AWS Security Overview

Ionut Dragoi

Sr. Solutions Architect, AWS

Cloud security challenges

Innovation roadblock
The traditional security approach has earned the security team the reputation of "the Department of No."

Expertise shortage
Existing security teams work at capacity and spend their limited time on repetitive and low-value tasks

Evolving threat landscape
Shifting tactics and new technologies create an ever changing risk dynamic.

Data protection & privacy demands
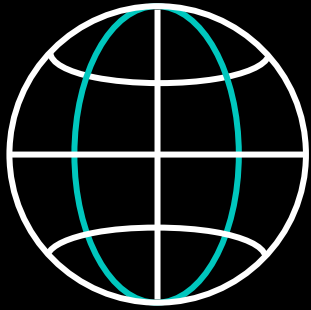To maintain customer trust, organizations must meet industry regulations.
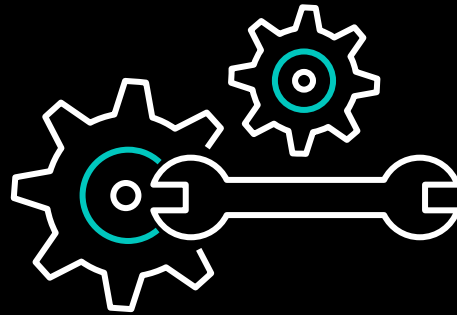
Before…

Move fast **OR** Stay secure

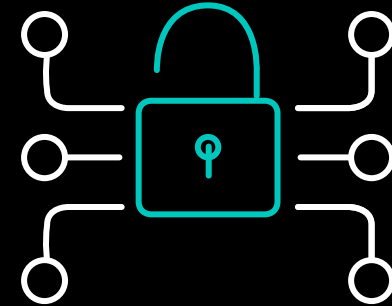Now…

Move fast **AND** Stay secure

4

Proven security to accelerate innovation

The most secure infrastructure

Security automation that drives speed and agility
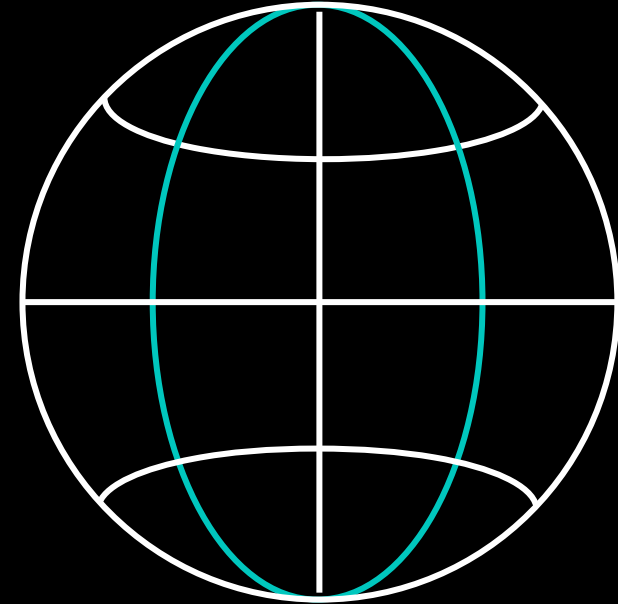
End-to-end security and guidance

The most secure infrastructure

Challenge

- Build on a cloud that provides the security and confidence to accelerate innovation.

AWS approach

- 143 security and compliance certifications

- Secure-by-design

- Most operational experience

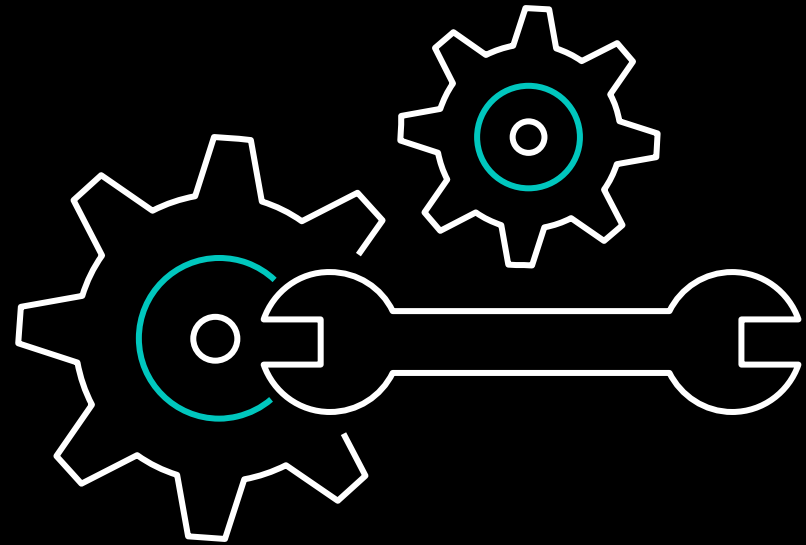# Inherit global security and compliance controls

Security automation that drives speed and agility

Challenge

- Automate security checks to continually enforce controls and mathematically prove the highest levels of security.

AWS approach

- Provable security

- Automatically detect security events

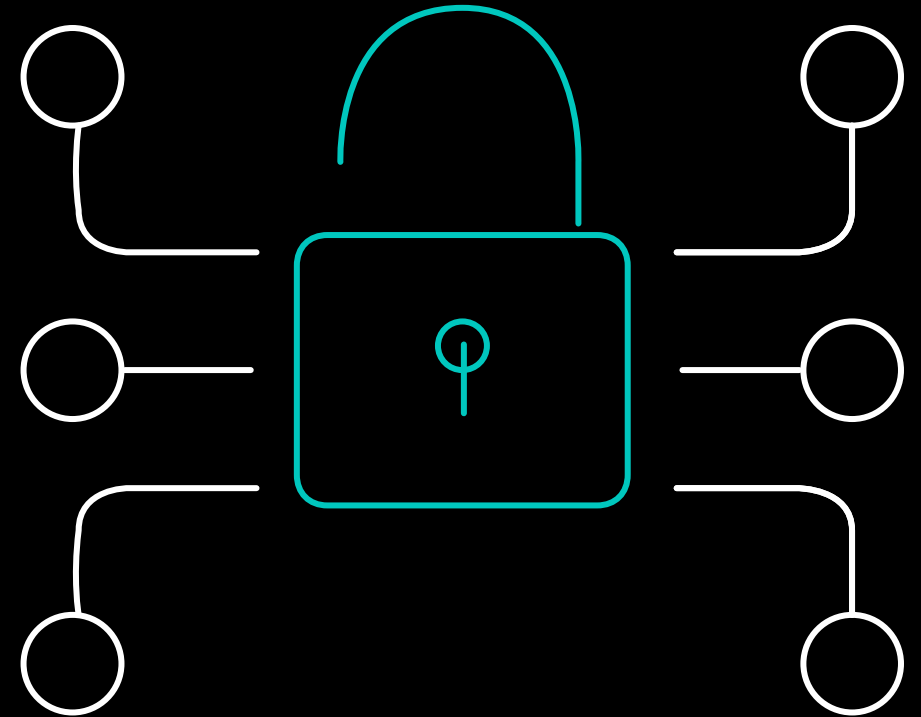- Security automation at scale

End-to-end security and guidance

Challenge

- Implement every step of your organization's optimal security posture.

AWS approach

- 300+ security services and features
- Thousands of security solutions on AWS Marketplace
- Open Source Security

Shared responsibility model

Security IN the Cloud
Customer responsibility is determined by the AWS Cloud services a customer selects.

Security OF the Cloud
AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Customers

AWS
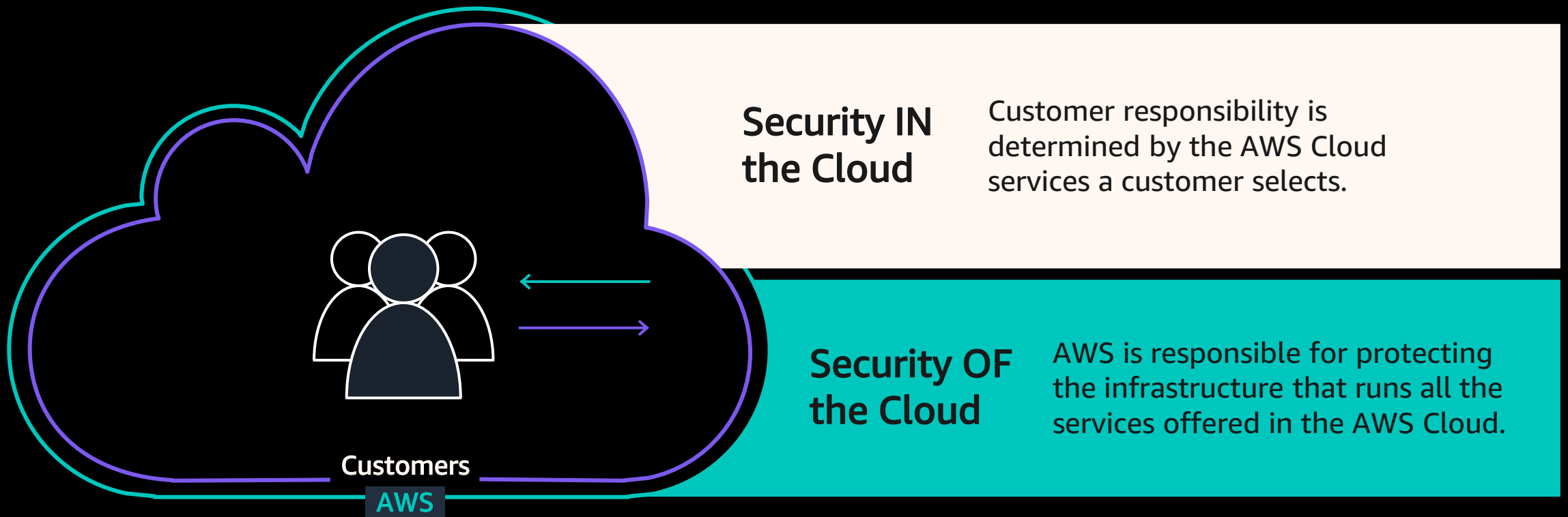
Identity and access management

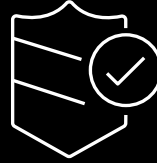AWS Identity and Access Management (IAM)

AWS IAM Identity Center

AWS Organizations

AWS Directory Service

Amazon Cognito

AWS Resource Access Manager

Amazon Verified Permissions

Detection and response

AWS Security Hub

Amazon GuardDuty

Amazon Security Lake

Amazon Inspector

Amazon Macie

Amazon Detective

Amazon CloudWatch

AWS Config

AWS CloudTrail

Network and app protection

AWS Firewall Manager

AWS Network Firewall

AWS Shield

AWS WAF

Amazon VPC

AWS PrivateLink

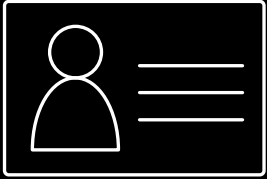AWS Systems Manager

AWS Verified Access

Data protection

Amazon Macie

AWS Key Management Service (KMS)

AWS CloudHSM

AWS Certificate Manager

AWS Private CA

AWS Secrets Manager

AWS Payment Cryptography

Server-Side Encryption

Compliance

AWS Artifact

AWS Audit Manager

Identity and access management

Securely manage and govern access for your customers, workforce, and workloads

AWS Identity and Access Management (IAM)
Securely manage access to AWS services and resources

AWS IAM Identity Center
Centrally manage workforce access to multiple AWS accounts and applications

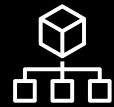## AWS Directory Service
Managed Microsoft Active Directory in AWS

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

AWS Organizations
Policy-based management for multiple AWS accounts

AWS Resource Access Manager
Simple, secure service for sharing AWS resources

Amazon Verified Permissions
Fine-grained permissions and authorization for your applications

Detection and response

Continuously detect and respond to security risks to help protect your workloads, at scale

AWS Security Hub
Automate AWS security checks and centralize security alerts.

Amazon GuardDuty
Protect your AWS accounts with intelligent threat detection.

Amazon Inspector
Automated and continual vulnerability management at scale.

Amazon CloudWatch
Observe and monitor resources and applications on AWS, on premises, and on other clouds.

AWS Config
Assess, audit, and evaluate configurations of your resources.

AWS CloudTrail
Track user activity and API.

Amazon Detective
Analysis and visualization of security data to get to the root cause of potential security issues quickly

Amazon Security Lake
Automatically centralize your security data in a few steps.

Data protection

A suite of services designed to automate and simplify many data protection and security tasks ranging from key management and storage to credential management.

Amazon Macie
Discover and protect your sensitive data at scale.

AWS Key Management Service (AWS KMS)
Create and control keys used to encrypt or digitally sign your data.

AWS CloudHSM
Manage single-tenant hardware security modules (HSMs) on AWS.

AWS Certificate Manager
Provision and manage SSL/TLS certificates with AWS services and connected resources.

AWS Secrets Manager
Centrally manage the lifecycle of secrets.

AWS Payment Cryptography
Simplify your cryptography operations in your cloud-hosted payment applications.

Server-Side Encryption
Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys.

AWS Private CA
Create private certificates to identify resources and protect data.

Network and application protection

Enforce fine-grained security policy at every network control point

AWS Firewall Manager
Centrally configure and manage firewall rules across your accounts.

AWS Network Firewall
Deploy network firewall security across your VPCs.

AWS Shield
Maximize application availability and responsiveness with managed DDoS protection.

AWS WAF
Protects your web applications from common exploits.

Amazon Virtual Private Cloud
Define and launch AWS resources in a logically isolated virtual network.

AWS PrivateLink
Establish connectivity between VPCs and AWS services without exposing data to the internet.

AWS Systems Manager
Gain operational insights into AWS and on-premises resources.

AWS Verified Access
Provide secure access to corporate applications without a VPN.

Compliance

AWS supports 143 security standards and compliance certifications. Governments around the world have accredited AWS to run their highest classified workloads.

AWS Artifact
No-cost, self-service portal for on-demand access to AWS compliance reports

AWS Audit Manager
Continuously audit your AWS usage to simplify how you assess risk and compliance

Thank you!

Ionut Dragoi

ionudra@amazon.com