AWS GuardDuty

AWS GuardDuty is a managed threat detection service that continuously monitors for malicious or unauthorized activity in your AWS environment. It leverages machine learning, anomaly detection, and integrated threat intelligence to identify potential security threats. GuardDuty analyzes various data sources, including VPC flow logs, CloudTrail event logs, DNS logs, and more, to detect and alert on suspicious behavior.

Usage and Benefits

1. Threat Detection: GuardDuty helps identify and prioritize potential security threats, such as unauthorized access, compromised instances, or malicious activity within your AWS environment.

2. Easy Integration: It seamlessly integrates with existing AWS services like CloudWatch and CloudTrail, providing comprehensive visibility into activities and events.

3. Low Operational Overhead: As a fully managed service, GuardDuty requires minimal configuration and maintenance, allowing organizations to focus on responding to incidents rather than managing the underlying infrastructure.

4. Scalability: GuardDuty scales automatically based on your AWS usage, ensuring continuous monitoring regardless of the size of your environment.

5. Global Threat Intelligence: GuardDuty leverages threat intelligence from various sources to enhance its detection capabilities, providing a more comprehensive defense against emerging threats.

Costs

GuardDuty provides a cost estimation feature to help users understand the potential daily average usage costs. The estimates cover various metrics such as Account ID, Data Source (e.g., VPC flow logs, CloudTrail logs), Feature (e.g., CloudTrail data events, EKS Audit Log Monitoring), and S3 buckets. During the **30-day free trial period**, the cost estimation projects what your estimated costs will be after the trial period.

GuardDuty usage costs are calculated based on the past 7 to 30 days of usage, and the estimates are for the current Region only. The trial usage cost estimate includes foundational data sources and features in the trial period.

Pricing:

- **AWS CloudTrail management event analysis:** GuardDuty continuously analyzes CloudTrail management events. Management events (also known as control plane) provide information about management operations that are performed on resources in your AWS account. CloudTrail management event analysis is charged per 1 million events per month and is prorated.

Per one million events / month	**$4.60 per one million events**

- **Amazon Virtual Private Cloud (VPC) Flow Log and DNS query log analysis:** GuardDuty continuously analyzes Amazon VPC Flow Logs and Domain Name System (DNS) query logs. VPC Flow Log and DNS query log analysis is charged per gigabyte (GB) per month. Both VPC Flow Log and DNS query log analyses are discounted with volume.

First 500 GB / month	**$1.15 per GB**
Next 2,000 GB / month	**$0.58 per GB**
Next 7,500 GB / month	**$0.29 per GB**
Over 10,000 GB / month	**$0.17 per GB**

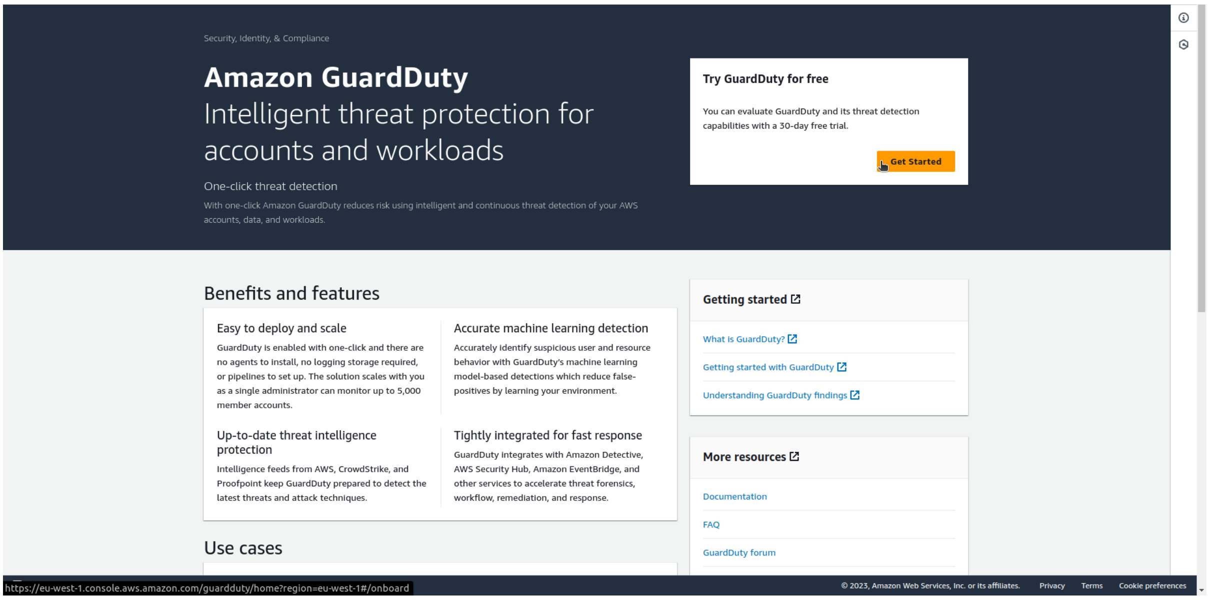
How to Enable GuardDuty

1. Sign in to the AWS Management Console:

   - Navigate to the GuardDuty console.

2. Get Started:

   - On the main screen click on “Get Started”.



Security, Identity, & Compliance

Amazon GuardDuty

Intelligent threat protection for accounts and workloads

One-click threat detection

With one-click Amazon GuardDuty reduces risk using intelligent and continuous threat detection of your AWS accounts, data, and workloads.

Try GuardDuty for free

You can evaluate GuardDuty and its threat detection capabilities with a 30-day free trial.

Get Started

Benefits and features

Easy to deploy and scale

GuardDuty is enabled with one-click and there are no agents to install, no logging storage required, or pipelines to set up. The solution scales with you as a single administrator can monitor up to 5,000 member accounts.

Accurate machine learning detection

Accurately identify suspicious user and resource behavior with GuardDuty's machine learning model-based detections which reduce false-positives by learning your environment.

Up-to-date threat intelligence protection

Intelligence feeds from AWS, CrowdStrike, and Proofpoint keep GuardDuty prepared to detect the latest threats and attack techniques.

Tightly integrated for fast response

GuardDuty integrates with Amazon Detective, AWS Security Hub, Amazon EventBridge, and other services to accelerate threat forensics, workflow, remediation, and response.

Use cases

Getting started

What is GuardDuty?

Getting started with GuardDuty

Understanding GuardDuty findings

More resources

Documentation

FAQ

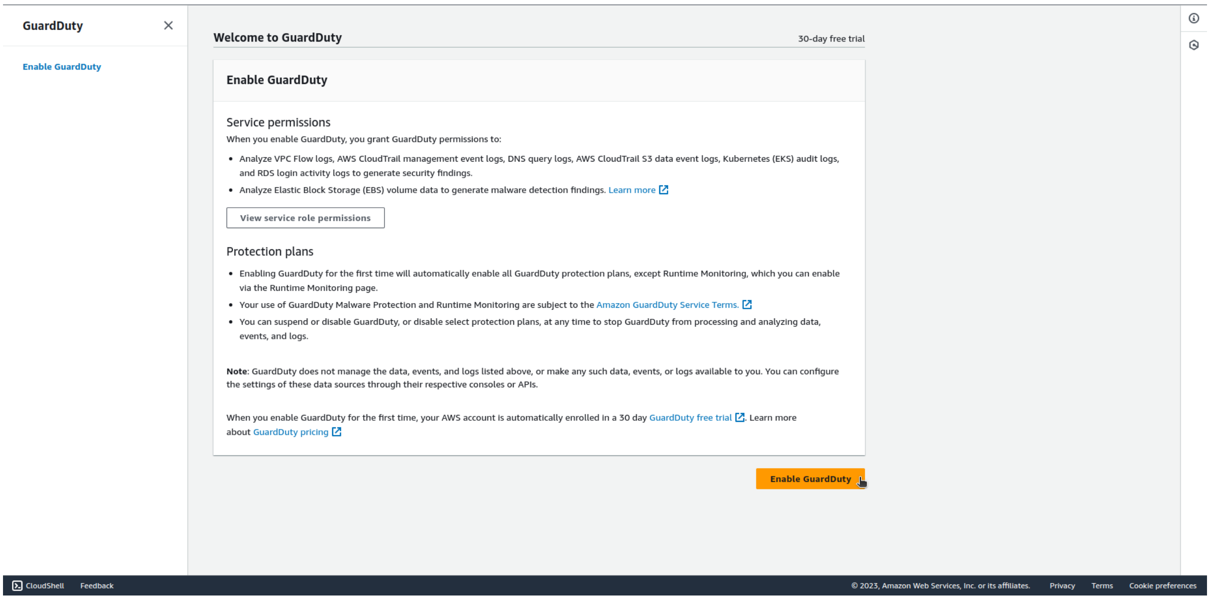
GuardDuty forum

https://eu-west-1.console.aws.amazon.com/guardduty/home?region=eu-west-1#/onboard

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

3. Enable GuardDuty:

   - Click on "Enable GuardDuty”.



Welcome to GuardDuty

30-day free trial

Enable GuardDuty

Service permissions

When you enable GuardDuty, you grant GuardDuty permissions to:

- Analyze VPC Flow logs, AWS CloudTrail management event logs, DNS query logs, AWS CloudTrail S3 data event logs, Kubernetes (EKS) audit logs, and RDS login activity logs to generate security findings.
- Analyze Elastic Block Storage (EBS) volume data to generate malware detection findings. Learn more

Protection plans

- Enabling GuardDuty for the first time will automatically enable all GuardDuty protection plans, except Runtime Monitoring, which you can enable via the Runtime Monitoring page.
- Your use of GuardDuty Malware Protection and Runtime Monitoring are subject to the Amazon GuardDuty Service Terms.
- You can suspend or disable GuardDuty, or disable select protection plans, at any time to stop GuardDuty from processing and analyzing data, events, and logs.

Note: GuardDuty does not manage the data, events, and logs listed above, or make any such data, events, or logs available to you. You can configure the settings of these data sources through their respective consoles or APIs.

When you enable GuardDuty for the first time, your AWS account is automatically enrolled in a 30 day GuardDuty free trial. Learn more about GuardDuty pricing

4. Review and Confirm:

   - Review Protection plans and turn off the ones You don’t need.

5. Start Monitoring:

   - GuardDuty will start monitoring your AWS environment for security threats based on the configured settings.

By following these steps, you can enable AWS GuardDuty and enhance the security of your AWS environment. Regularly review GuardDuty findings to respond promptly to potential security incidents.