquer subcontratado acesse qualquer dado de propriedade do cliente, a AWS atualizará seu site para informar os clientes.

Para notificações de subprocessadores nos termos do Adendo de processamento de dados da AWS, consulte a nova página [aqui](#).

[Cadastre-se](#) para ser notificado de mudanças na lista dessa página

<https://aws.amazon.com/pt/compliance/third-party-access/>

Security Bulletins



The screenshot shows the AWS Security Bulletins page. At the top is the AWS logo and navigation links: Products, Solutions, Pricing, Documentation, Learn, Partner Network, AWS Marketplace, and Explore More. A search icon is also present. On the right, there are links for Contact Sales, Support, English, My Account, and a Sign In to the Console button. The main heading is "Latest Bulletins" with a sub-link "to like information on a Bulletin". Below this is a navigation bar with links for Cloud Security, Penetration Testing, Security Bulletins (selected), Resources, Compliance, and Partners. A job opportunity banner for the AWS Security Team is displayed. A paragraph explains that AWS publishes security bulletins to notify customers of security and privacy events. Below this is a table of recent security bulletins.

ID	Date	Type	Subject
AWS-2019-002	February 11, 2019	Important	Container Security Issue (CVE-2019-3736)
AWS-2018-Q01	January 4, 2019	Important	Kubernetes Security Issues (CVE-2018-18264 and kubelet proxy)
AWS-2018-Q20	December 4, 2018	Important	Kubernetes Security Issue (CVE-2018-1002109)
AWS-2018-Q19	August 14, 2018	Important	L1 Terminal Fault Speculative Execution Issue
AWS-2018-Q18	August 6, 2018	Important	Linux Kernel Updates to address SegmentSmack & FragmentSmack

<https://aws.amazon.com/security/security-bulletins/>

AWS Cloud Computing Resiliency



Ascending levels of DR options

Backup & Restore

Backup of on-premises data to AWS to use in a DR event



Pilot Light

Replicate data and minimal running services into AWS, ready to take over and flare up



Warm Standby

Replicate data and services into AWS ready to take over



Hot-Site

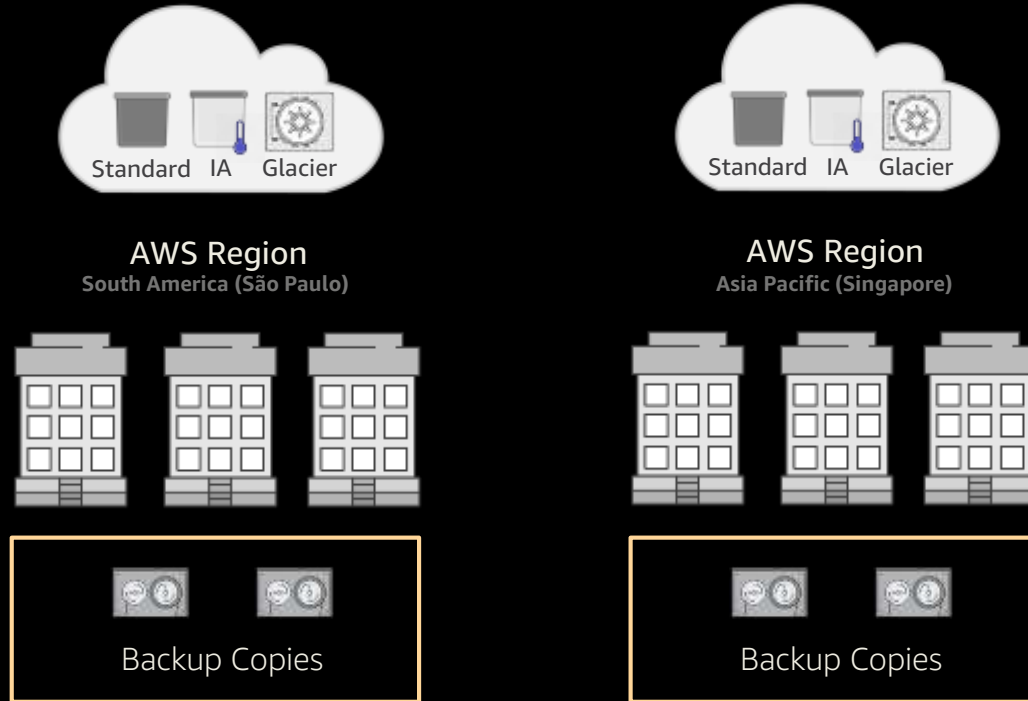
Replicated and load balanced environments that are both actively taking production traffic



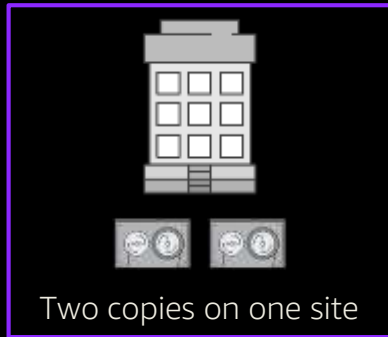
Business continuity
begins

Un-interrupted Business
continuity

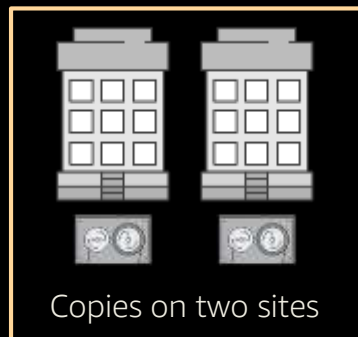
Resiliency / Business Continuity / DR



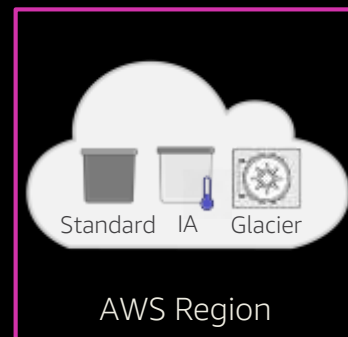
Understanding Durability



designed for
99.99%
durability



designed for
99.999%
durability



designed for
99.9999999999%
durability

AWS Cloud Computing Close-out, Next Steps, and Goodbye

