Security:

A Driving Force Behind Moving to the Cloud

Michael South
Americas Regional Leader,
Public Sector Security & Compliance

Why is security traditionally so hard?

Lack of Visibility

Lack of Resiliency

Defense-in-Depth Challenges

Low degree of Automation

Financial Industry Regulatory Authority

"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

FINRA

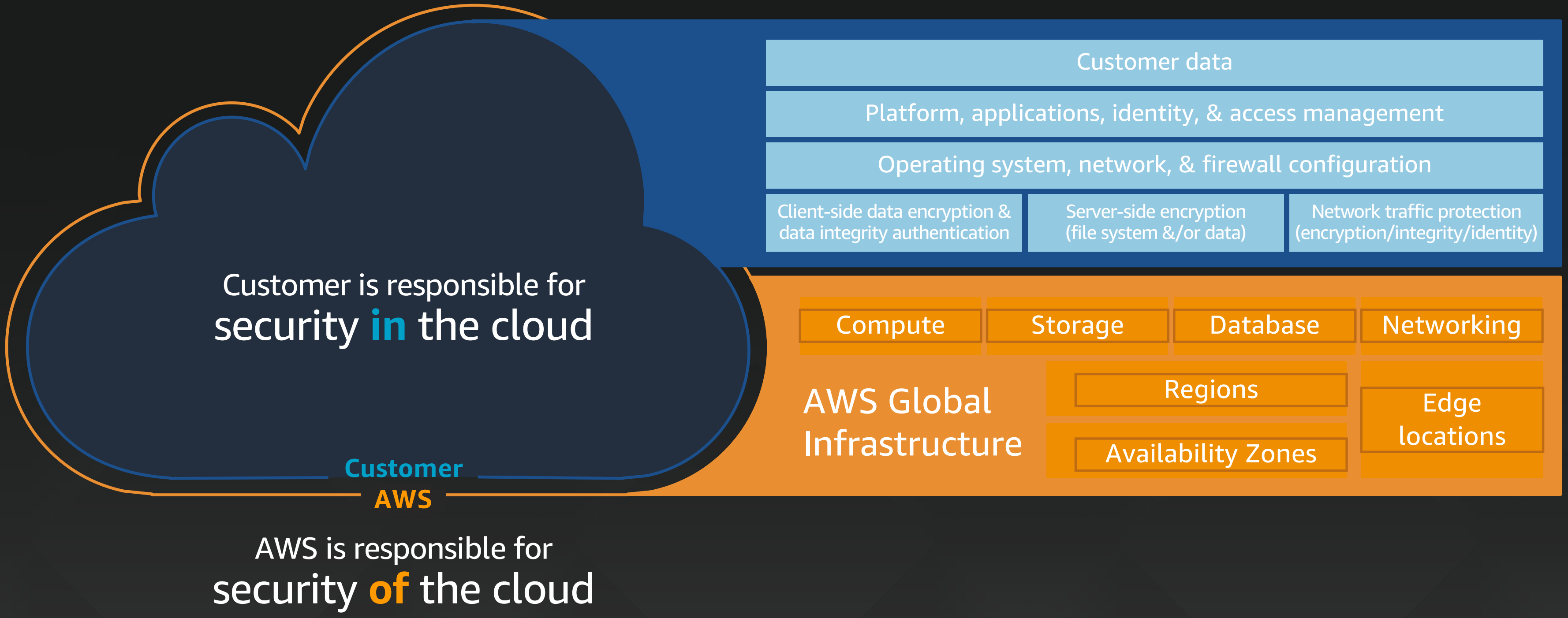
Looks for fraud, abuse, and insider trading over nearly 6 billion shares traded in U.S. equities markets every day

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

aws

Share your security responsibility with AWS



Customer data

Platform, applications, identity, & access management

Operating system, network, & firewall configuration

Client-side data encryption & data integrity authentication	Server-side encryption (file system &/or data)	Network traffic protection (encryption/integrity/identity)

Compute | Storage | Database | Networking

AWS Global Infrastructure

Regions

Availability Zones

Edge locations

Customer is responsible for
security **in** the cloud

Customer

AWS

AWS is responsible for
security **of** the cloud

U.S. Government Compliance

Sensitive Data Protection

Defense Data

Healthcare Data

Criminal Data

Student Data

Tax Data

Weapons Data

Financial Data

Credit Card Data

Frameworks and Processes

FISMA

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1

NIST CSF

FIPS 199 / SP 800-60
Starting Point
Categorize System
Select Controls
Implement Controls
Assess Controls
Authorize System
Monitor Controls
Organization-wide Risk Management SP 800-39
SP 800-53A

NIST RMF

FedRAMP

AWS Artifact

Self-service for AWS compliance reports

Standards

NIST National Institute of Standards and Technology

CNSS

FIPS 140-2

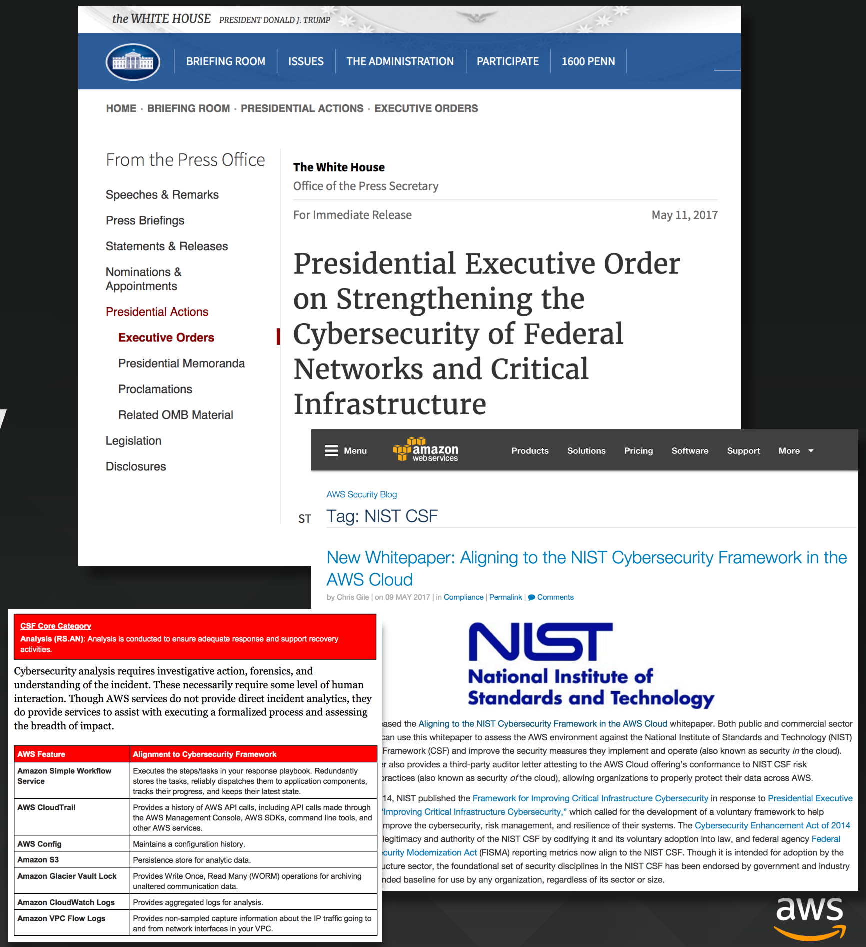
COMMON CRITERIA

Implementing NIST's Cyber Security Framework (CSF)

Executive Order directs all Federal agencies to use NIST's CSF to manage cyber risk

Amazon provides guidance on how AWS services align to CSF

Customers can leverage shared cloud services and FedRAMP P-ATOs and Agency-ATOs



The White House

Office of the Press Secretary

For Immediate Release May 11, 2017

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure

Tag: NIST CSF

New Whitepaper: Aligning to the NIST Cybersecurity Framework in the AWS Cloud

by Chris Gile | on 09 MAY 2017 | in Compliance | Permalink | Comments

ased the Aligning to the NIST Cybersecurity Framework in the AWS Cloud whitepaper. Both public and commercial sector can use this whitepaper to assess the AWS environment against the National Institute of Standards and Technology (NIST) Framework (CSF) and improve the security measures they implement and operate (also known as security *in* the cloud). r also provides a third-party auditor letter attesting to the AWS Cloud offering's conformance to NIST CSF risk ractices (also known as security *of* the cloud), allowing organizations to properly protect their data across AWS.

14, NIST published the Framework for Improving Critical Infrastructure Cybersecurity in response to Presidential Executive 'Improving Critical Infrastructure Cybersecurity," which called for the development of a voluntary framework to help mprove the cybersecurity, risk management, and resilience of their systems. The Cybersecurity Enhancement Act of 2014 legitimacy and authority of the NIST CSF by codifying it and its voluntary adoption into law, and federal agency Federal curity Modernization Act (FISMA) reporting metrics now align to the NIST CSF. Though it is intended for adoption by the ucture sector, the foundational set of security disciplines in the NIST CSF has been endorsed by government and industry nded baseline for use by any organization, regardless of its sector or size.

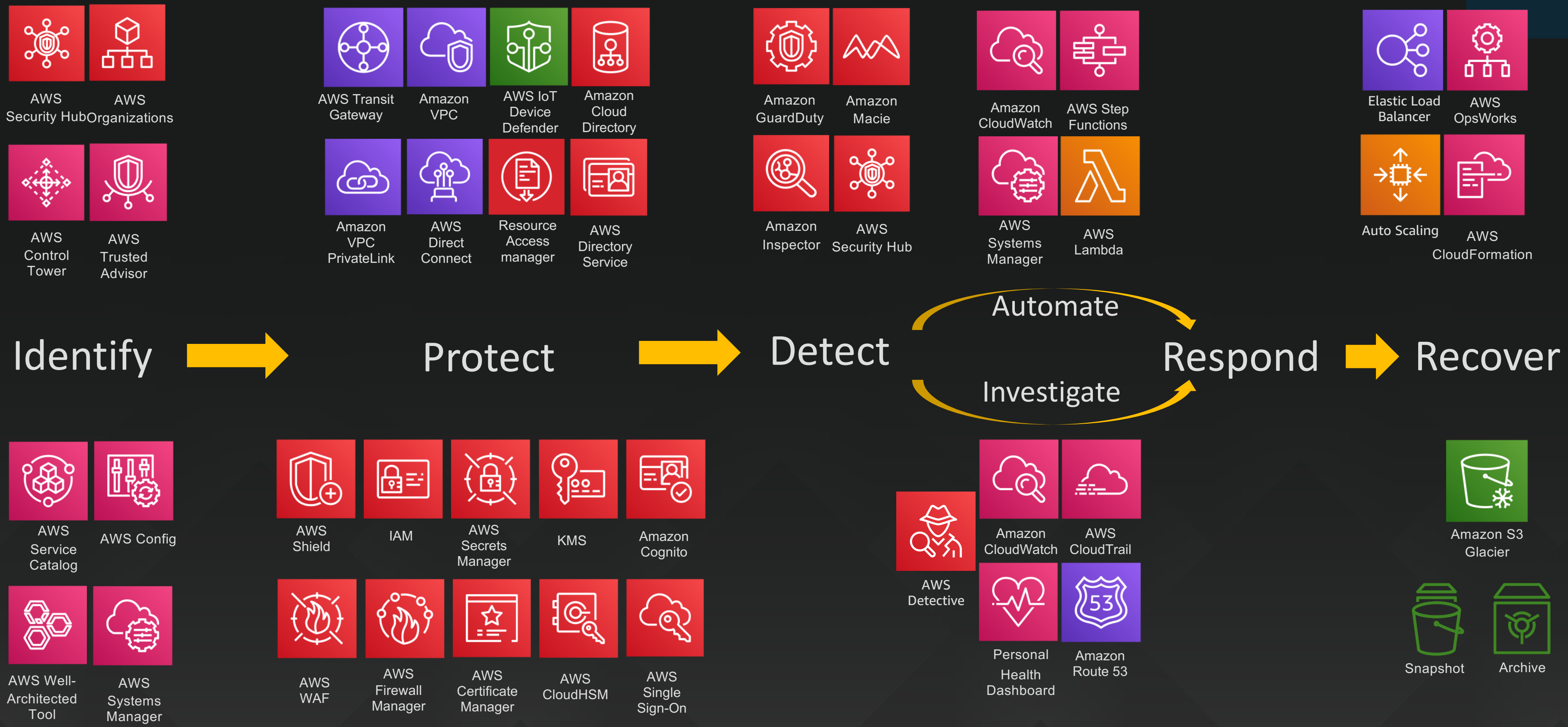
CSF Core Category

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.

Cybersecurity analysis requires investigative action, forensics, and understanding of the incident. These necessarily require some level of human interaction. Though AWS services do not provide direct incident analytics, they do provide services to assist with executing a formalized process and assessing the breadth of impact.

AWS Feature	Alignment to Cybersecurity Framework
Amazon Simple Workflow Service	Executes the steps/tasks in your response playbook. Redundantly stores the tasks, reliably dispatches them to application components, tracks their progress, and keeps their latest state.
AWS CloudTrail	Provides a history of AWS API calls, including API calls made through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
AWS Config	Maintains a configuration history.
Amazon S3	Persistence store for analytic data.
Amazon Glacier Vault Lock	Provides Write Once, Read Many (WORM) operations for archiving unaltered communication data.
Amazon CloudWatch Logs	Provides aggregated logs for analysis.
Amazon VPC Flow Logs	Provides non-sampled capture information about the IP traffic going to and from network interfaces in your VPC.

AWS Foundational and Layered Security Services



Identify

AWS Security Hub

AWS Organizations

AWS Control Tower

AWS Trusted Advisor

AWS Service Catalog

AWS Config

AWS Well-Architected Tool

AWS Systems Manager

Protect

AWS Transit Gateway

Amazon VPC

AWS IoT Device Defender

Amazon Cloud Directory

Amazon VPC PrivateLink

AWS Direct Connect

Resource Access manager

AWS Directory Service

AWS Shield

IAM

AWS Secrets Manager

KMS

Amazon Cognito

AWS WAF

AWS Firewall Manager

AWS Certificate Manager

AWS CloudHSM

AWS Single Sign-On

Detect

Amazon GuardDuty

Amazon Macie

Amazon Inspector

AWS Security Hub

AWS Detective

Automate

Amazon CloudWatch

AWS Step Functions

AWS Systems Manager

AWS Lambda

Investigate

Amazon CloudWatch

AWS CloudTrail

Personal Health Dashboard

Amazon Route 53

Respond

Recover

Elastic Load Balancer

AWS OpsWorks

Auto Scaling

AWS CloudFormation

Amazon S3 Glacier

Snapshot

Archive

AWS Supports 18 of the CIS Top 20 Controls!

✓ 1. Inventory of Authorized and Unauthorized Devices
✓ 2. Inventory of Authorized and Unauthorized Software
✓ 3. Secure Configurations for Hardware and Software
✓ 4. Continuous Vulnerability Assessment and Remediation
✓ 5. Controlled Use of Administrative Privileges

✓ 6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
✓ 8. Malware Defenses
✓ 9. Limitation and Control of Network Ports
✓ 10. Data Recovery Capability
✓ 11. Secure Configurations for Network Devices
✓ 12. Boundary Defense
✓ 13. Data Protection
✓ 14. Controlled Access Based on the Need to Know
15. Wireless Access Control
✓ 16. Account Monitoring and Control
✓ 17. Security Skills Assessment and Appropriate Training to Fill Gaps
✓ 18. Application Software Security
✓ 19. Incident Response and Management
✓ 20. Penetration Tests and Red Team Exercises*

First 5 CIS Controls
Eliminates the vast majority of an organization's vulnerabilities

AKA "Cyber Hygiene"

All 20 CIS Controls
Secure your entire organization against today's most pervasive threats

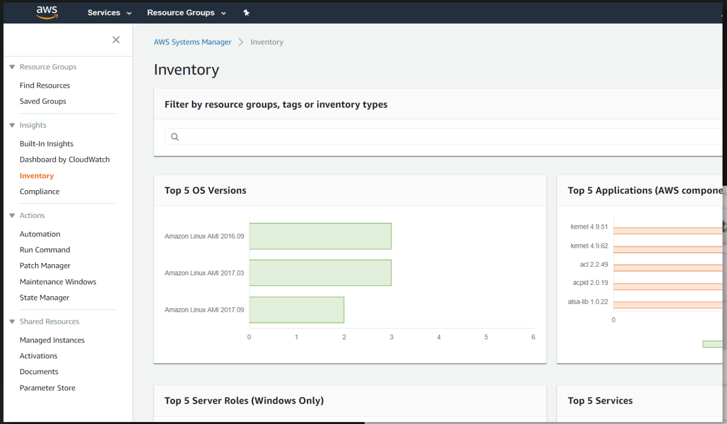
Center for Internet Security

aws

Visibility

Means of obtaining Visibility

Console



AWS Systems Manager > Inventory

Inventory

- Resource Groups
  - Find Resources
  - Saved Groups
- Insights
  - Built-In Insights
  - Dashboard by CloudWatch
  - Inventory
  - Compliance
- Actions
  - Automation
  - Run Command
  - Patch Manager
  - Maintenance Windows
  - State Manager
- Shared Resources
  - Managed Instances
  - Activations
  - Documents
  - Parameter Store

Filter by resource groups, tags or inventory types

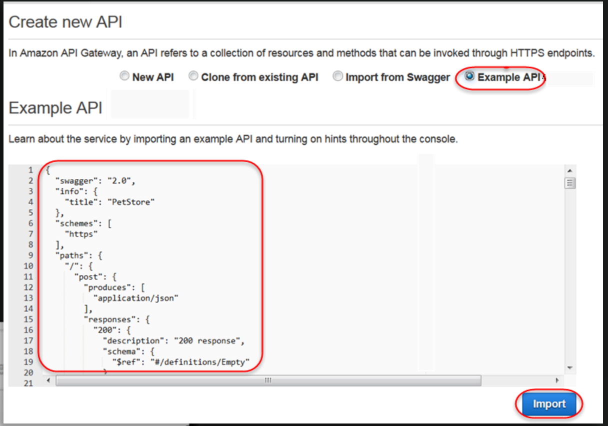
Top 5 OS Versions

Top 5 Applications (AWS compone

Top 5 Server Roles (Windows Only)

Top 5 Services

API Queries



Create new API

In Amazon API Gateway, an API refers to a collection of resources and methods that can be invoked through HTTPS endpoints.

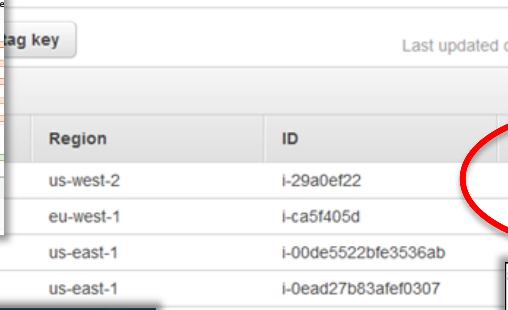
○ New API ○ Clone from existing API ○ Import from Swagger ● Example API

Example API

Learn about the service by importing an example API and turning on hints throughout the console.

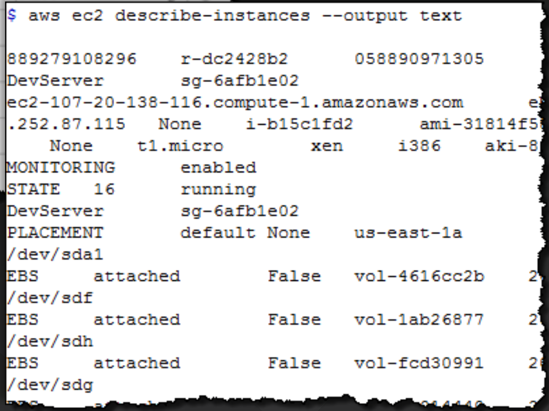
```
{
  "swagger": "2.0",
  "info": {
    "title": "PetStore"
  },
  "schemes": [
    "https"
  ],
  "paths": {
    "/": {
      "post": {
        "produces": [
          "application/json"
        ],
        "responses": {
          "200": {
            "description": "200 response",
            "schema": {
              "$ref": "#/definitions/Empty"
            }
```

Use of resource tags



	Region	ID	ProjectCode
	us-west-2	i-29a0ef22	P100
	eu-west-1	i-ca5f405d	P100
EC2 Instance	us-east-1	i-00de5522bfe3536ab	P200
EC2 Instance	us-east-1	i-0ead27b83afef0307	
		i-0134ced7d56d94d29	
		i-127e6e9c	
		i-647969ea	

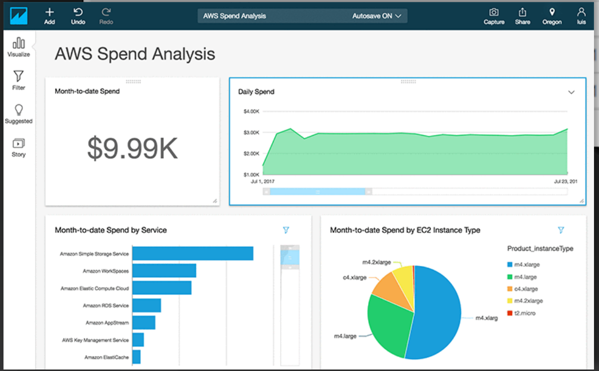
CLI Describe



```
$ aws ec2 describe-instances --output text

889279108296    r-dc2428b2      058890971305
DevServer       sg-6afb1e02
ec2-107-20-138-116.compute-1.amazonaws.com      e
.252.87.115    None     i-b15c1fd2      ami-31814f5
    None     t1.micro      xen      i386     aki-8
MONITORING      enabled
STATE   16      running
DevServer       sg-6afb1e02
PLACEMENT       default None     us-east-1a
/dev/sda1
EBS     attached        False   vol-4616cc2b    2
/dev/sdf
EBS     attached        False   vol-1ab26877    2
/dev/sdh
EBS     attached        False   vol-fcd30991    2
/dev/sdg
```

Business Intelligence Tools



AWS Spend Analysis

Month-to-date Spend

$9.99K

Daily Spend

Month-to-date Spend by Service

Amazon Simple Storage Service
Amazon WorkSpaces
Amazon Elastic Compute Cloud
Amazon RDS Service
Amazon AppStream
AWS Key Management Service
Amazon ElastiCache

Month-to-date Spend by EC2 Instance Type

AWS Services that provide Operational Visibility

Network & Perimeter

AWS WAF

Track application access/denials

Amazon VPC

Flow logs

Track network activity of VPC

OS and Applications

AWS Systems Manager

Inventory and manage instances

Amazon Inspector

Analyze OS and application security

AWS Services & Activity

AWS Trusted Advisor

Guidance to reduce cost, increase performance, and improve security

Personal Health Dashboard

Personalized view of AWS services' health

AWS CloudTrail

Track user activity and API usage

Amazon CloudWatch

Monitor resources and applications

Detection & Analysis

Amazon GuardDuty

Intelligent threat detection

AWS Security Hub

Unified security and compliance Center

Amazon Macie

Discover, classify, and protect sensitive data

Amazon Detective

Analyze and Investigate events

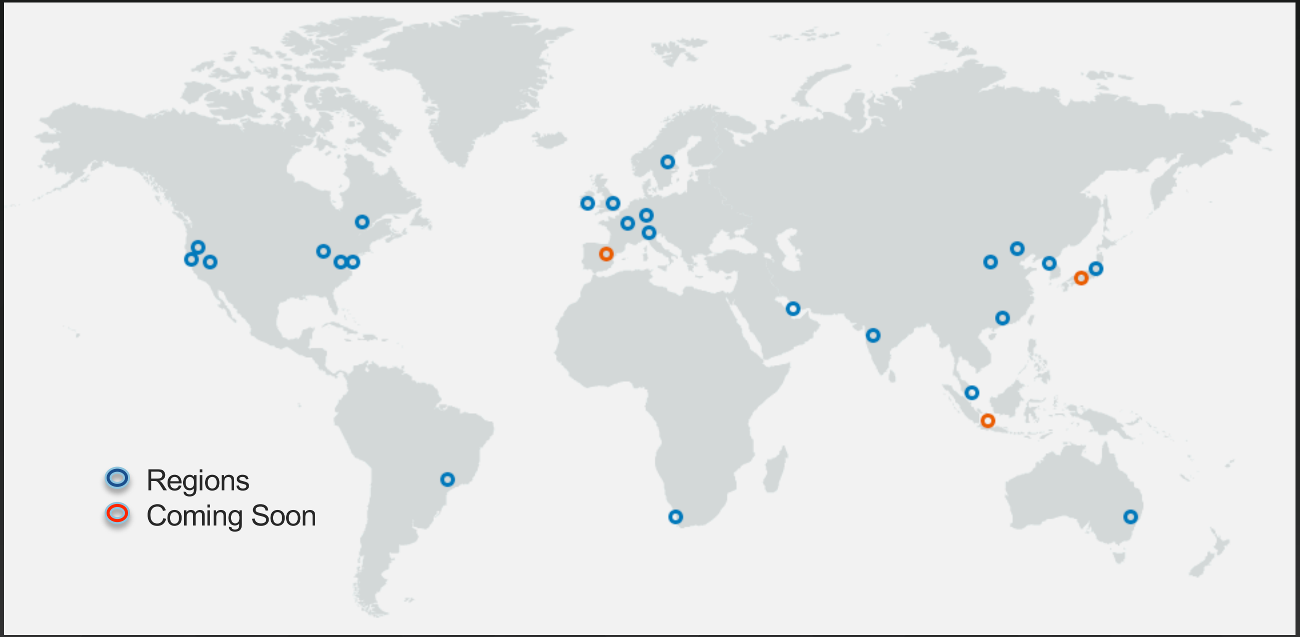
Resiliency

AWS Global Infrastructure

24
Regions

77
Availability Zones

205
Edge Locations

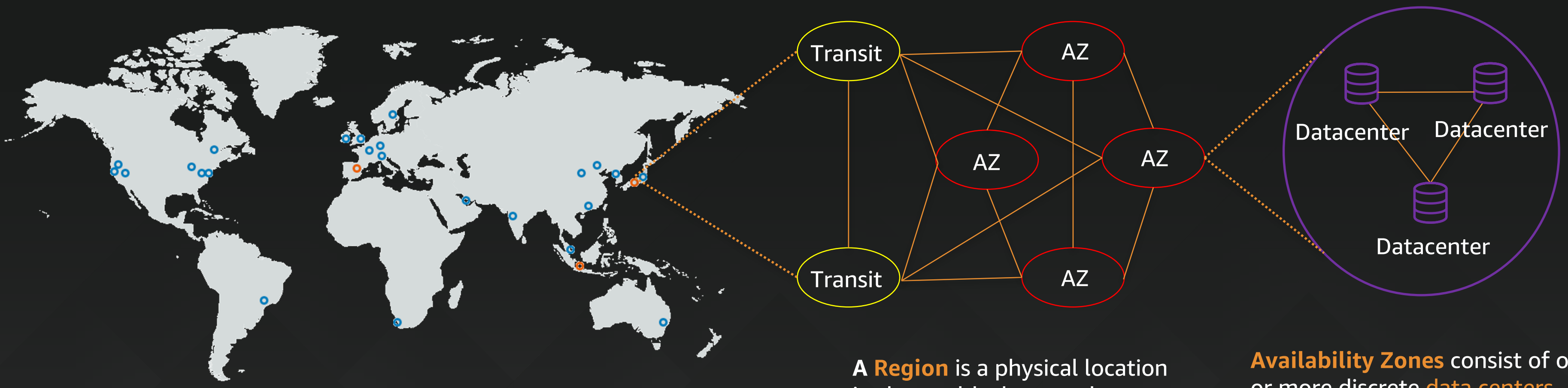


Scale globally with resilience **in every region**

The largest global foot print consistently built with a multi-AZ and multi-datacenter design

AWS Region

AWS Availability Zone (AZ)

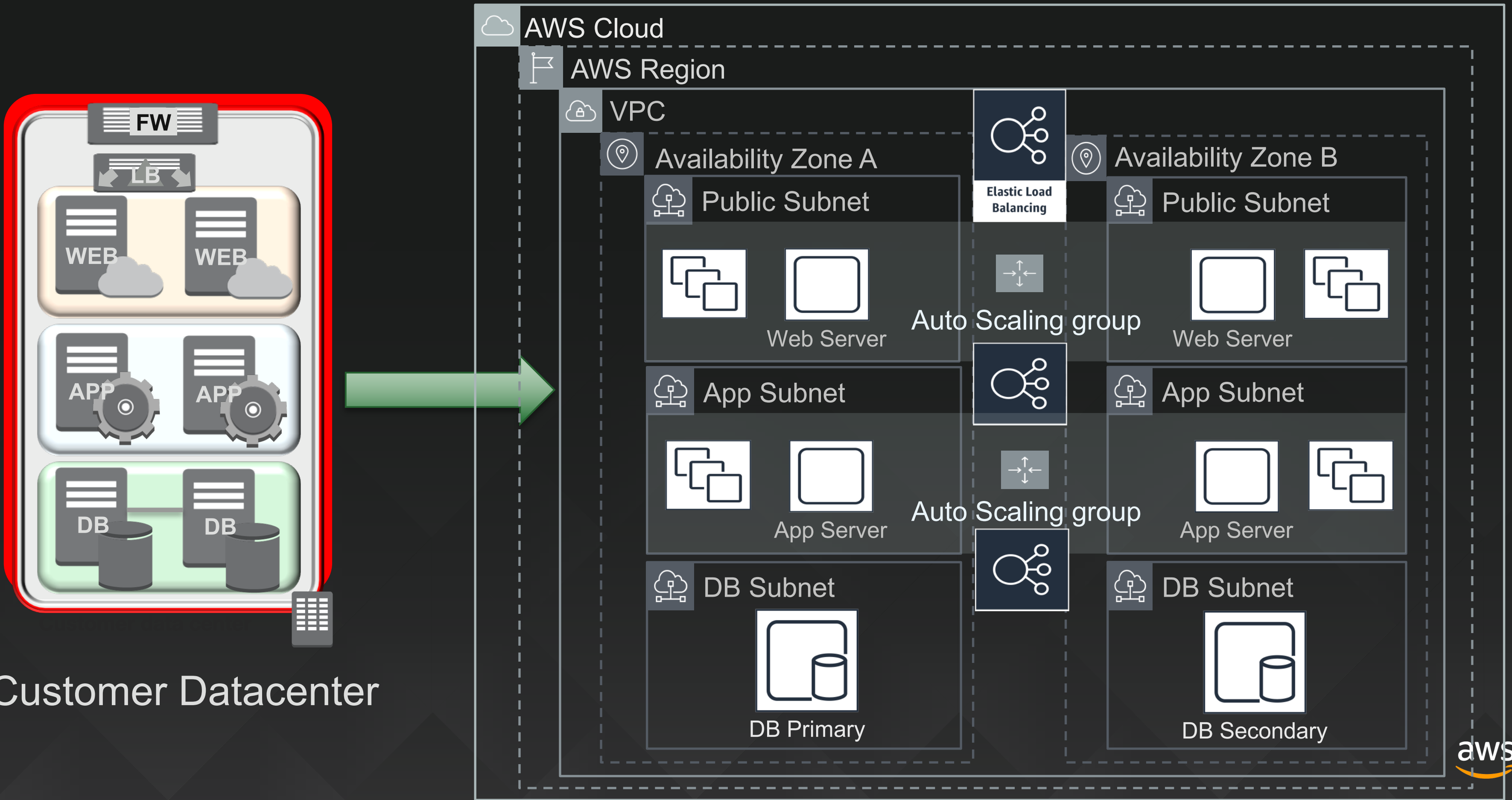


○ Regions
○ Coming Soon

A Region is a physical location in the world where we have multiple **Availability Zones.**

Availability Zones consist of one or more discrete data centers, each with redundant power, networking, and connectivity, housed in separate facilities.

Achieving High Availability in AWS



Customer Datacenter

Defense in Depth

Reality of Many On-Prem Network Defenses

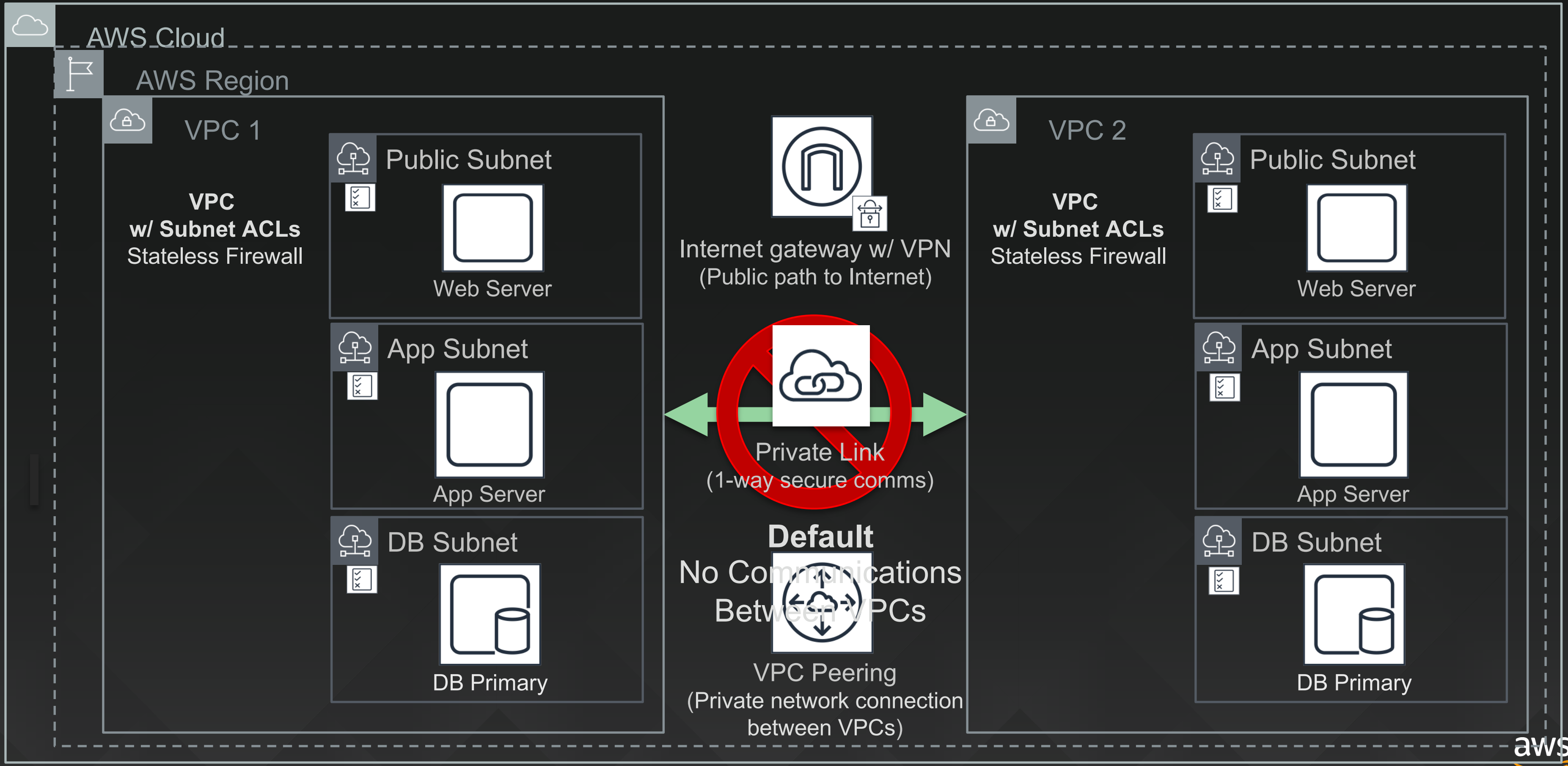
Hard Outer Shell
(Perimeter)

WAF
Firewall
IDS/IPS
DLP

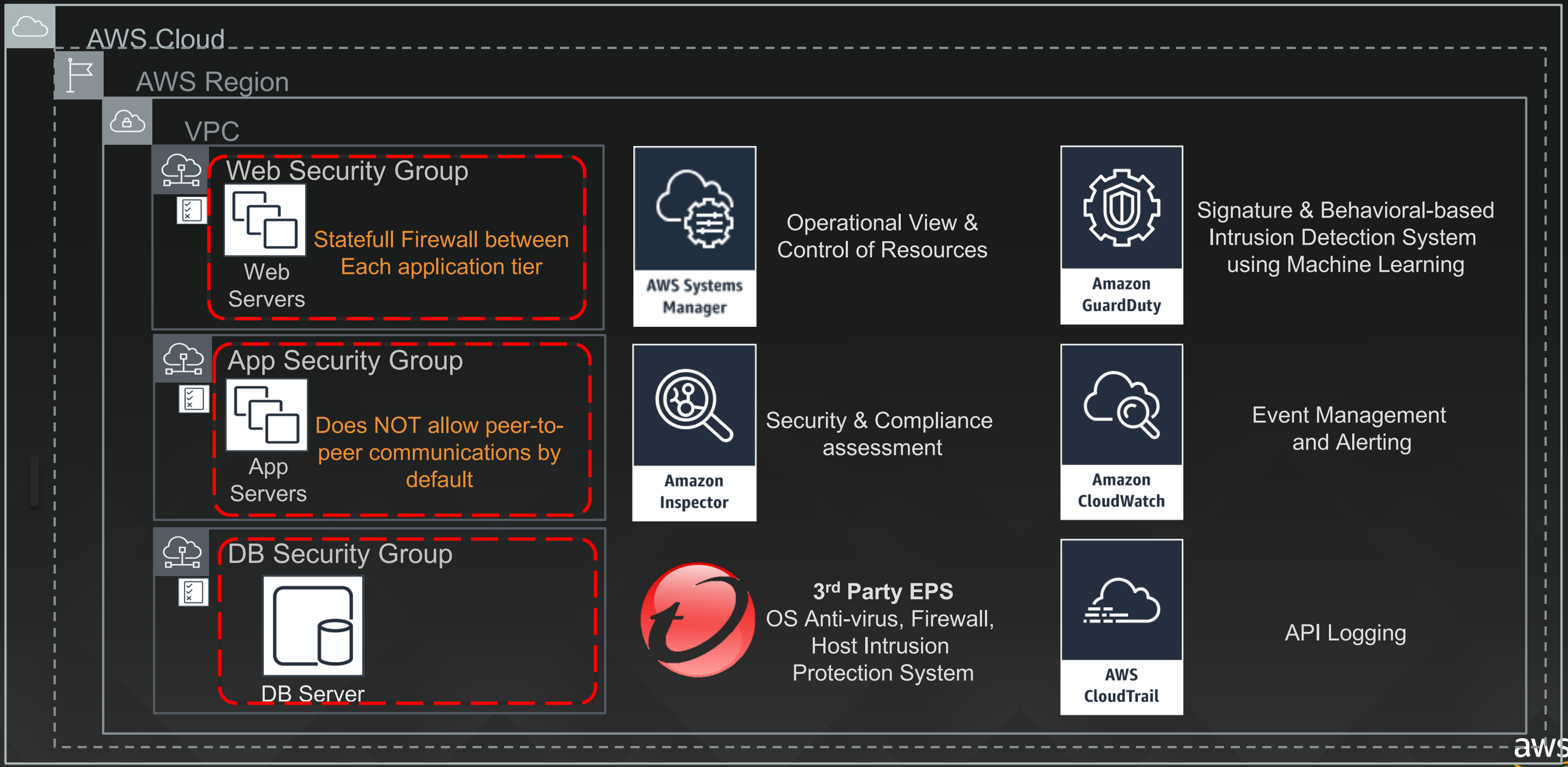
Soft and Gooey Middle
(LAN / Datacenter)

VLANs
ACLs
EPS

Defense-in-Depth in AWS between Workloads



Defense-in-Depth in AWS inside the Workload



AWS Cloud

AWS Region

VPC

Web Security Group

Web Servers

Statefull Firewall between Each application tier

App Security Group

App Servers

Does NOT allow peer-to-peer communications by default

DB Security Group

DB Server

AWS Systems Manager

Operational View & Control of Resources

Amazon GuardDuty

Signature & Behavioral-based Intrusion Detection System using Machine Learning

Amazon Inspector

Security & Compliance assessment

Amazon CloudWatch

Event Management and Alerting

3rd Party EPS
OS Anti-virus, Firewall, Host Intrusion Protection System

AWS CloudTrail

API Logging

Automation

Amazon GuardDuty IDS

Reconnaissance

- Instance recon:
  - Port probe / accepted comm
  - Port scan (intra-VPC)
  - Brute force attack (IP)
  - Drop point (IP)
  - Tor communications
  - Account recon
  - Tor API call (failed)

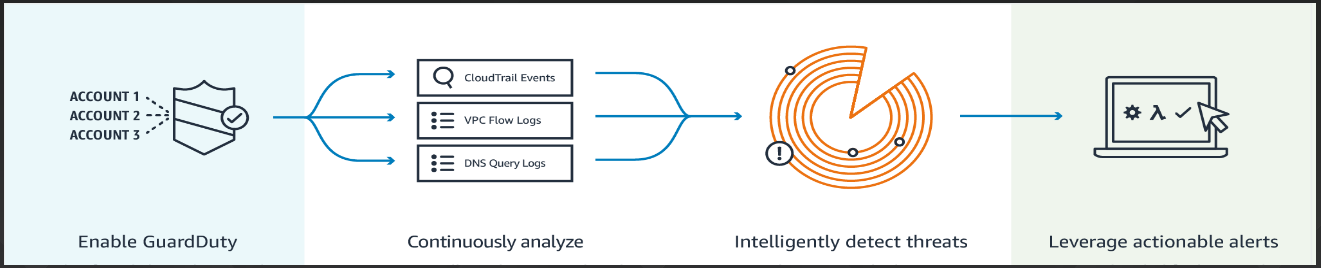
- Detections in gray are signature based, state-less findings
- Detections in blue are behavioral, state-full findings / anomaly detections

Instance compromise

- C&C activity
- Malicious domain request
- EC2 on threat list
- Drop point IP
- Malicious comms (ASIS)
- Bitcoin mining
- Outbound DDoS
- Spambot activity
- Outbound SSH brute force
- Unusual network port
- Unusual traffic volume/direction
- Unusual DNS requests

Account compromise

- Malicious API call (bad IP)
- Tor API call (accepted)
- CloudTrail disabled
- Password policy change
- Instance launch unusual
- Region activity unusual
- Suspicious console login
- Unusual ISP caller
- Mutating API calls (create, update, delete)
- High volume of describe calls
- Unusual IAM user added



ACCOUNT 1
ACCOUNT 2
ACCOUNT 3

CloudTrail Events
VPC Flow Logs
DNS Query Logs

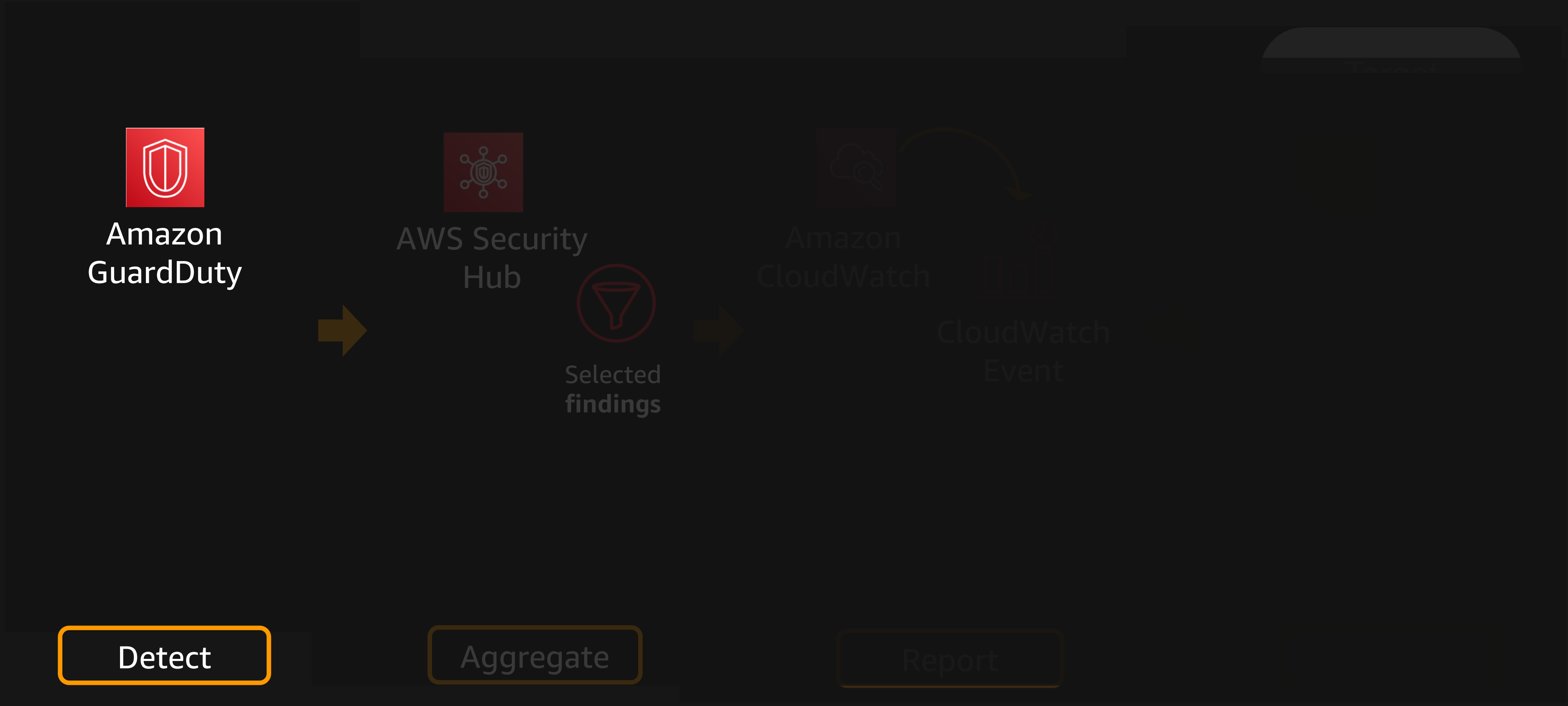
Enable GuardDuty

Continuously analyze

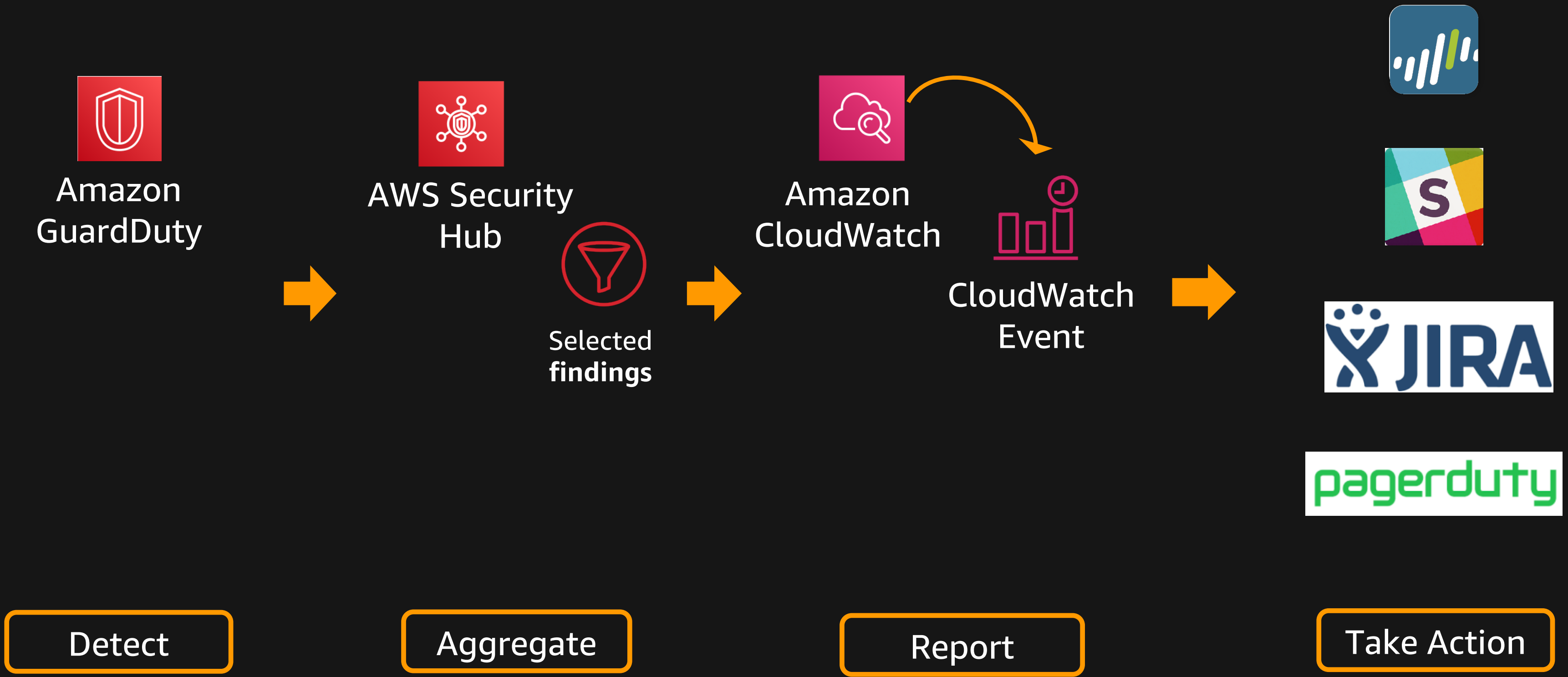
Intelligently detect threats

Leverage actionable alerts

Automate with integrated services



Automate with integrated services



Amazon GuardDuty

AWS Security Hub

Selected **findings**

Amazon CloudWatch

CloudWatch Event

Detect

Aggregate

Report

Take Action

AWS security solutions

Identity

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

Detective control

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

Infrastructure security

- AWS Shield
- AWS Firewall Manager
- AWS Web Application Firewall (WAF)
- AWS Firewall Manager
- Amazon Virtual Private Cloud (VPC)
- Amazon EC2 Systems Manager
- Amazon Inspector

Data protection

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

Incident response

- AWS Config Rules
- AWS Lambda

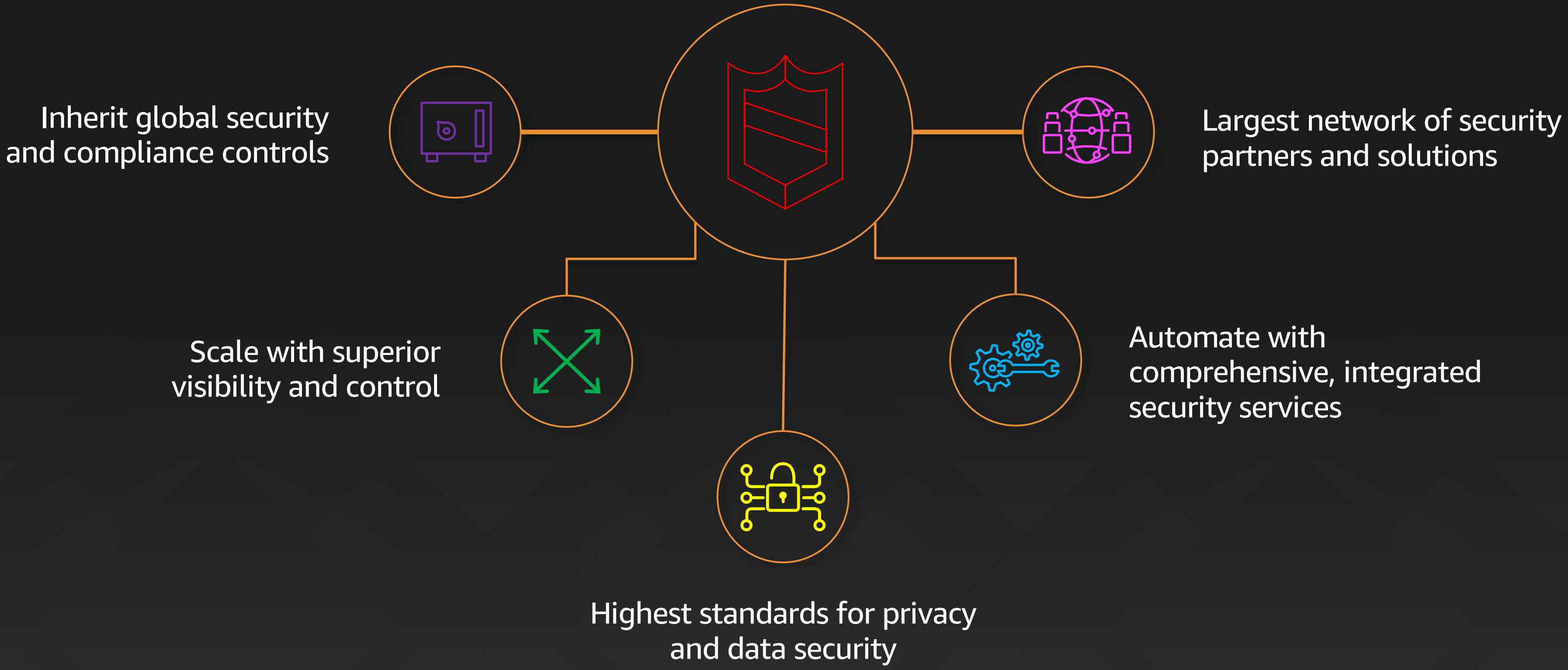
Improving security with the cloud

“Based on our experience, I believe that we can be even more secure in the AWS cloud than in our own datacenters.”

-Tom Soderstrom, CTO, NASA JPL

For more details, see Re:Invent 2013 presentations by NASA JPL cyber security engineer Matt Derenski (http://awsps.com/videos/SEC205E-640px.mp4)

Elevate your security with AWS



Inherit global security and compliance controls

Largest network of security partners and solutions

Scale with superior visibility and control

Automate with comprehensive, integrated security services

Highest standards for privacy and data security

Thank you!

Questions?

mlsouth@amazon.com