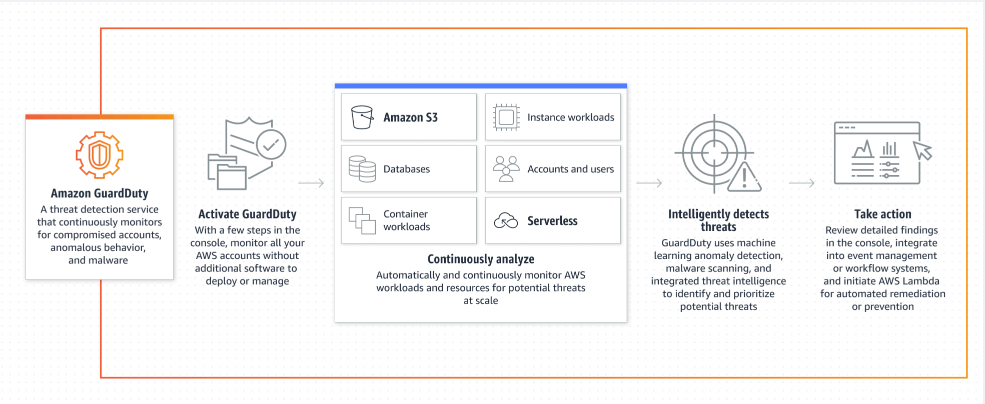
Lab 3 - Enabling Malware Protection for S3 by using GuardDuty

Malware Protection for S3 helps you detect potential presence of malware by scanning newly uploaded objects to your selected Amazon Simple Storage Service (Amazon S3) bucket. When an S3 object or a new version of an existing S3 object gets uploaded to your selected bucket, GuardDuty automatically starts a malware scan.

In this lab we will configure GuardDuty Malware Protection for S3 independently and test the configuration by uploading an object.


Amazon GuardDuty
A threat detection service that continuously monitors for compromised accounts, anomalous behavior, and malware
Activate GuardDuty
With a few steps in the console, monitor all your AWS accounts without additional software to deploy or manage
Amazon S3
Instance workloads
Databases
Accounts and users
Container workloads
Serverless
Continuously analyze
Automatically and continuously monitor AWS workloads and resources for potential threats at scale
Intelligently detects threats
GuardDuty uses machine learning anomaly detection, malware scanning, and integrated threat intelligence to identify and prioritize potential threats
Take action
Review detailed findings in the console, integrate into event management or workflow systems, and initiate AWS Lambda for automated remediation or prevention

Previous Next