

The background features a dark blue gradient on the left, transitioning into large, overlapping, semi-transparent shapes in shades of purple, magenta, and orange on the right. These shapes create a sense of depth and movement, with the orange shape being the most prominent in the foreground.

AWS re:Invent

NOV. 27 – DEC. 1, 2023 | LAS VEGAS, NV

CON325

Securing containerized workloads on Amazon ECS and AWS Fargate

Spiros Tsitsonis

(he/him)

Sr. Product Manager Technical
Services

Amazon Elastic Container Services

Yumeng Xie

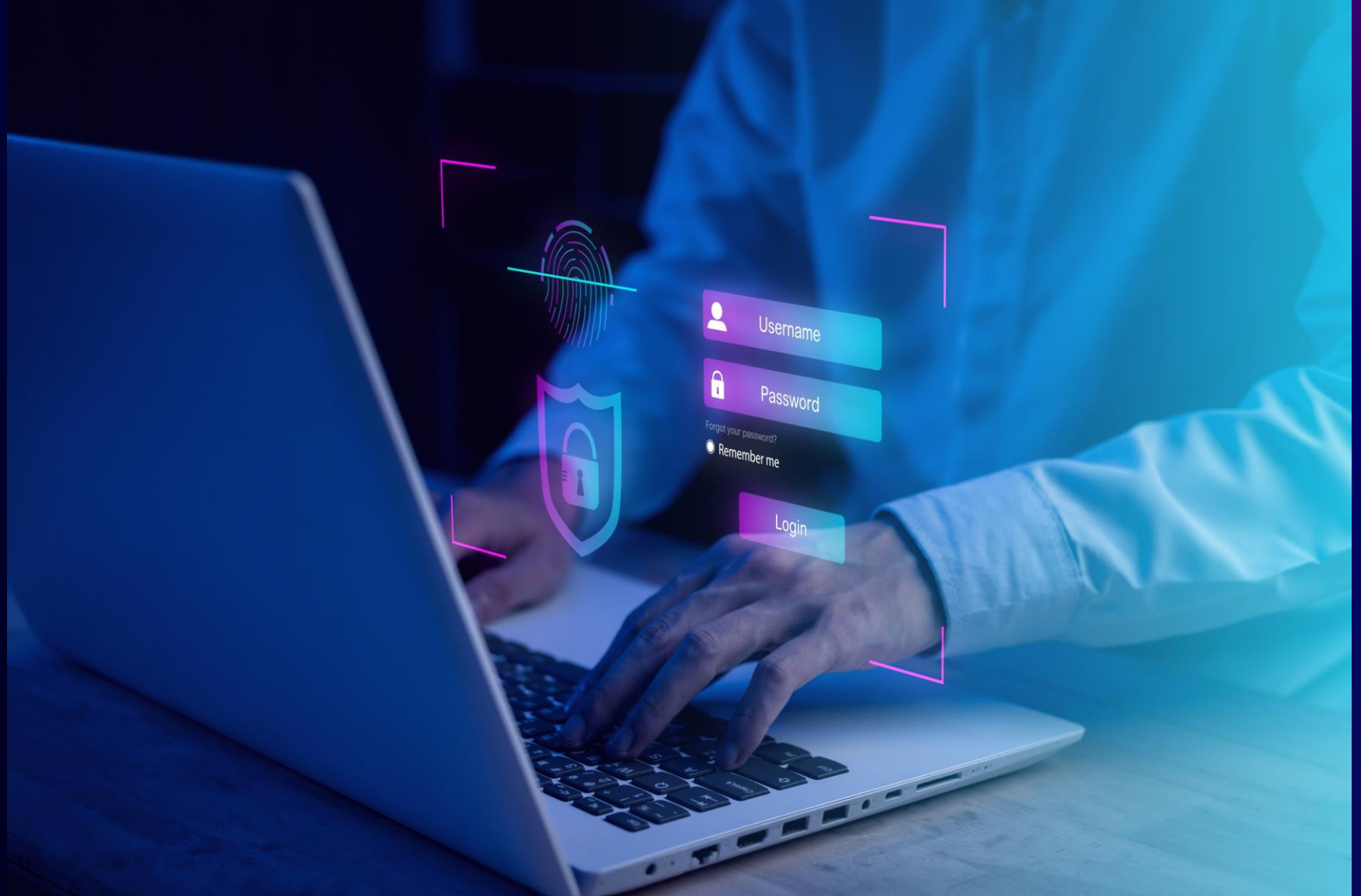
(she/her)

Sr. Software Development Engineer
Amazon Elastic Container Services



© 2023, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Small Misses...



... can lead to unauthorized application behavior



Compliance is important to your business...



...and trust even more so



Container Security in Amazon ECS & AWS Fargate

The ECS Security Model & Enhanced Security Features

Amazon GuardDuty Runtime Monitoring for ECS & Fargate

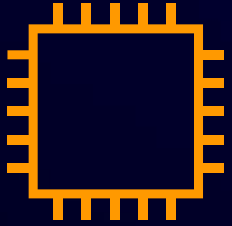
Demo

The ECS Security Model & Enhanced Features



ECS Security Model

Inherent Security at the host instance or task level



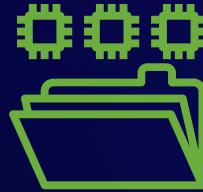
Hardware
virtualization

isolated compute



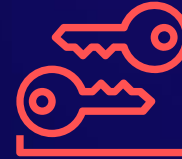
Network
isolation

dedicated ENIs



Storage
isolation

dedicated storage



Credentials
isolation

Isolated long-term
credentials

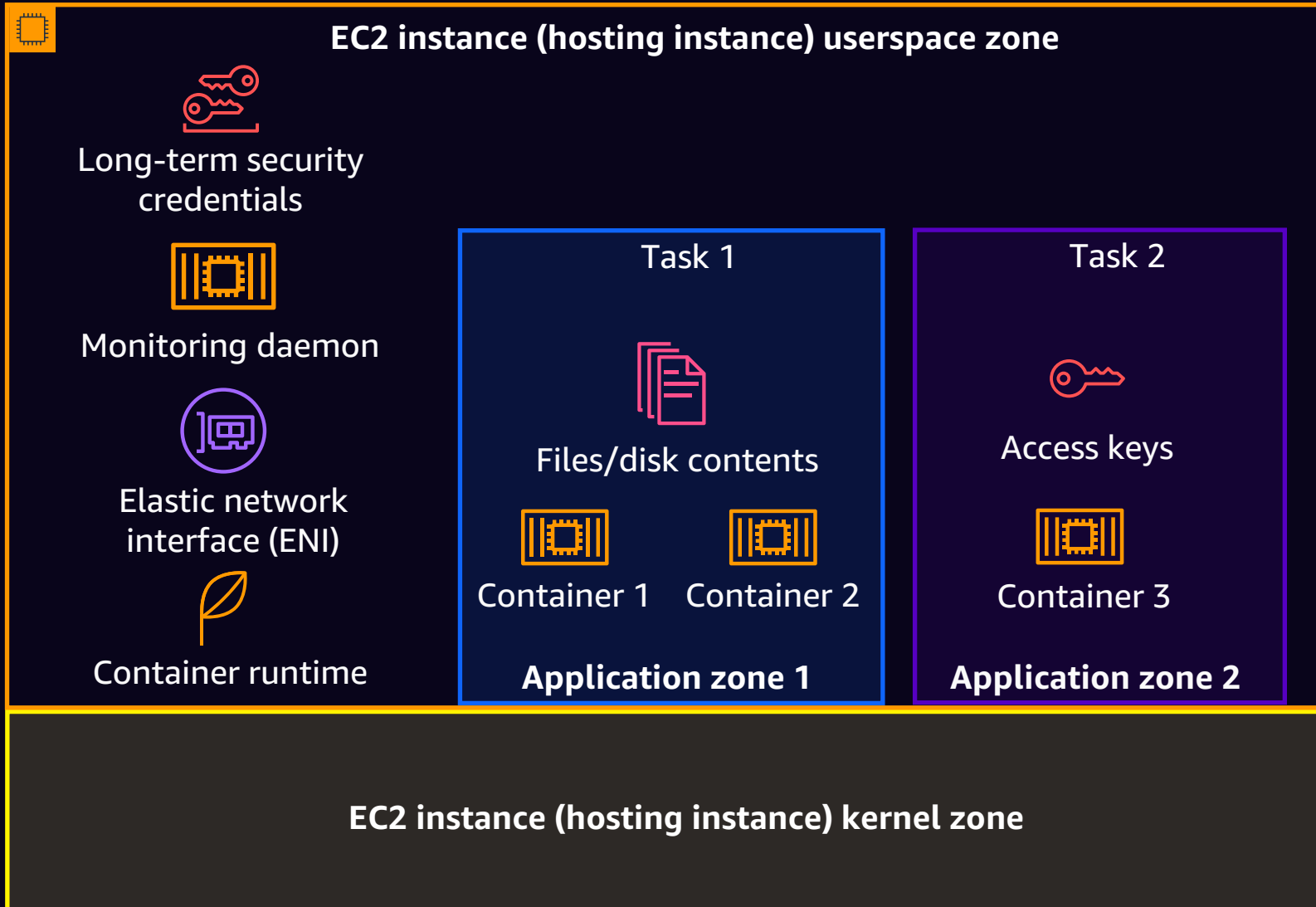


Hands-off
patching

Infrastructure always
patched

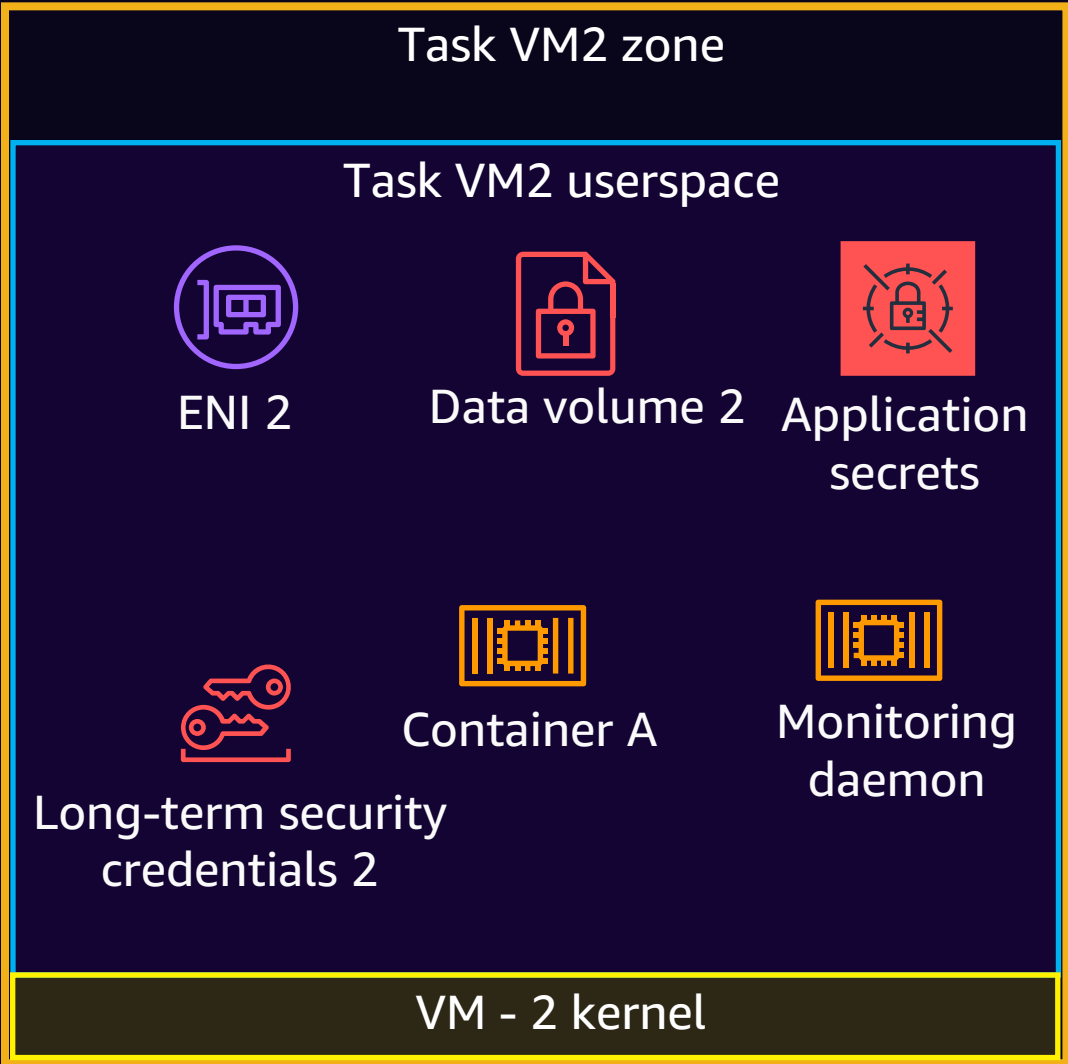
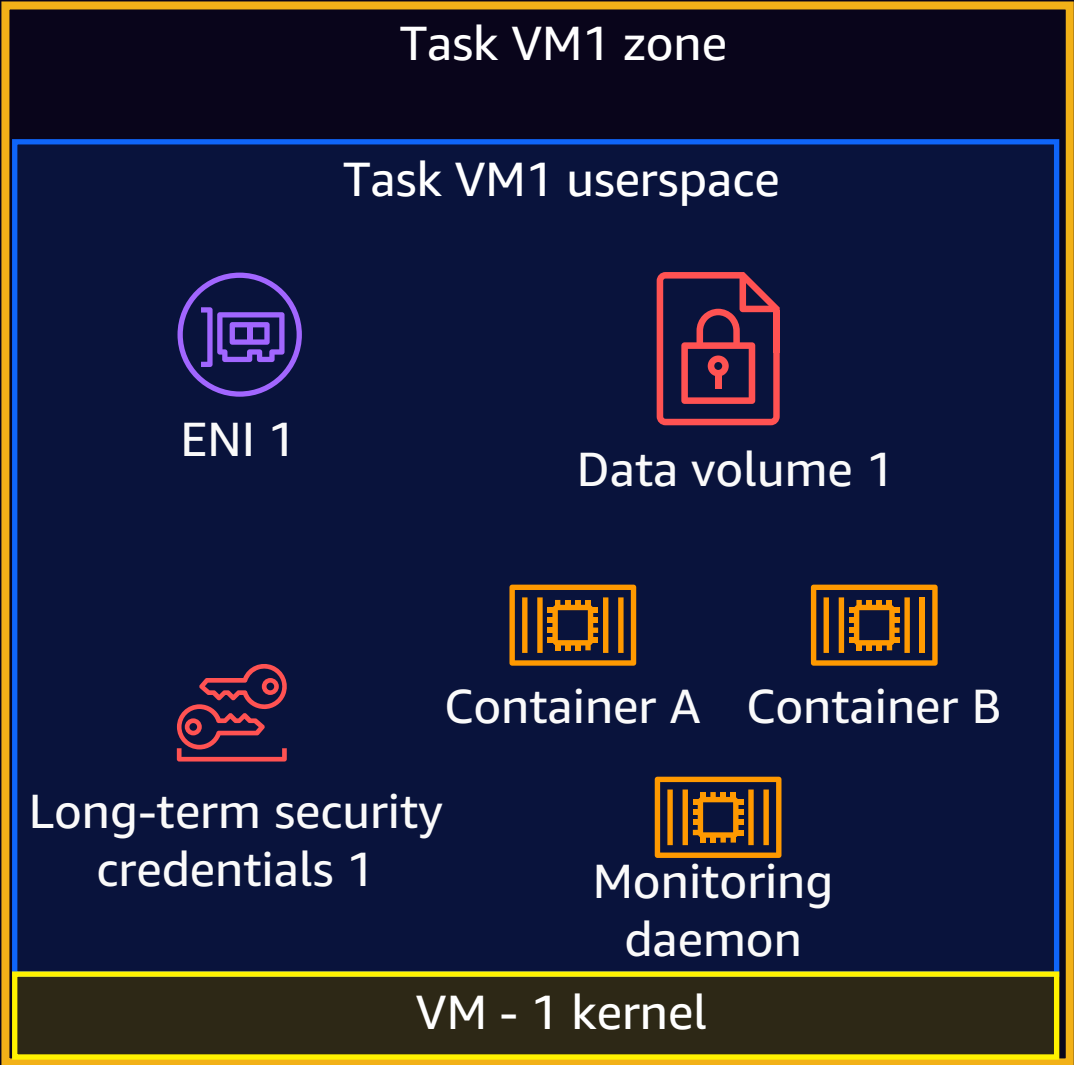
ECS Trust boundaries

Amazon EC2 compute

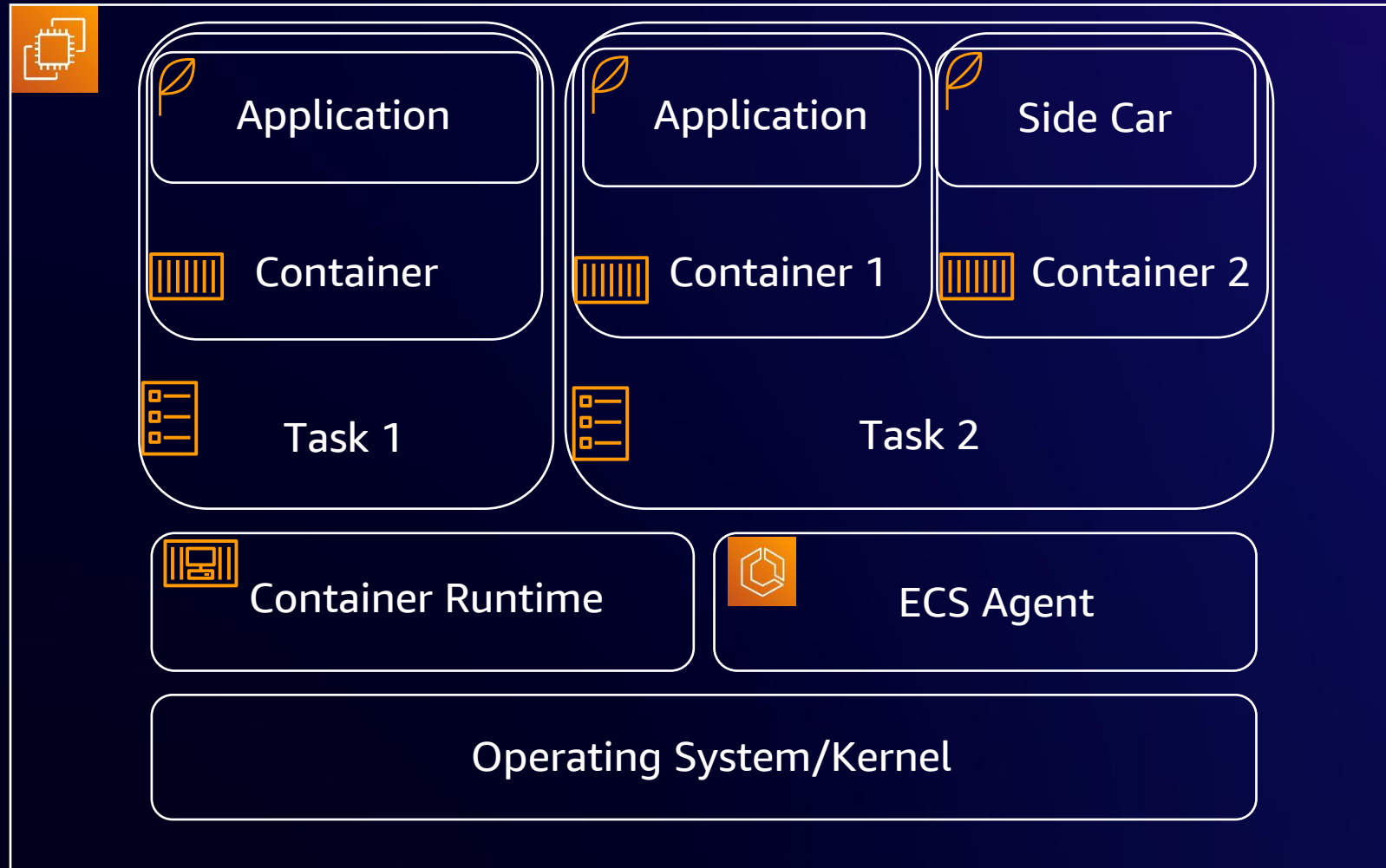


ECS Trust boundaries

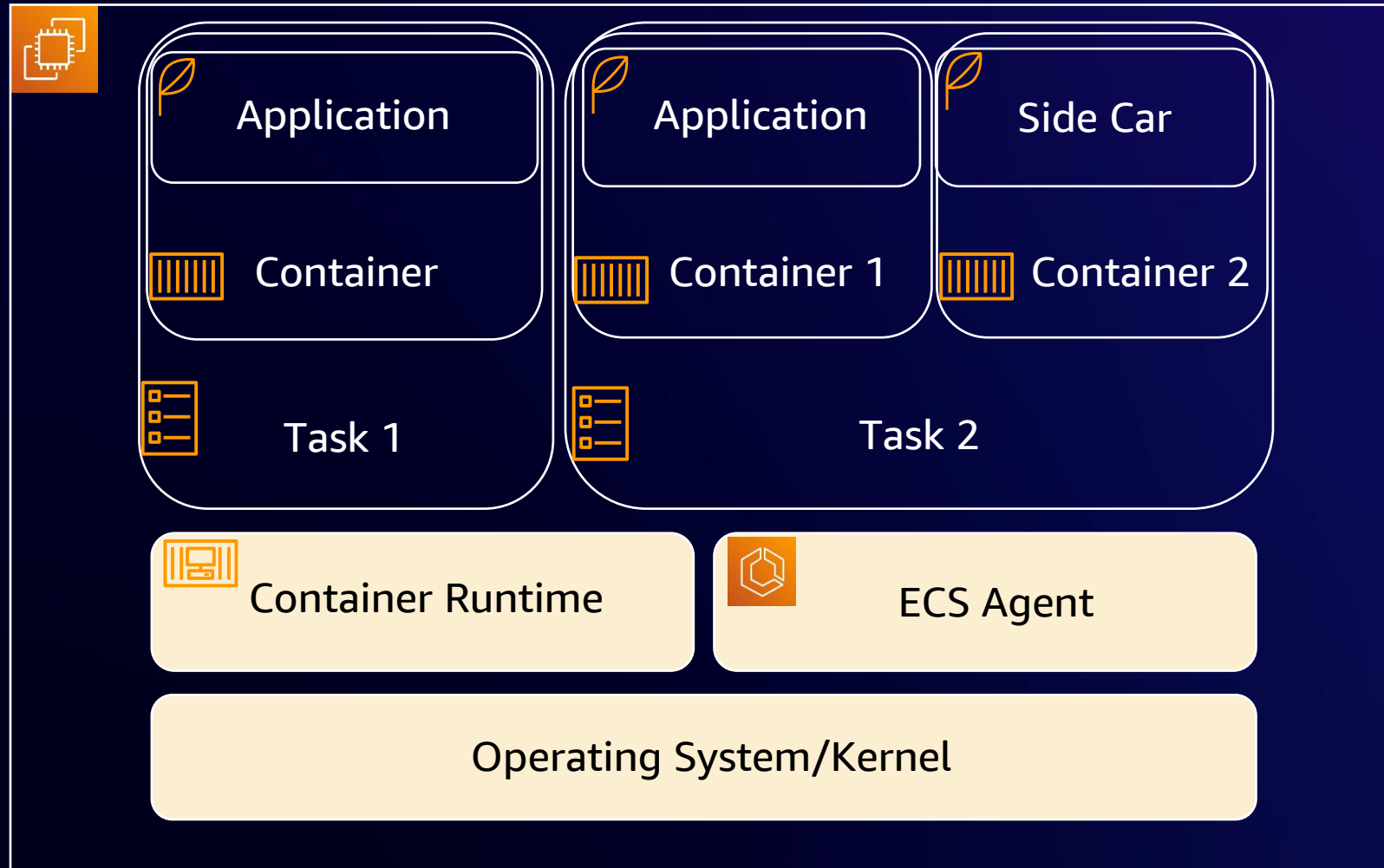
Fargate compute



ECS Infrastructure

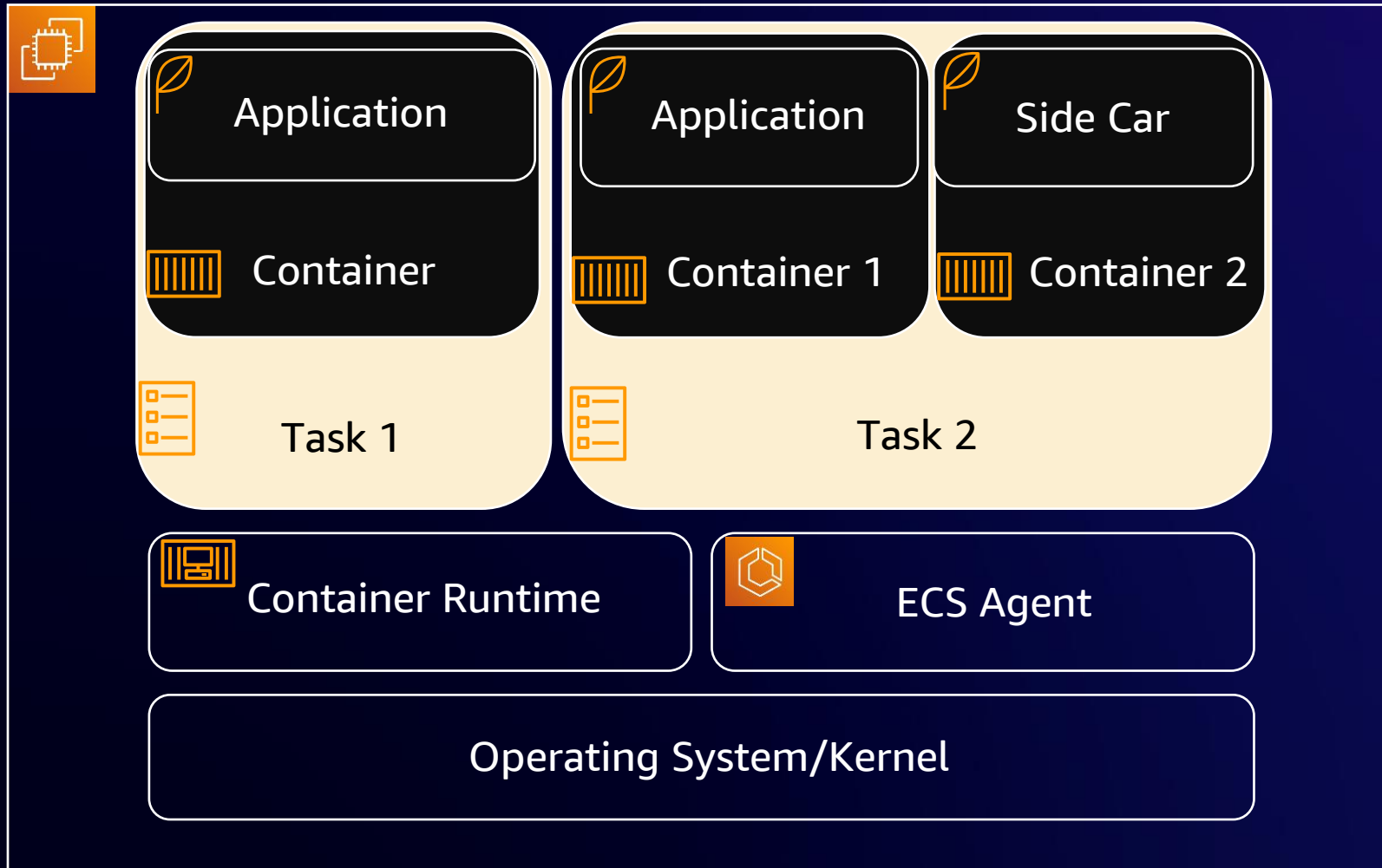


Compute/Infrastructure Security



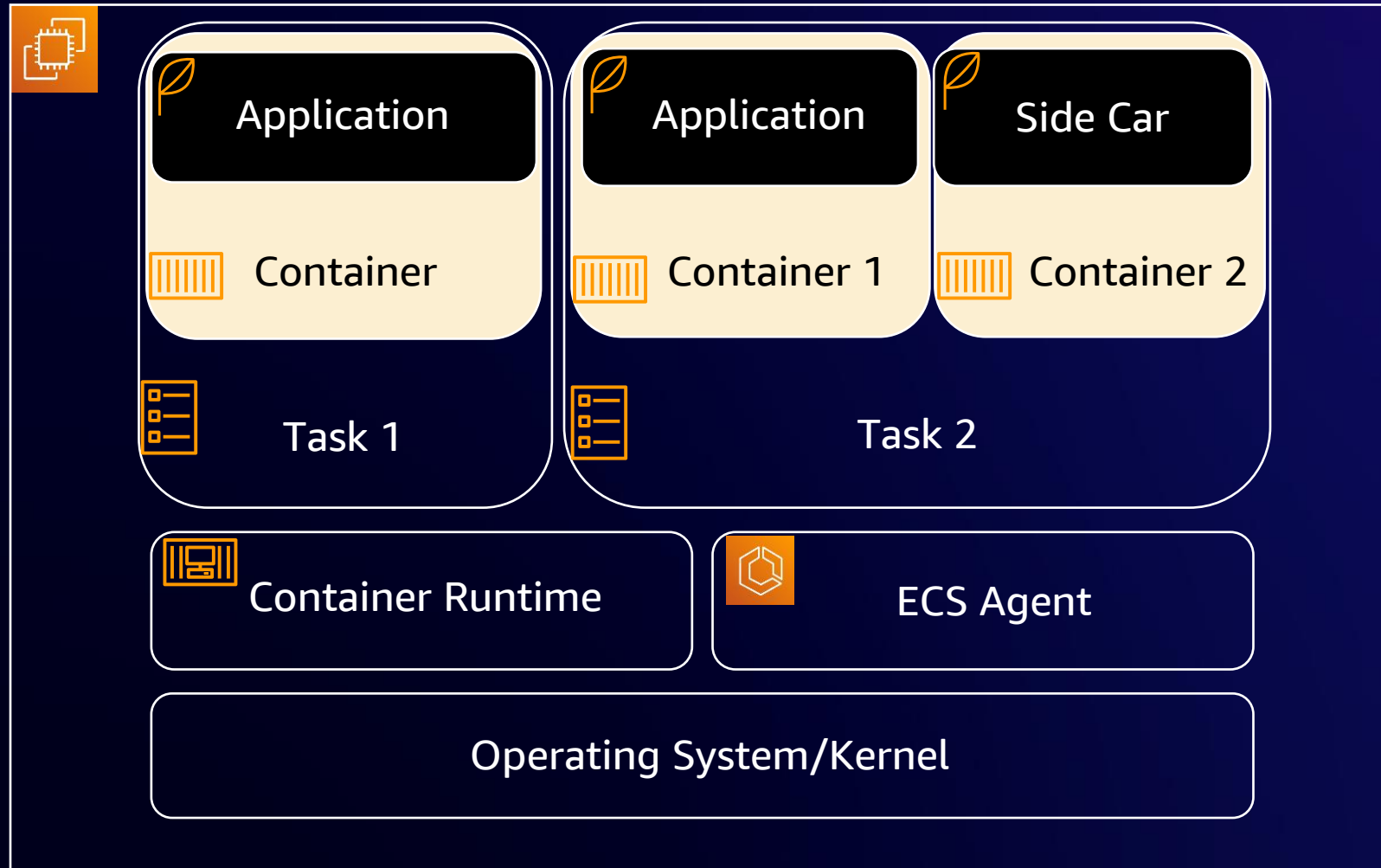
- Compute Separation
- Infrastructure Patching
- Security Groups, Network ACLs, IAM Role for Container Instances
- AWS PrivateLink

Task Security



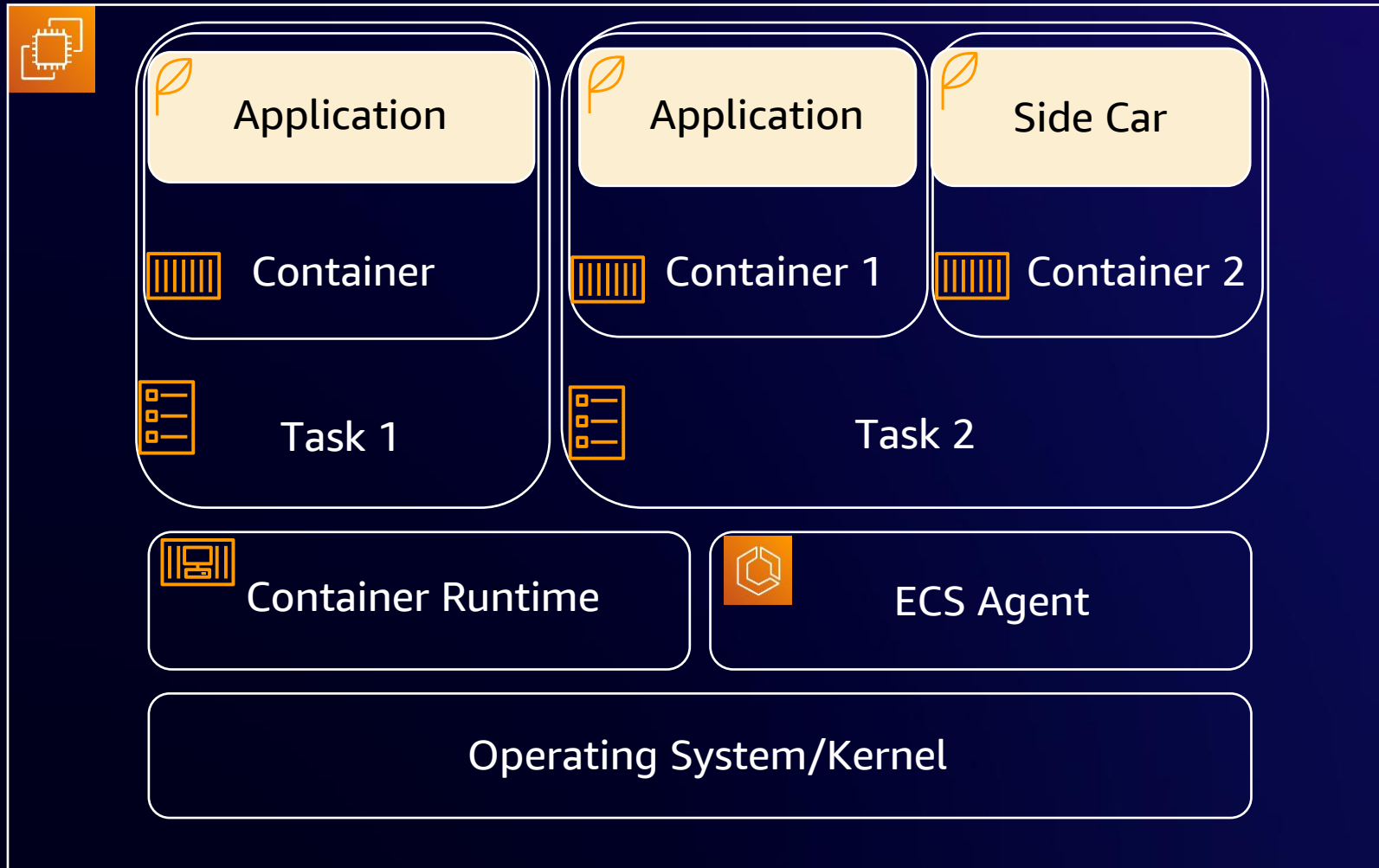
- IAM Role for Tasks
- Task Execution Role
- Dedicated ENI for Tasks

Container Security



- Container Secrets
- Linux Kernel capabilities
- Privileged Mode
- Ulimits
- Image Scanning
- Image Pruning

Application Security



- Transport Layer Security (TLS)
- Tag-based Access Control
- Log Routing
- Metrics Reporting
- Audit & Tracing
- Debugging Options

Introducing Amazon GuardDuty Runtime Monitoring Support for Amazon ECS & AWS Fargate



Amazon GuardDuty ECS Runtime Monitoring

RUNTIME THREAT DETECTION FOR AMAZON ECS



Fully managed runtime threat detection for serverless containers, removing organizational complexity



Uniquely detect entire attack chains of events with machine learning and integrated threat intelligence

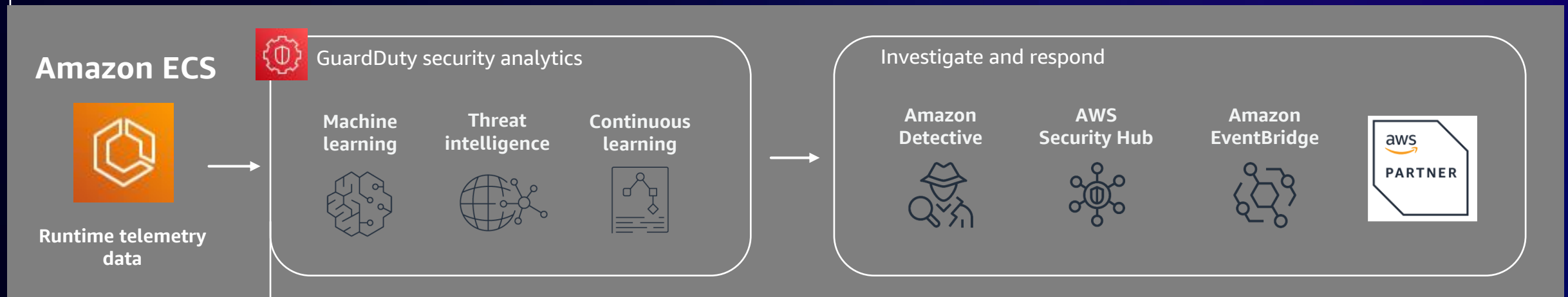


Accurately detect and respond to threats early—before they escalate to broader business-impacting breaches

Get the coverage and visibility required to protect your container workloads from an evolving threat landscape

GuardDuty ECS Runtime Monitoring

GuardDuty begins scanning for malicious activity as soon as a new Amazon ECS compute capacity is discovered.



GuardDuty then identifies and prioritizes threats to your Amazon ECS environment and sends findings to downstream security and partner services for investigation and response.

GuardDuty Monitoring on Amazon ECS

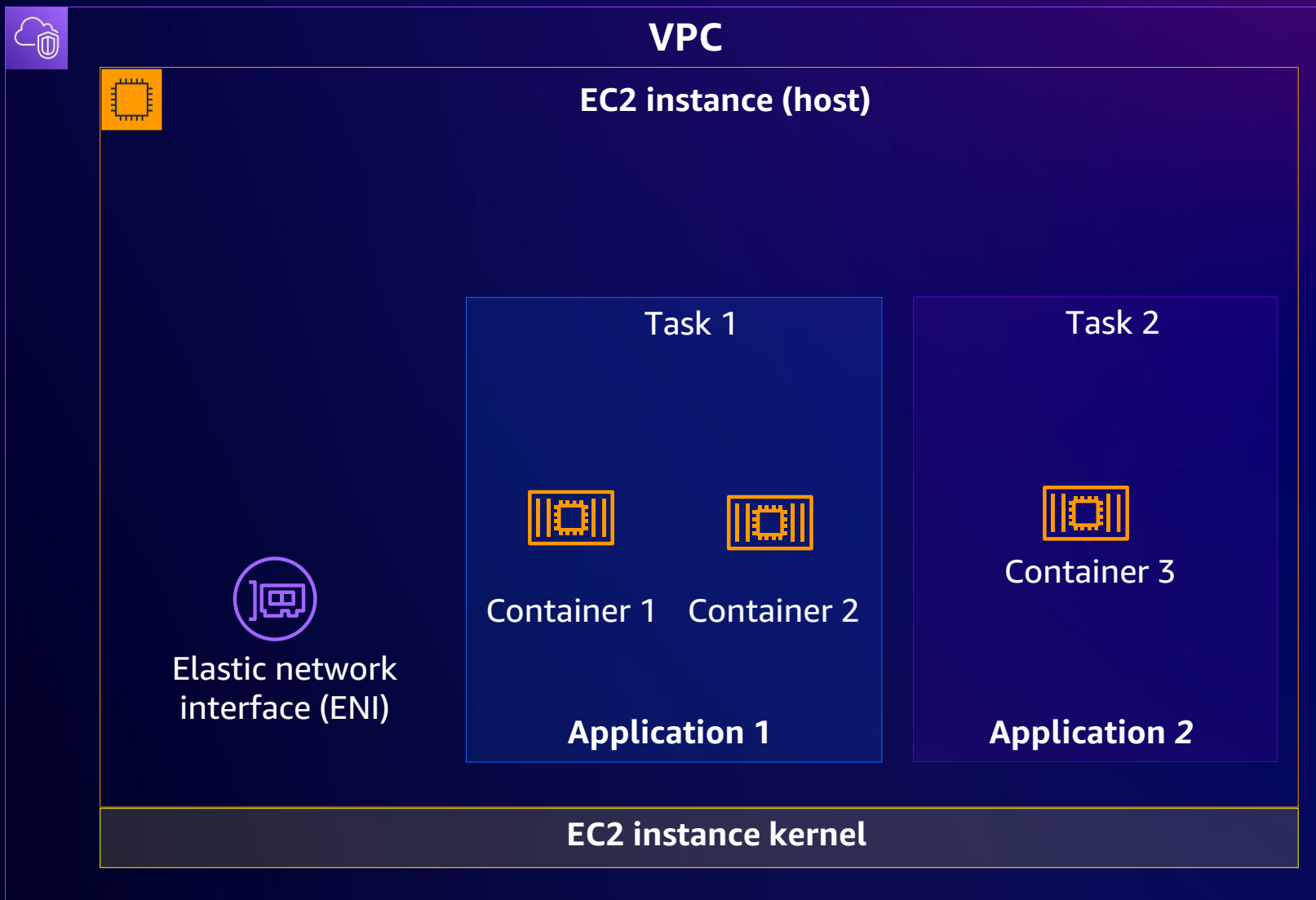
AMAZON EC2



GuardDuty Runtime Monitoring Agent



AWS Systems Manager



GuardDuty Monitoring on Amazon ECS

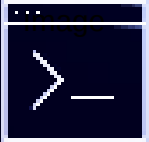
AMAZON EC2



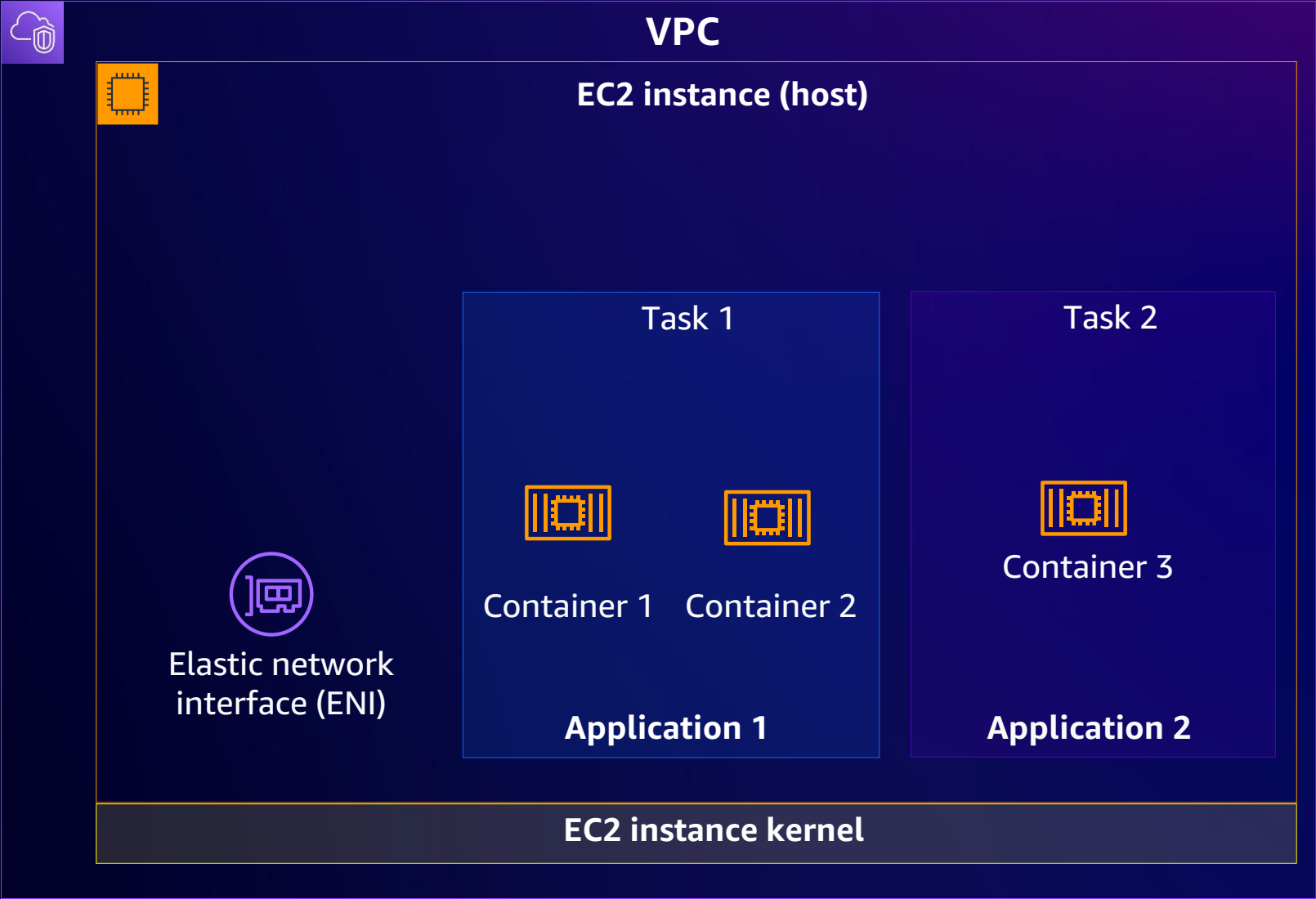
Amazon S3



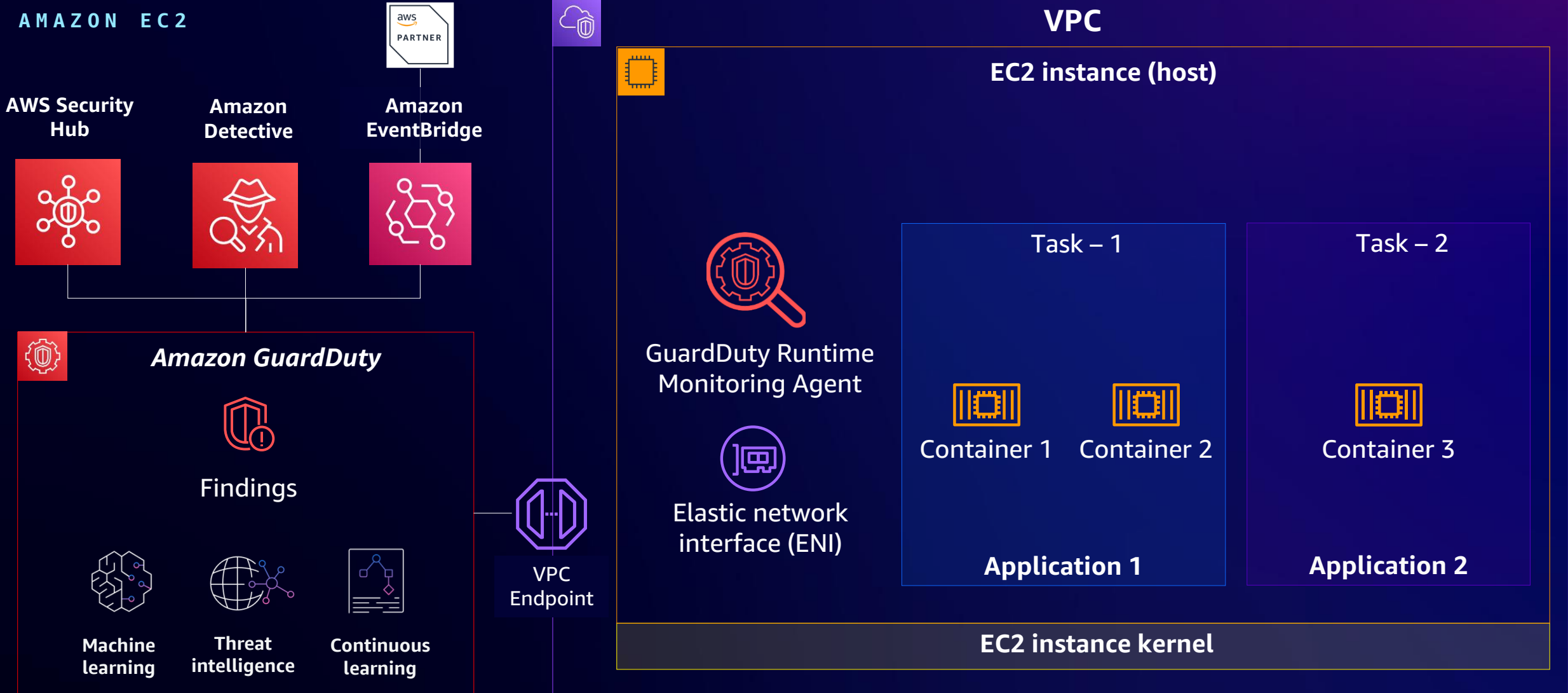
GuardDuty Runtime Monitoring Agent



Linux CLI



GuardDuty Monitoring on Amazon ECS



GuardDuty Monitoring on Amazon ECS

AWS FARGATE

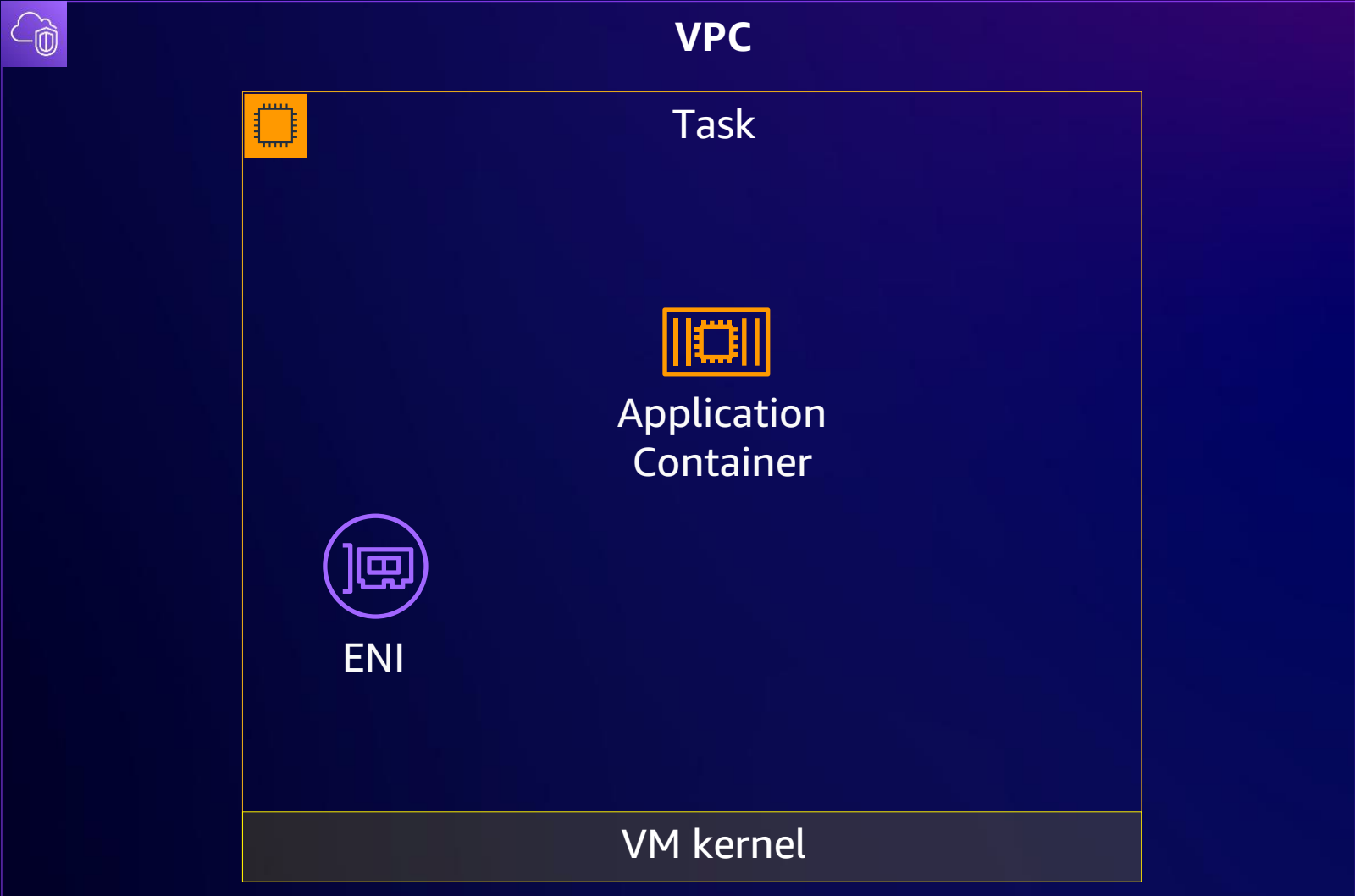


Amazon ECR



GuardDuty runtime monitoring agent

Task Execution Role to allow Fargate to pull image



GuardDuty Monitoring on Amazon ECS

AWS FARGATE



AWS Security Hub



Amazon Detective



Amazon EventBridge



Amazon GuardDuty



Findings



Machine learning



Threat intelligence



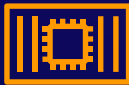
Continuous learning



VPC



Task



Application Container



ENI



GuardDuty Runtime Monitoring Agent



VPC Endpoint

VM kernel



Demo



Use Case 1:

Platform operators manually opt-in ECS clusters on Fargate

- Prerequisites
- Resource Monitoring
- GuardDuty Runtime Monitoring Agent Deployment

Use Case 2:

Platform operators install GuardDuty Agent on ECS on EC2

- GuardDuty Runtime Monitoring Agent Installation
- Security Findings
- Coverage Dashboard

ONE RUNTIME MONITORING SOLUTION ACROSS YOUR COMPUTE ON AWS



Amazon ECS and AWS Fargate at re:Invent 2023

Breakout Sessions

Session	Topic
CON315	Advancements in storage options for deploying data-aware apps at scale
CON401	Deep dive into Amazon ECS resilience and availability
CON318	Boosting efficiency: How to realize 70% cost reduction with AWS Fargate

Builders' Sessions

Session	Topic
CON301-R2 CON301-R3	Build cost-optimized workloads on Amazon ECS
CON324-R3	Architecting Amazon ECS workloads for data protection & compliance

AWS Modern Application and Open Source Zone

BOOTH #1390

Located in the Developer Solutions Zone

Booth #1390

Stop by and network with AWS experts, ask questions, watch demos, collect SWAG, play games, whiteboard out architecture diagrams, and relax with good food and drinks

Expo hours

Tuesday, November 28

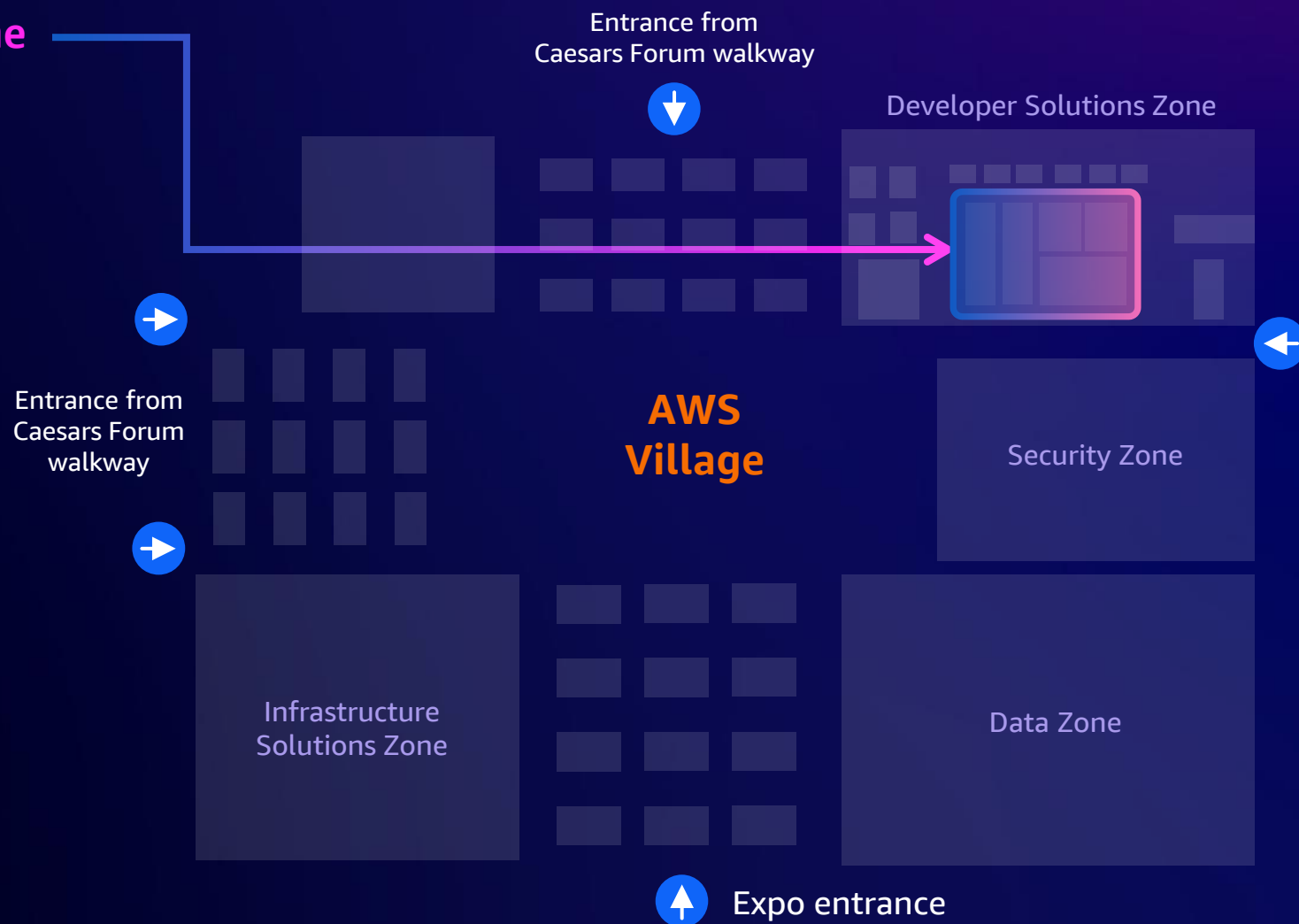
10:00 AM – 6:00 PM

Wednesday, November 29

10:00 AM – 6:00 PM

Thursday, November 30

10:00 AM – 4:00 PM



Thank you!



Please complete the session survey in the mobile app

Spiros Tsitsonis
spirosts@amazon.com

Yumeng Xie
yumex@amazon.com

