ONLINE TECH TALK

Enhanced threat detection for Amazon EKS with Amazon GuardDuty

Amit Megiddo (He/Him)

Principal Product Manager
AWS

Muhammad Wasiq (He/Him)

Principal Security Engineer
AWS

What is Amazon GuardDuty?

Amazon GuardDuty is a threat detection service that uses **machine learning**, anomaly detection, and **integrated threat intelligence** to identify and prioritize potential threats to your AWS environment.

Tens of thousands of customers across industries and geographies

Used by over 90% of the top-2000 AWS customers

Protects hundreds of millions of Amazon EC2 instances

Analyzes tens of billions of events per minute

GuardDuty overview

Single-click organization-wide activation

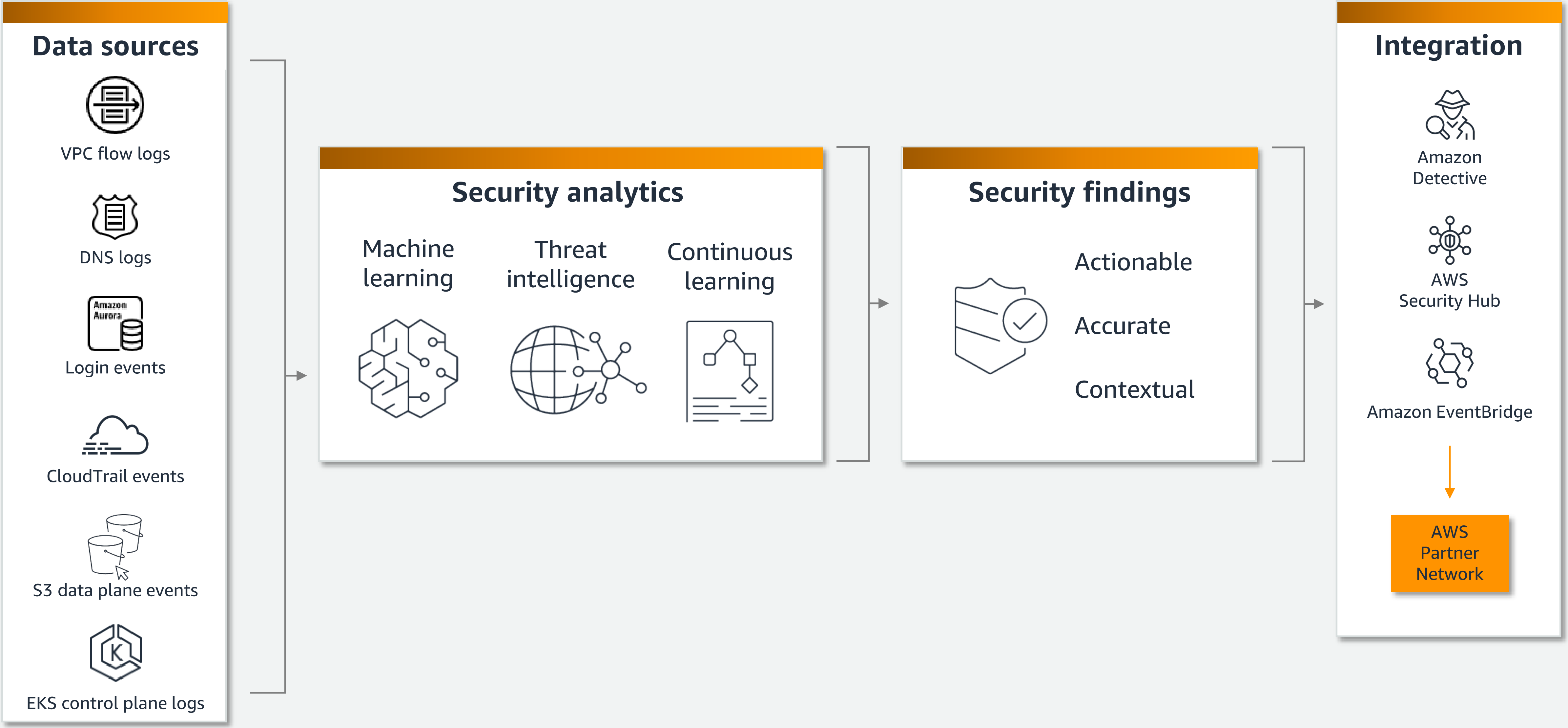
Continuous monitoring of AWS accounts and resources

ML to detect evasive attack techniques

Threat intelligence from AWS and leading third-parties

Enterprise-wide consolidation & management

How GuardDuty works



Data sources

- VPC flow logs
- DNS logs
- Login events
- CloudTrail events
- S3 data plane events
- EKS control plane logs

Security analytics

- Machine learning
- Threat intelligence
- Continuous learning

Security findings

- Actionable
- Accurate
- Contextual

Integration

- Amazon Detective
- AWS Security Hub
- Amazon EventBridge
- AWS Partner Network

Introducing Amazon GuardDuty EKS Runtime Monitoring

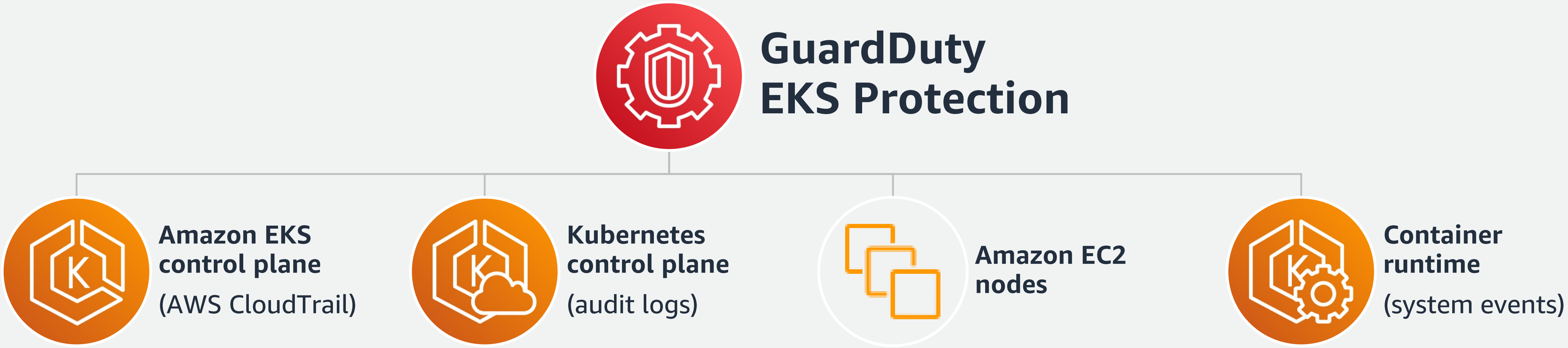
Protect your Amazon EKS workloads with a new GuardDuty security agent that adds visibility into individual Kubernetes **container runtime activities**, such as file access, process execution, and network connections.

Continuously monitor all Amazon EKS clusters across your organization with a few steps in the GuardDuty console.

Over two dozen new threat detections leveraging high fidelity system-level events, tailored for known container attack techniques, and providing container-level context.

Detect threats at each layer of Kubernetes deployment on Amazon EKS

VPC Flow Logs and DNS logs continue to be monitored: defense in depth



GuardDuty EKS Protection

Amazon EKS control plane (AWS CloudTrail)

Kubernetes control plane (audit logs)

Amazon EC2 nodes

Container runtime (system events)

Leveraging GuardDuty threat intelligence to detect potentially compromised Amazon EKS containers

Partner feeds: CrowdStrike and Proofpoint

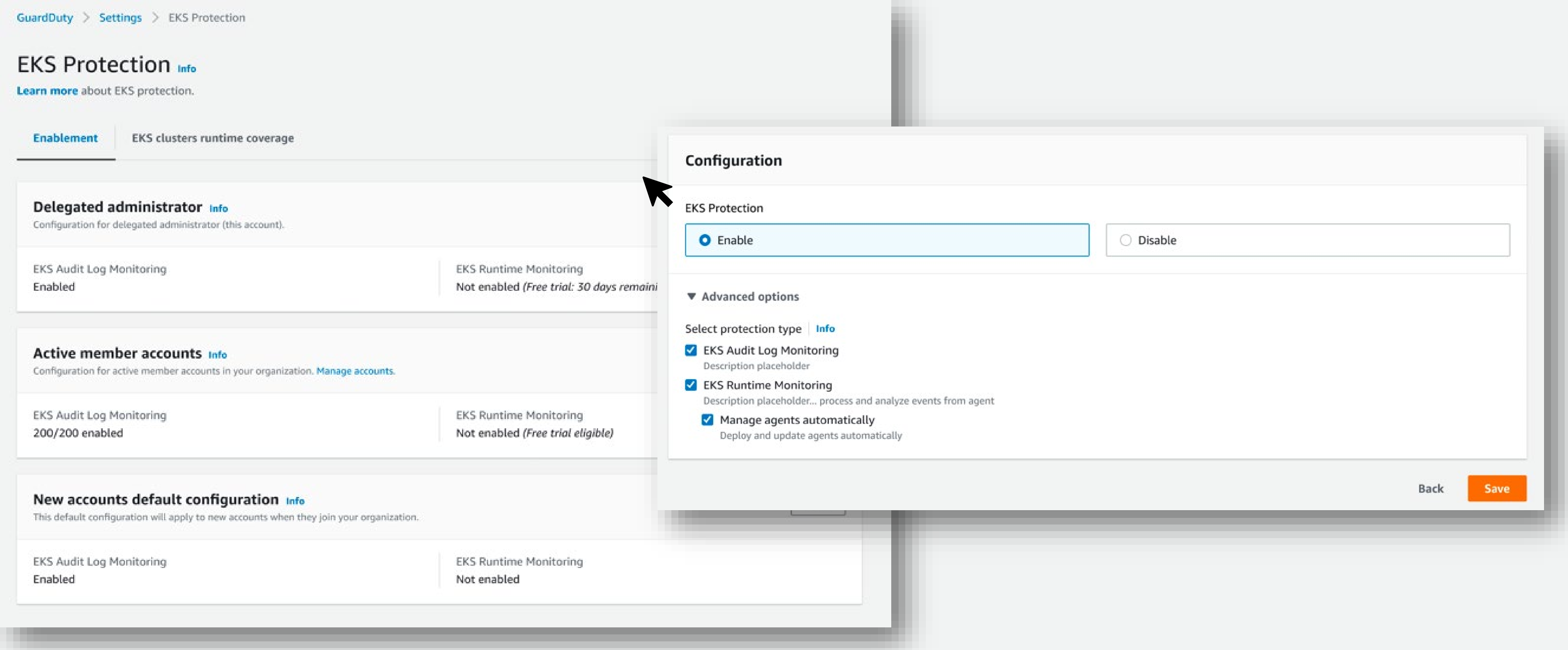
Amazon Security research: top nation-state and crime group actors

Customer-provided and third-party integration

Cryptocurrency pools

Domain reputation machine learning models

Easily achieve organization-wide coverage



GuardDuty > Settings > EKS Protection

EKS Protection Info

Learn more about EKS protection.

Enablement | EKS clusters runtime coverage

Delegated administrator Info

Configuration for delegated administrator (this account).

EKS Audit Log Monitoring: Enabled

EKS Runtime Monitoring: Not enabled *(Free trial: 30 days remaini*

Active member accounts Info

Configuration for active member accounts in your organization. Manage accounts.

EKS Audit Log Monitoring: 200/200 enabled

EKS Runtime Monitoring: Not enabled *(Free trial eligible)*

New accounts default configuration Info

This default configuration will apply to new accounts when they join your organization.

EKS Audit Log Monitoring: Enabled

EKS Runtime Monitoring: Not enabled

Configuration

EKS Protection

● Enable ○ Disable

▼ Advanced options

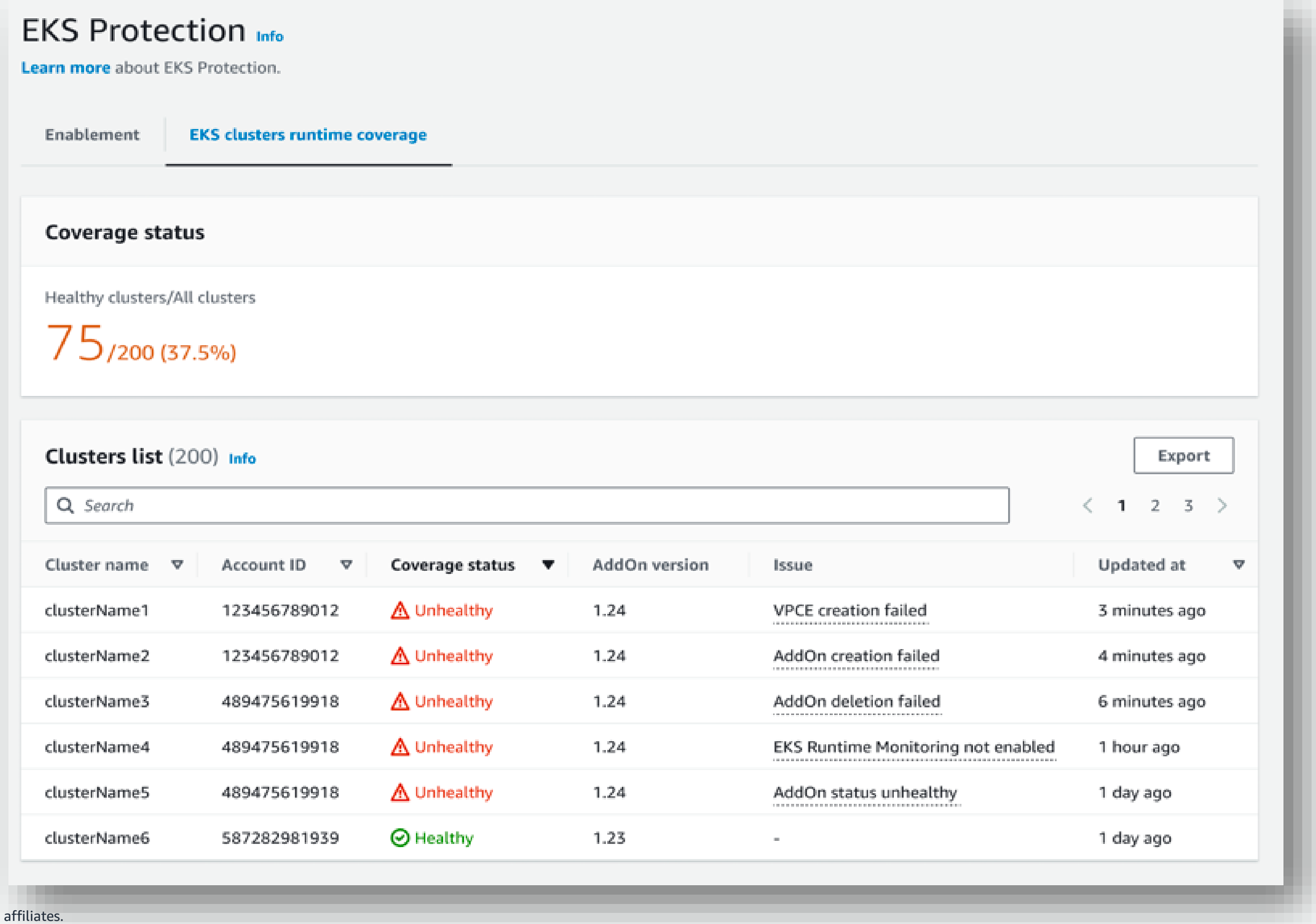
Select protection type | Info

☑ EKS Audit Log Monitoring
Description placeholder

☑ EKS Runtime Monitoring
Description placeholder... process and analyze events from agent

☑ Manage agents automatically
Deploy and update agents automatically

… and identify potential coverage gaps



EKS Protection Info

Learn more about EKS Protection.

Coverage status

Healthy clusters/All clusters

75/200 (37.5%)

Clusters list (200) Info

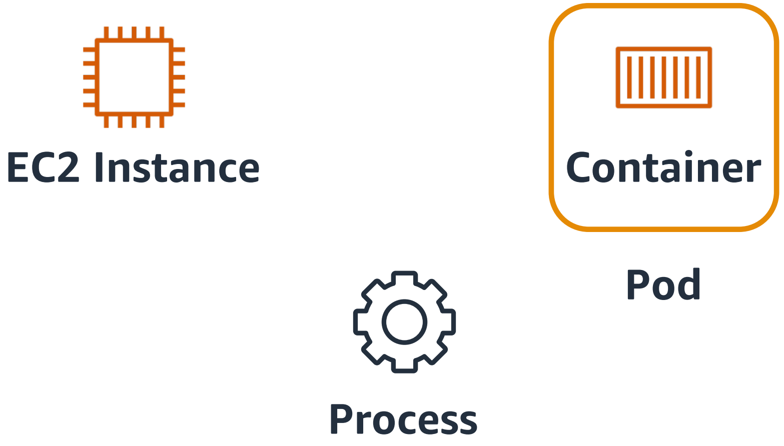
Cluster name	Account ID	Coverage status	AddOn version	Issue	Updated at
clusterName1	123456789012	⚠ Unhealthy	1.24	VPCE creation failed	3 minutes ago
clusterName2	123456789012	⚠ Unhealthy	1.24	AddOn creation failed	4 minutes ago
clusterName3	489475619918	⚠ Unhealthy	1.24	AddOn deletion failed	6 minutes ago
clusterName4	489475619918	⚠ Unhealthy	1.24	EKS Runtime Monitoring not enabled	1 hour ago
clusterName5	489475619918	⚠ Unhealthy	1.24	AddOn status unhealthy	1 day ago
clusterName6	587282981939	✓ Healthy	1.23	-	1 day ago

Rich container and process context

Customers demand container-level details in detections

EKS Runtime Monitoring finding

`CryptoCurrency:Runtime/BitcoinTool.B`



EC2 Instance

Container

Pod

Process

VPC Flow Logs finding

`CryptoCurrency:EC2/BitcoinTool.B`

EC2 Instance

Rich container and process context

Container details

- Container ID
- Container image
- Container name

Kubernetes pod details

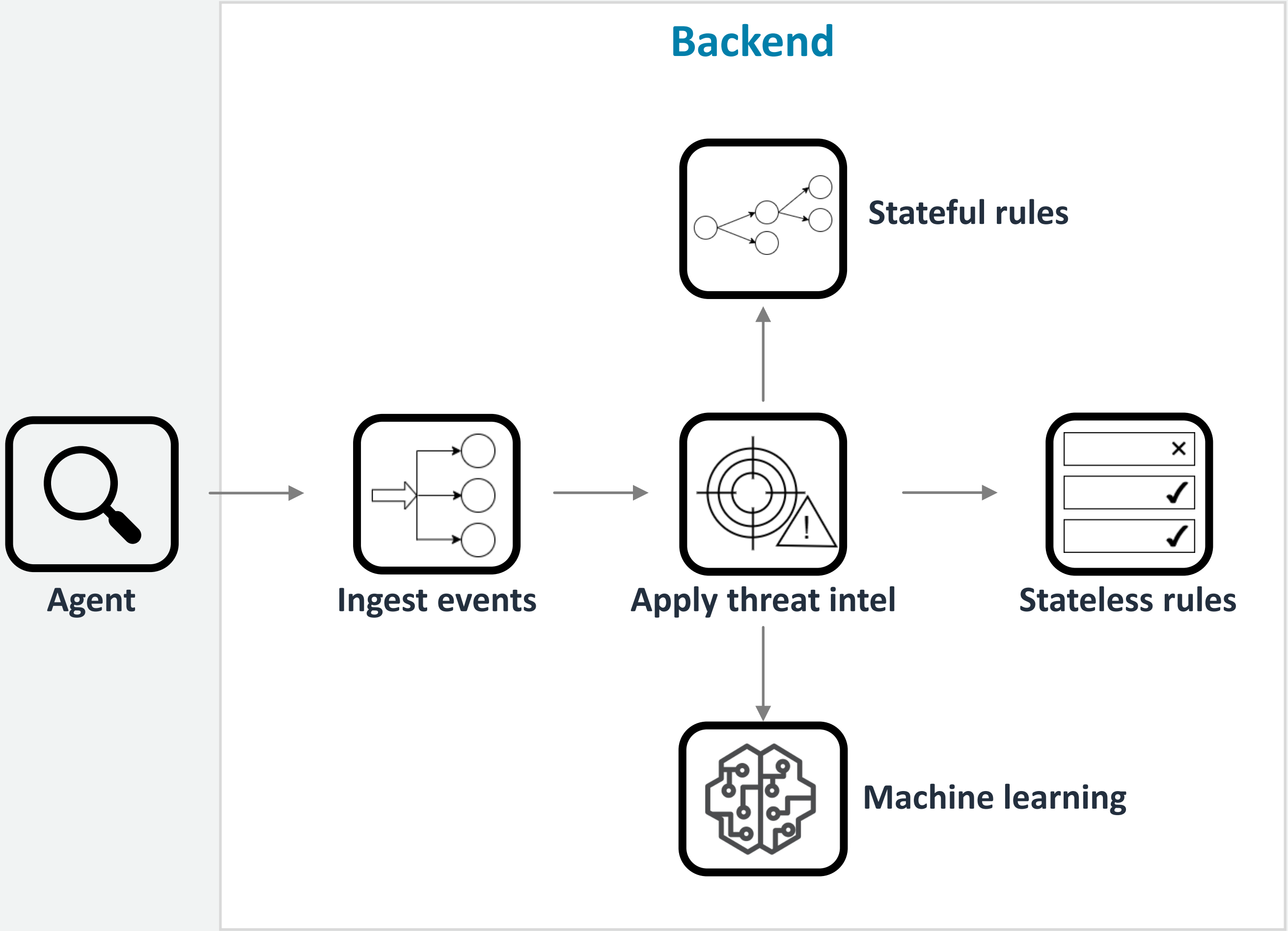
- Pod ID
- Pod name
- Pod namespace

Process details

- Process ID
- Executable path
- Parent PID
- Executable SHA-256 hash
- User ID
- Effective user ID
- Process lineage (all ancestors of the process)

High-level architecture

- Agent collects and sends events
- GuardDuty backend processes events



Runtime protection: Threat intel-based detections

IP-based

- `CryptoCurrency:Runtime/BitcoinTool.B`
- `Backdoor:Runtime/C&CActivity.B`
- `UnauthorizedAccess:Runtime/TorRelay`
- `UnauthorizedAccess:Runtime/TorClient`
- `Trojan:Runtime/BlackholeTraffic`
- `Trojan:Runtime/DropPoint`

Domain name-based

- `CryptoCurrency:Runtime/BitcoinTool.B!Dns`
- `Backdoor:Runtime/C&CActivity.B!Dns`
- `Trojan:Runtime/BlackholeTraffic!Dns`
- `Trojan:Runtime/DropPoint!Dns`
- `Trojan:Runtime/DGADomainRequest.C!DNS`
- `Trojan:Runtime/DriveBySourceTraffic!DNS`
- `Trojan:Runtime/PhishingDomainRequest!DNS`
- `Impact:Runtime/AbusedDomainRequest.Reputation`
- `Impact:Runtime/BitcoinDomainRequest.Reputation`
- `Impact:Runtime/MaliciousDomainRequest.Reputation`
- `Impact:Runtime/SuspiciousDomainRequest.Reputation`

Runtime protection: Suspicious process behavior

Container runtime drift

- `Execution:Runtime/NewBinaryExecuted`
- `Execution:Runtime/NewScriptExecuted`
- `Execution:Runtime/NewLibraryLoaded`

Container escapes

- `PrivilegeEscalation:Runtime/ContainerMountsHostDirectory`
- `PrivilegeEscalation:Runtime/DockerSocketAccessed`
- `PrivilegeEscalation:Runtime/RuncContainerEscape`
- `PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified`

Runtime protection: Suspicious process behavior

Execution

- `Execution:Runtime/ReverseShell`

Impact

- `Impact:Runtime/CryptoMinerExecuted`

Defense evasion

- `DefenseEvasion:Runtime/FilelessExecution`
- `PrivilegeEscalation:Runtime/UserfaultfdUsage`

Demo

ONLINE TECH TALK

Thank You!

Amit Megiddo (He/Him)

Principal Product Manager
AWS

Muhammad Wasiq (He/Him)

Principal Security Engineer
AWS