Amazon GuardDuty

Protect your AWS accounts with intelligent threat detection

New features, Roadmap

Security and compliance challenges

Lack of visibility into security threats

Ever-changing threat landscape, and not enough security experts

Complex investigation and response workflows

What is Amazon GuardDuty?

A managed **threat detection** service that uses **machine learning (ML)**, anomaly detection, and **integrated threat intelligence** to identify and prioritize potential threats

One-step activation across your AWS organization

Continuous monitoring of AWS accounts and resources

Unique detection capabilities powered by ML and threat intel

Threat intelligence from AWS and leading third parties

Fully managed AWS workload protection

How GuardDuty works

Foundational data sources

VPC Flow Logs, DNS logs

CloudTrail events involving AWS IAM access keys and Amazon EC2

AWS workload protection sources

- Amazon S3 data plane events
- Amazon EKS audit logs
- Amazon Aurora login events
- AWS Lambda network activity
- Runtime activity

Security analytics

AI/ML

Threat intelligence

Continuous learning

Security findings

Actionable

Accurate

Contextual

Integration and Remediation

Amazon Detective

AWS Security Hub

Amazon EventBridge

aws PARTNER

How customers use GuardDuty

Detect suspicious activity in your **generative AI workloads**

Assist **analysts** in investigations and **automate remediation**

Protect against **ransomware** and other types of malware

Centralize threat detection for AWS **container workloads**

More easily meet **compliance requirements,** like PCI DSS

GuardDuty for AWS workload protection

S3 Protection

Identify potential security risks such as data exfiltration for data within your S3 buckets

EKS Protection

EKS Audit Log Monitoring analyzes Kubernetes audit logs from your Amazon EKS clusters for potentially malicious and suspicious activity

Malware Protection

Identify your resources compromised by malware or those resources that are at risk

RDS Protection

Analyze and profile RDS login activity for potential access threats to your Amazon Aurora databases[1]

Lambda Protection

Continuously monitor network activity, starting with VPC Flow Logs, to detect threats to AWS Lambda functions

Runtime Monitoring

Monitor and analyze operating system-level events on Amazon EKS, Amazon ECS (including AWS Fargate), and Amazon EC2 to help detect potential threats

[1]Amazon Aurora MySQL-Compatible Edition and Aurora PostgreSQL-Compatible Edition

Amazon GuardDuty Runtime Monitoring

Continuously monitor for malicious activity and unauthorized behavior, with near real time visibility into on-host, operating system–level activities occurring across your Amazon EC2 workloads, ECS on Fargate or EC2, and EKS.

Accuracy and visibility

Defense in depth across your Amazon EC2, ECS, EKS workloads, with new detections available at launch.

Identify threats sooner

Accurately detect and respond to threats early—before they escalate to broader business-impacting breaches. Runtime activity visibility at a cluster, instance, and container level

Less friction and operational overhead

Fully managed, lightweight security agent can be automatically deployed across your organization—no third-party tooling required.

Detect threats to your compute workloads

SINGLE RUNTIME MONITORING SOLUTION FOR YOUR COMPUTE ON AWS

	Amazon Elastic Kubernetes Service (Amazon EKS)	Amazon Elastic Container Service (Amazon ECS)	AWS Fargate	Amazon Elastic Compute Cloud (Amazon EC2) Instance / Container
Node-level network (IP & DNS)	✓	✓	—	✓
Malware detection (EBS)	✓	✓	—	✓
Control plane	✓	✓	✓	✓
Container level network (IP & DNS)	✓	✓	✓	✓
Container specific threats	✓	✓	✓	✓
Process events threat detection	✓	✓	✓	✓

Enhanced threat detection with runtime monitoring

	GuardDuty VPC Flow Log and DNS log coverage	GuardDuty Runtime Monitoring coverage
RUNTIME CONTEXT	***instance*** i-1234567890abcdef0 is communicating with known malware c&c server	Process ID: 491 (***executable*** path- /usr/bin/curl, ***sha256Hash*** c2a9f390c006469243ea5aafae2985a0cd165de59a3fc00e2c410513a4ecd8c2) resulted in connection to a known CnC server from ***container*** application-metadata-11, using ***image*** docker.io/ubuntu, running on ***task*** ecs-linux-deployment-764959fd66-txdcw , on ***instance*** i-1234567890abcdef0 that is part of ***cluster*** ProdCluster in ***namespace*** - ecs-app. The process was initiated by the following ***parent processes*** /usr/sbin/nginx (PID:31), /bin/sh (PID: 42)
CONTAINER CONTEXT		
TIMELY	Mostly post-compromise	Early detection of compromise

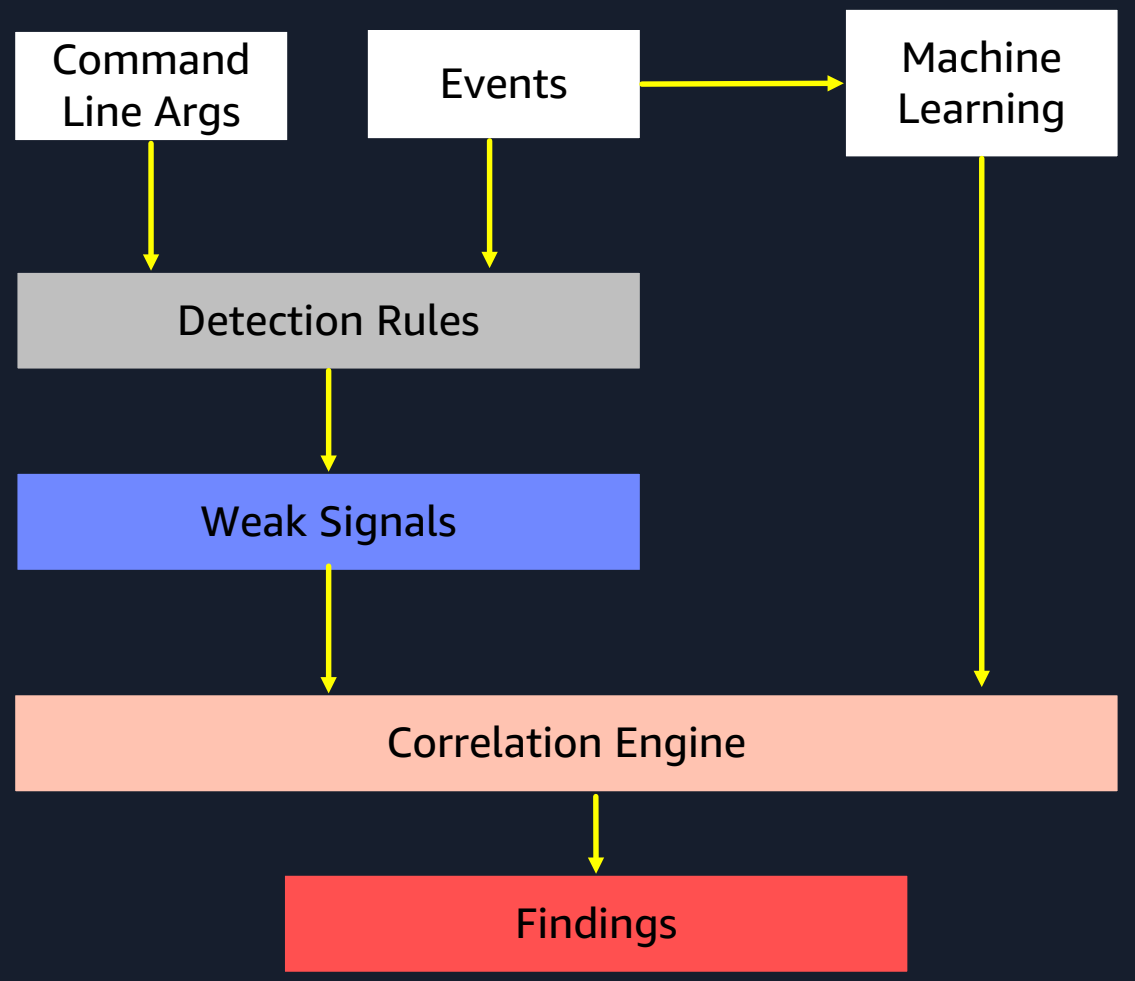
GuardDuty Runtime Monitoring threat detection

36+ RUNTIME MONITORING FINDING TYPES

Category	Example finding types
MALWARE INFECTION	Backdoor:Runtime/C&CActivity.B Execution:Runtime/MaliciousFileExecuted Impact:Runtime/MaliciousDomainRequest.Reputation
CRYPTOCURRENCY MINING	CryptoCurrency:Runtime/BitcoinTool.B Impact:Runtime/CryptoMinerExecuted
COMMAND LINE MONITORING	Execution:Runtime/SuspiciousCommand
CONTAINER DRIFT AND ESCAPE	Execution:Runtime/NewBinaryExecuted PrivilegeEscalation:Runtime/ContainerMountsHostDirectory PrivilegeEscalation:Runtime/RuncContainerEscape
REMOTE CODE EXECUTION	Execution:Runtime/Rever seShell
DEFENSE EVASION	DefenseEvasion:Runtime/FilelessExecution PrivilegeEscalation:Runtime/UserfaultfdUsage DefenseEvasion:Runtime/SuspiciousCommand

Sophisticated detection techniques

- Tracking **Command line Arguments** for threat detection
  - Suspicious command line patterns
  - Known malware command line patterns
- **Correlations**
- **Machine Learning** based **Anomaly Detection**

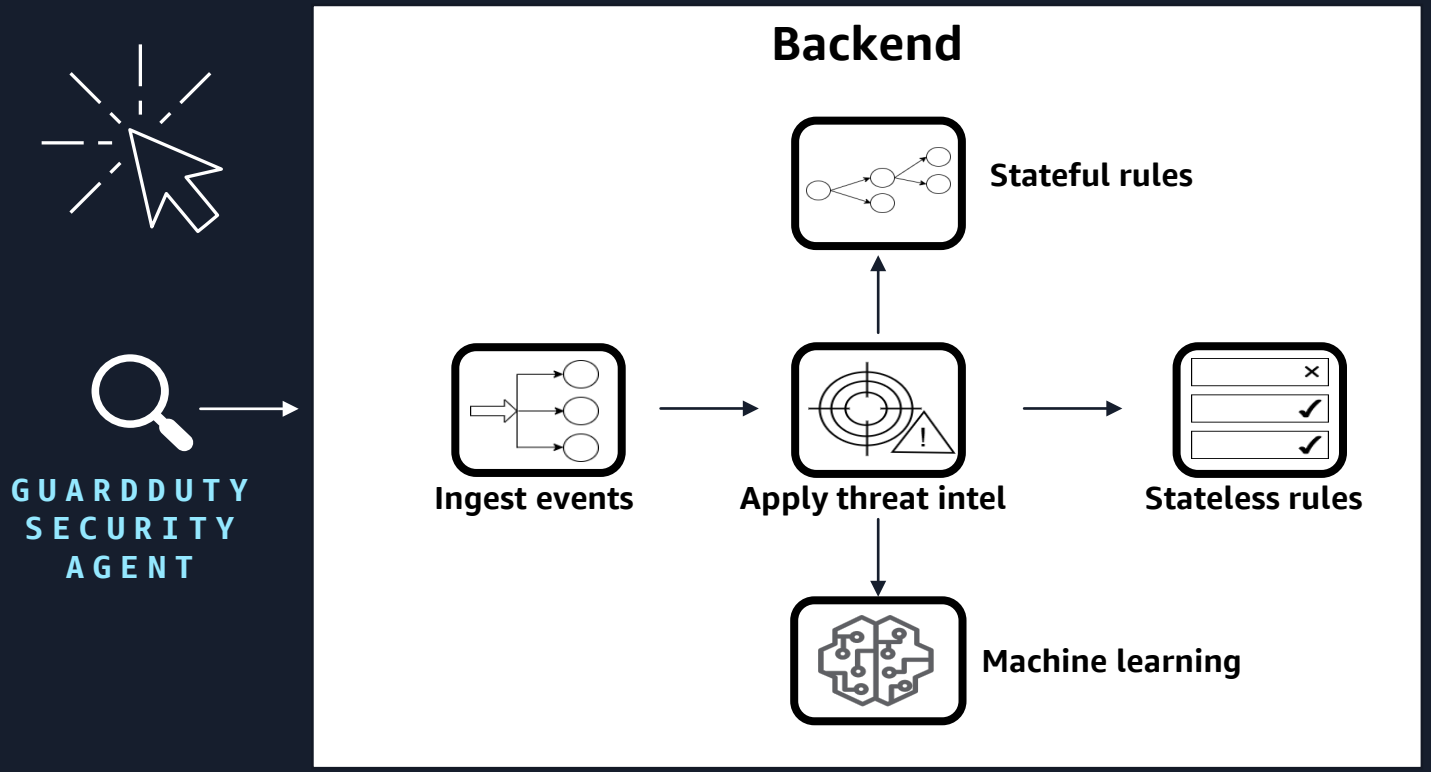


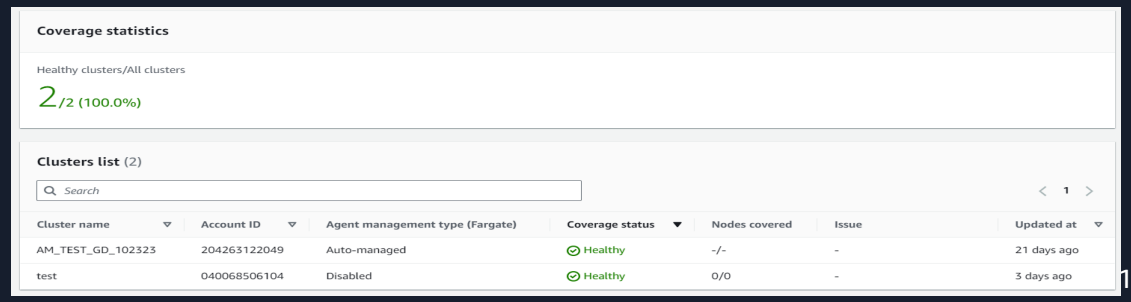
Runtime monitoring built for the cloud

Low friction automated agent deployment and management leveraging AWS Organizations, AWS System Manager, and GuardDuty-ECS integration

Balance security, availability, and performance with a lightweight eBPF agent, analytics on the backend, no impact to running tasks, and built-in resource limits

Help ensure coverage with detailed status and automated alerts on gaps





Coverage statistics

Healthy clusters/All clusters

2/2 (100.0%)

Clusters list (2)

Search

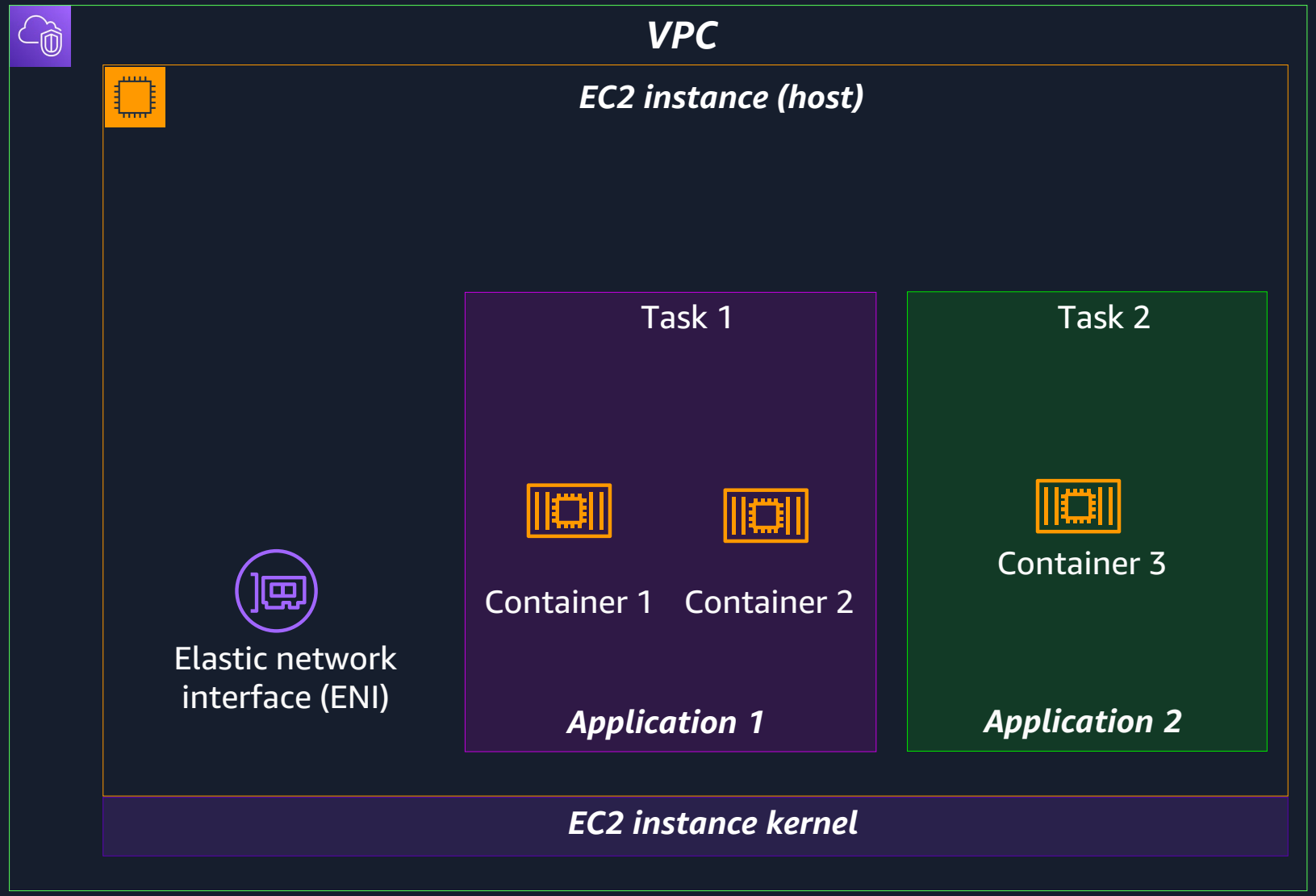
Cluster name	Account ID	Agent management type (Fargate)	Coverage status	Nodes covered	Issue	Updated at
AM_TEST_GD_102323	204263122049	Auto-managed	Healthy	-/-	-	21 days ago
test	040068506104	Disabled	Healthy	0/0	-	3 days ago

GuardDuty Monitoring on Amazon ECS

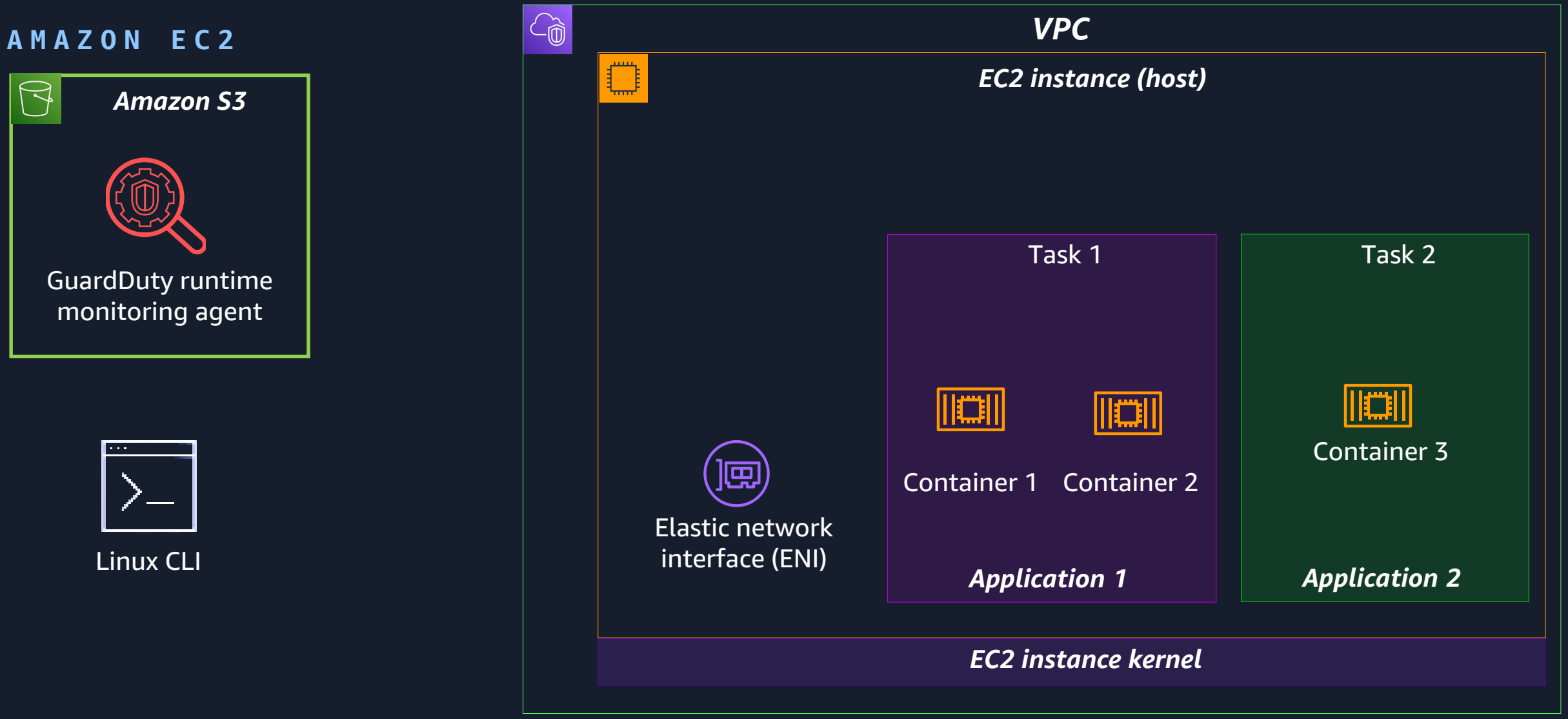
AMAZON EC2

GuardDuty runtime monitoring agent

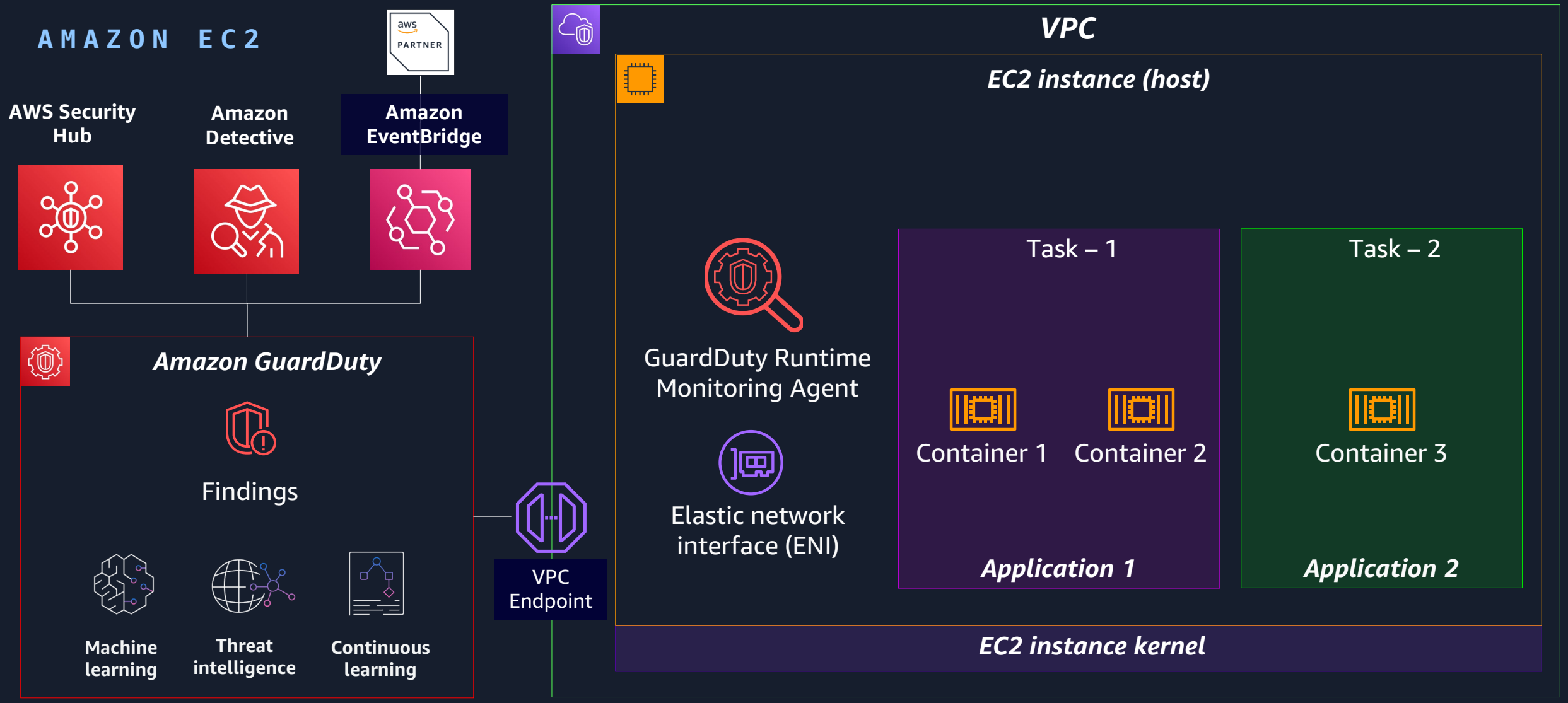
AWS Systems Manager (SSM)



GuardDuty Monitoring on Amazon ECS



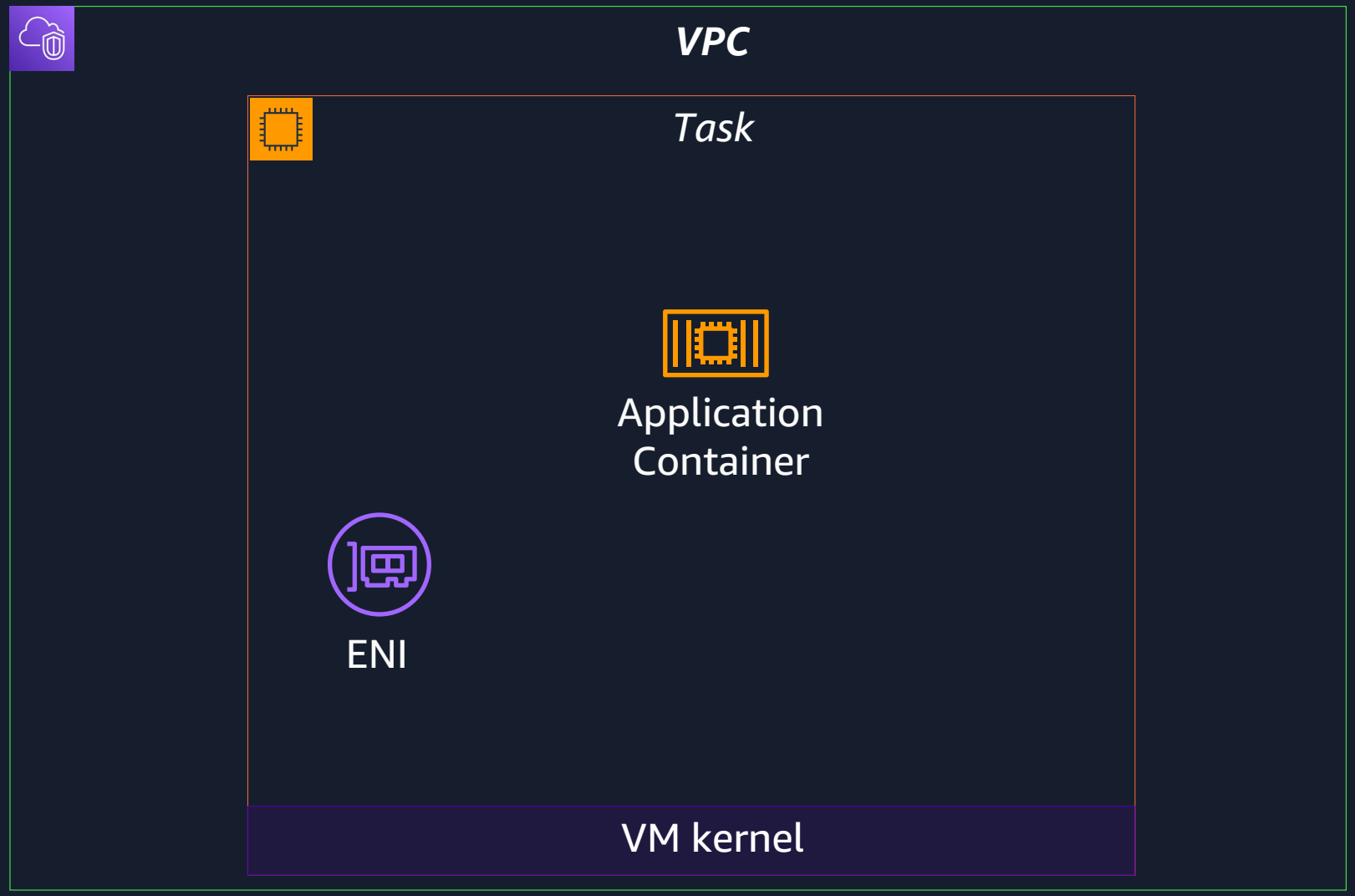
GuardDuty Monitoring on Amazon ECS



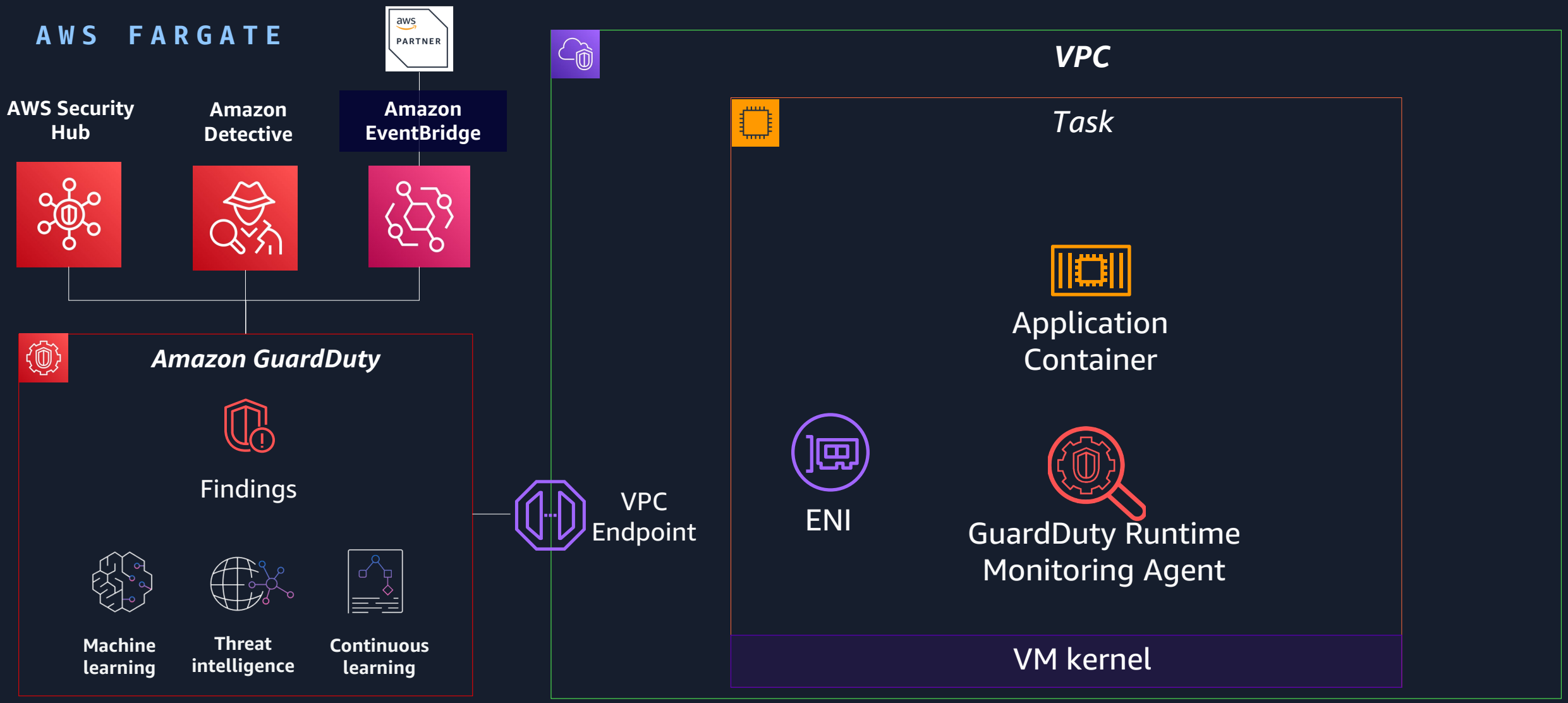
GuardDuty Monitoring on Amazon ECS

AWS FARGATE

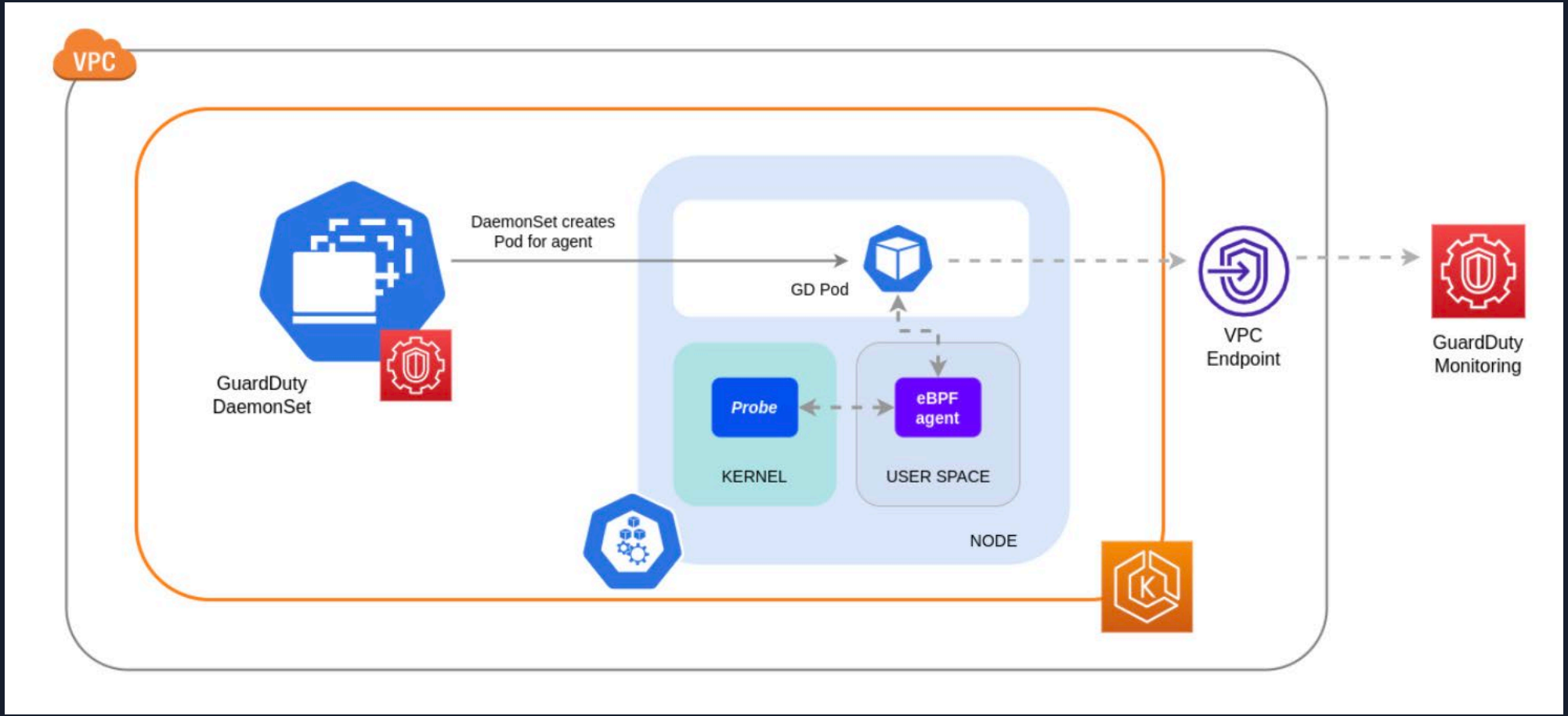
Task Execution Role to allow Fargate to pull image



GuardDuty Monitoring on Amazon ECS



How does GuardDuty EKS Runtime Protection Work?



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)

19

GuardDuty Runtime Monitoring Pricing

GuardDuty Runtime Monitoring pricing is based on the number and size of protected EKS/ ECS (Fargate)/ EC2, measured in vCPUs.

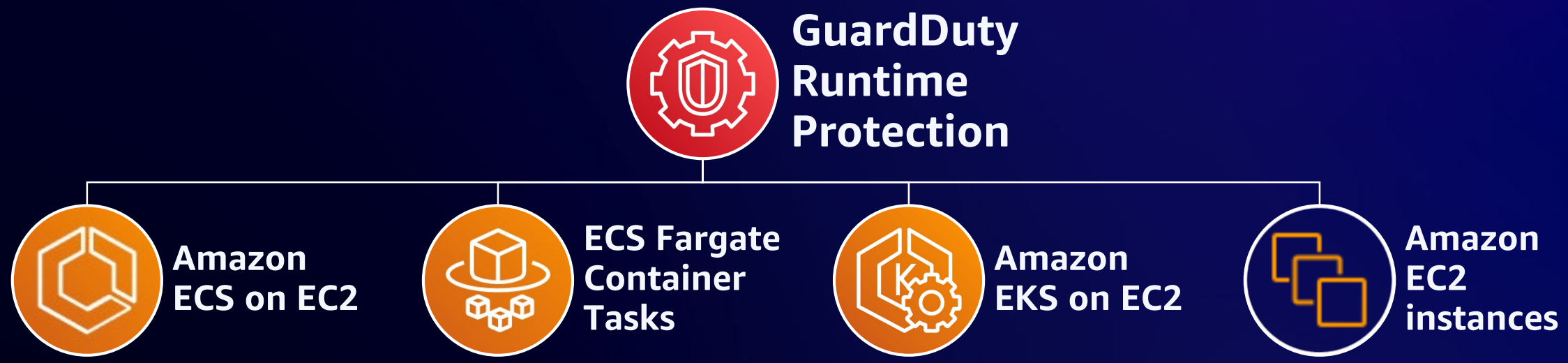
Runtime Monitoring Analysis	Pricing per vCPU
First 500 vCPUs / month (for monitored instances)	$1.50 per vCPU
Next 4,500 vCPUs / month (for monitored instances)	$0.75 per vCPU
Over 5,000 vCPUs / month (for monitored instances)	$0.25 per vCPU

30-day free trial for all existing and new GuardDuty accounts

- During the trial period, you can view the post -trial costs estimate on the GuardDuty console usage page
- GuardDuty cost savings: You will not be charged for VPC Flow logs from instances where GuardDuty security agent is installed for EC2 Runtime Monitoring and EKS Runtime Monitoring.

Detect threats at each layer of container deployment on Amazon

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



Easily achieve organization-wide coverage

EKS Protection Info

Monitor Kubernetes audit logs and runtime activity to detect threats to your EKS clusters.

Configuration | EKS clusters runtime coverage

EKS Audit Log Monitoring Configuration Info

Edit

Monitor Kubernetes audit logs that capture API activity within your EKS cluster to detect threats.

Delegated Administrator (this account)	Auto enable for new accounts	Active member accounts
Enabled	Enabled	0/8 active accounts
		Actions ▼ Manage accounts

EKS Runtime Monitoring Configuration Info

Edit

Monitor runtime activity collected by the GuardDuty agent from your EKS workloads to detect threats.

EKS Runtime Monitoring

Delegated Administrator (this account)	Auto enable for new accounts	Active member accounts
Enabled	Enabled	0/8 active accounts
		Actions ▼ Manage accounts

- **All EKS clusters:** For GuardDuty to receive the runtime events from all of your EKS clusters in an account, choose GuardDuty agent management or Manage agent manually
- **Selective EKS clusters:** For GuardDuty to receive the runtime events from selective EKS clusters in an account, use Inclusion tags or Exclusion tags

GuardDuty agent management

Delegated Administrator (this account)	Auto enable for new accounts	Active member accounts
Enabled	Enabled	8/8 active accounts
		Actions ▼ Manage accounts

Edit EKS Runtime Monitoring configuration

EKS Runtime Monitoring

- ○ Enable for all accounts
  Enable EKS Runtime Monitoring for all active GuardDuty accounts in the organization. This includes new accounts that join the organization.
  Recommended
- ◉ Configure accounts manually
  Selectively enable EKS Runtime Monitoring

Delegated Administrator (this account)

- ◉ Enable
- ○ Disable

☑ Automatically enable for new member accounts
This will apply to any new accounts when they are added to the organization

GuardDuty agent management

GuardDuty deploys and manages the agent in your EKS clusters on your behalf. For GuardDuty to monitor and analyze the runtime events, you must enable EKS Runtime Monitoring. Learn more

- ○ Enable for all accounts
  Enable GuardDuty agent management for all active GuardDuty accounts in the organization. This includes new accounts that join the organization.
  Recommended
- ◉ Configure accounts manually
  Selectively enable GuardDuty agent management

Delegated Administrator (this account)

- ◉ Enable
- ○ Disable

☑ Automatically enable for new member accounts
This will apply to any new accounts when they are added to the organization

After you save the updated configuration, you can configure EKS Runtime Monitoring for individual active member accounts using the Accounts page.

Cancel | Save

… and identify potential coverage gaps

EKS Protection Info

Monitor Kubernetes audit logs and runtime activity to detect threats to your EKS clusters.

Configuration | EKS clusters runtime coverage

Coverage statistics

Healthy clusters/All clusters

4/4 (100.0%)

Clusters list (4) Info

Search

1

Cluster name	Account ID	Coverage status	AddOn version	Issue	Updated at
Test-GD-Runtime-Monitoring	204263122049	Healthy	v1.0.0-eksbuild.1	-	7 minutes ago
test-gd-1	204263122049	Healthy	v1.0.0-eksbuild.1	-	10 minutes ago
wasiq-test	476472268746	Healthy	v1.0.0-eksbuild.1	-	4 minutes ago
amit_megiddo_EKS_test-cluster	204263122049	Healthy	v1.0.0-eksbuild.1	-	4 minutes ago

Introducing GuardDuty Malware Protection

DELIVERS AGENTLESS DETECTION OF MALWARE ON AWS WORKLOADS

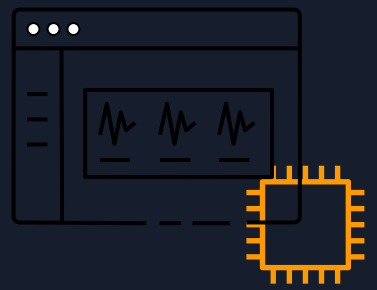
Single-click organization-wide malicious file detection

Centralized monitoring, automation, and investigation

Contextualized findings to validate suspicious behavior

No agents to install, update, or maintain

Container aware



No performance impact or hidden Amazon EC2 costs for scanning

GuardDuty findings triggering a malware scan

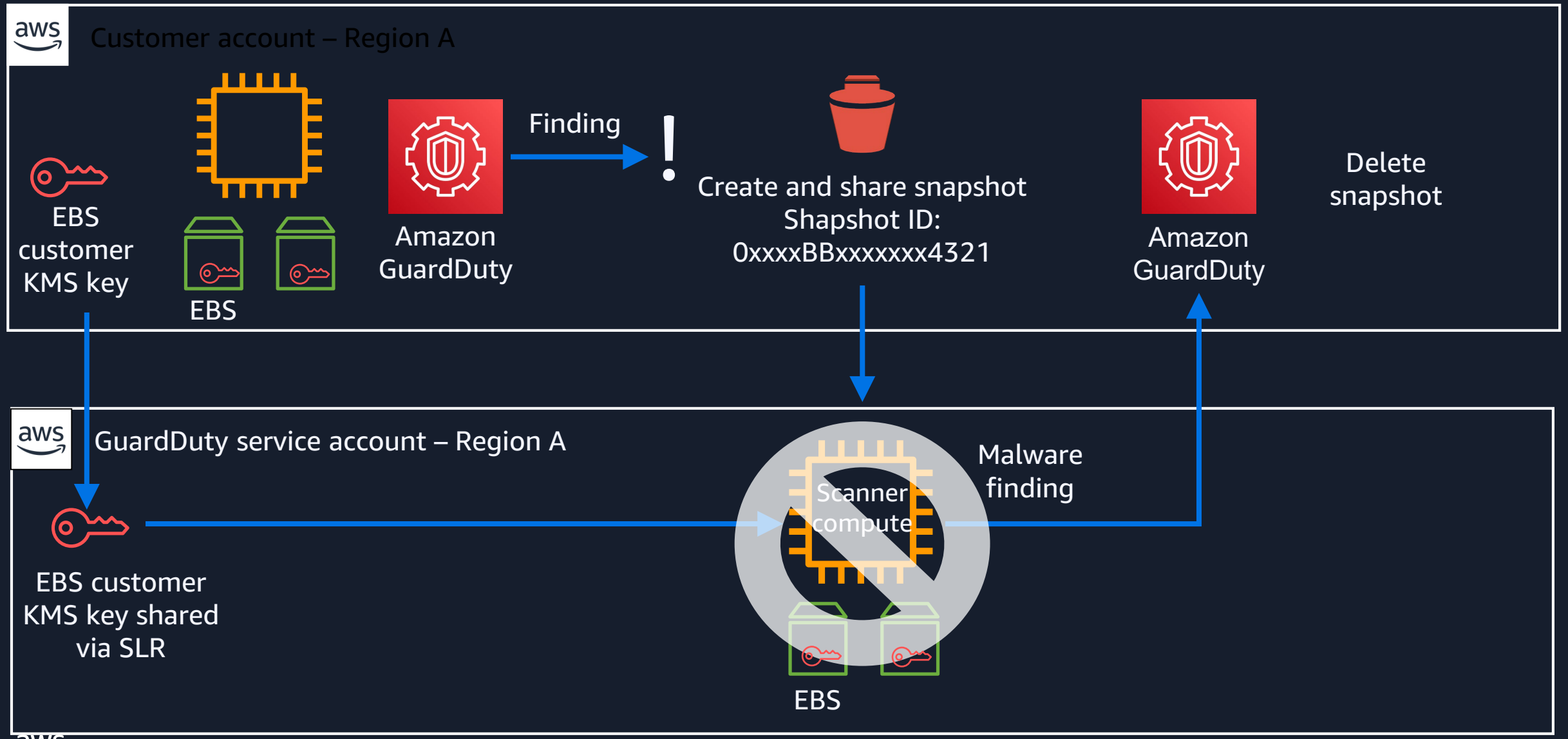
Backdoor:EC2/C&CActivity.B
Backdoor:EC2/C&CActivity.B!DNS
Backdoor:EC2/DenialOfService.Dns
Backdoor:EC2/DenialOfService.Tcp
Backdoor:EC2/DenialOfService.Udp
Backdoor:EC2/DenialOfService.UdpOnTcpPorts
Backdoor:EC2/DenialOfService.UnusualProtocol

Backdoor:EC2/Spambot
CryptoCurrency:EC2/BitcoinTool.B
CryptoCurrency:EC2/BitcoinTool.B!DNS
Impact:EC2/AbusedDomainRequest.Reputation
Impact:EC2/BitcoinDomainRequest.Reputation
Impact:EC2/MaliciousDomainRequest.Reputation
Impact:EC2/PortSweep
Impact:EC2/WinRMBruteForce **Outbound**
Recon:EC2/Portscan

Trojan:EC2/BlackholeTraffic
Trojan:EC2/BlackholeTraffic!DNS
Trojan:EC2/DGADomainRequest.B
Trojan:EC2/DGADomainRequest.C!DNS
Trojan:EC2/DNSDataExfiltration
Trojan:EC2/DriveBySourceTraffic!DNS
Trojan:EC2/DropPoint
Trojan:EC2/DropPoint!DNS
Trojan:EC2/PhishingDomainRequest!DNS
UnauthorizedAccess:EC2/RDPBruteForce **Outbound**
UnauthorizedAccess:EC2/SSHBruteForce **Outbound**
UnauthorizedAccess:EC2/TorClient
UnauthorizedAccess:EC2/TorRelay

29 finding types

How does it work?



Snapshot retention

GuardDuty > Settings > Malware Protection

Malware Protection Info

Malware Protection

Initiate malware scan when there is a finding related to an EC2 instance

Malware Protection is not enabled on this account Enable

A malware scan is automatically initiated on an EC2 instance upon a GuardDuty finding.
Learn more about how GuardDuty scans EC2 instances for malware. Learn more

General settings | Scan options

Snapshots retention Info

Retain scanned snapshots if malware is detected. Snapshots costs apply (included in 30-day free trial). Learn more about Amazon EBS pricing

Scanning inclusion or exclusion

GuardDuty > Settings > Malware Protection

Malware Protection Info

Malware Protection

Initiate malware scan when there is a finding related to an EC2 instance

- **Malware Protection is enabled on this account** Disable
- **Malware Protection is enabled for all your active member accounts** See Accounts

A malware scan is automatically initiated on an EC2 instance upon a GuardDuty finding.
Learn more about how GuardDuty scans EC2 instances for malware. Learn more

General settings | Scan options

Inclusion/Exclusion tags Info

Add tags

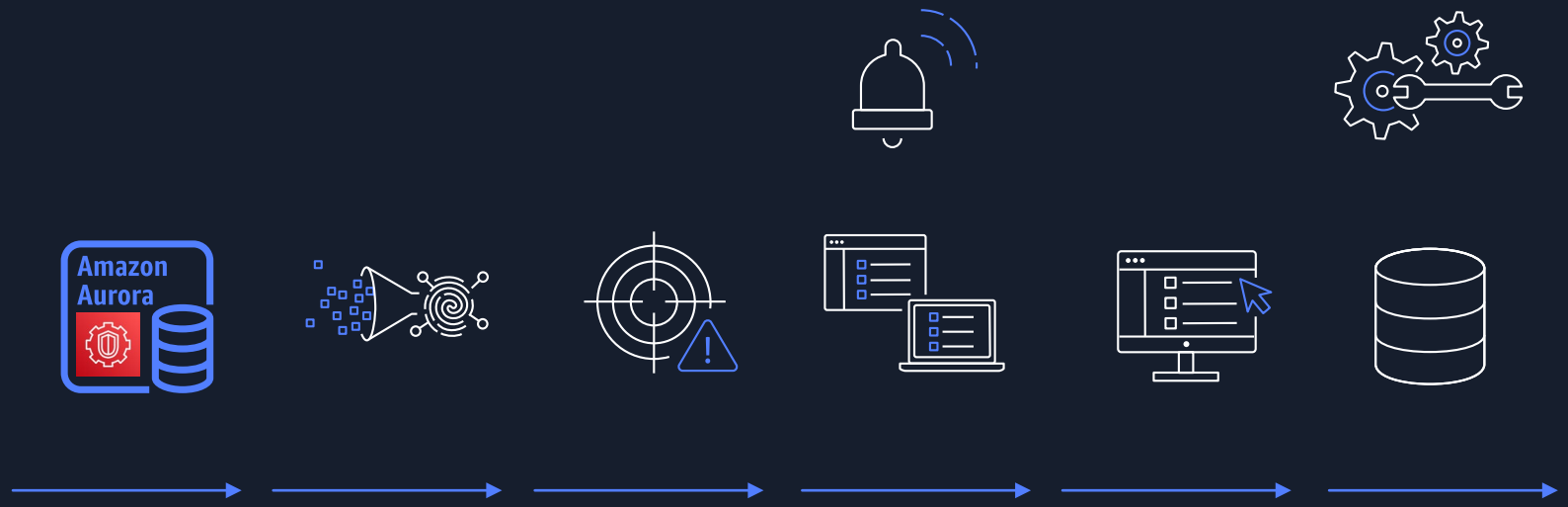
If you have assigned tags to your EC2 instances, you can limit malware scans by using inclusion tags or exclusion tags.

- If you choose inclusion tags, GuardDuty will only scan EC2 instances with the tags in the list.
- If you choose exclusion tags, GuardDuty will skip scanning EC2 instances with the tags in the list.

Introducing Amazon GuardDuty RDS Protection

- Identify potential threats to data stored in your Amazon Aurora databases using machine learning
- Continuously monitor suspicious logins in existing and new Amazon Aurora databases in your organization
- Designed to have no database performance impact or modifications needed
- Get started with a few steps in the GuardDuty console

Amazon GuardDuty RDS Protection: How it works



Aurora + GuardDuty RDS Protection → Metrics ingestion → Detect suspicious activity → GuardDuty → Evaluate → Remediate

What threats does GuardDuty RDS Protection detect?

- Anomalous successful login
- Anomalous failed login
- Successful brute force login
- Login or probe through malicious or Tor IP address

Warner Bros Discovery quickly scales container threat detection with GuardDuty

With Amazon GuardDuty, we can seamlessly integrate anomaly detection within our EKS clusters and broader AWS environment and leverage its machine learning models to proactively receive alerts that we'd have to build very complex queries for traditionally. It helped us to quickly scale out anomaly detection across all our infrastructure and scale advanced threat detection capabilities quickly and efficiently.

Mrunal Shah

Head of container security, Warner Bros. Discovery

Volkswagen Group centrally manages security threats on AWS using GuardDuty

VOLKSWAGEN GROUP

CHALLENGE

Volkswagen uses over 200 AWS services, including Amazon EC2, a web service that provides secure, resizable compute capacity in the cloud. As the company continued to adopt AWS services, it wanted to strengthen security and vulnerability detection across AWS accounts.

SOLUTION

Volkswagen developed a solution using GuardDuty alongside its on-premises security information and event management service powered by Splunk, a software solution that captures, indexes, and correlates near real-time data in a searchable interface.

OUTCOME

- ✓ Automatically deploys security services when accounts are provisioned
- ✓ Saves time for security team members
- ✓ Scales to support increased application hosting
- ✓ Reduced AWS account provisioning time by 20–27 minutes per batch

Dropbox layers AWS security services to scale its Signature Service protection

Dropbox Sign

CHALLENGE

Dropbox wanted to make its service both secure and highly available, which required protecting its services from distributed denial of service (DDoS) and other security events.

SOLUTION

In just 6 months, Dropbox Sign (formerly HelloSign) upgraded its security by using a suite of scalable, customized security tools from AWS, implementing best practices, saving developer time, improving security response time, and averting security events.

OUTCOME

- ✓ Averted 12 DDoS security events
- ✓ Saved roughly 120 hours of work time a week through automation
- ✓ Gained visibility into security posture, implemented security best practices, and customized security tools
- ✓ Automated security features within 3 months

Get started with GuardDuty

Try GuardDuty for 30 days at no cost
You will receive full access to GuardDuty features and its detection findings during the free trial

Explore GuardDuty features
Learn more about accurate, account-level threat detection, optimized for the cloud

Consult the GuardDuty user guide
Deep-dive into finding types, data sources, and integrations

Discover more resources
Get hands-on, find an AWS Partner, and read answers to frequently asked questions

Thank you!

Shachar Hirshberg

Senior Product Manager,
Amazon GuardDuty

https://www.linkedin.com/in/shachar-hirshberg/

Sujay Doshi

Senior Product Manager,
Amazon GuardDuty

https://www.linkedin.com/in/sujaydoshi/

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

38

Runtime protection: Suspicious process behavior

Container runtime drift

- Execution:Runtime/NewBinaryExecuted
- 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`