

Cybersecurity: A Driving Force Behind Cloud Adoption

Varun Pole
Solutions Architect
AWS



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

What is cloud computing?



The on-demand delivery of IT resources over public or private networks with zero up-front costs, no long-term contracts, and pay-as-you-go pricing

Education is Built on AWS



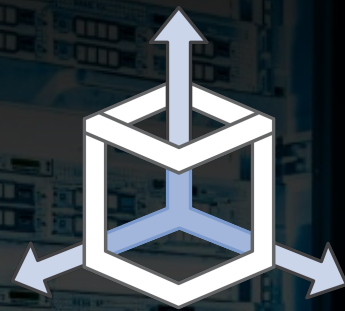
Industry leaders are building on AWS



Why is security traditionally so hard?



**Lack of
Visibility**



**Lack of
Resiliency**



**Defense-in-Depth
Challenges**



**Low degree
of Automation**

Four Security Benefits of the Cloud

Increased *visibility*

Increased *availability* and *resiliency*

True *Defense-in-Depth*

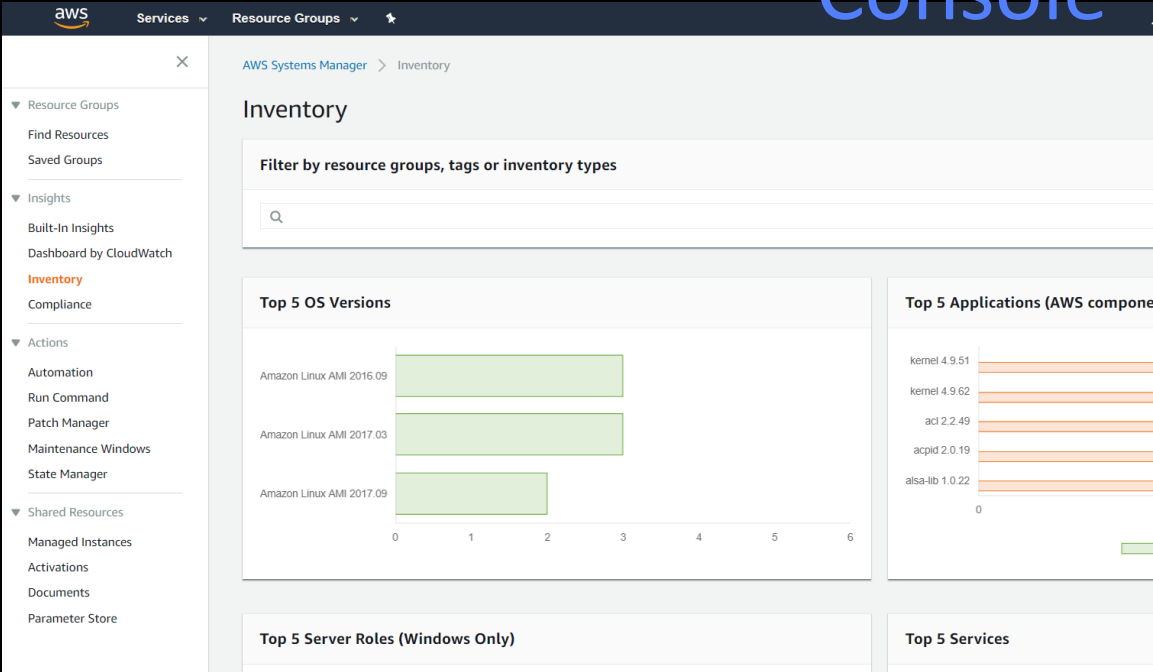
Ability to *automate* for governance and Security Operations

Visibility



Means of obtaining Visibility

Console



Use of resource tags

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

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.

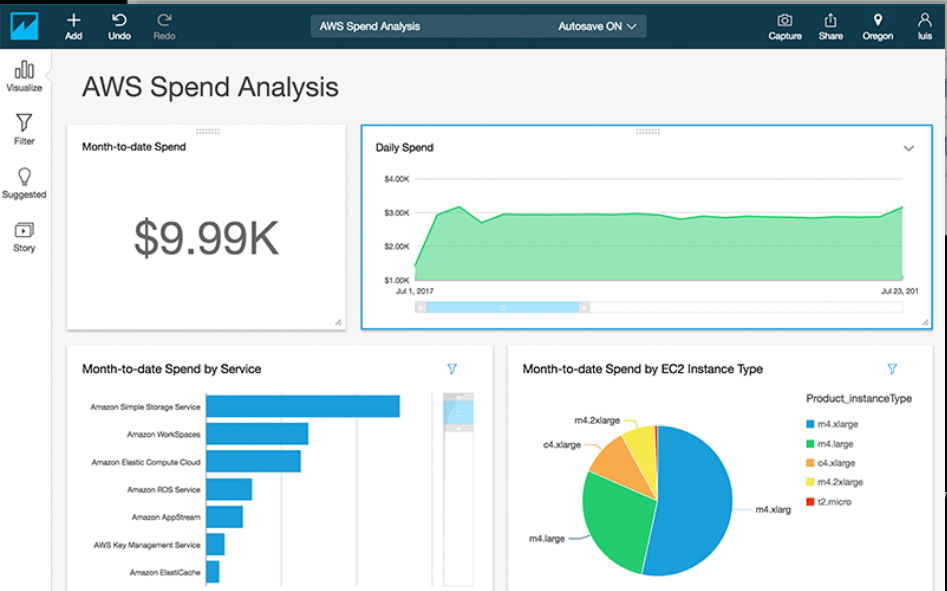
```
{
  "swagger": "2.0",
  "info": {
    "title": "PetStore"
  },
  "schemes": [
    "https"
  ],
  "paths": {
    "/": {
      "post": {
        "produces": [
          "application/json"
        ],
        "responses": {
          "200": {
            "description": "200 response",
            "schema":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

Import

CLI Describe

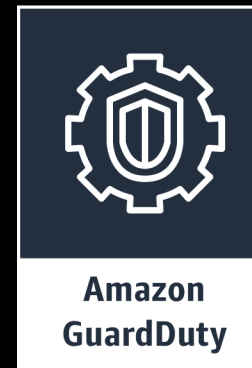
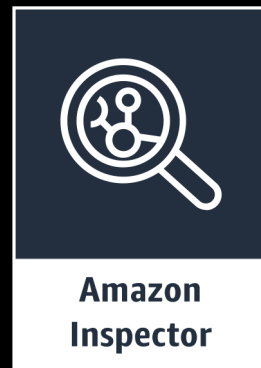
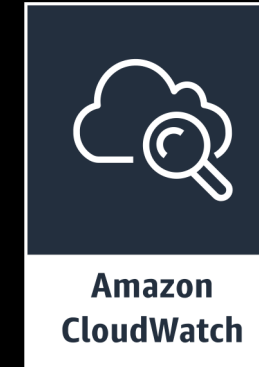
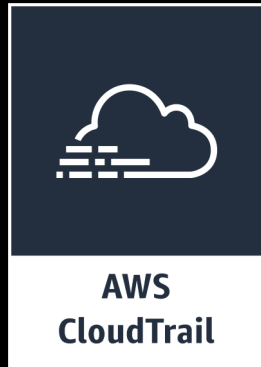
```
$ aws ec2 describe-instances --output text
889279108296    r-dc2428b2    058890971305
DevServer      sg-6afb1e02
ec2-107-20-138-116.compute-1.amazonaws.com    e
.252.87.115    None    i-b15c1fd2    ami-31814f5
None    t1.micro    xen    i386    aki-8
MONITORING    enabled
STATE    16    running
DevServer      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


















ices, Inc. or its affiliates. All rights reserved.

AWS Services that provide Operational Visibility



Inherit global security and compliance controls



















Certifications / Attestations


| | |
|-----------------------|---|
| C5 |  |
| Cyber Essentials Plus |  |
| DoD SRG |  |
| FedRAMP |  |
| FIPS |  |
| IRAP |  |
| ISO 9001 |  |
| ISO 27001 |  |
| ISO 27017 |  |
| ISO 27018 |  |
| K-ISMS |  |
| MTCS |  |
| PCI DSS Level 1 |  |
| SEC Rule 17-a-4(f) |  |
| SOC 1, SOC 2, SOC 3 |  |

Laws / Regulations / Privacy

| | |
|---------------------------|---|
| Argentina Data Privacy | |
| CISPE |  |
| EU Model Clauses |  |
| FERPA |  |
| GDPR |  |
| GLBA |  |
| HIPAA |  |
| HITECH |  |
| IRS 1075 |  |
| ITAR |  |
| My Number Act |  |
| UK DPA - 1988 |  |
| VPAT/Section 508 |  |
| Data Protection Directive |  |
| Privacy Act [Australia] |  |
| Privacy Act [New Zealand] |  |
| PDPA—2010 [Malaysia] |  |
| PDPA—2012 [Singapore] |  |
| PIPEDA [Canada] |  |
| Spanish DPA Authorization |  |
| Spanish DPA Authorization |  |

Alignments / Frameworks

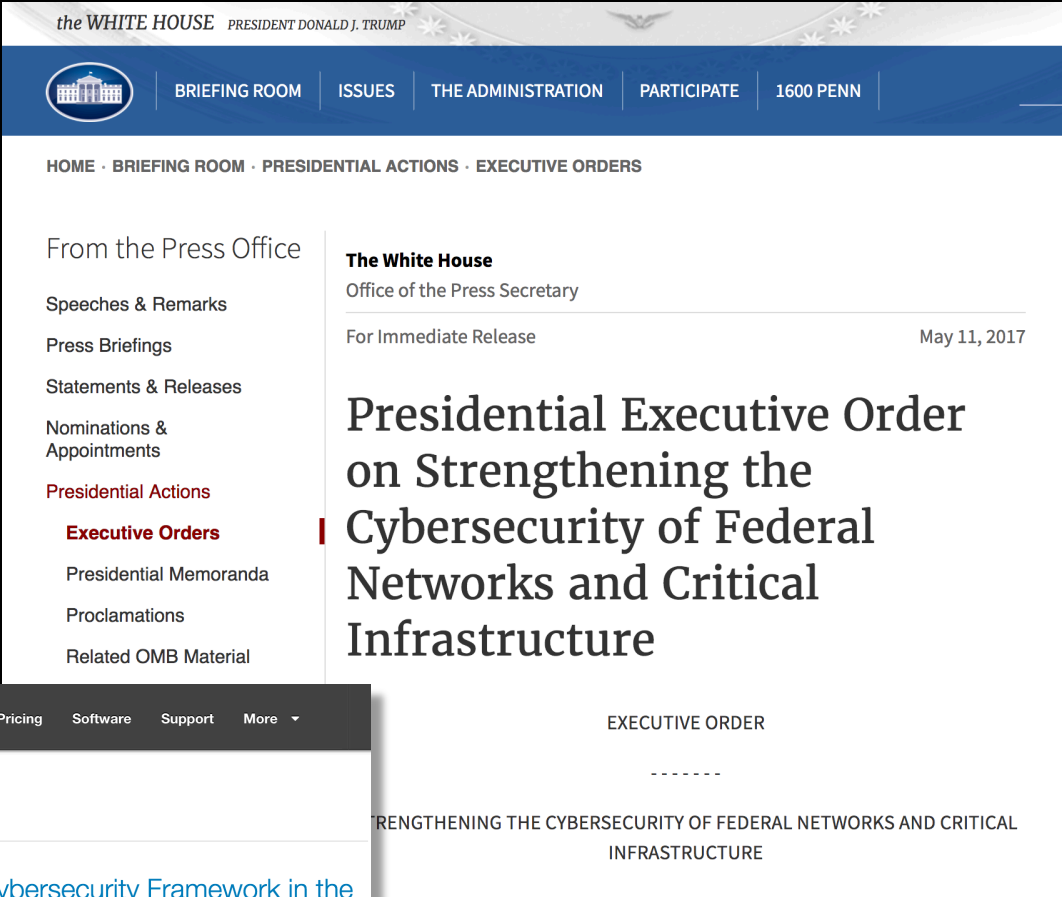
| | |
|------------------------------------|---|
| CIS (Center for Internet Security) |  |
| CJIS (US FBI) |  |
| CSA (Cloud Security Alliance) |  |
| ENS High |  |
| EU-US Privacy Shield |  |
| FFIEC |  |
| FISC |  |
| FISMA |  |
| G-Cloud |  |
| GxP (US FDA CFR 21 Part 11) |  |
| ICREA |  |
| IT Grundschutz |  |
| MITA 3.0 (US Medicaid) |  |
| MPAA |  |
| NIST |  |
| PHR |  |
| Uptime Institute Tiers |  |
| Cloud Security Principles |  |

 = industry or global standard



Implementing NIST's Cyber Security Framework (CSF)

- 1. Executive Order directs all U.S. Federal agencies to use NIST's CSF to manage cyber risk
- 2. Amazon provides guidance on how AWS services align to CSF
- 3. Customers can leverage shared cloud services and FedRAMP P-ATOs and ATOs from other agencies



| 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. |



Resiliency



AWS Global Infrastructure

22

Regions

69

Availability
Zones

176

Edge
Locations

Region & Number of Availability Zones

AWS GovCloud

Oregon (3)

Ohio (3)

US West

Oregon (3)

Northern California (3)

US East

N. Virginia (6)

Ohio (3)

Canada

Central (2)

South America

São Paulo (3)

Announced Regions

Jakarta, Milan, Cape Town

EU

Ireland (3)

Frankfurt (3)

London (3)

Paris (3)

Stockholm (3)

Asia

Singapore (3)

Sydney (3)

Tokyo (4)

Seoul (2)

Mumbai (2)

Hong Kong (3)

Bahrain(3)

China

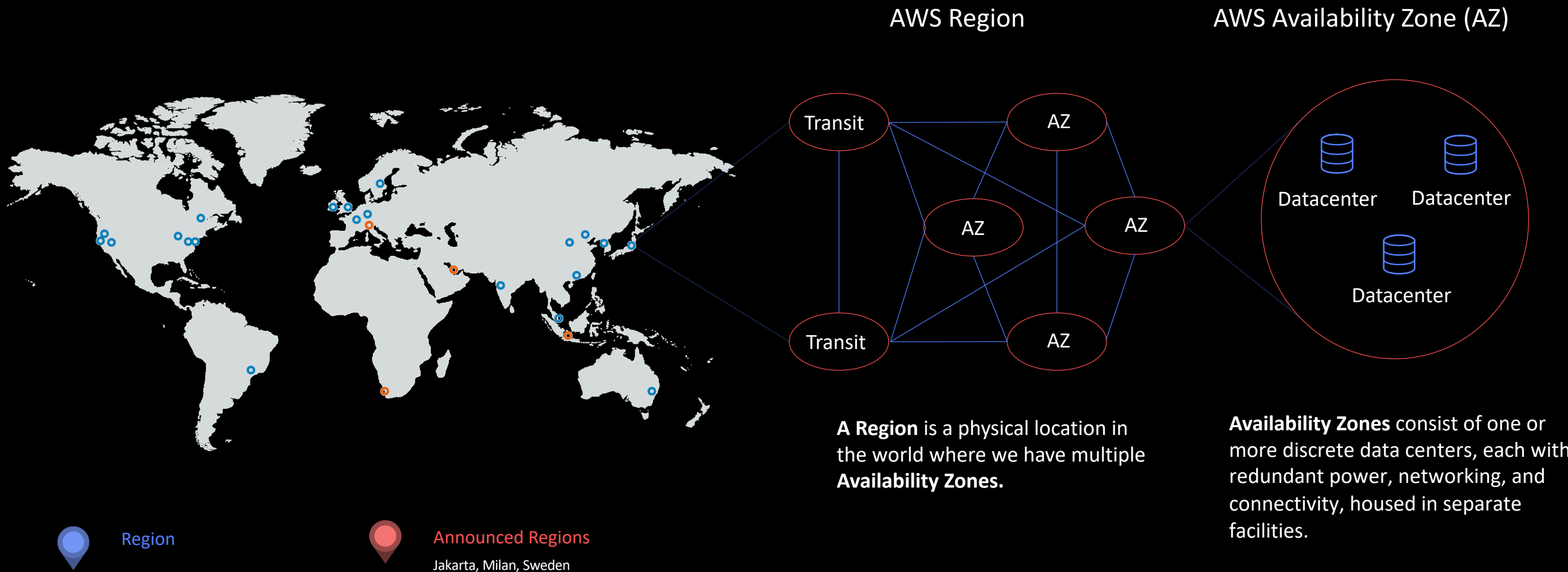
Beijing (2)

Ningxia (3)

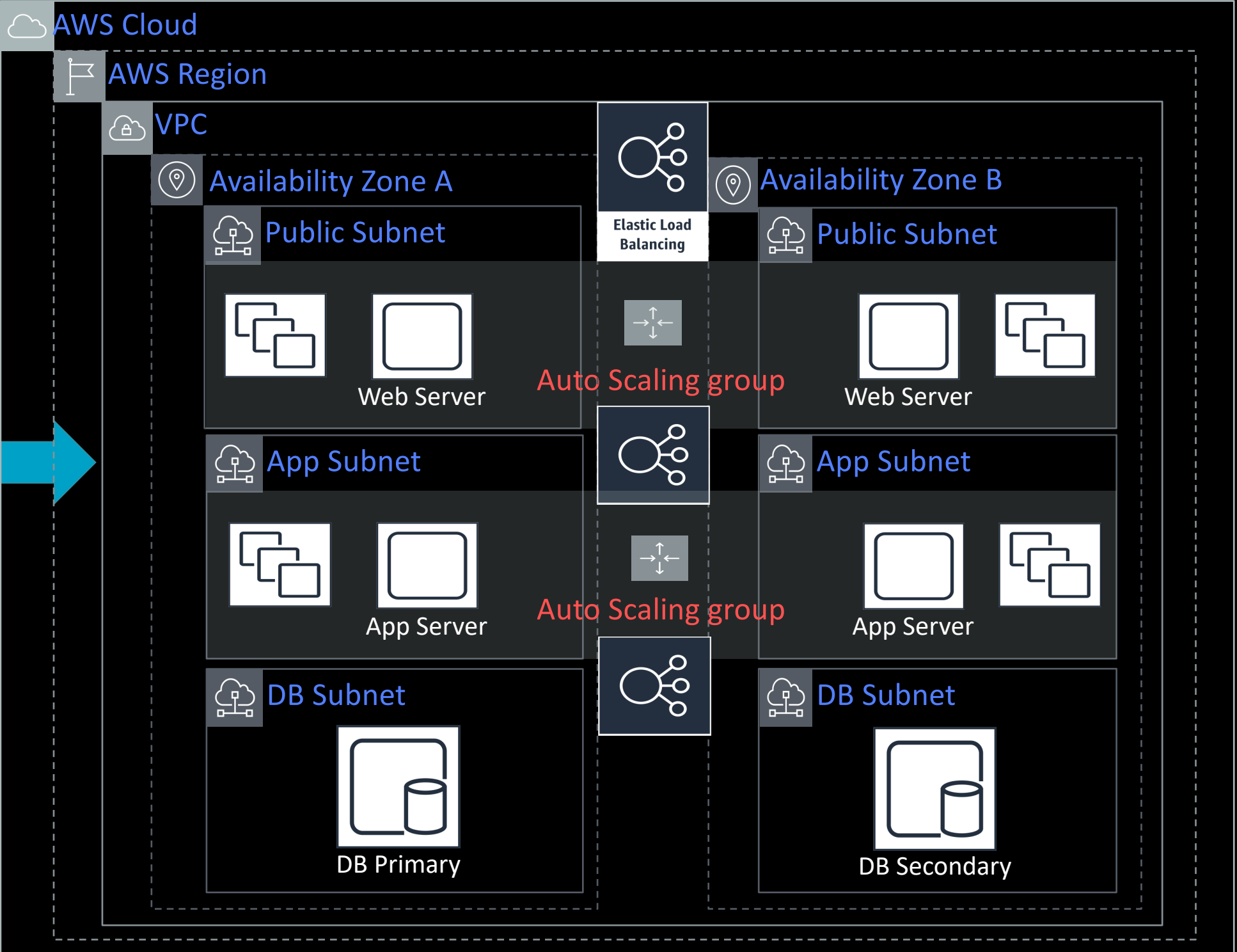
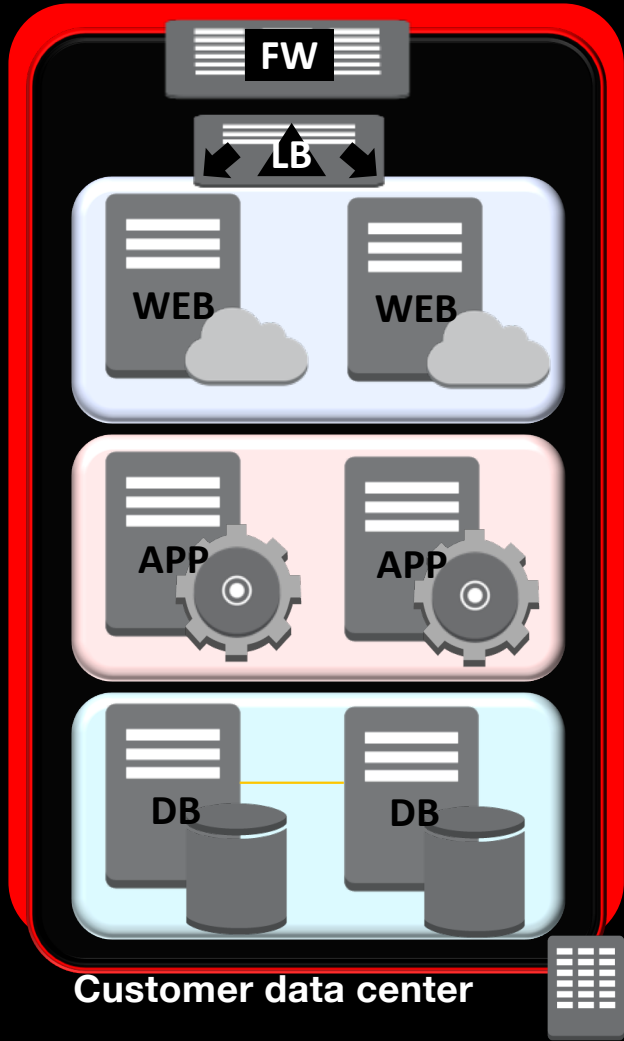


Scale globally with resilience in every region

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



Architecting for Resiliency in AWS



Defense in Depth



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

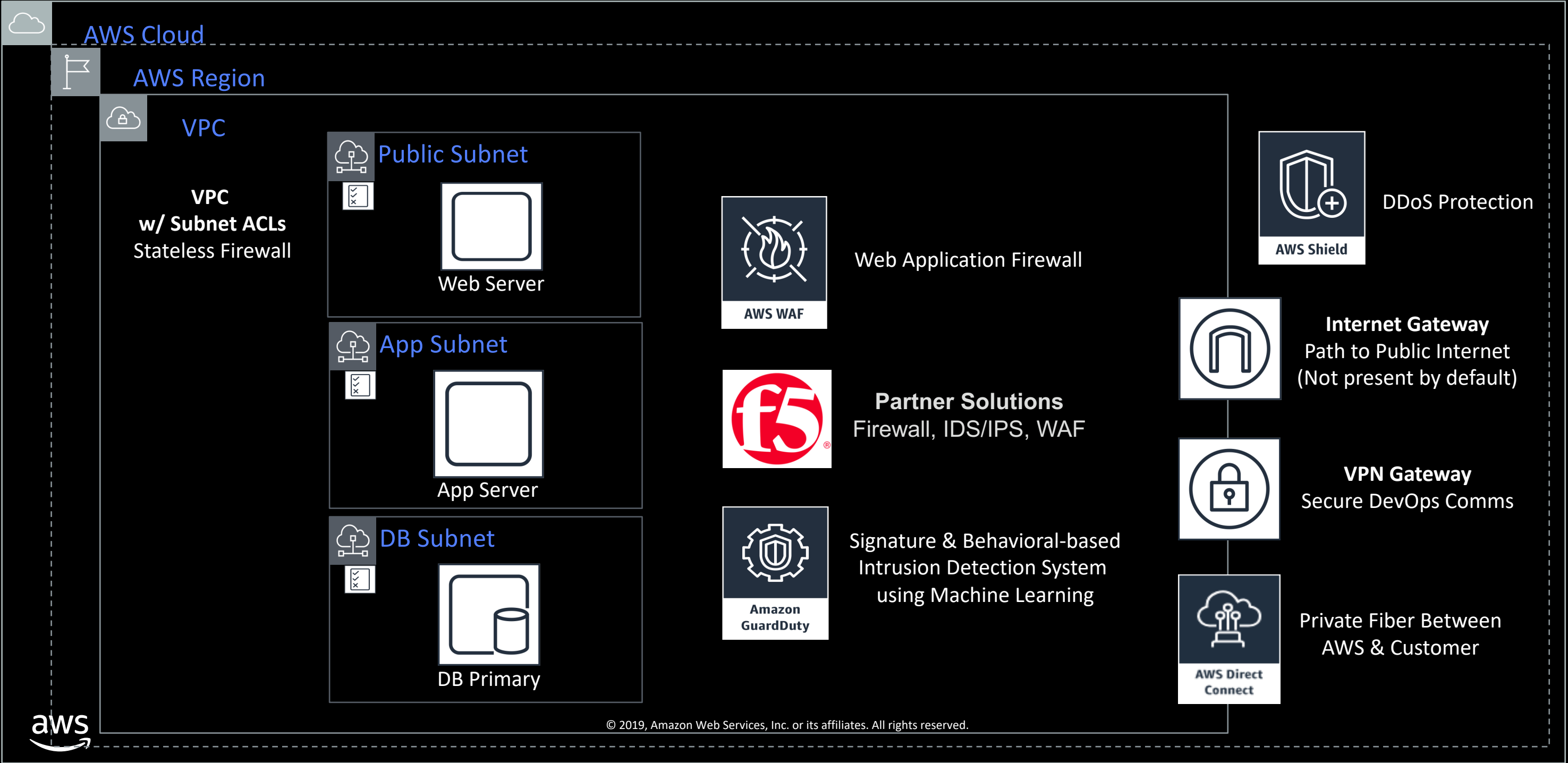
Reality of Many On-Prem Network Defenses

Hard Outer Shell
(Perimeter)

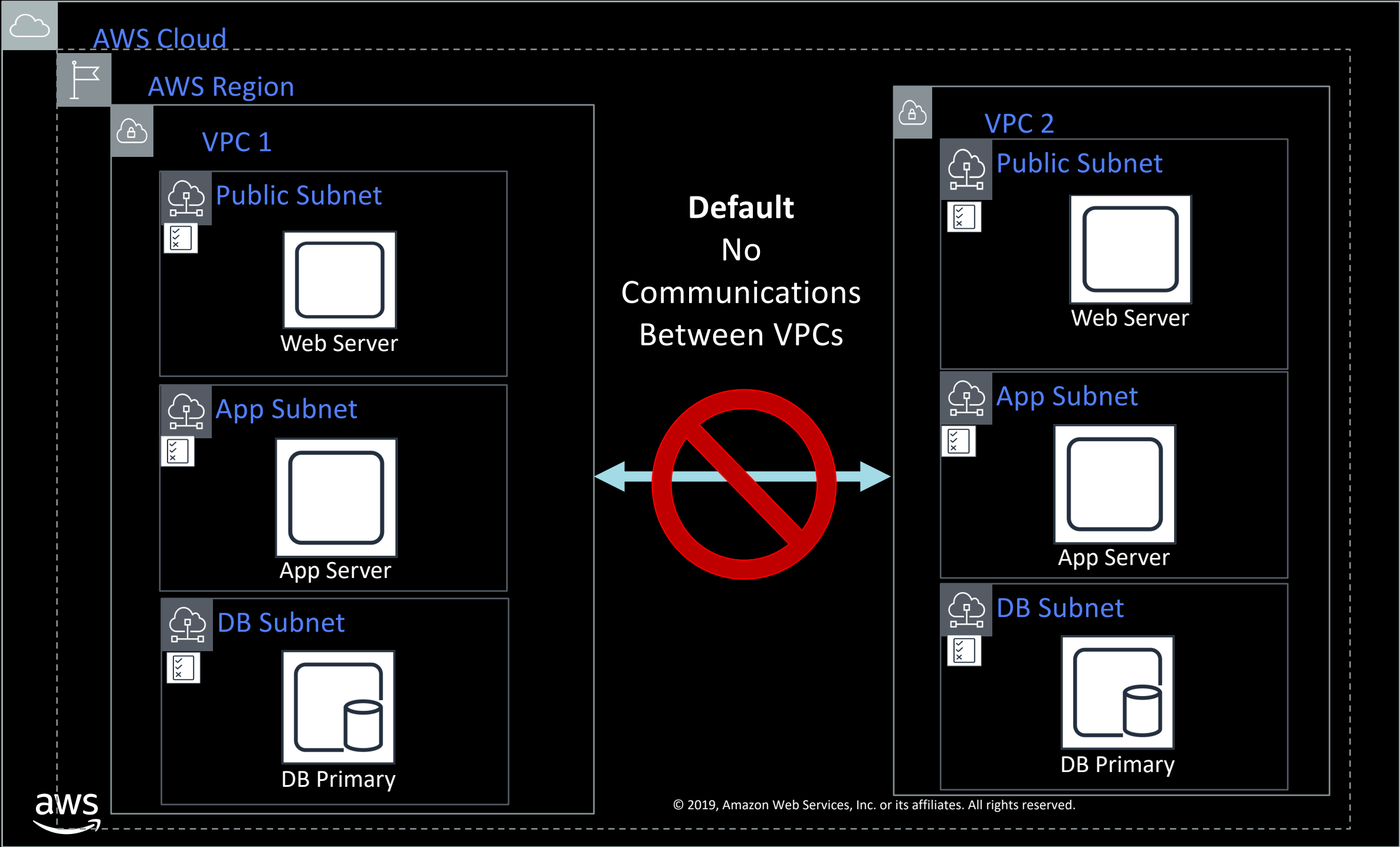



Soft and Gooey Middle
(LAN / Datacenter)

Defense-in-Depth in AWS at the **Perimeter**



Defense-in-Depth in AWS between Workloads

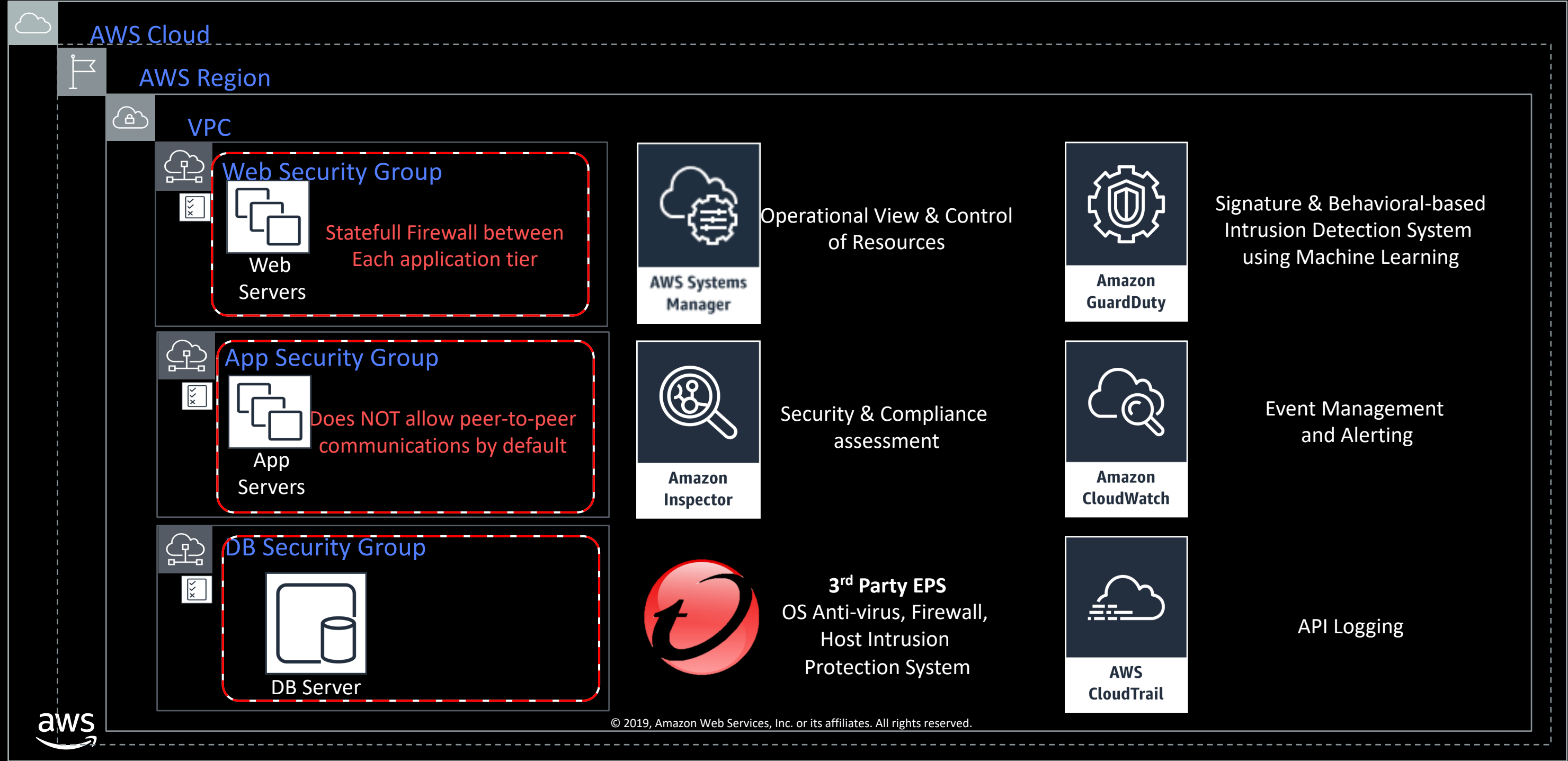



VPC Peering
(Private network connection between VPCs)


Internet gateway w/ VPN
(Public path to Internet)


Private Link
(1-way secure comms)

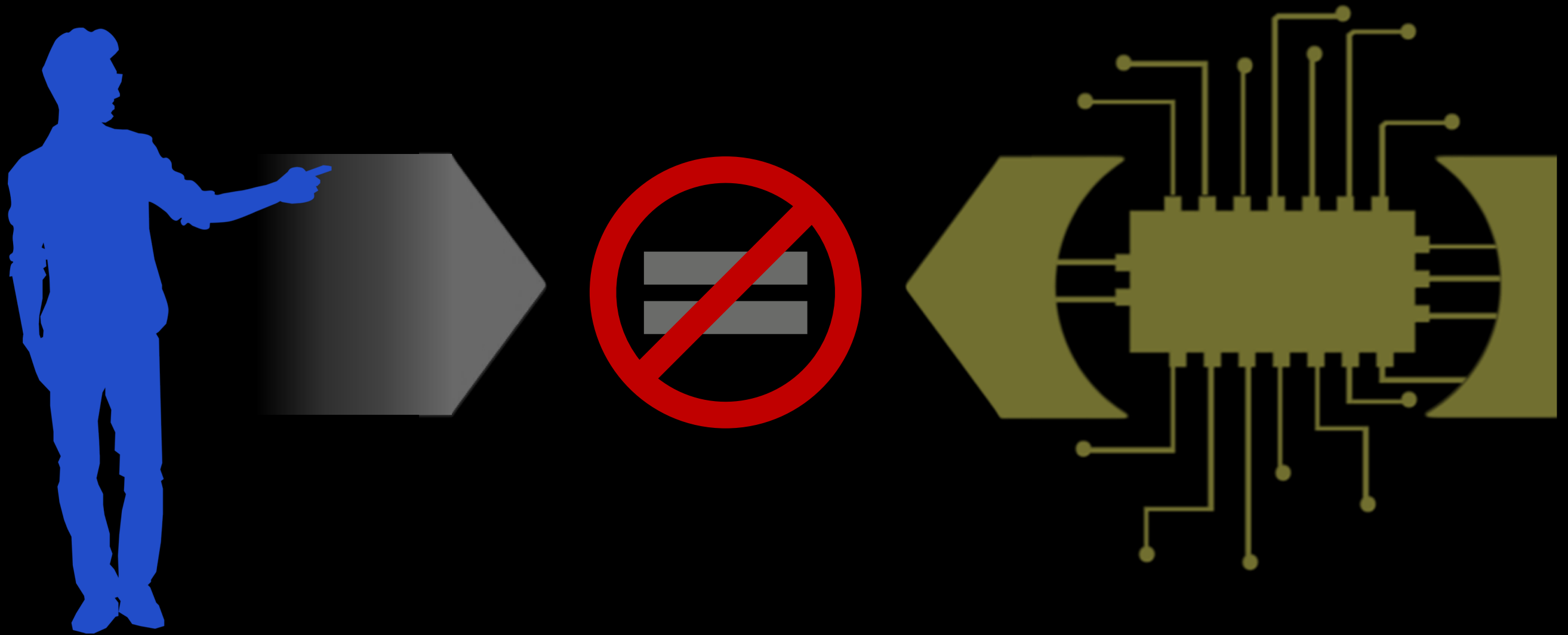
Defense-in-Depth in AWS inside the Workload



Automation



Remove Humans from the Data



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)

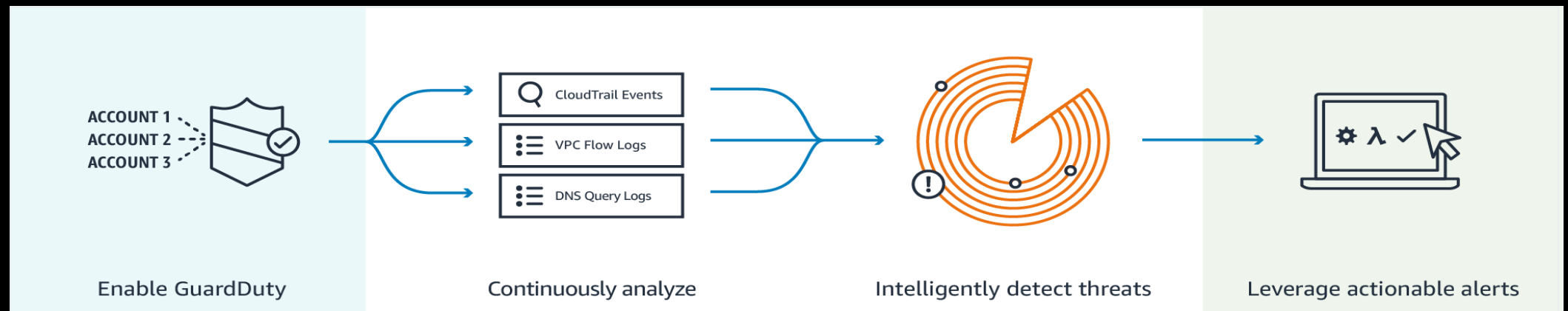
- Detections in white are signature based, state-less findings
- Detections in blue are behavioral, state-full findings / anomaly detections

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

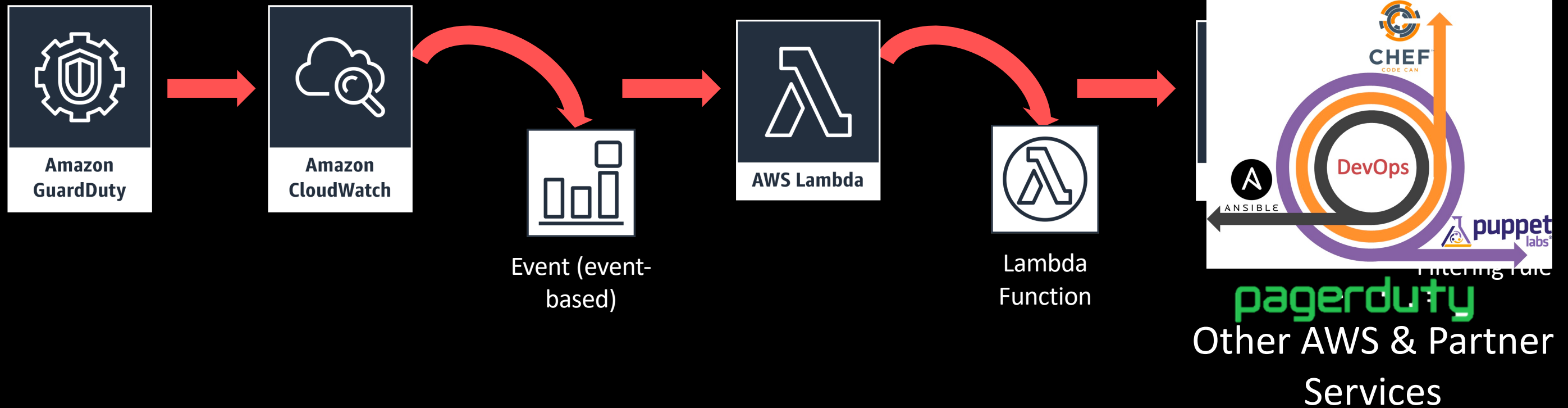
Account compromise

- 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



Automate with integrated services

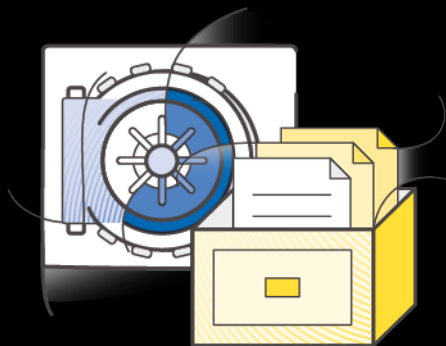
Automated threat remediation



Workloads appropriate for AWS



Web applications
and websites



Backup,
recovery
and archiving



Disaster
recovery



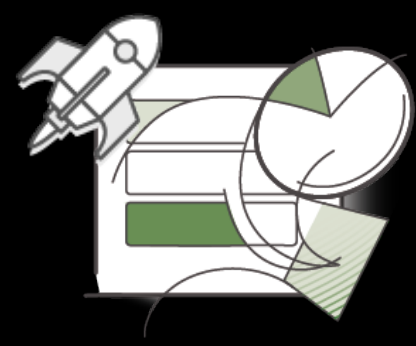
**Security
Operations**



Development
and test



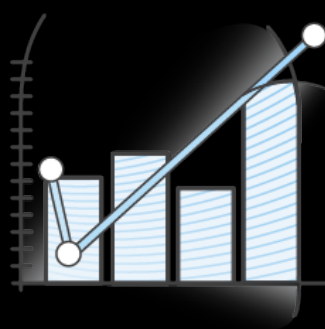
Data center
migration
and hybrid



Mission critical
applications



Enterprise IT



Big data



High-performance
computing



Mobile



IoT



Thank you!

Varun Pole
varrampo@amazon.com

