AWS GuardDuty  
  
is a fully managed, AI/ML-driven threat detection service that continuously monitors your AWS environment for suspicious activity using CloudTrail, VPC Flow Logs, DNS logs, and integrated threat intelligence .  
  
Protection Plans   
1. Foundational Detection : Included automatically when you enable GuardDuty Covers CloudTrail management, VPC Flow, DNS logs .  
  
2. S3 Protection   
Purpose: Monitors CloudTrail data plane API calls (GetObject, PutObject, DeleteObject) for anomalies like unusual downloads or mass deletion .  
Steps to Enable:  
In the console: Protection Plans → S3 Protection → Enable.  
<https://docs.aws.amazon.com/guardduty/latest/ug/s3-protection.html>  
  
3. Runtime Monitoring   
adds an extra layer of protection by deploying a lightweight security agent that monitors process execution, file access, and network activity within hosts and containers—detecting runtime threats like crypto-mining, malware execution, and escalation attacks .  
Steps to Enable:   
1.Navigate to Protection Plans → Runtime Monitoring click Enable .  
2. GuardDuty will automatically:  
2.1 Create a VPC endpoint and security group for agent communication.  
2.2 Deploy a GuardDuty sidecar container into each new Fargate task or service with fresh deployment.

3. How It Works :  
The sidecar agent collects runtime telemetry—processes, file operations, network behavior—from each container.  
Data is sent securely through the VPC endpoint to GuardDuty’s detection engine.  
No agent management is needed on your part; it's fully managed by GuardDuty .  
  
https://docs.aws.amazon.com/guardduty/latest/ug/how-runtime-monitoring-works-ecs-fargate.html  
  
4.  
  
  
Steps to Enable :  
1.