aws professional services

AWS Security Overview

AWS Security Workshop

Agenda

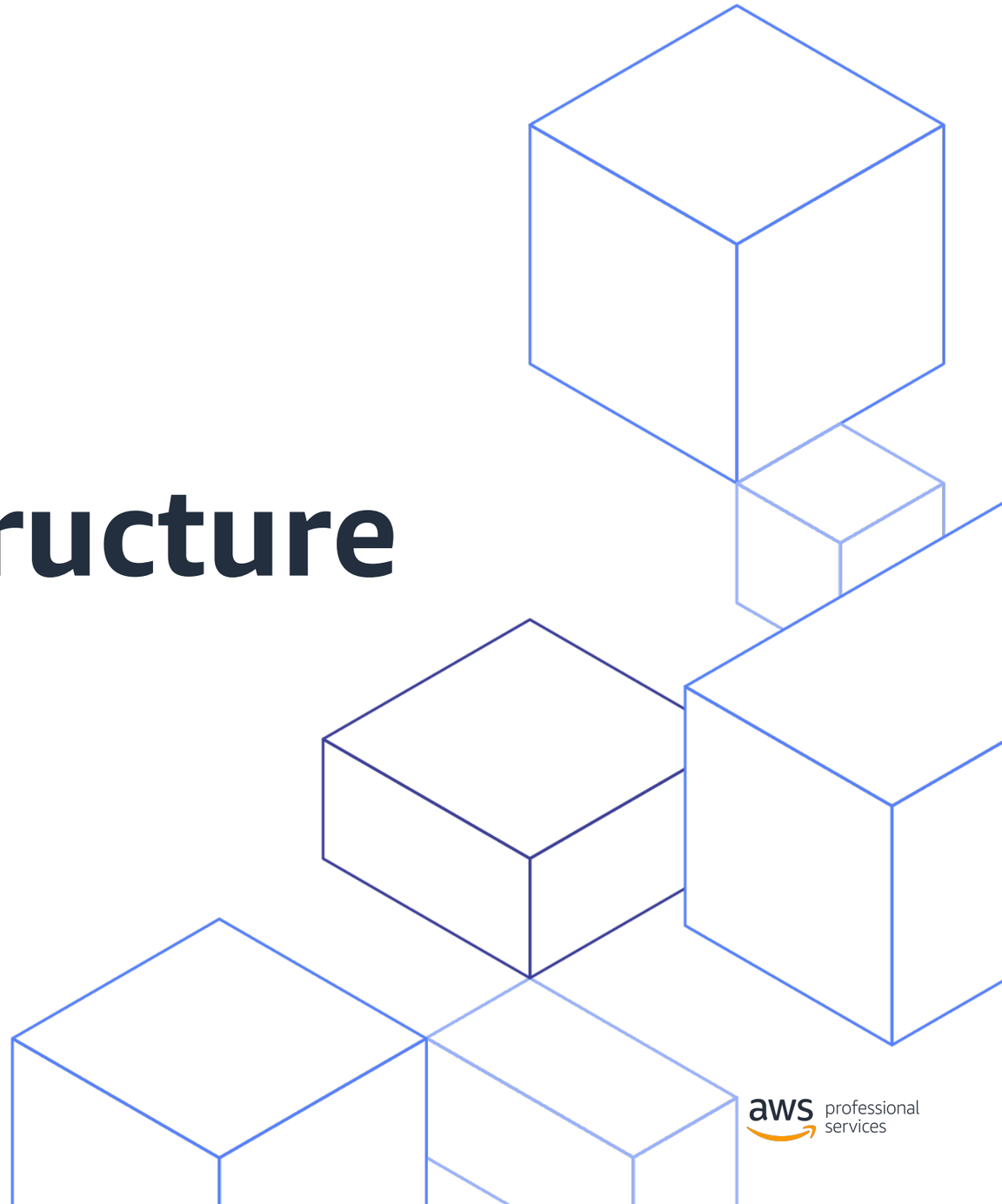
- Global Infrastructure
- Shared Responsibility
- Security Assurance
- Customer responsibility

Goals

- Learn how AWS approaches security
- Understand how AWS protects the cloud
- Understand your responsibility in the cloud

AWS Global Infrastructure

AWS Security Overview



aws professional services

Global Portfolio of Customers in 240 Countries/Territories

aws professional services

AWS Global Infrastructure

25 Regions – **81** Availability Zones – **218+** Edge Locations

Regions & Number of Availability Zones

US East
N. Virginia (6), Ohio (3)

US West
N. California (3), Oregon (4)

Asia Pacific
Mumbai (3), Seoul (4), Singapore (3), Sydney (3), Tokyo (4), Hong Kong (3), Osaka (3)

Canada
Central (3)

China
Beijing (3), Ningxia (3)

Europe
Frankfurt (3), Ireland (3), London (3), Paris (3), Stockholm (3), Milan (3)

South America
São Paulo (3)

South Africa
Cape Town(3)

Middle East
Bahrain (3)

AWS GovCloud (US)
US-East (3), US-West (3)

Announced Regions

Australia, India, Indonesia, Spain, and Switzerland

aws professional services

North America

US East (N. Virginia) Region

EC2 Availability Zones: 6

US East (Ohio) Region

EC2 Availability Zones: 3

US West (Oregon) Region

EC2 Availability Zones: 4

US West (N. California) Region

EC2 Availability Zones: 3*

AWS GovCloud (US-West) Region

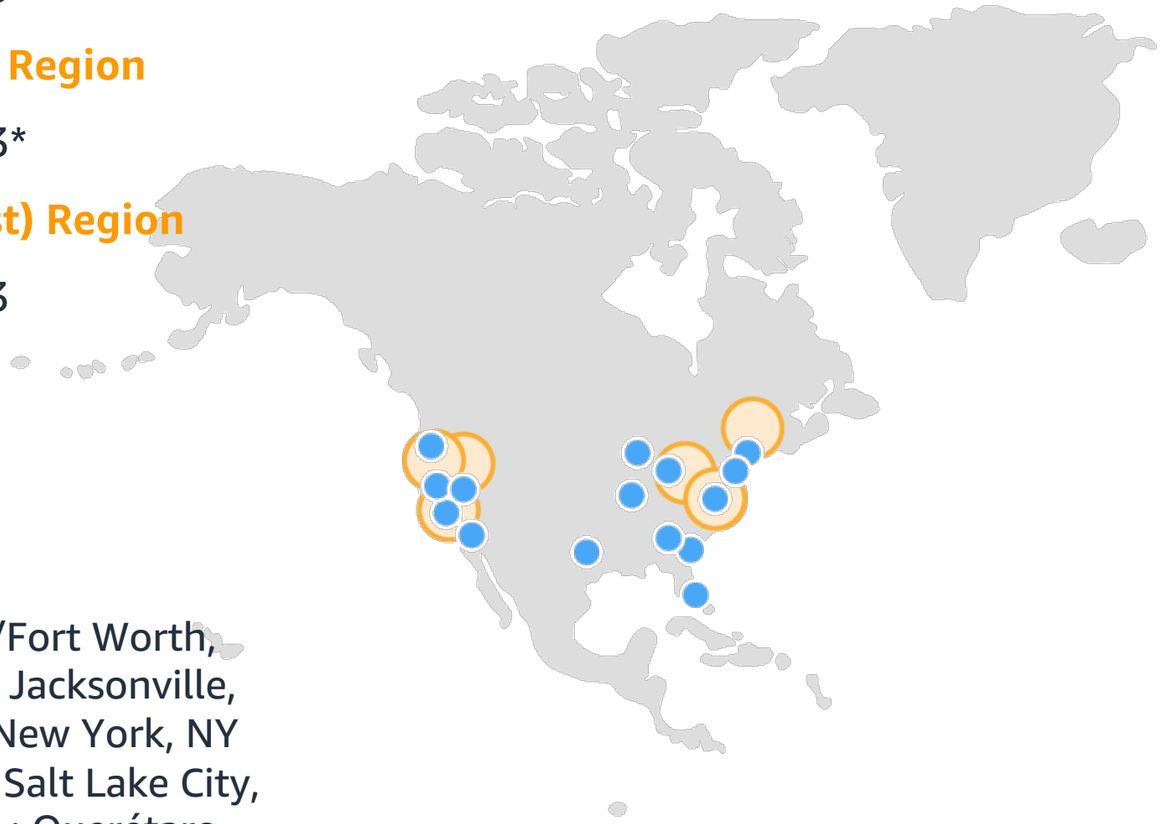
EC2 Availability Zones: 3

AWS GovCloud (US-East) Region

EC2 Availability Zones: 3

Canada (Central) Region

EC2 Availability Zones: 2



AWS Edge Locations

Ashburn, VA (6); Atlanta, GA (6); Boston, MA (3); Chicago, IL (6); Dallas/Fort Worth, TX (6); Denver, CO (2); Hayward, CA; Hillsboro, OR (3); Houston, TX (4); Jacksonville, FL; Los Angeles, CA (5); Miami, FL (4); Minneapolis, MN; Montreal, QC; New York, NY (2); Newark, NJ (7); Palo Alto, CA; Philadelphia, PA (2); Phoenix, AZ (2); Salt Lake City, Utah; San Jose, CA (2); Seattle, WA (3); Toronto, ON (2); Vancouver, BC ; Querétaro, MX (2)

AWS Local Zones Los Angeles, Boston, Houston, Miami

aws professional services

South America

São Paulo Region

EC2 Availability Zones: 3*

*New customers can access two EC2 Availability Zones in South America (São Paulo)

AWS Edge Locations

Rio de Janeiro (2), Brazil; Sao Paulo, Brazil (2); Bogota, Colombia; Buenos Aires, Argentina; Santiago, Chile

Regional Edge Caches

Sao Paulo, Brazil

Europe / Middle East / Africa

EU (Ireland) Region

Availability Zones: 3

EU (Frankfurt) Region

Availability Zones: 3

EU (London) Region

Availability Zones: 3

EU (Paris) Region

Availability Zones: 3

EU (Milan) Region

Availability Zones: 3

EU (Stockholm) Region

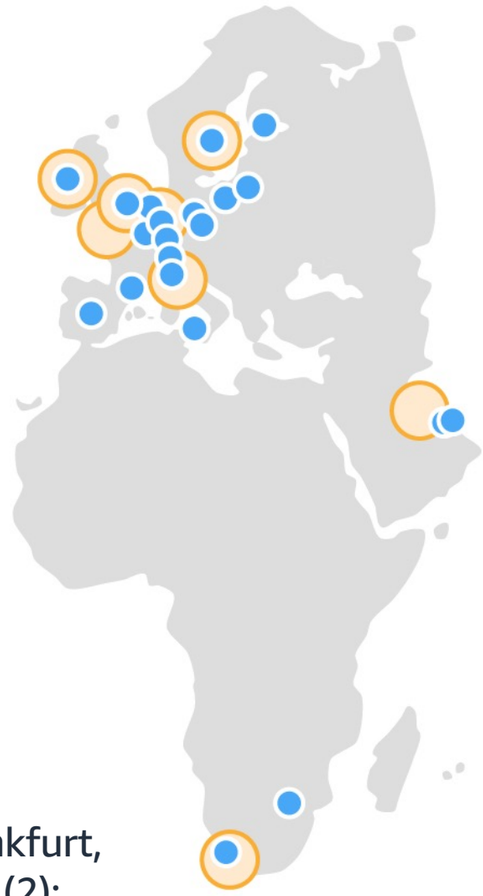
Availability Zones: 3

AWS Africa (Cape Town) Region

Availability Zones: 3

Middle East (Bahrain) Region

Availability Zones: 3



AWS Edge Locations

Amsterdam, The Netherlands (2); Berlin, Germany; Cape Town, South Africa; Dublin, Ireland; Frankfurt, Germany (10); Helsinki, Finland; Johannesburg, South Africa; London, England (7); Madrid, Spain (2); Manchester, England; Marseille, France; Milan, Italy; Munich, Germany; Dusseldorf, Germany; Palermo, Italy; Paris, France (3); Prague, Czech Republic; Stockholm, Sweden (3); Vienna, Austria; Warsaw, Poland; Zurich, Switzerland; Lisbon, Portugal; Brussels, Belgium; Athens, Greece; Bucharest, Romania; Budapest, Hungary; Nairobi, Kenya; Sofia, Bulgaria

Regional Edge Caches Frankfurt, Germany; London, England

Asia Pacific and China

Asia Pacific (Singapore) Region
Availability Zones: 3

Asia Pacific (Tokyo) Region
Availability Zones: 4*

Asia Pacific (Osaka) Region
Availability Zones: 3

Asia Pacific (Sydney) Region
Availability Zones: 3

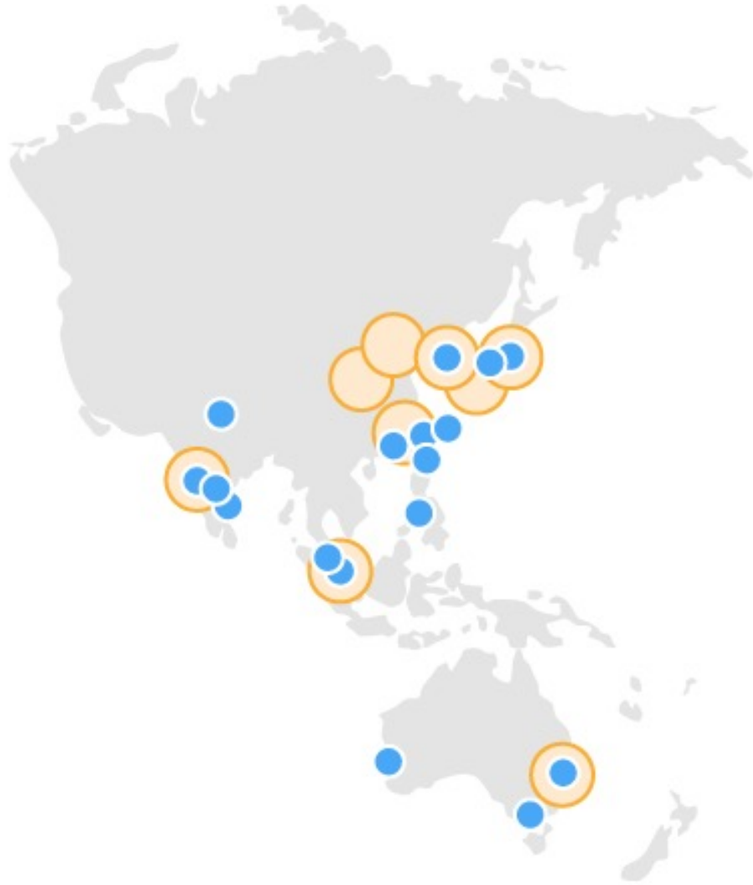
Asia Pacific (Hong Kong) Region
Availability Zones: 3

Asia Pacific (Seoul) Region
Availability Zones: 4

Asia Pacific (Mumbai) Region
Availability Zones: 3

Mainland China (Beijing) Region
Availability Zones: 3

Mainland China (Ningxia) Region
Availability Zones: 3



AWS Edge Locations

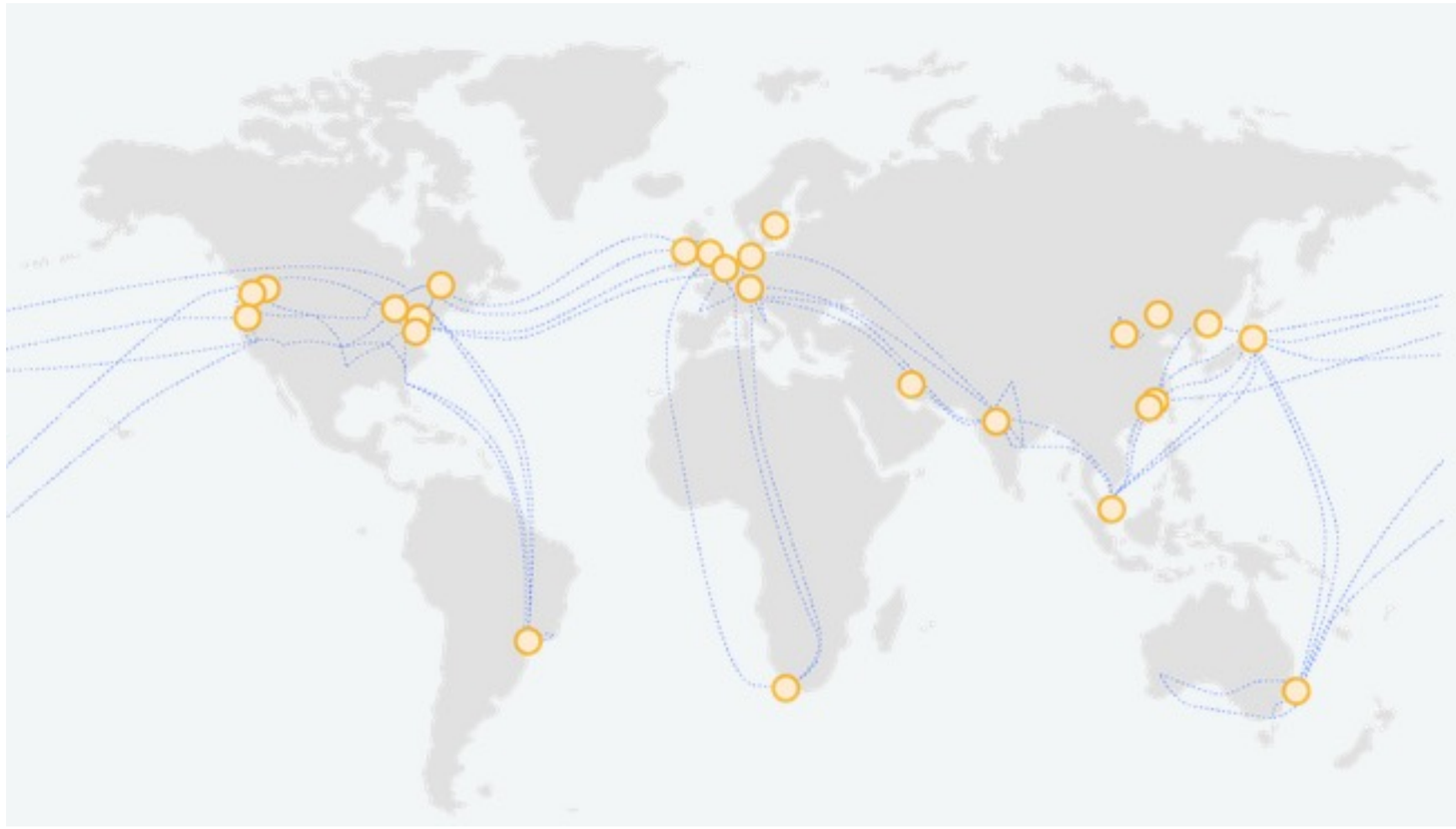
Bangalore, India (3); Chennai, India (2); Hong Kong SAR, China (3); Hyderabad, India (4); Kuala Lumpur, Malaysia; Mumbai, India (2); Manila, Philippines; New Delhi, India (5); Osaka, Japan; Seoul, South Korea (4); Singapore (3); Taipei, Taiwan(3); Tokyo, Japan (16); Melbourne; Perth; Sydney (2); Beijing, China (1); Shanghai, China (1); Zhongwei, China (1); Shenzhen, China (1)

aws professional services

AWS Backbone in the Global infrastructure

Every data centre, AZ, and AWS Region is interconnected via a purpose-built, highly available, and low-latency private global network infrastructure.

The network is built on a global, fully redundant, parallel 100 GbE metro fiber network that is linked via trans-oceanic cables across the Atlantic, Pacific, and Indian Oceans, as well as the Mediterranean, Red Sea, and South China Seas.



https://aws.amazon.com/about-aws/global-infrastructure/global_network/

aws professional services

AWS Shared Responsibility

AWS Security Overview

aws professional services

What is AWS Shared Responsibility?

Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services

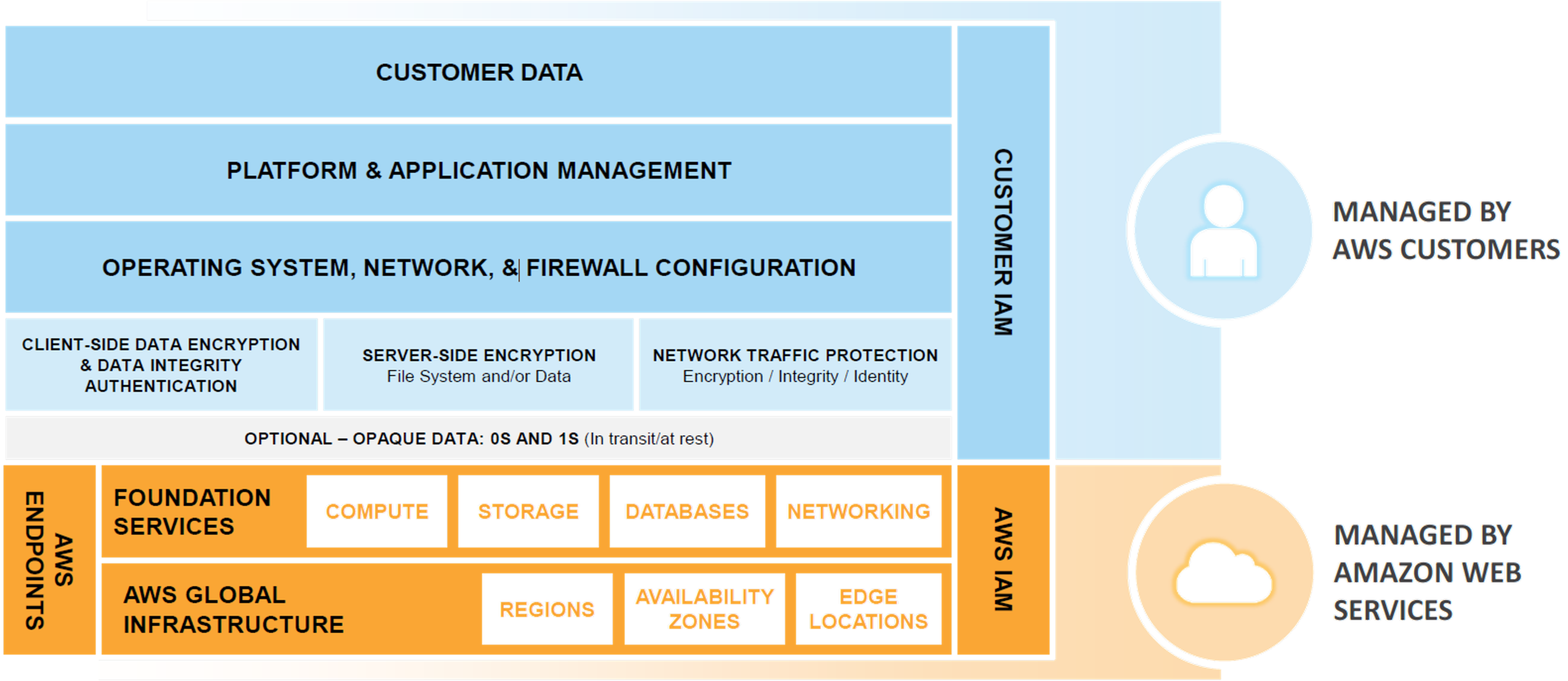
SECURITY **IN** THE CLOUD

Security measures that the cloud service provider (AWS) implements and operates

SECURITY **OF** THE CLOUD

aws professional services

What is AWS Shared Responsibility?



aws professional services

Security “in” and “of” AWS

MANAGED BY CUSTOMERS (**IN**)

Configure AWS security features

Can implement and manage own controls

Choose additional assurance above AWS controls

Gain access to a mature vendor marketplace

MANAGED BY AWS (**OF**)

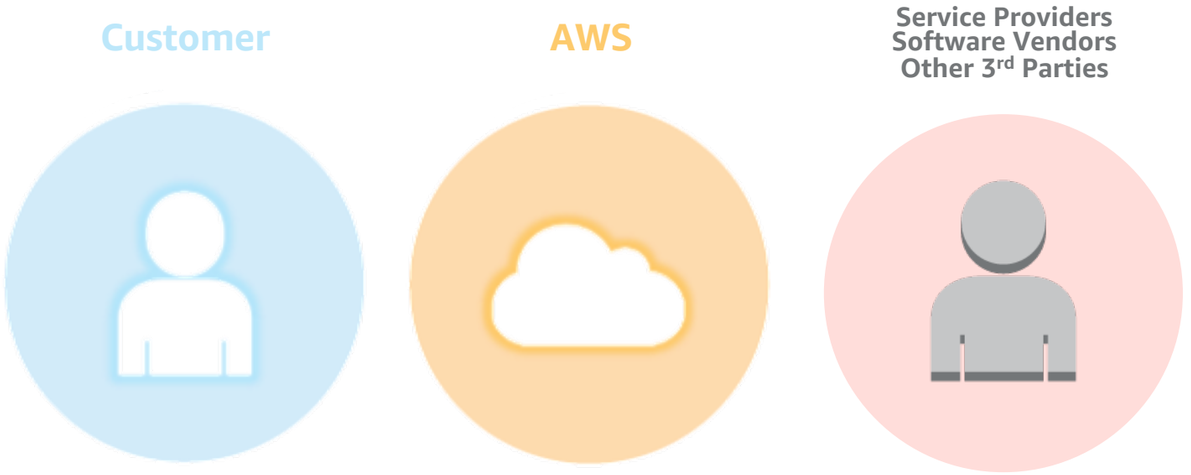
Ongoing audit and assurance programs

Protection of the global infrastructure that runs all of the AWS services

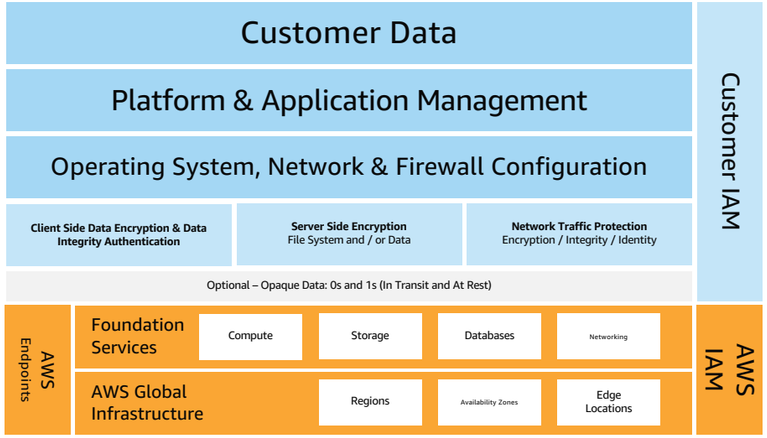
Protection of large-scale AWS service endpoints

Culture of security and improvement

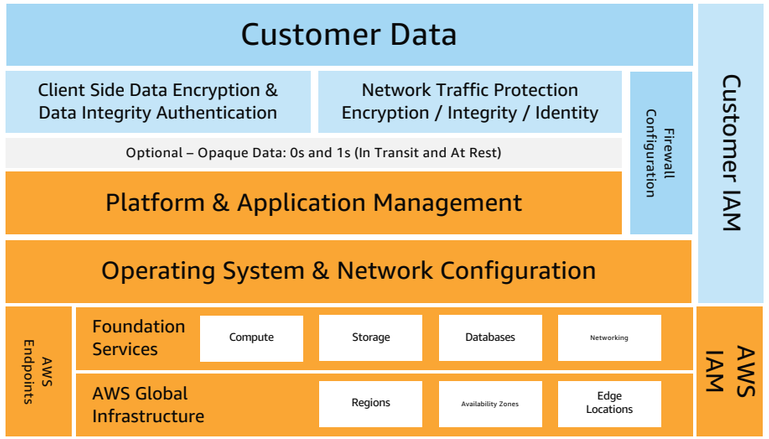
Shared Responsibility is not Static



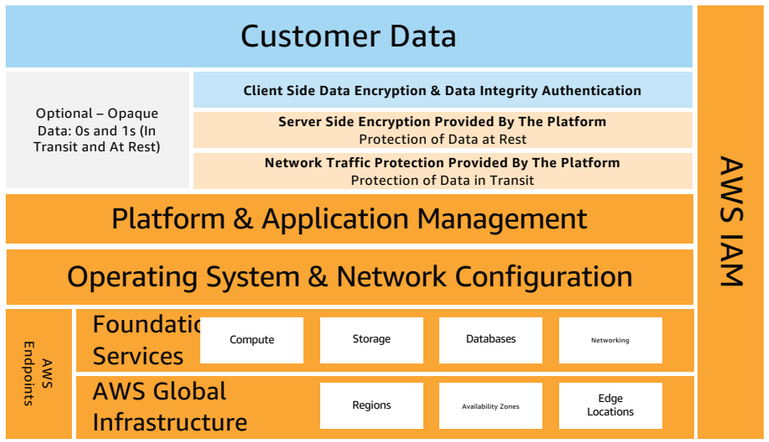
Infrastructure Services



Container Services



Abstracted Services

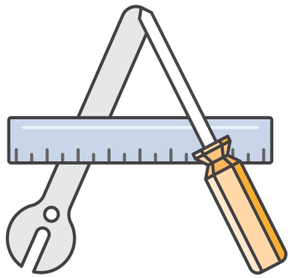


AWS Professional Services Security Workshop v6.0
AWS Security Overview

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

aws professional services

Security is Our Number 1 Priority



Designed for Security

Constantly Monitored

Highly Automated

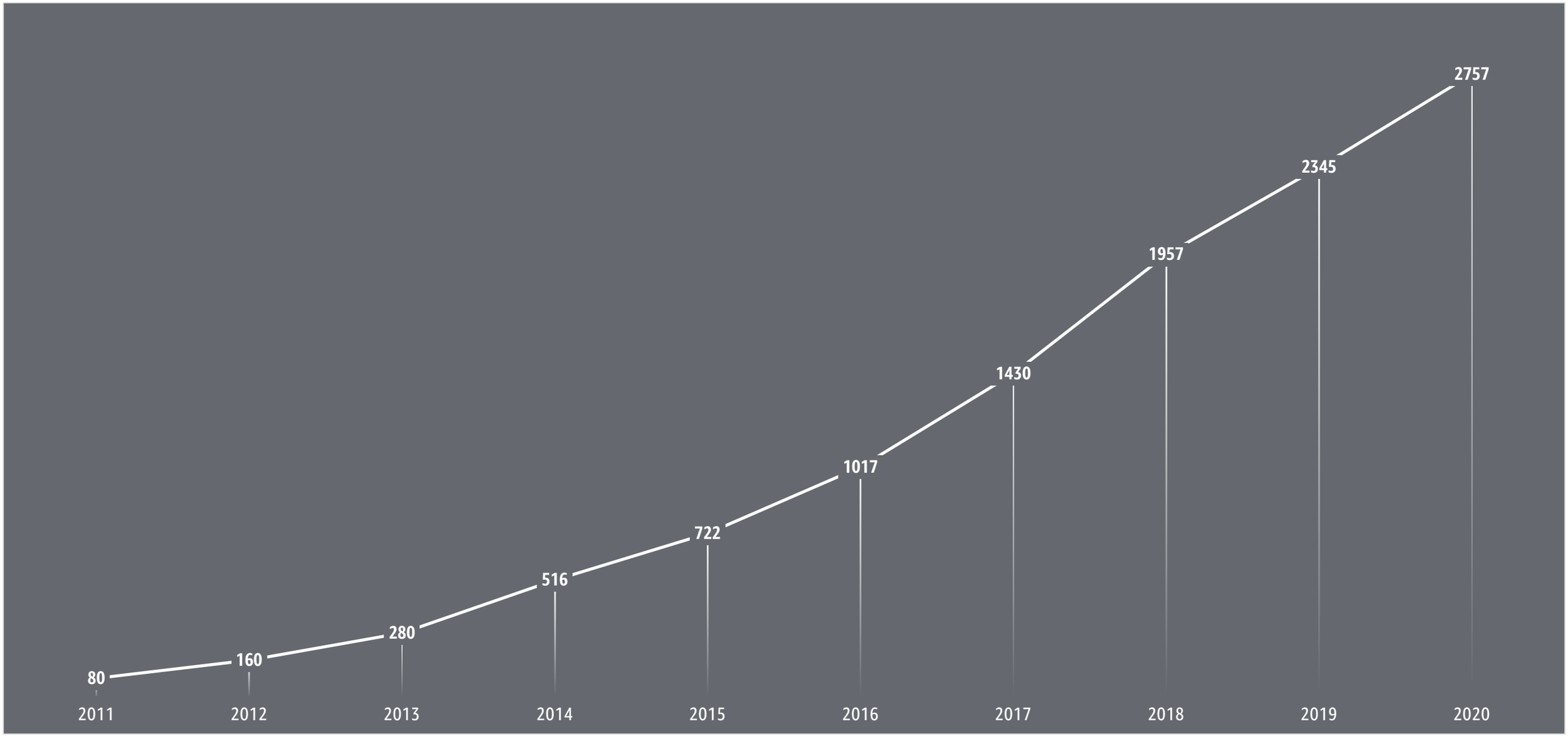
Highly Available

Highly Accredited

aws professional services


I WAS A
SOLID
STATE
DRIVE

AWS Pace of Innovation



aws professional services

Who is AWS Security?

AWS Employees

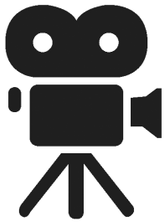
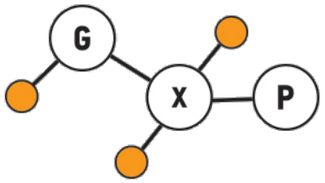
AWS Security (CISO Staff)	AWS Security Assurance	AWS Security Solution Architects
Security Operations Center (SOC)	AWS Abuse Team	AWS Professional Services SRC Practice
AWS Service Team Security SDEs	AWS Lookout Team	Support Security SMEs & TAMs

aws professional services

AWS Compliance Programs

Global

United States


aws professional services

AWS Compliance Programs

Asia Pacific

FIEC

irap®

정보보호관리체계인증 ISMS Information Security Management System

iDA SINGAPORE

Europe

C5

CYBER ESSENTIALS PLUS

GOV.UK

TÜV AUSTRIA

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

TISAX ENX ASSOCIATION

All customers benefit from the same security

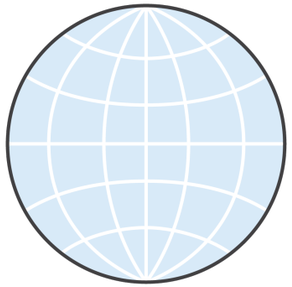
60+ Assurance programs, including

- **SOC 1** (SSAE 16 & ISAE 3402) Type II
- **SOC 2 Type II** and public SOC 3 report
- **ISO 27001**
- **ISO 9001**
- **PCI DSS Level 1** - Service Provider
- **ISO 27017** (security of the cloud)
- **ISO 27018** (personal data)
- **BSI C5** (Germany) – ESCloud (EU)
- **CISPE** - GDPR

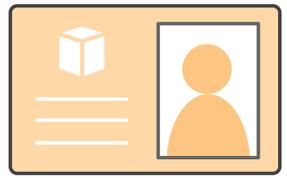
aws professional services

Find Compliance Reports on AWS Artifact

Reports On-Demand



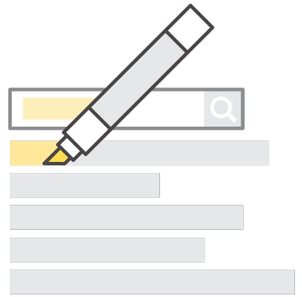
Globally Available



Easy Identification

Quick Assessments

Continuous Monitoring



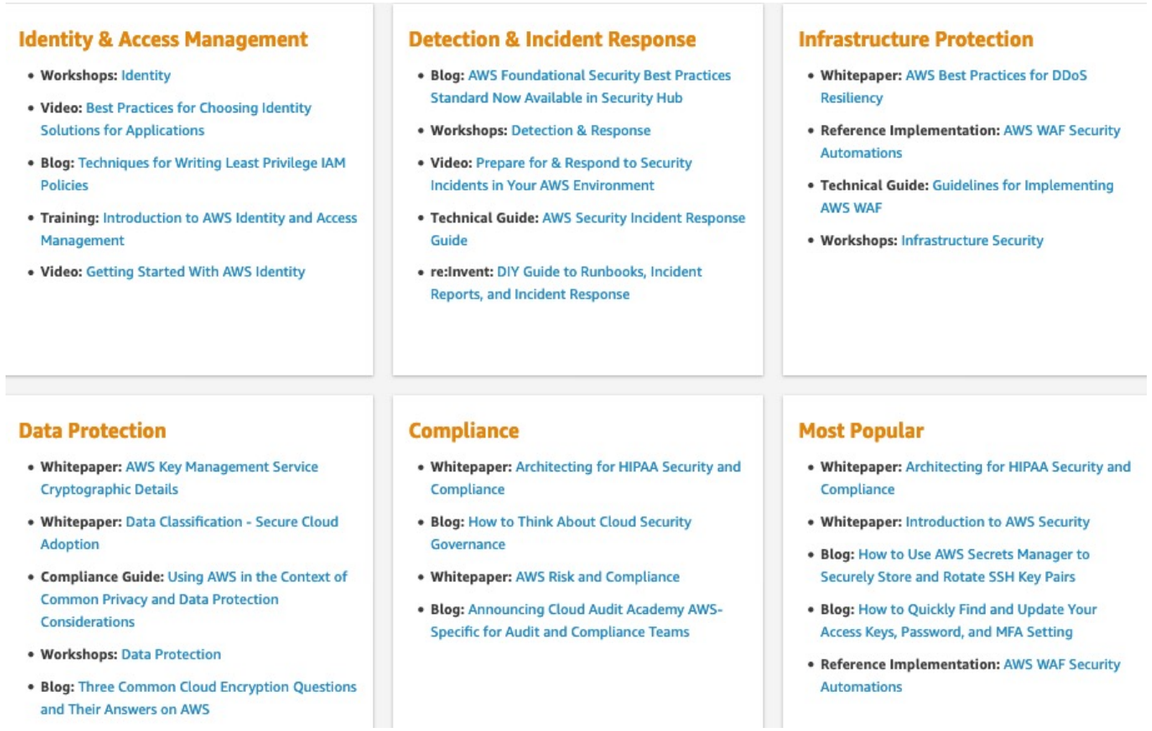
Enhanced Transparency

https://aws.amazon.com/artifact/

What does this mean?

- You benefit from an environment built for the most security sensitive organizations
- AWS manages 1,800+ security controls **so you don’t have to**
- You get to define the right security controls for your workload sensitivity
- You always have full ownership and control of your data

Security “of” AWS



Identity & Access Management

- **Workshops:** Identity
- **Video:** Best Practices for Choosing Identity Solutions for Applications
- **Blog:** Techniques for Writing Least Privilege IAM Policies
- **Training:** Introduction to AWS Identity and Access Management
- **Video:** Getting Started With AWS Identity

Detection & Incident Response

- **Blog:** AWS Foundational Security Best Practices Standard Now Available in Security Hub
- **Workshops:** Detection & Response
- **Video:** Prepare for & Respond to Security Incidents in Your AWS Environment
- **Technical Guide:** AWS Security Incident Response Guide
- **re:Invent:** DIY Guide to Runbooks, Incident Reports, and Incident Response

Infrastructure Protection

- **Whitepaper:** AWS Best Practices for DDoS Resiliency
- **Reference Implementation:** AWS WAF Security Automations
- **Technical Guide:** Guidelines for Implementing AWS WAF
- **Workshops:** Infrastructure Security

Data Protection

- **Whitepaper:** AWS Key Management Service Cryptographic Details
- **Whitepaper:** Data Classification - Secure Cloud Adoption
- **Compliance Guide:** Using AWS in the Context of Common Privacy and Data Protection Considerations
- **Workshops:** Data Protection
- **Blog:** Three Common Cloud Encryption Questions and Their Answers on AWS

Compliance

- **Whitepaper:** Architecting for HIPAA Security and Compliance
- **Blog:** How to Think About Cloud Security Governance
- **Whitepaper:** AWS Risk and Compliance
- **Blog:** Announcing Cloud Audit Academy AWS-Specific for Audit and Compliance Teams

Most Popular

- **Whitepaper:** Architecting for HIPAA Security and Compliance
- **Whitepaper:** Introduction to AWS Security
- **Blog:** How to Use AWS Secrets Manager to Securely Store and Rotate SSH Key Pairs
- **Blog:** How to Quickly Find and Update Your Access Keys, Password, and MFA Setting
- **Reference Implementation:** AWS WAF Security Automations

AWS Security Whitepaper
AWS Global Security Infrastructure
Physical and Environmental Security
Business Continuity Management
Network Security
AWS Employee Access
Secure Design Principles
Change Management
AWS Account Security Features
AWS Service-Specific Security

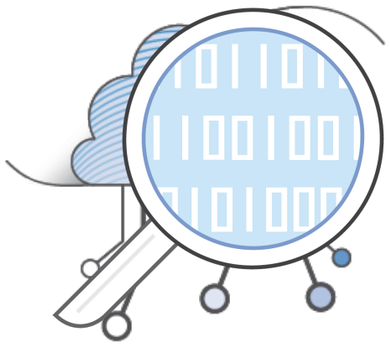
aws professional services

Customer Security Operations on AWS

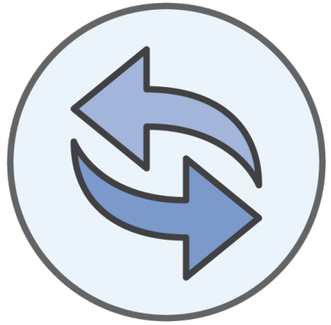
AWS Security Overview

aws professional services

Modernizing Technology Governance

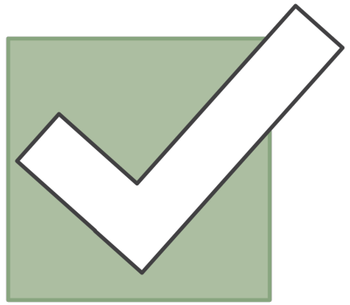


Automate Governance



Automate Deployments

Automate Security Operations



Continuous Compliance & Audit Reporting

Access a deep set of cloud security tools

Networking


Amazon VPC


AWS Direct Connect


Flow logs

Route table


AWS VPN


AWS Transit Gateway


Amazon VPC PrivateLink


AWS WAF


AWS Shield


AWS Firewall Manager

Identity


AWS Identity and Access Management


Amazon Cognito


AWS Directory Service


AWS Organizations


AWS Single Sign-On


AWS Secrets Manager


Active Directory integration


SAML Federation


Temporary security credentials

MFA

Governance, Compliance, and Encryption


AWS Security Hub


AWS Artifact


Amazon Macie


Amazon GuardDuty


AWS Service Catalog


AWS Systems Manager


AWS Trusted Advisor


Amazon Inspector


Amazon CloudWatch


AWS CloudTrail


AWS Control Tower


AWS Config


AWS CloudHSM


AWS Key Management Service


AWS Certificate Manager


Client-side Encryption

New


Amazon Detective


AWS Audit Manager


AWS Network Firewall


AWS Signer

aws professional services

What is the Cloud Adoption Framework?

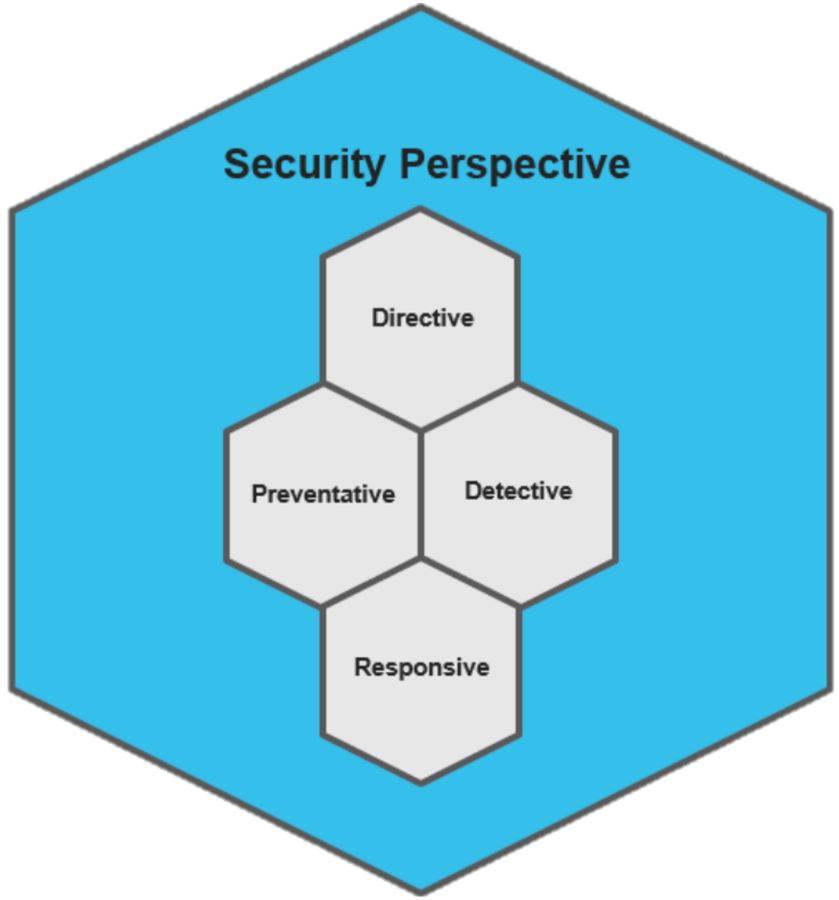
CAF identifies stakeholders that are critical to cloud adoption

It groups related stakeholders into 6 Perspectives.

The Perspectives allow us to understand Cloud Adoption from the view of those stakeholders.

Security Perspective

- **Directive** controls establish the governance, risk, and compliance models the environment will operate within.
- **Preventive** controls protect your workloads and mitigate threats and vulnerabilities.
- **Detective** controls provide full visibility and transparency over the operation of your deployments in AWS.
- **Responsive** controls drive remediation of potential deviations from your security baselines.



Directive Controls

Concepts	Examples
Account Ownership and contact information	Assignment of AWS Accounts to business units
Change and asset management	Assigning customer-specific tags to resources
Least privilege access	Assignment of AWS roles to customer staff

Preventative Controls

Concepts	Examples
Identity and access	Deny `ec2::CreateVpc` to AWS IAM users with “Dev” role
Infrastructure protection	Deny packets from public subnet to sensitive subnet
Data protection	Require MFA delete on sensitive S3 bucket

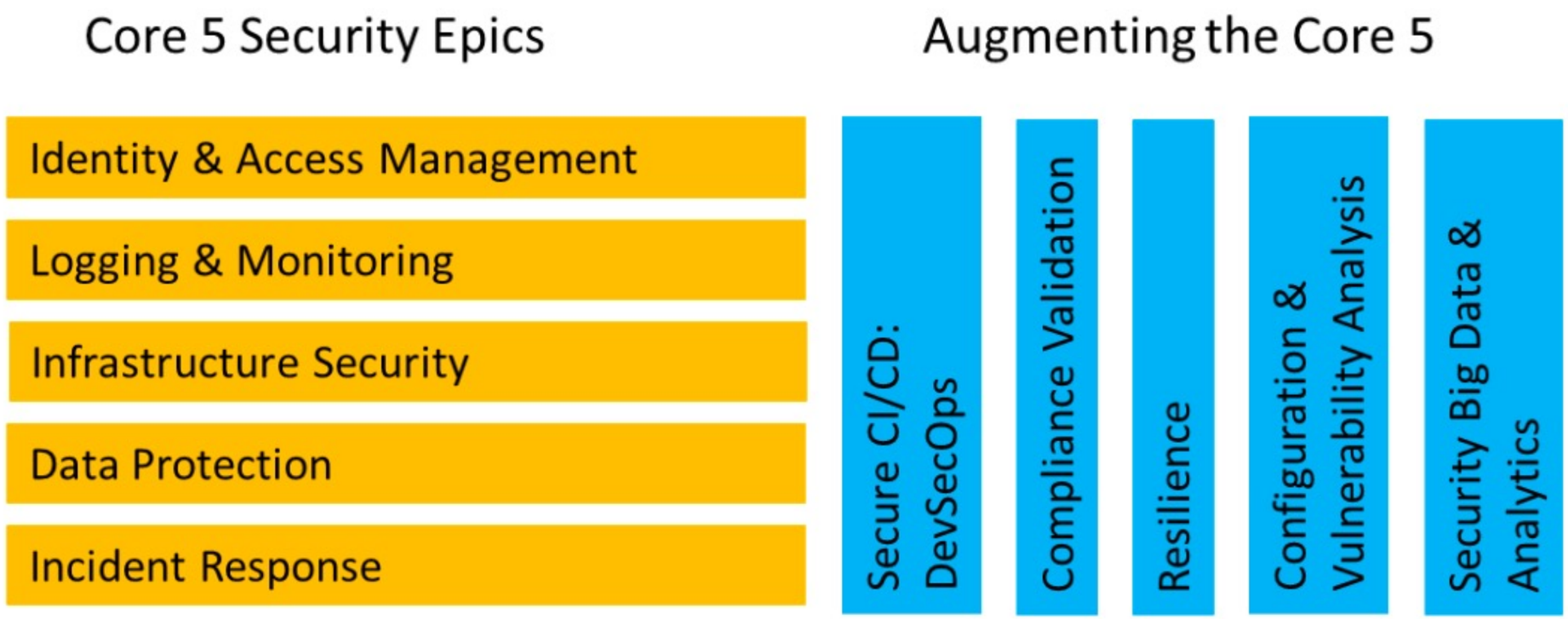
Detective Controls

Concepts	Examples
Logging and monitoring	Log all AWS API activity via CloudTrail
Asset inventory	Alert cloud administrators if any AWS Config rules are non-compliant
Change detection	Alert on denied AWS IAM API requests

Responsive Controls

Concepts	Examples
Vulnerabilities	Initiate operating system security patching
Privilege escalation	Revert dangerous changes in IAM
DDoS attack	Blocklist source IP address(es)

Security Epics



AWS Professional Services Security Journey

Align

Launch

Scale

Optimize

Goals

AWS Jam

Security on AWS Workshop

SRC Blueprint

Innovation

Identity & Access Mgt

Logging & Monitoring

Infrastructure Security

Data Protection

Incident Response

Migration

Security Incident Response Simulation

Security Assessment

Business Outcomes

Enable your organization to understand Cloud Security

Identify tactical plans for quick wins
Define a target state design and kick off a program to get there

5 Core Security Epics Accelerator Engagements

Deliver solutions based on a specific scope & objective aligned with security / product teams

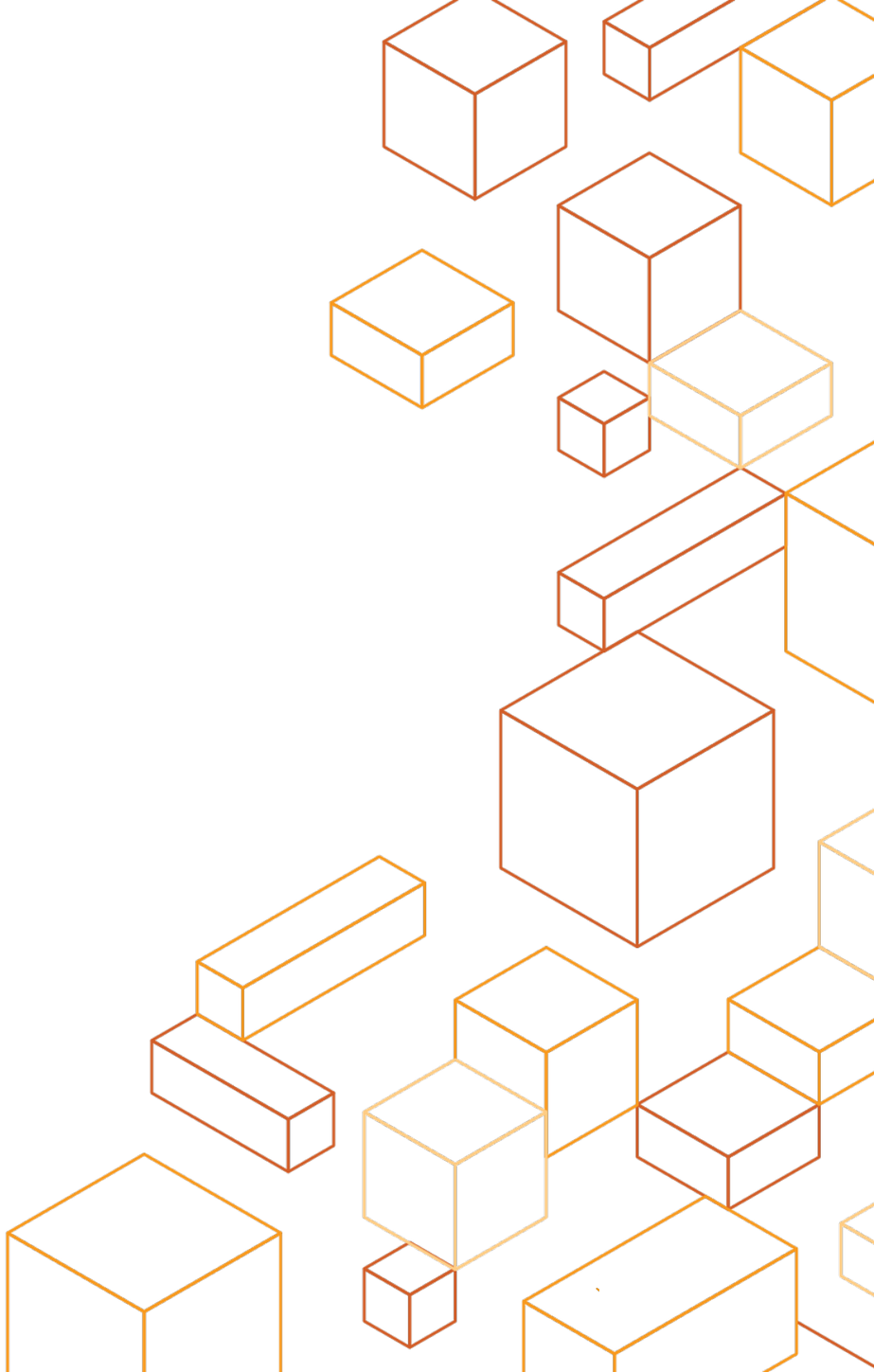
Operationalize and automate to optimize coverage and efficiency for each security epic

Check the overall cloud security maturity of the organization
Act on recommendations to improve security posture

aws professional services

aws professional services

Questions?



Develop a Security Strategy

Appendix A

aws professional services

Appendix A – Develop a Security Strategy

Review your current security strategy to determine if portions of the strategy would benefit from change as part of a cloud adoption initiative.

Map your AWS cloud adoption strategy against the level of risk your business is willing to accept, your approach to meeting regulatory and compliance objectives, as well as your definitions for what needs to be protected and how it will be protected.

Appendix A – Develop a Security Strategy

Example Security Strategy

Infrastructure as code

- Skill up security team in code and automation; move to DevSecOps

Design guardrails not gates

- Architecture drives toward good behavior.

Use the cloud to protect the cloud.

- Build, operate, and manage security tools in the cloud.

Stay current; run secure.

- Consume new security features; patch and replace frequently.

Reduce reliance on persistent access.

- Establish role catalog; automate KMI via secrets service.

Appendix A – Develop a Security Strategy

Example Security Strategy

Total visibility

- Aggregate AWS logs and metadata with OS and app logs.

Deep insights

- Implement a security data warehouse with BI and analytics.

Scalable incident response (IR)

- Update IR and Forensics standard operating procedure (SOP) for shared responsibility framework.

Self-Healing

- Automate correction and restoration to known-good state.

Develop a Security Program

Appendix B

aws professional services

Appendix B – Develop a Security Program

Consider using the CAF Security Epics

- The Security Epics consist of groups of user stories (use cases and abuse cases) that you can work on during sprints.
- Each of these epics has multiple iterations addressing increasingly complex requirements and layering in robustness.
- Although we advise the use of agile, the epics can also be treated as general work streams or topics that help in prioritizing and structuring delivery using any other framework.
- Multiple sprints will lead to increased maturity while retaining flexibility to adapt to business pace and demand.

Develop Security Operations

Appendix C

aws professional services

Appendix C – Develop Security Operations

In an environment where infrastructure is code, security must also be treated as code.

The Security Operations component provides a means to communicate and operationalize the fundamental tenets of security as code:

- Use the cloud to protect the cloud.
- Security infrastructure should be cloud-aware.
- Expose security features as services using the API.
- Automate everything, so that your security and compliance can scale.

Security Whitepapers

Appendix D

Appendix D – Security Whitepapers

AWS Security Whitepaper

- https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf

AWS Risk & Compliance

- http://d0.awsstatic.com/whitepapers/compliance/AWS_Risk_and_Compliance_Whitepaper.pdf

AWS Security Best Practices

- https://aws.amazon.com/architecture/security-identity-compliance/

Overview AWS Lambda Security

- https://docs.aws.amazon.com/whitepapers/latest/security-overview-aws-lambda/security-overview-aws-lambda.html