



AWS Security Overview

AWS Security Workshop

Agenda

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

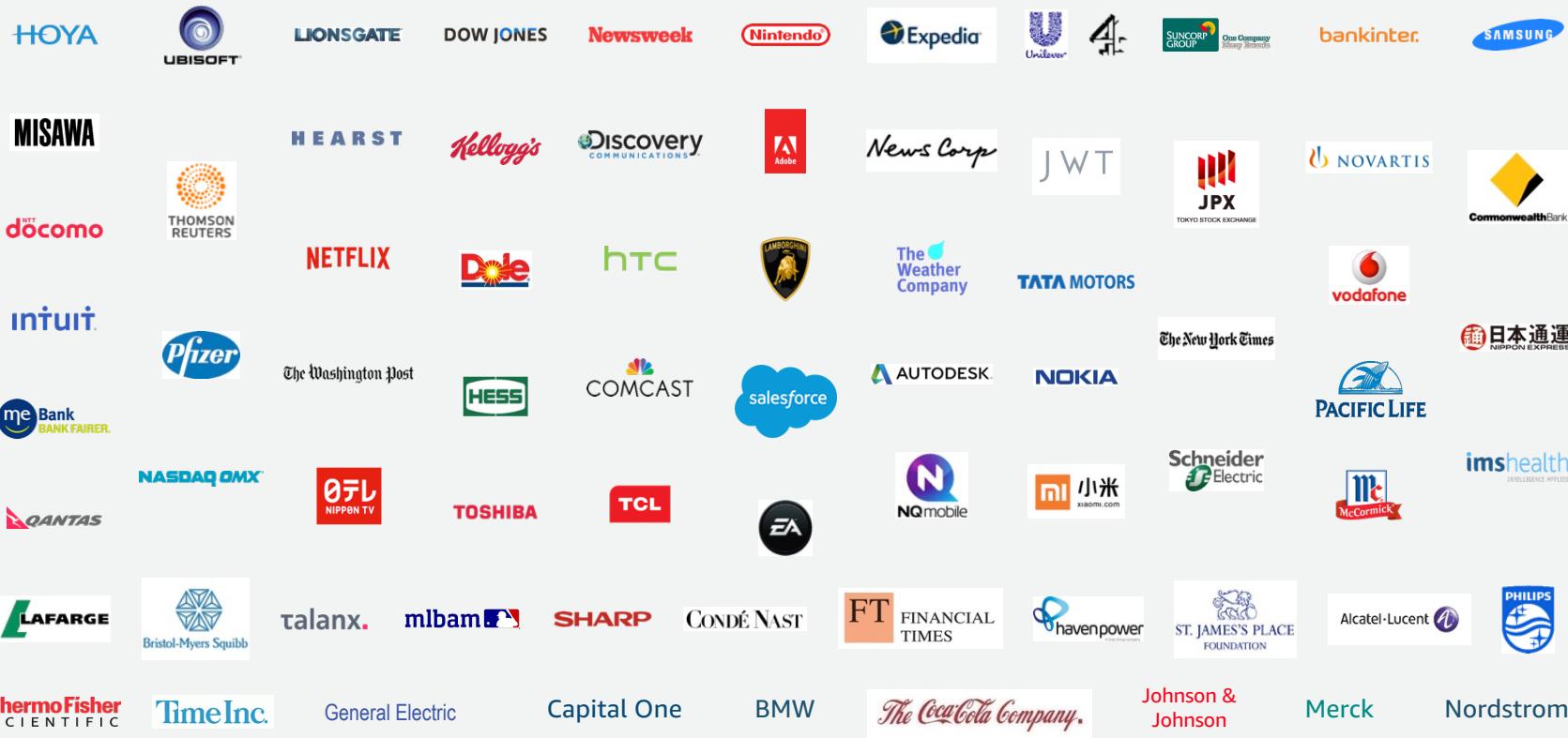
Goals

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

AWS Global Infrastructure



Global Portfolio of Customers in 190 Countries



AWS Global Infrastructure

21 Regions – 66 Availability Zones – 176 Edge Locations



Regions
Coming Soon

Announced Regions

Jakarta, Cape Town, Milan

Amazon Confidential
© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

Region & Number of Availability Zones

US East

N. Virginia (6), Ohio (3)

China

Beijing (2), Ningxia (3)

US West

N. California (3), Oregon (4)

Europe

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

Asia Pacific

Mumbai (2), Seoul (2), Singapore (3), Sydney (3), Tokyo (4), Hong Kong (3), Osaka-Local (1)

South America

São Paulo (3)

AWS GovCloud (US)

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

Canada

Central (2)

AWS Security Workshop v5.1
AWS Security Overview

aws professional services

North America

US East (N. Virginia) Region

EC2 Availability Zones: 6

US West (Oregon) Region

EC2 Availability Zones: 4

AWS GovCloud (US-West) Region

EC2 Availability Zones: 3

Canada (Central) Region

EC2 Availability Zones: 2

US East (Ohio) Region

EC2 Availability Zones: 3

US West (N. California) Region

EC2 Availability Zones: 3*

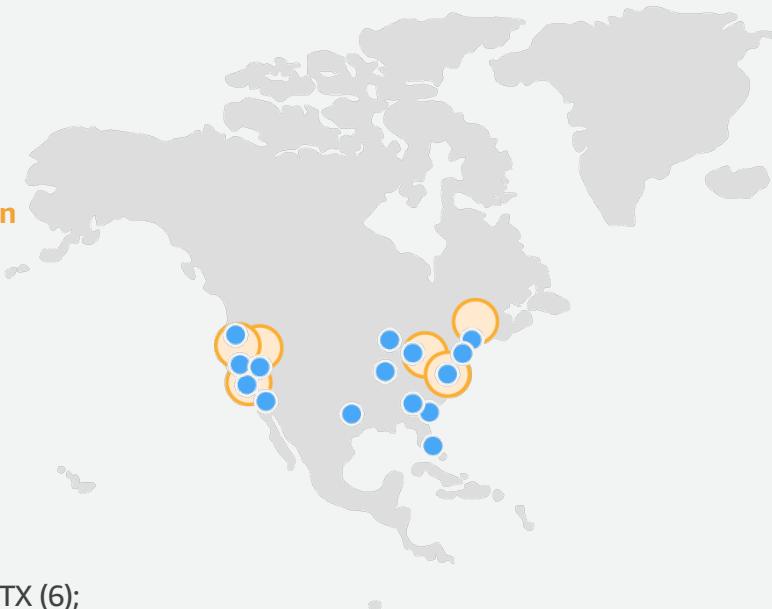
AWS GovCloud (US-East) Region

EC2 Availability Zones: 3

*New customers can access two EC2 Availability Zones in N. California

AWS Edge Locations

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



South America

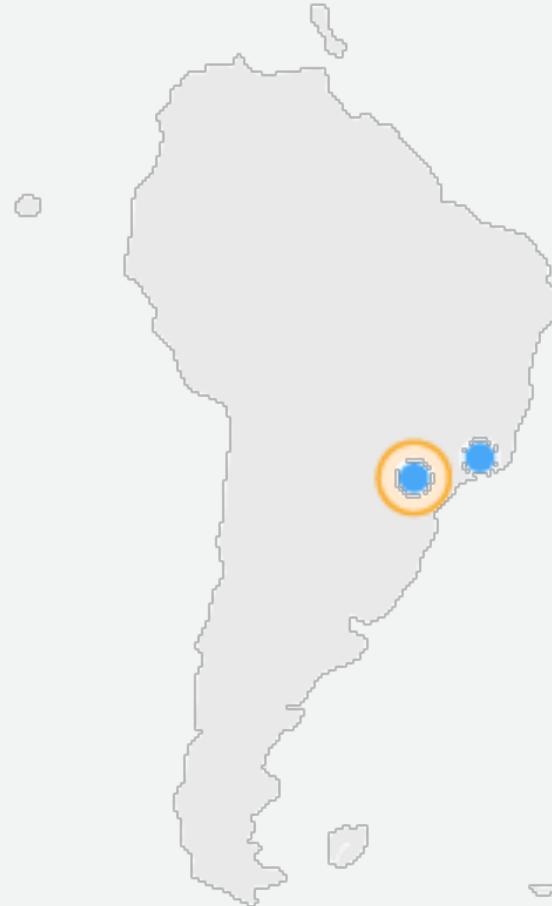
São Paulo Region

EC2 Availability Zones: 3*

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

AWS Edge Locations

Rio de Janeiro, Brazil (3), São Paulo, Brazil (2)



Europe / Middle East / Africa

EU (Ireland) Region

EC2 Availability Zones: 3

EU (Frankfurt) Region

EC2 Availability Zones: 3

EU (London) Region

EC2 Availability Zones: 3

EU (Paris) Region

EC2 Availability Zones: 3

EU (Stockholm) Region

EC2 Availability Zones: 3

AWS Edge Locations

Amsterdam, The Netherlands (2); Berlin, Germany (2); Cape Town, South Africa; Copenhagen, Denmark; Dubai, United Arab Emirates; Dublin, Ireland; Frankfurt, Germany (8); Fujairah, United Arab Emirates; Helsinki, Finland; Johannesburg, South Africa; London, England (9); Madrid, Spain (2); Manchester, England; Marseille, France; Milan, Italy; Munich, Germany (2); Oslo, Norway; Palermo, Italy; Paris, France (5); Prague, Czech Republic; Stockholm, Sweden (3); Vienna, Austria; Warsaw, Poland; Zurich, Switzerland



Asia Pacific

Asia Pacific (Singapore) Region

EC2 Availability Zones: 3

Asia Pacific (Tokyo) Region

EC2 Availability Zones: 4*

Asia Pacific (Osaka) Local Region

EC2 Availability Zones: 1

Asia Pacific (Sydney) Region

EC2 Availability Zones: 3

Asia Pacific (Hong Kong) Region

EC2 Availability Zones: 3

*New customers can access two EC2 Availability Zones in Tokyo.

AWS Edge Locations

Bangalore, India; Chennai, India (2); Hong Kong SAR, China (3); Hyderabad, India (2); Kuala Lumpur, Malaysia; Manila, The Philippines; Melbourne, Australia; Mumbai, India (2); New Delhi, India (3); Osaka, Japan; Perth, Australia; Seoul, Korea (4); Singapore (3); Sydney, Australia; Taipei, Taiwan (3); Tokyo, Japan (11)

Asia Pacific (Seoul) Region

EC2 Availability Zones: 3

Asia Pacific (Mumbai) Region

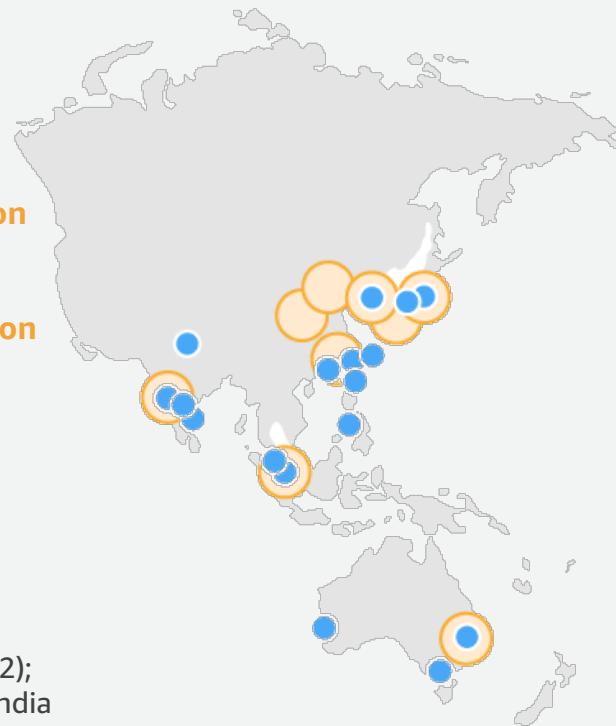
EC2 Availability Zones: 3

Mainland China (Beijing) Region

EC2 Availability Zones: 2

Mainland China (Ningxia) Region

EC2 Availability Zones: 3



AWS Shared Responsibility

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

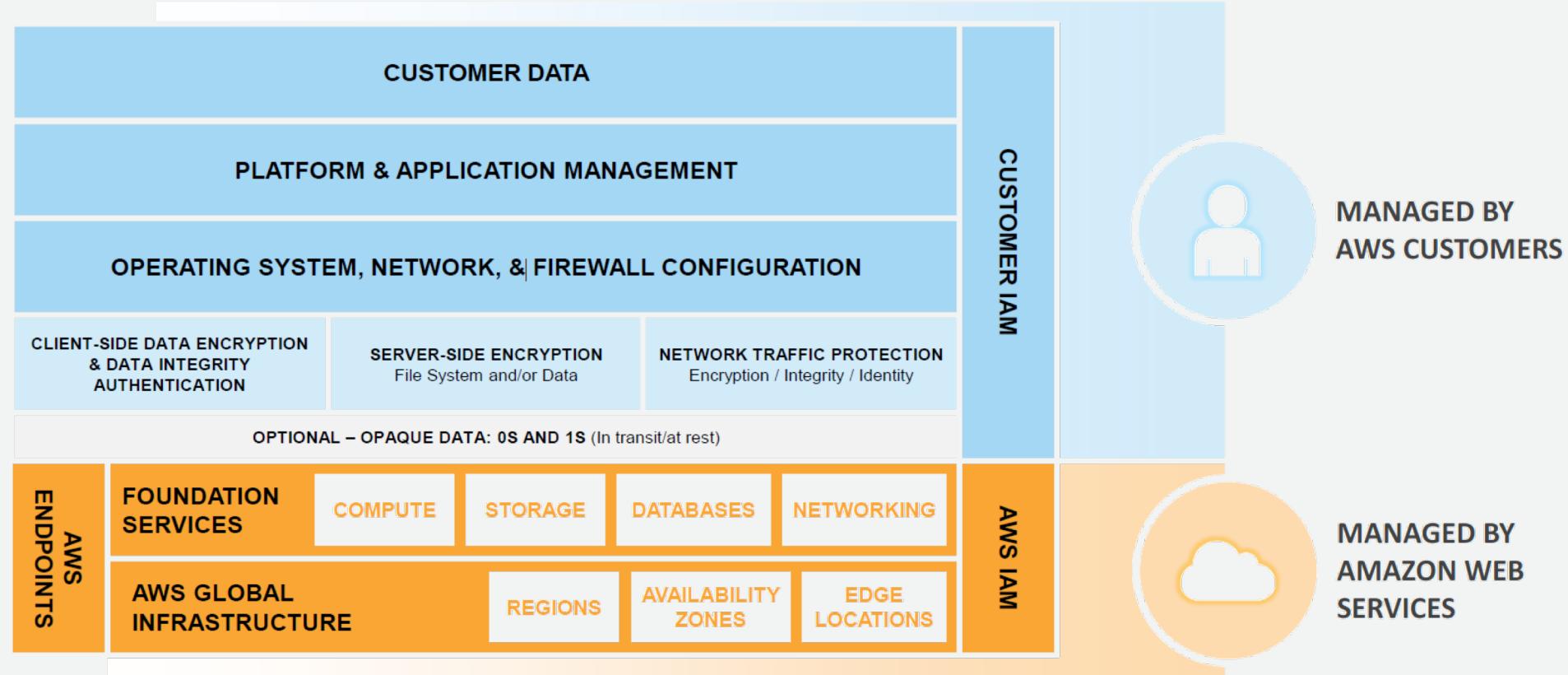


SECURITY IN
THE CLOUD

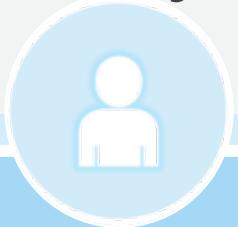


SECURITY OF
THE CLOUD

What is AWS Shared Responsibility?



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**)

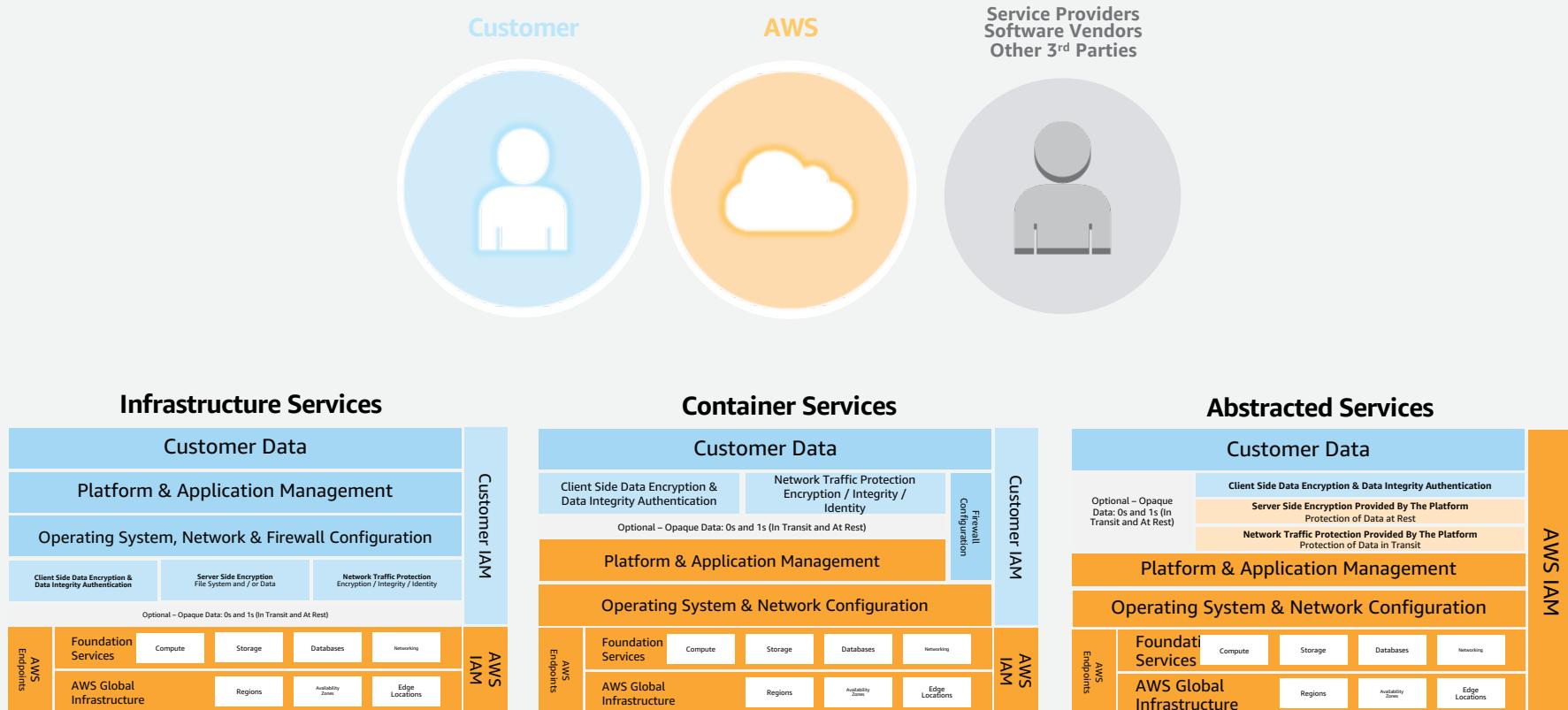
Ongoing audit and assurance programs

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



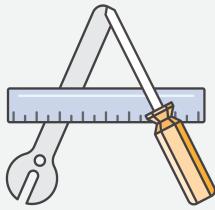
Amazon Confidential

© 2019, Amazon Web Services, Inc. or its Affiliates. All rights reserved.
<https://aws.amazon.com/compliance/shared-responsibility-model/>

AWS Security Workshop v5.1
AWS Security Overview

 professional services

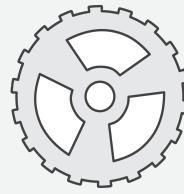
Security is Our Number 1 Priority



Designed for
Security



Constantly
Monitored



Highly
Automated



Highly
Available

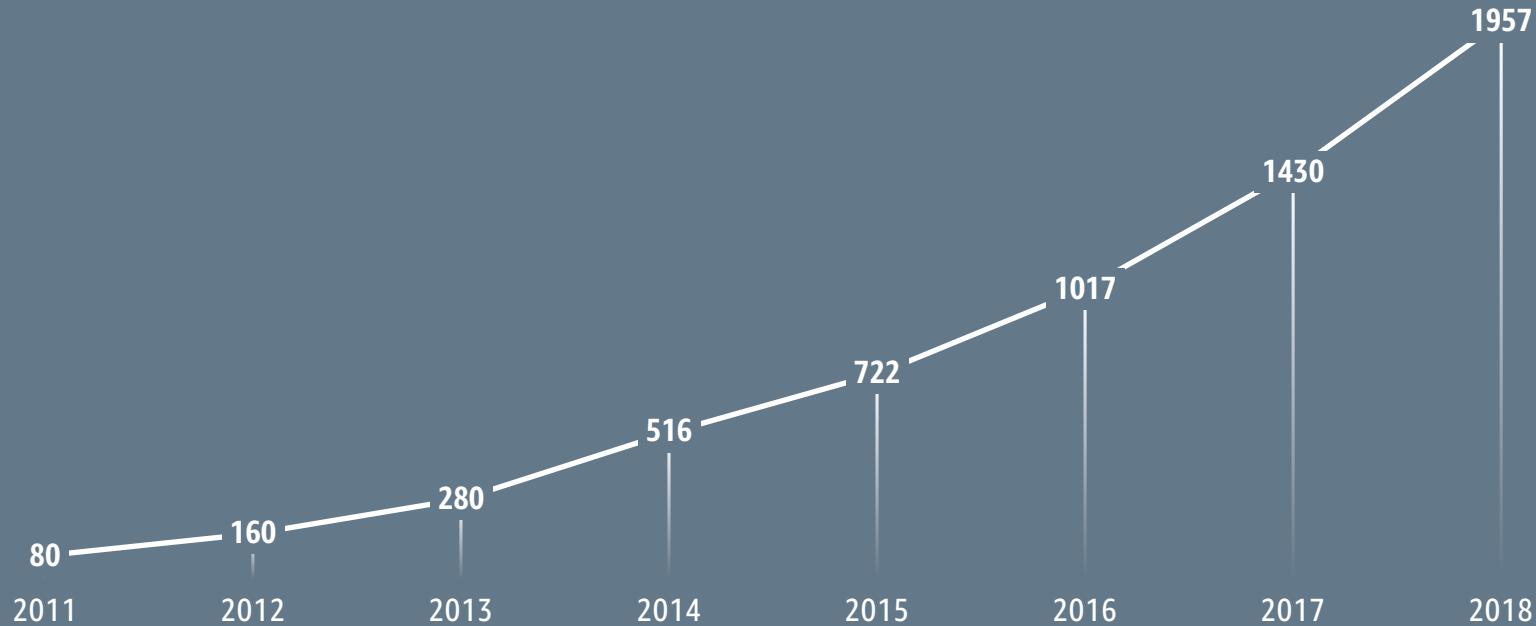


Highly
Accredited



I WAS A
SOLID
STATE
DRIVE

AWS Pace of Innovation



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

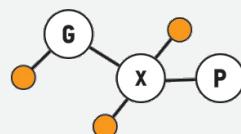
Support Security SMEs & TAMs

AWS Compliance Programs

Global



United States



AWS Compliance Programs

Asia Pacific



Europe



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**



Find Compliance Reports on AWS Artifact



Reports On-Demand



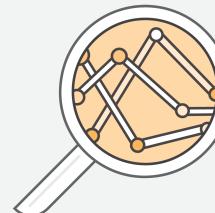
Globally Available



Easy Identification



Quick Assessments



Continuous Monitoring



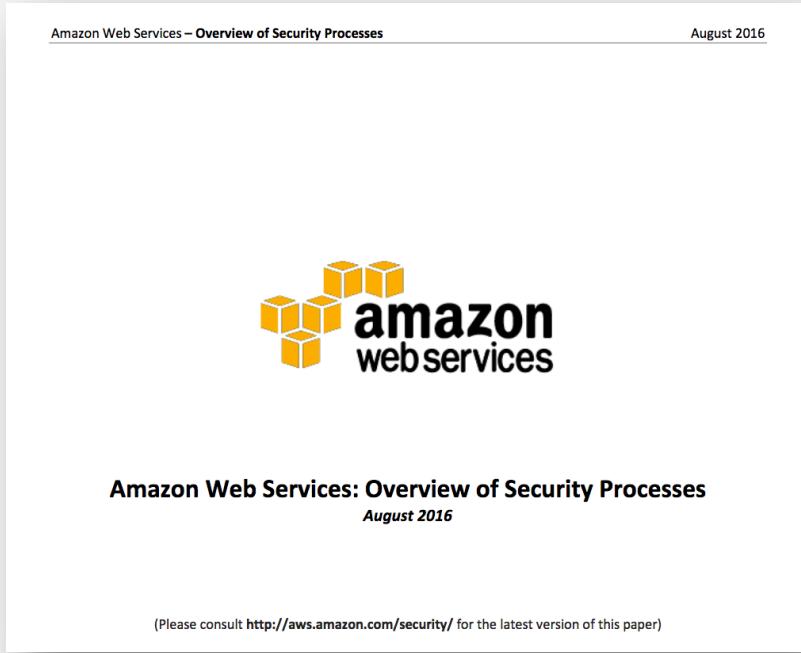
Enhanced Transparency

<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



AWS Security Whitepaper

AWS Global Security Infrastructure

Physical and Environmental Security

Business Continuity Management

Network Security

AWS Employee Access

Secure Design Principles

Change Management

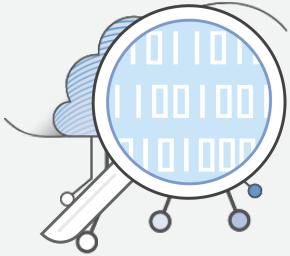
AWS Account Security Features

AWS Service-Specific Security

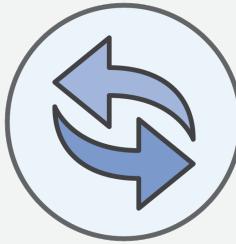
Customer Security Operations in AWS



Modernizing Technology Governance



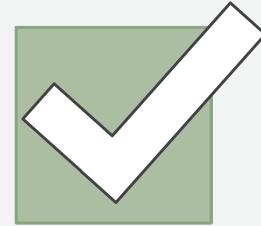
Automate
Governance



Automate
Deployments



Automate Security
Operations



Continuous
Compliance &
Audit Reporting

Access a deep set of cloud security tools

Networking



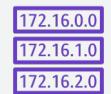
Amazon VPC



AWS Direct Connect



Flow logs



Route table



AWS VPN



AWS Security Hub



AWS Artifact



Amazon Macie



Amazon GuardDuty



AWS Transit Gateway



Amazon VPC PrivateLink



AWS WAF



AWS Shield



AWS Firewall Manager



AWS Service Catalog



AWS Systems Manager



AWS Trusted Advisor



Amazon Inspector



AWS Identity and Access Management



Amazon Cognito



AWS Directory Service



AWS Organizations



AWS Single Sign-On



Amazon CloudWatch



AWS CloudTrail



AWS Control Tower



AWS Config



AWS Secrets Manager



Active Directory integration



SAML Federation



Temporary security credentials



MFA



AWS CloudHSM



AWS Key Management Service



AWS Certificate Manager



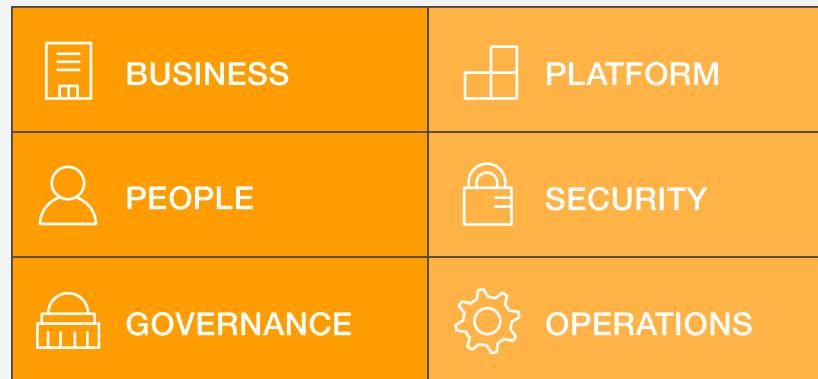
Client-side Encryption

What is the Cloud Adoption Framework?

CAF identifies stakeholders that are critical to cloud adoption

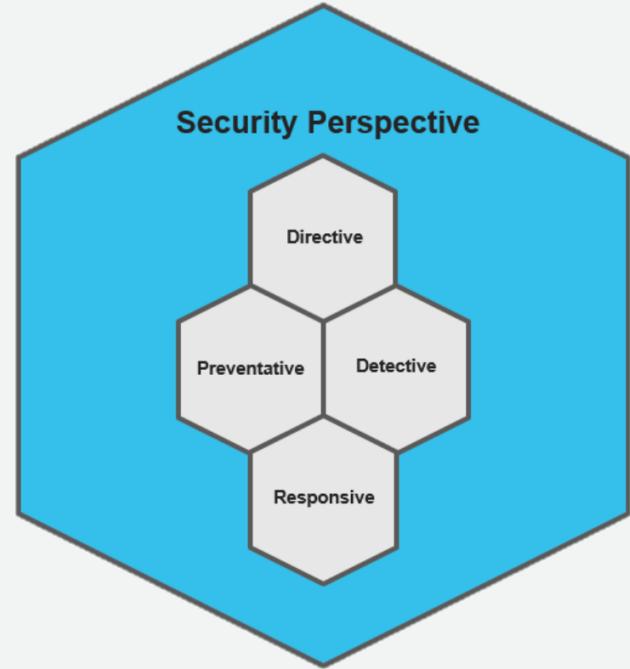
It groups related stakeholders into 6 Perspectives.

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 <code>ec2::CreateVpc</code> 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	Blacklist source IP address(es)

Security Epics

Core 5 Security Epics

Identity & Access Management

Logging & Monitoring

Infrastructure Security

Data Protection

Incident Response

Augmenting the Core 5

Secure CI/CD:
DevSecOps

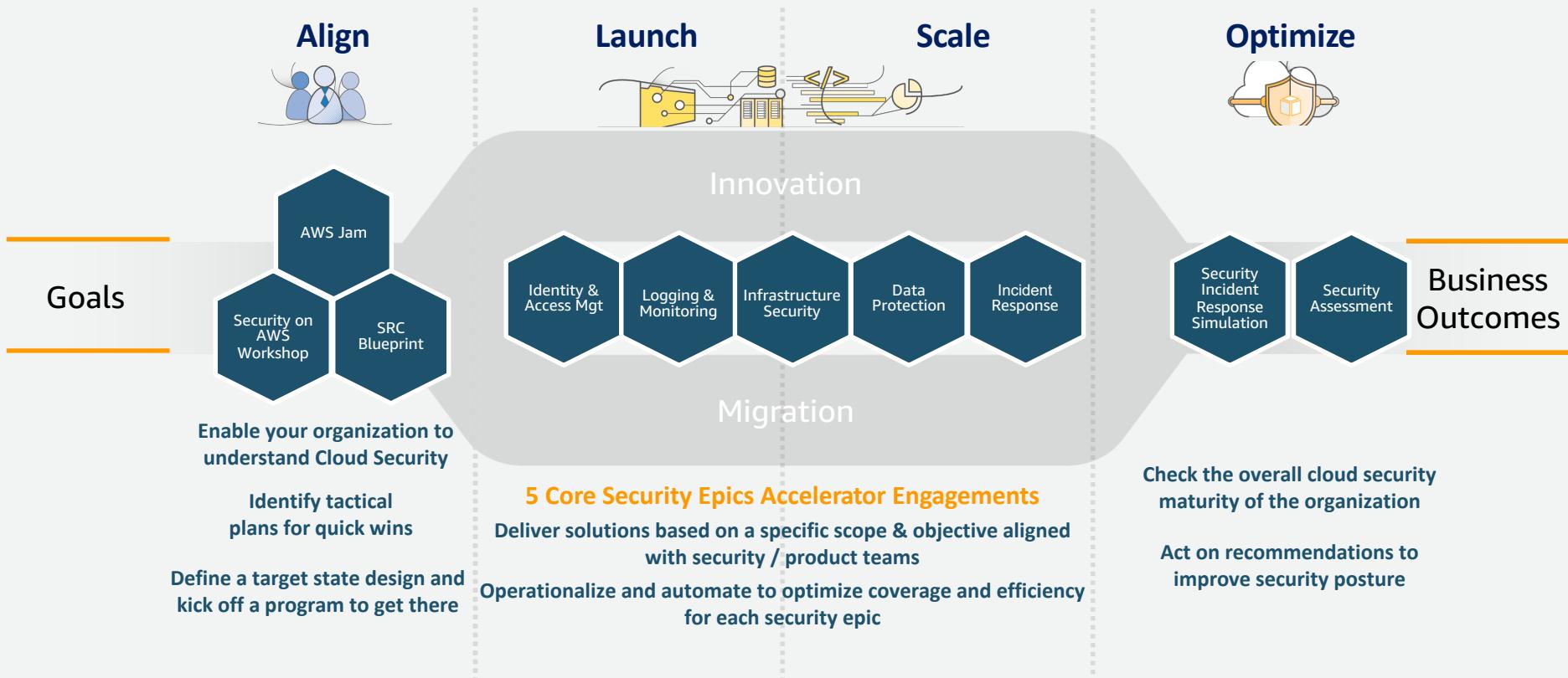
Compliance Validation

Resilience

Configuration &
Vulnerability Analysis

Security Big Data &
Analytics

AWS Professional Services Security Journey



Questions?

Appendix A

Develop a Security Strategy

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.

Appendix B

Develop a Security Program

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.

Appendix C

Develop Robust Security Operations

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.

Appendix D

Security Whitepapers

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://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

Overview AWS Lambda Security

- <https://d1.awsstatic.com/whitepapers/Overview-AWS-Lambda-Security.pdf>