EIGHTH ANNUAL LEADERSHIP EVENT

CS SUMMIT

Security solutions through collaboration.

Securing Microservices

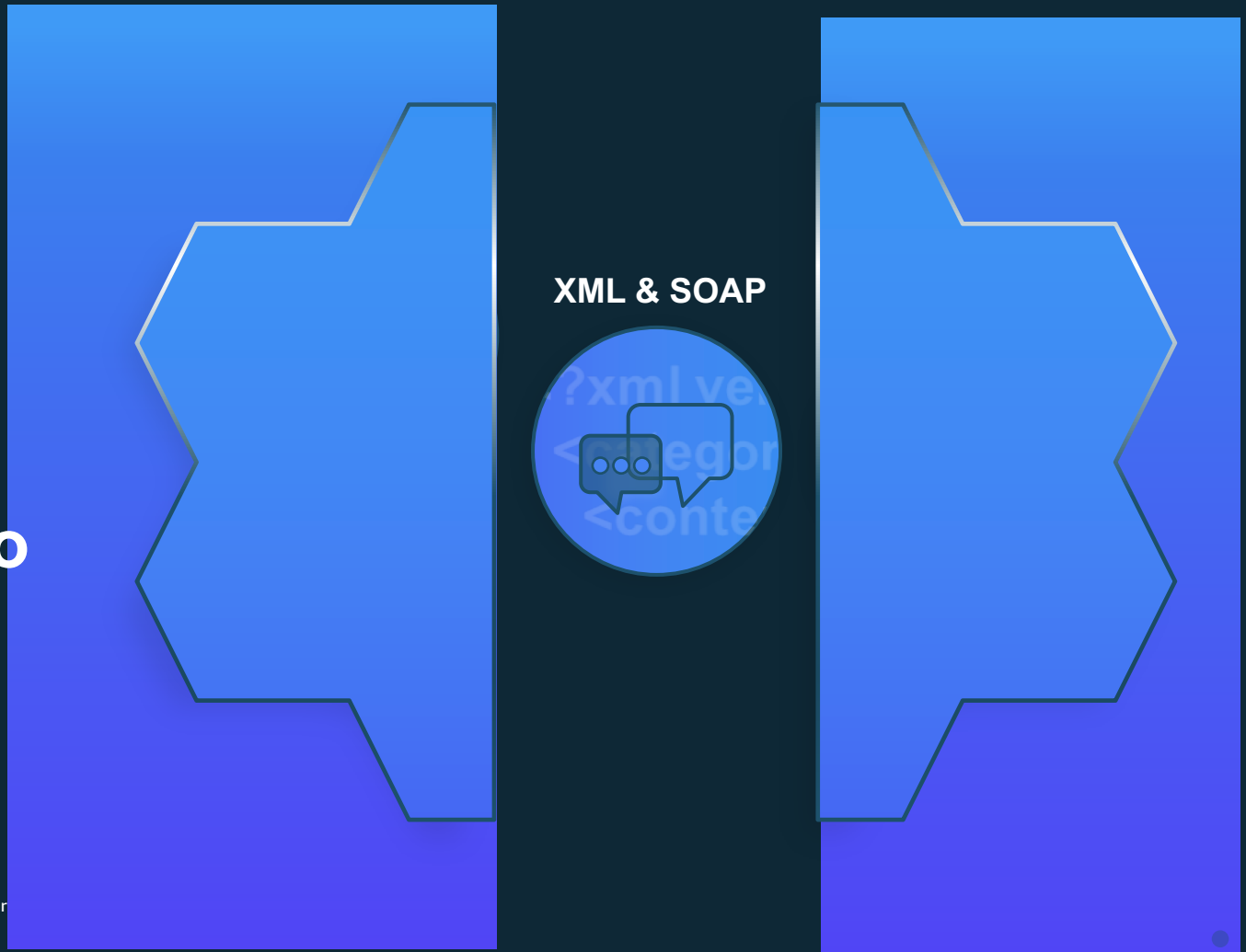
Containerized Security in AWS

Mike Gillespie, Solutions Architect, Amazon Web Services

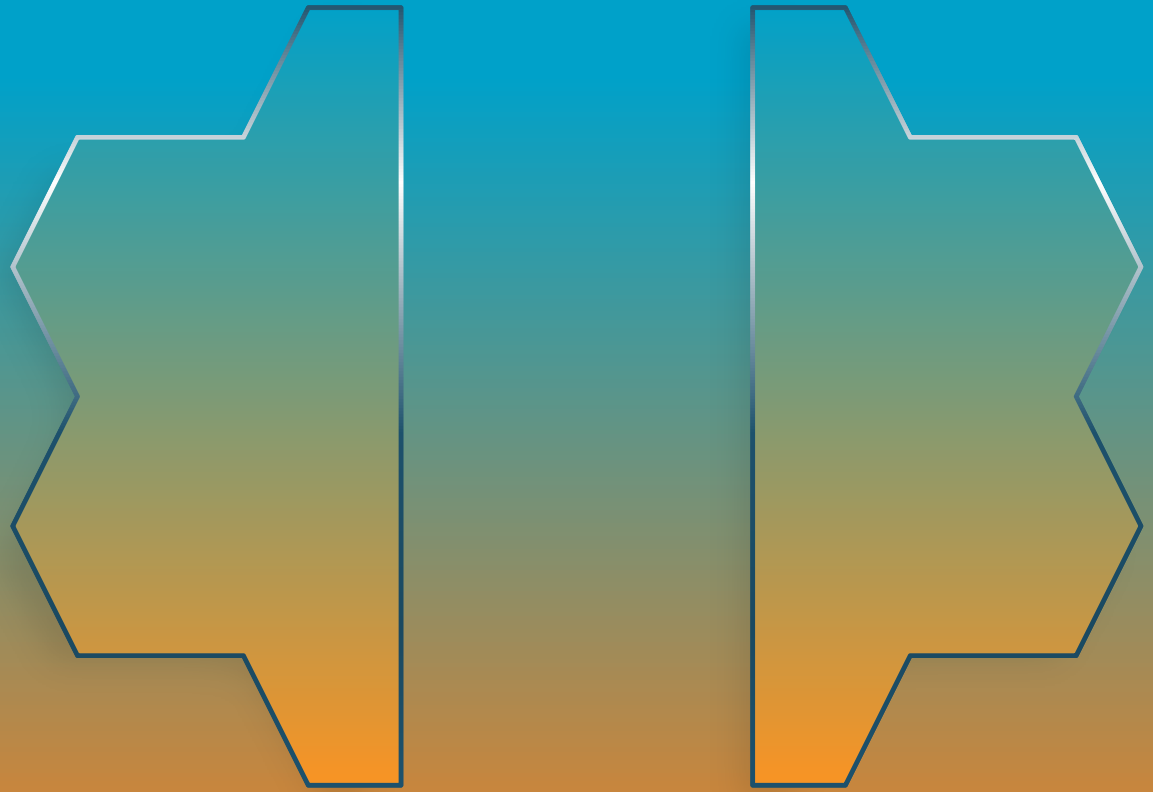
Splitting Monoliths Ten Years Ago

aws

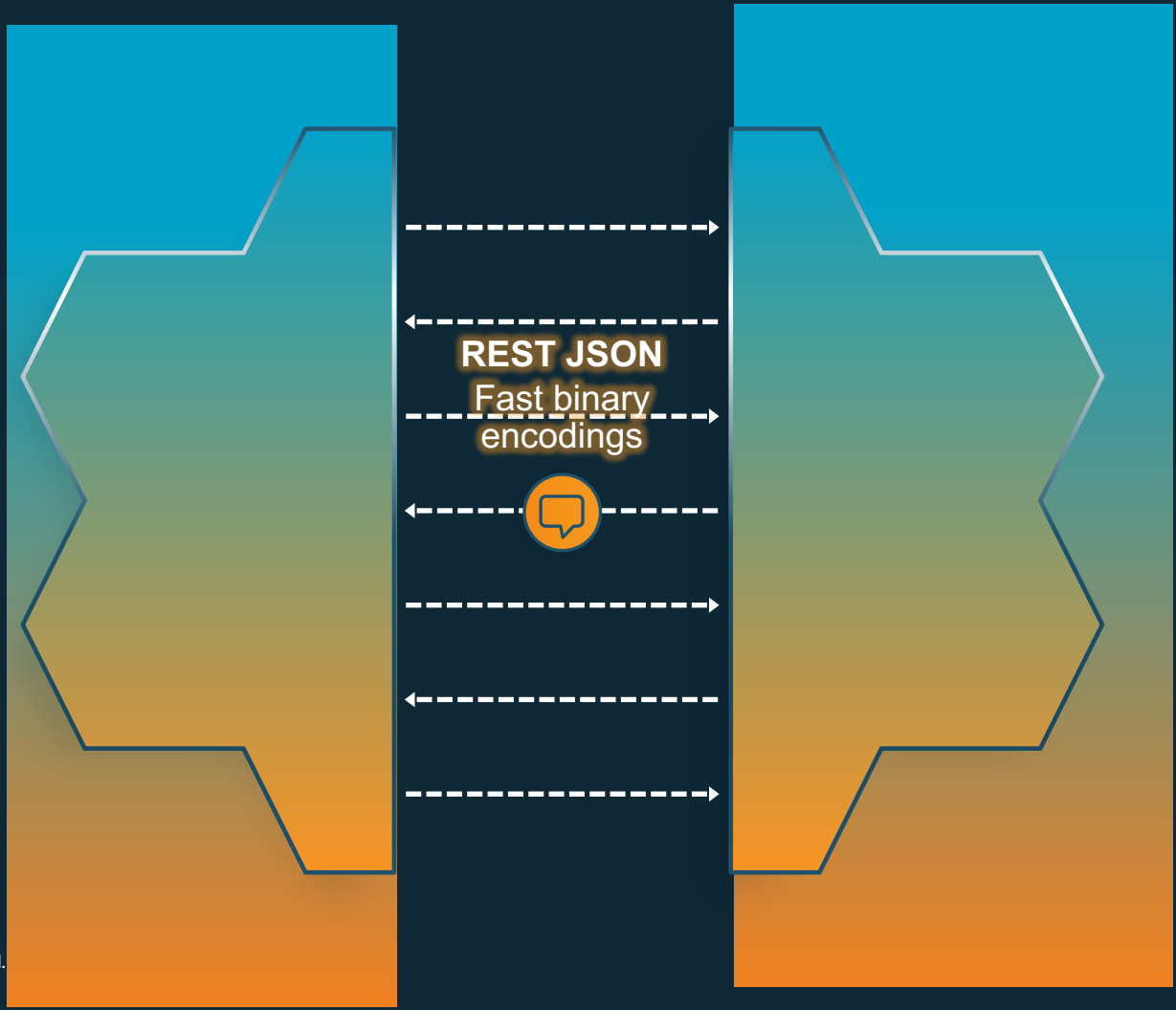
Splitting Monoliths Ten Years Ago

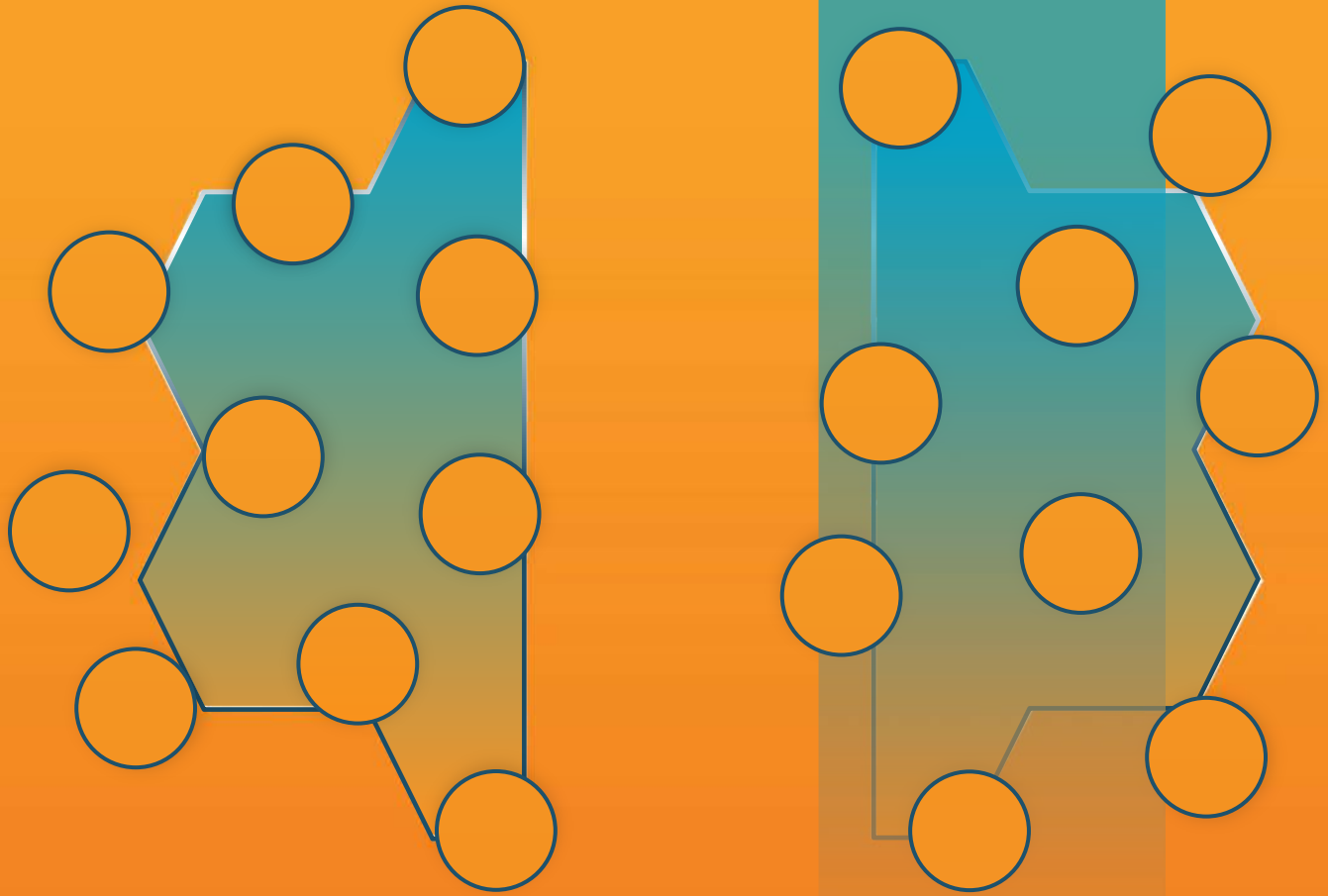


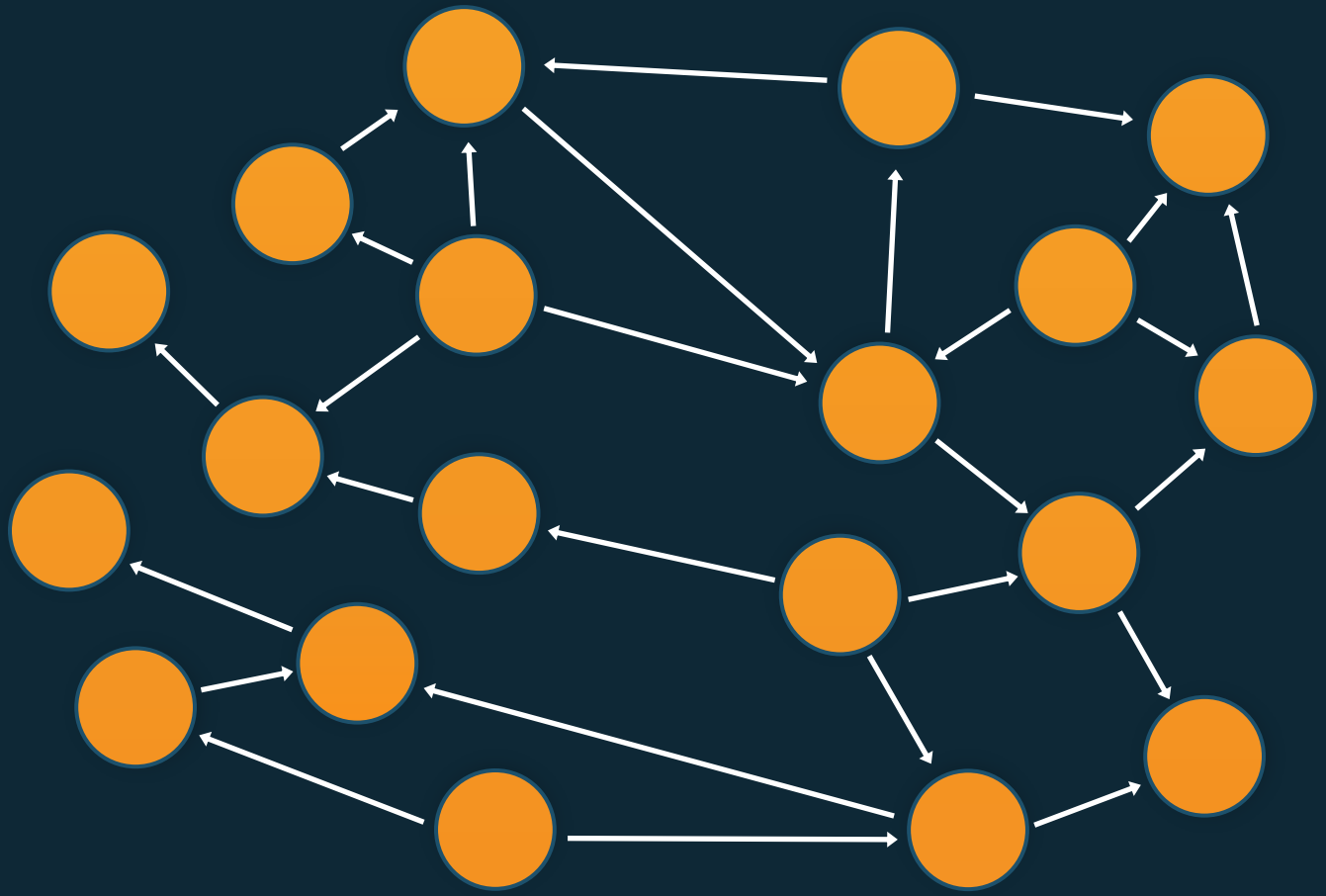
Splitting Monoliths Five Years Ago



Splitting Monoliths Five Years Ago



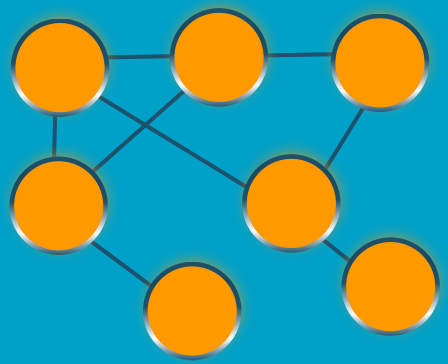




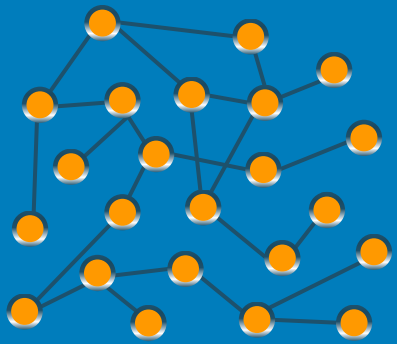
Microservices

Evolution of Business Logic

Monolith

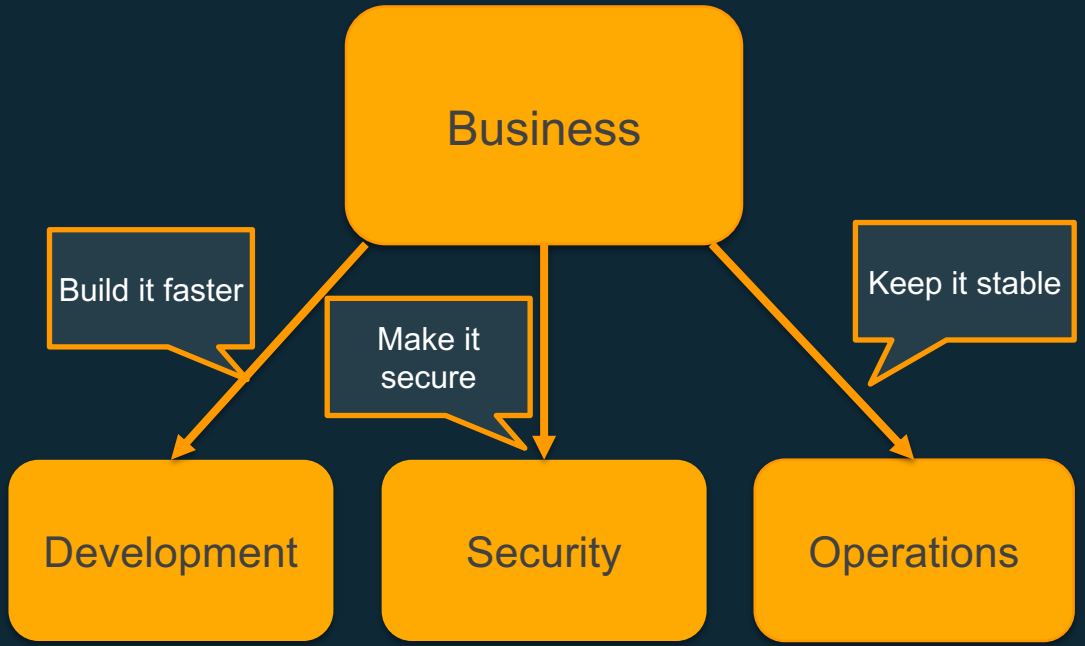


Microservices



Functions

Competing Forces



Access a deep set of cloud security tools

Networking

Virtual Private Cloud
Isolated cloud resources

Web Application Firewall
Filter Malicious Web Traffic

Shield
DDoS protection

Certificate Manager
Provision, manage, and deploy SSL/TSL certificates

Encryption

Key Management Service
Manage creation and control of encryption keys

CloudHSM
Hardware-based key storage

Server-Side Encryption
Flexible data encryption options

Identity & Management

IAM
Manage user access and encryption keys

SAML Federation
SAML 2.0 support to allow on-prem identity integration

Directory Service
Host and manage Microsoft Active Directory

Organizations
Manage settings for multiple accounts

Compliance

Service Catalog
Create and use standardized products

Config
Track resource inventory and changes

CloudTrail
Track user activity and API usage

CloudWatch
Monitor resources and applications

Inspector
Analyze application security

Macie
Discover, Classify & Protect data

aws

Kernel and Host Security

Denial of Service

Containers and Serverless

Image & Instance

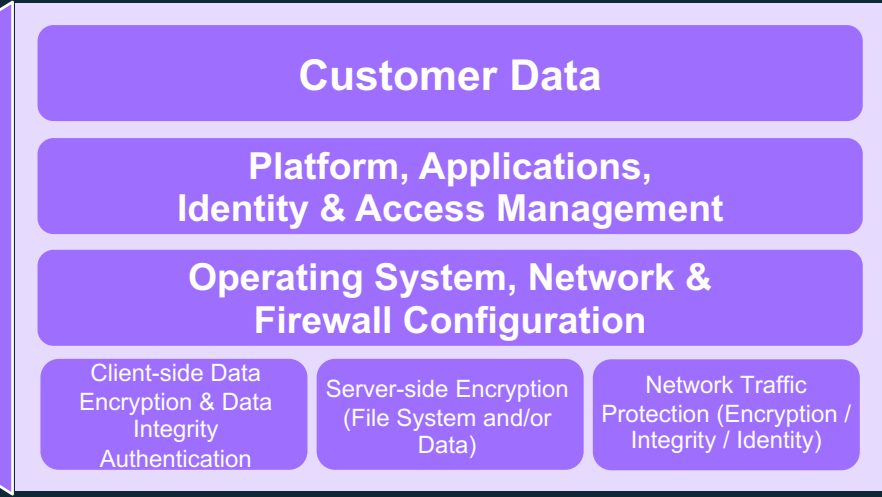
Secrets

Runtime

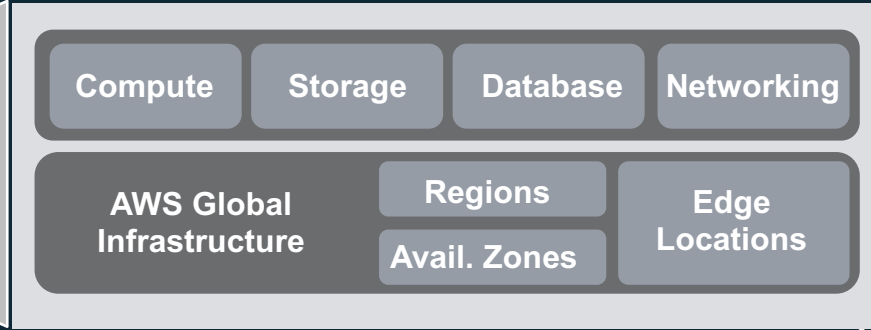
aws

With AWS, Security Is a Shared Responsibility

Customers are responsible for security *'in'* the Cloud



AWS is responsible for security *'of'* the Cloud



VPC Security

Instance Level Firewalls – Security Groups

Subnet Network Rules – NACLs

Intelligent Threat Protection – GuardDuty

Inline Network Security – 3rd Party Marketplace

Select tools that enable automation!

aws

Host-Based Agents

Amazon Inspector

AWS Simple Server Manager

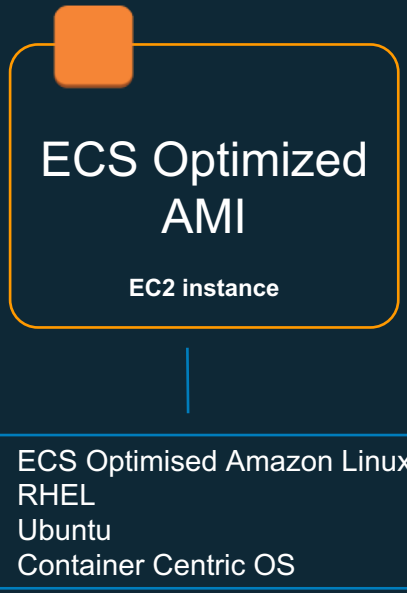
3rd Party Agents

- Anti-virus
- IPS
- DLP

Again - Select tools that enable automation!

aws

Amazon Machine Image Builds



API Gateway

Acts as a front door to the microservices and provides:

- Authentication
- Rate Throttling
- Monitoring
- Versioning

Select an API Gateway that support Automation

Kernel and Host Security

Denial of Service

Containers and Serverless

Image & Instance

Secrets

Runtime

aws

Web Application Firewall

WAFs provide Layer 7 protection for CVEs and OWASP Top 10.

AWS Web Application Firewall

AWS Marketplace

- SaaS WAF Offerings
- Virtual Appliances

Best practices

- Define your resource limits up front
- It’s not just memory and CPU.
- Monitor usage
- Leverage Auto Scaling
- Amazon Shield
- Infrastructure as Code

aws

BUILDING AN ECOSYSTEM

AWS Lambda

ECS

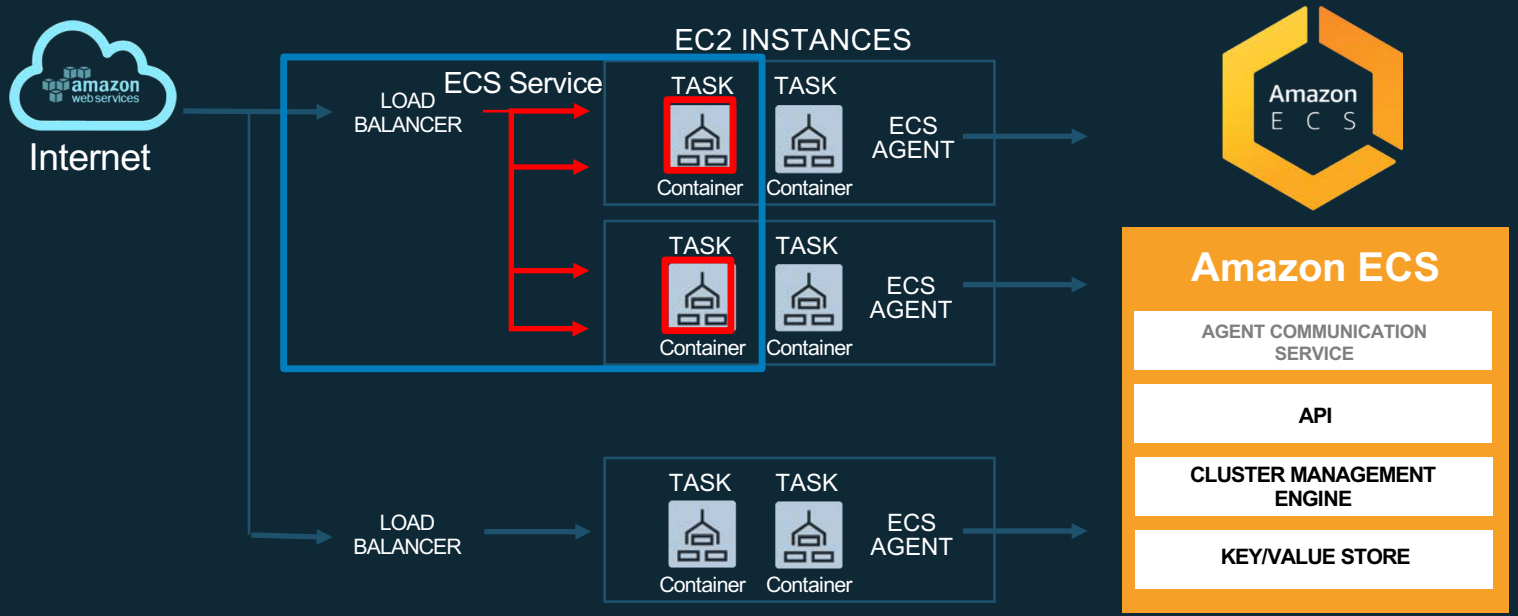
ECR

Fargate

EKS

aws

Amazon ECS—Task & Service



PRODUCTION WORKLOADS ON AWS

AWS VPC networking mode

Advanced task placement

Deep integration with AWS services

ECS CLI

Global footprint

Powerful scheduling engines

Auto scaling

CloudWatch metrics

Load balancers

aws

Amazon EKS

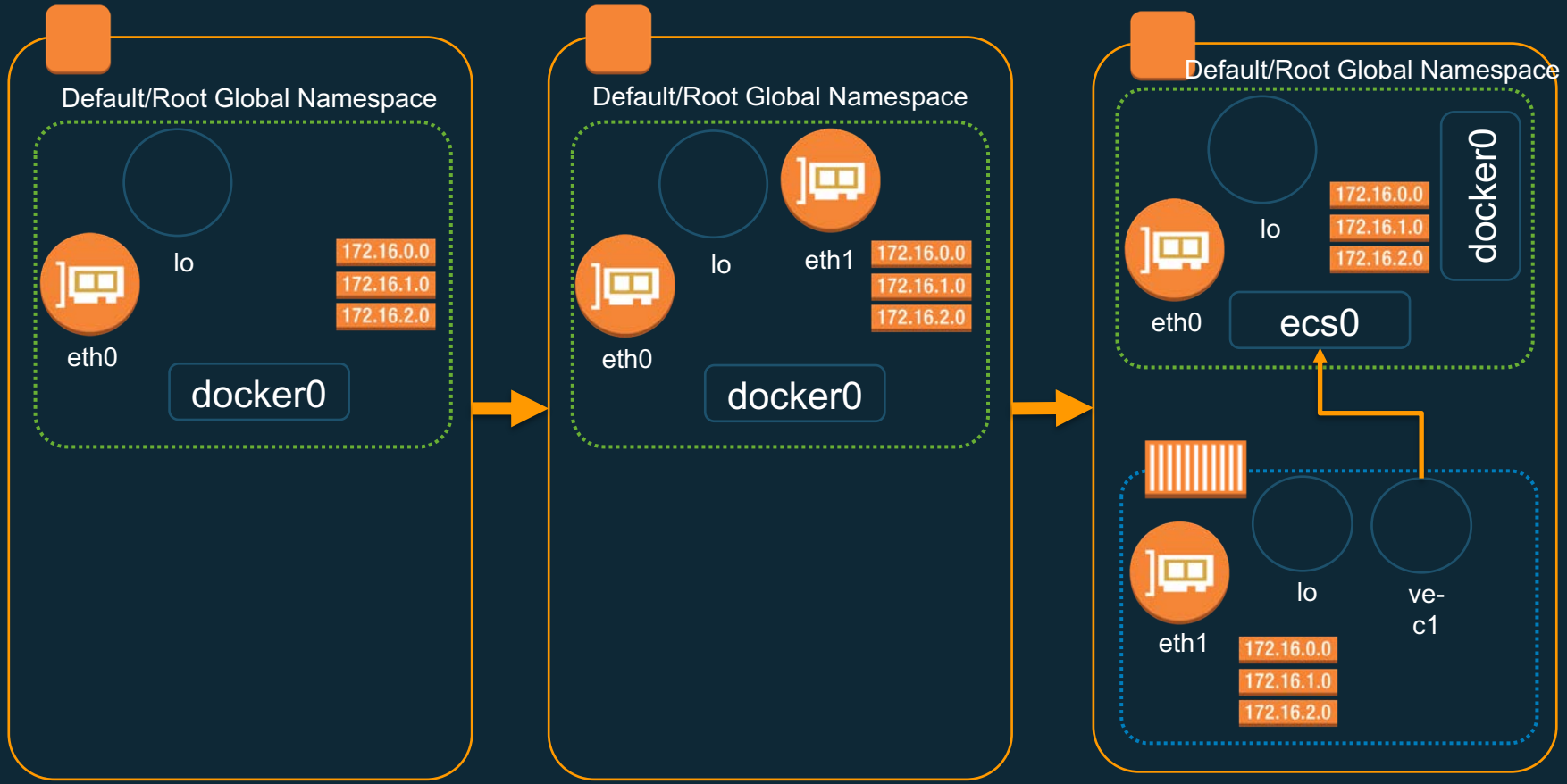
Highly available

Upstream

Production workloads

Integrated with AWS Services

aws



1. Pre ENI Attachment: The primary ENI (eth0) is in the default namespace

2. ENI Attached: The new ENI (eth1) is in the default namespace.

3. ENI Provisioned: The ECS Agent invokes CNI plugins to move the new ENI into a new namespace and configure it with the addresses and routes.

Best practices

- Signing container images (Docker content trust)
- Set filesystems to be read-only (readonlyRootFilesystem)
- Remove setuid/setgid binaries from images (defang)
- Set containers to run as non-root user
- Run Vulnerability Analysis on Container/VM Build in pipeline

aws

aws

Storing secrets in environment variables

```
"environment" : [
    { "name" : "DB_USERNAME", "value" : "admin" },
    { "name" : "DB_PASSWORD", "value" : "Pa$$word123" }
]
```

- Suggested by 12-factor apps (III. Config)
- Environment variables can be seen in too many places
  - Linked containers
  - ECS API calls
  - Docker inspect
- Can’t be deleted

https://12factor.net/

aws

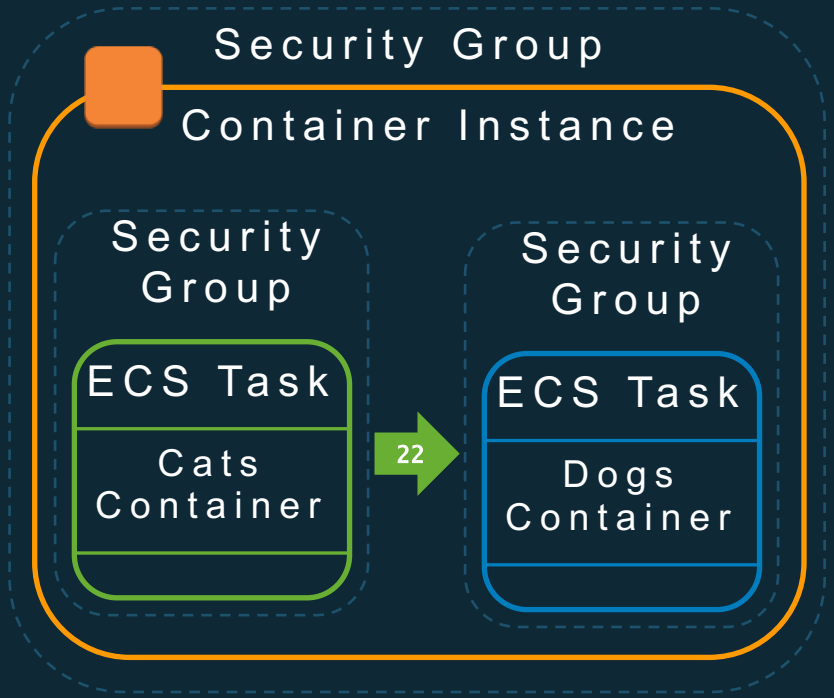
Protecting secrets using IAM roles for tasks

Benefits

- Simplify usage of AWS SDKs in containers
- Credential isolation between tasks/container
- Authorization per task/container
- Auditability in Amazon CloudTrail with taskArn

aws

VPC flow logs and Task ENI




```
630247214269 eni-0123456a 10.0.1.221
10.76.2.101 27039 22 6 5 268 1466491141
1466491200 REJECT OK
```

```
StopTask: {
    task: "52c…"
}
```

```
$ docker diff / inspect
```

AWS Partner Community

Foundation	DevOps	Monitoring and Logging	Security	Networking
CoreOS	shippable	circleci	aqua	linkerd
docker	CloudBees The Enterprise Jenkins Company	DATADOG	Twistlock	TiGERA CLOUD NETWORKS, SECURED
MESOSPHERE	GitLab	sysdig	NeuVector	weaveworks
	ATLASSIAN	New Relic.		

aws