

## 1. What is OCI?

- OCI, or Oracle Cloud Infrastructure, is Oracle's cloud computing platform. It offers a range of services for deploying and scaling applications with high performance and security. OCI is known for its global presence, robust infrastructure, and support for diverse workloads, making it a preferred choice for enterprises.

## 2. What is OCI Security?

- OCI security involves protective measures in Oracle Cloud Infrastructure to safeguard data and resources from unauthorized access and cyber threats, using features like encryption and identity management.

## 3. What is Cloud Guard?

- Oracle Cloud Guard is a security service in Oracle Cloud Infrastructure (OCI) that helps protect cloud resources by continuously monitoring for security threats and automating responses to potential issues. It uses machine learning, threat intelligence, and predefined policies to detect and mitigate security risks.

### Technical Example:

In a technical scenario, Cloud Guard might detect an unauthorized attempt to access sensitive data stored in an Oracle Cloud database. Using predefined security policies, it can automatically trigger actions like blocking the suspicious user, alerting administrators, and updating access controls to prevent further unauthorized access. This proactive response helps to secure the database and maintain data integrity.

### Non-Technical Example:

Think of Cloud Guard as a digital security guard for your cloud-based information. Imagine you have a virtual "security guard" watching your cloud files. If someone tries to access your confidential documents without permission, Cloud Guard acts like a vigilant guard, stopping the unauthorized access immediately. It's like having a trustworthy security system in the cloud that keeps your data safe from potential intruders.

## 4. Importance of Cloud Guard?

- The importance of Cloud Guard in Oracle Cloud Infrastructure (OCI) lies in its ability to enhance the security posture of cloud environments through continuous monitoring, threat detection, and automated response mechanisms. Here are key reasons highlighting the importance of Cloud Guard:

Proactive Threat Detection

Automated Remediation:

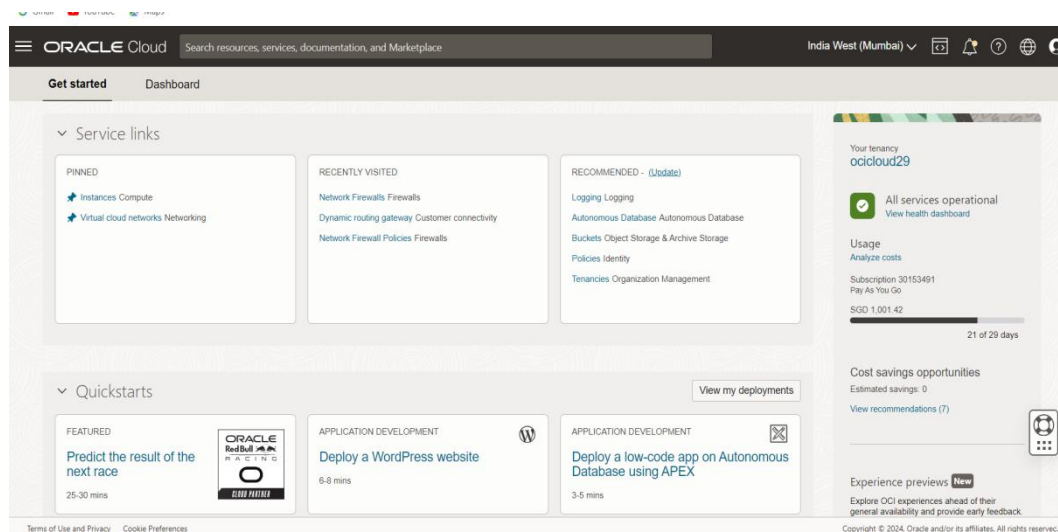
Policy Enforcement

Reduced Operational Overhead

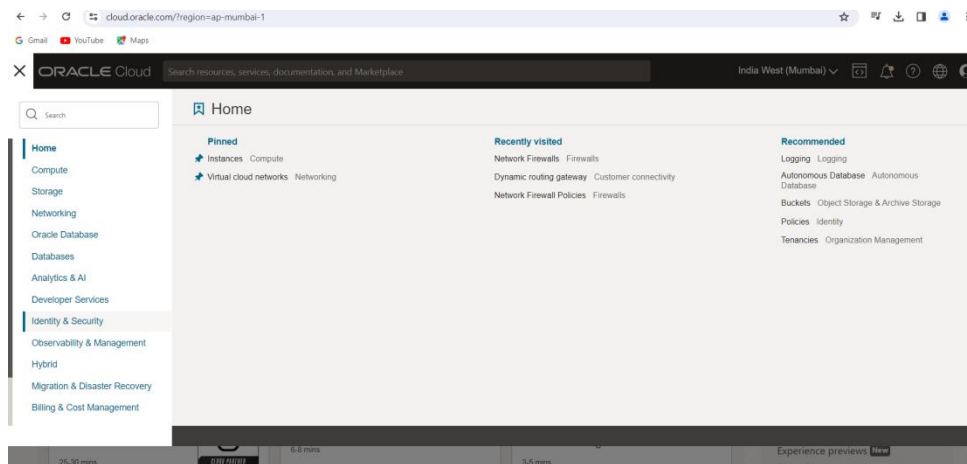
Enhanced Visibility

Adaptability to Dynamic Environment

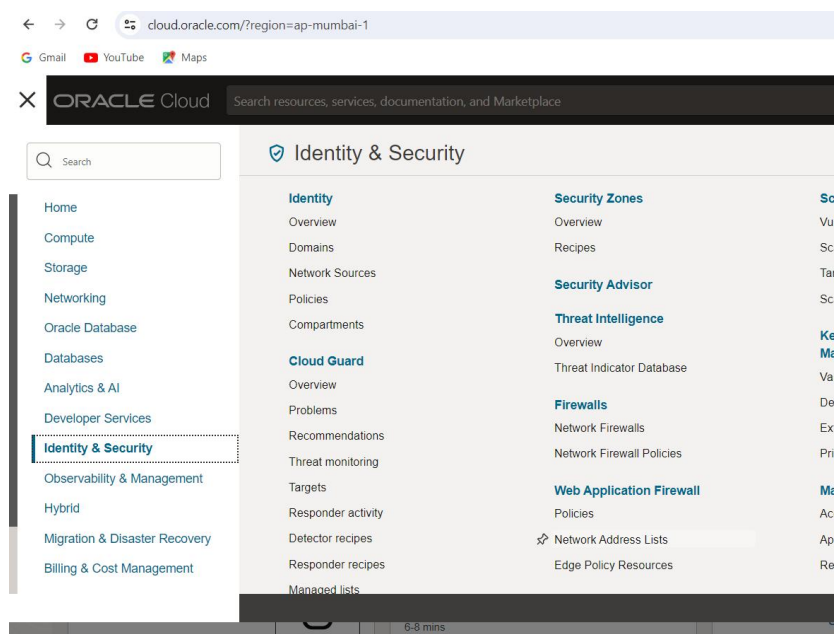
## Step 1 :- Login to cloud interface to get this Interface



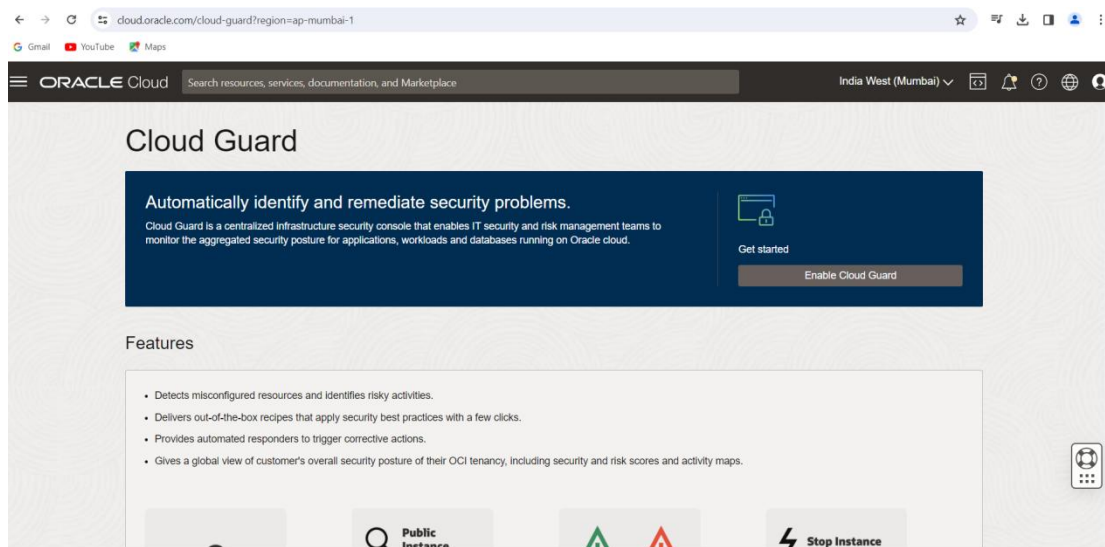
## Step 2:- Click on the 3 dash on the left corner



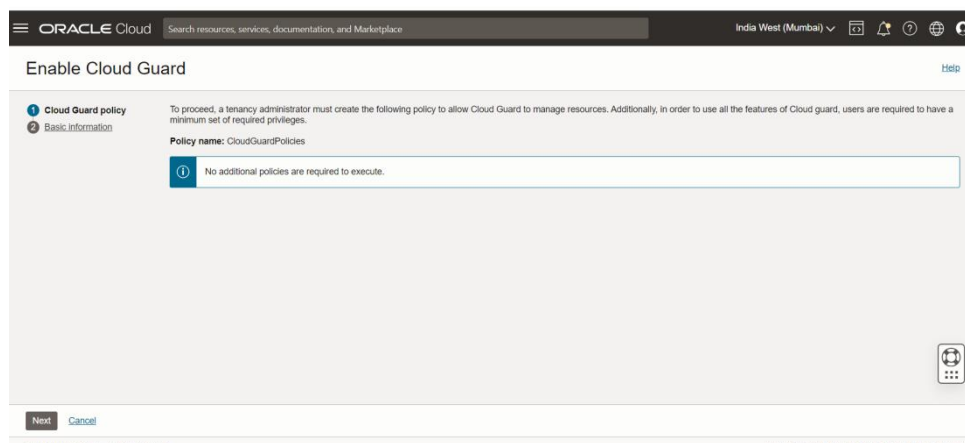
## Step 3:- Click on the Identity & Security



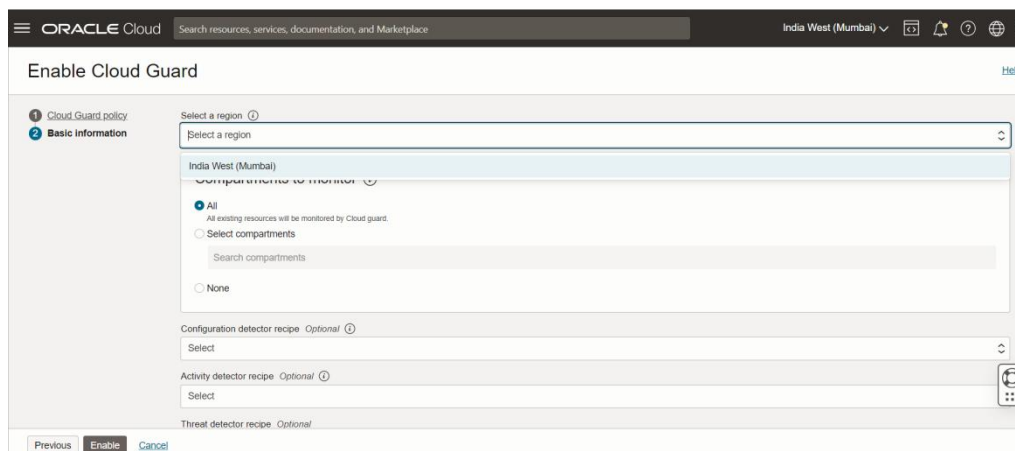
## Step 4:- Enable on the Cloud Guard



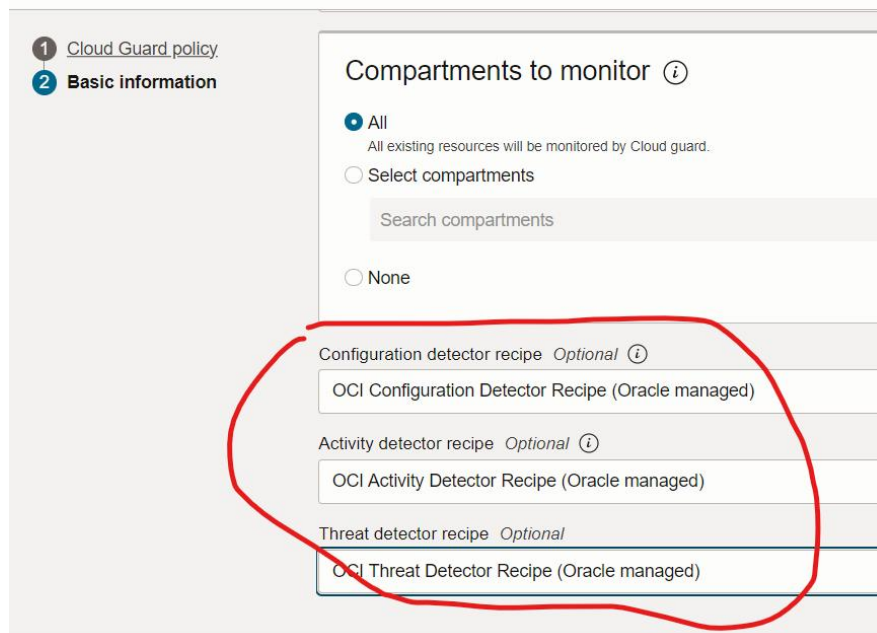
## Step 5:- Click on the Next



## Step 6:- Select a region



**Step 7:-** There are basic Configuration detector recipe, Activity detector recipe, Threat detector recipe, select the default one. Later on we can change it and make our own recipes.



1 Cloud Guard policy.  
2 Basic information

### Compartments to monitor ⓘ

☒ All  
All existing resources will be monitored by Cloud guard.

☐ Select compartments

Search compartments

☐ None

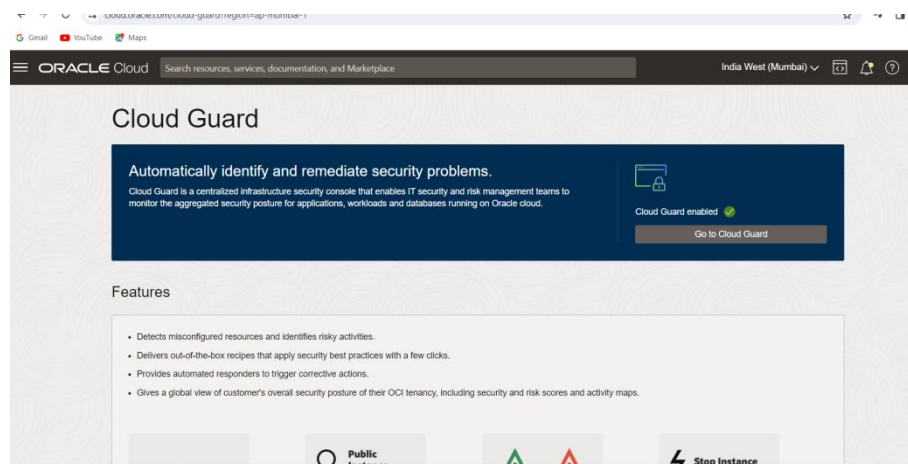
---

Configuration detector recipe *Optional* ⓘ  
OCI Configuration Detector Recipe (Oracle managed)

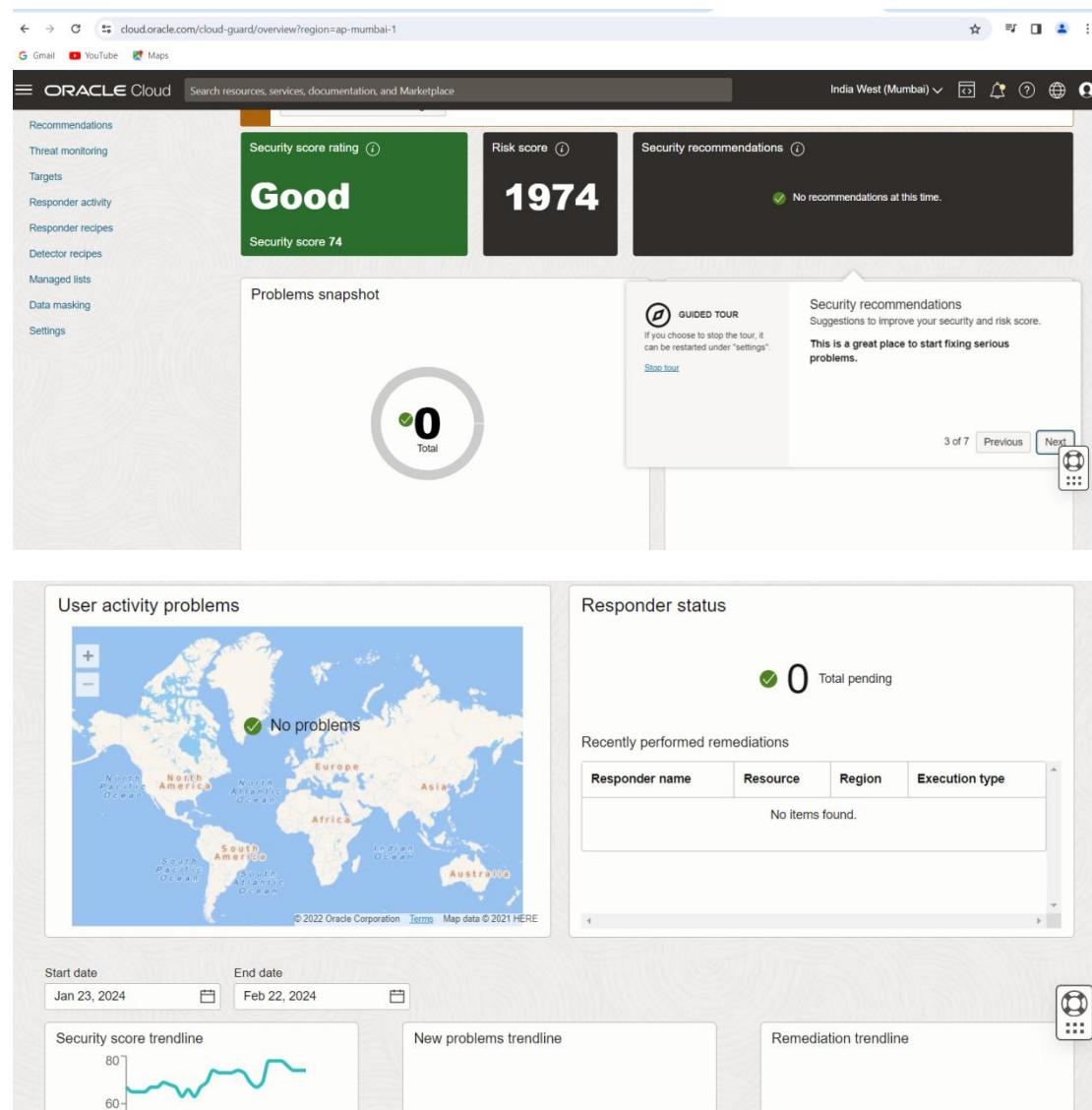
Activity detector recipe *Optional* ⓘ  
OCI Activity Detector Recipe (Oracle managed)

Threat detector recipe *Optional*  
OCI Threat Detector Recipe (Oracle managed)

**Step 8:-** Click on enable after that interface will like this, Cloud Guard is enabled.



**Step 9 :- This will be the interface of the Cloud Guard.**



## Features displayed on the Interface

### -Security Score Rating:

What: A numerical representation of your cloud environment's overall security health.

Why it's Important: Provides a quick snapshot of how well your resources align with security best practices.

### -Risk Score:

What: An assessment of potential security risks based on detected anomalies or vulnerabilities.

Why it's Important: Helps prioritize and address security issues, focusing on areas with the highest risk.

### -Security Recommendation:

What: Specific guidance on improving your cloud security posture.

Why it's Important: Offers actionable insights to enhance security and compliance, aiding in proactive risk mitigation.

-Problems Snapshot:

What: An overview of current security issues or anomalies.

Why it's Important: Enables quick identification and resolution of ongoing security concerns.

-User Activity Problem:

What: Alerts on unusual user activities that may indicate security threats.

Why it's Important: Detects and addresses potentially malicious behavior, enhancing user account security.

-Responder Status:

What: Indicates the automated response status to security incidents.

Why it's Important: Ensures automated actions are active, providing timely responses to security events.

-Security Score Trendline:

What: Graphical representation showing changes in security scores over time.

Why it's Important: Offers insights into the historical performance of your security measures, helping track improvements or potential regressions.

-New Problem Trendline:

What: Graphical display of the emergence of new security issues.

Why it's Important: Helps in spotting trends and patterns, aiding proactive measures to prevent recurring problems.

-Remediation Trendline:

What: Illustrates the effectiveness of remediation efforts over time.

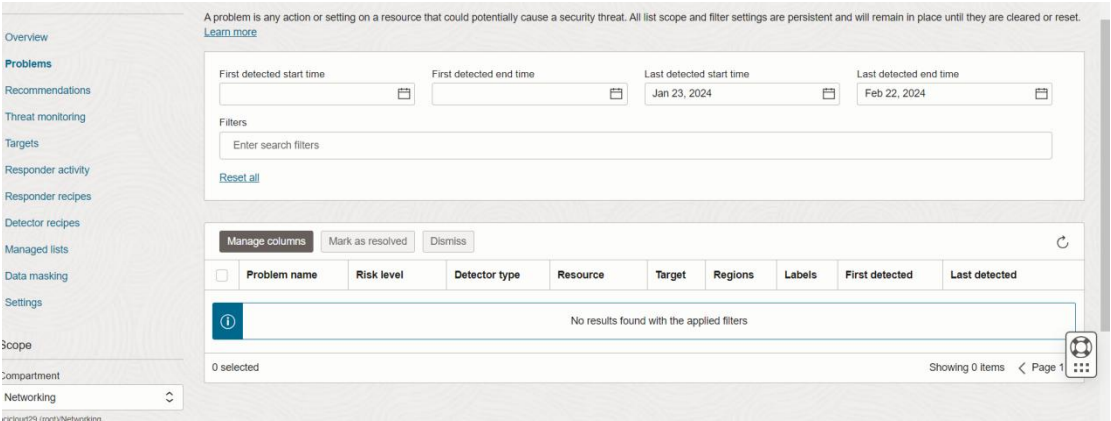
Why it's Important: Tracks the progress of resolving security issues, indicating the impact of implemented solutions.

Additional Features in the OCI Cloud Guard

On the left hand side there are many features to the OCI Cloud Guard

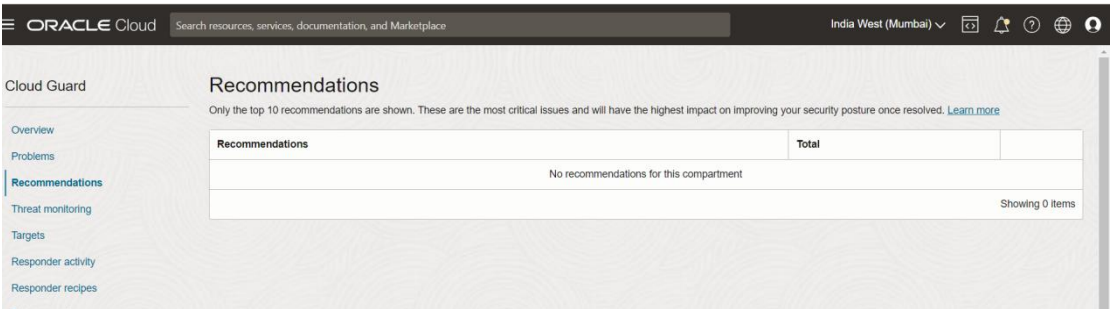
Problems:

Highlights current security issues or anomalies.  
Identifies ongoing security concerns for prompt resolution.



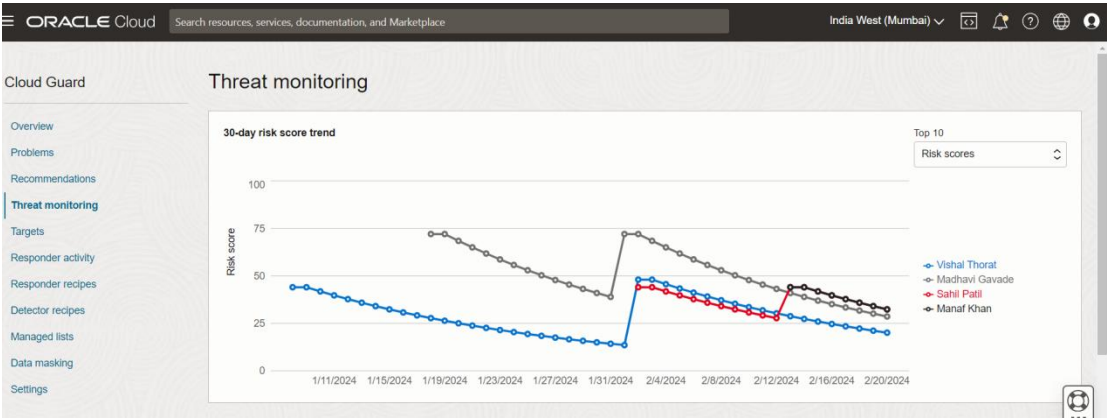
Recommendations:

Offers specific guidance to improve cloud security.  
Provides actionable insights for enhanced security and compliance.



Threat Monitoring:

Keeps a watch for potential security threats and abnormalities.  
Proactively detects and addresses security risks to prevent incidents.



Targets:

Identifies specific resources or areas under security monitoring.  
Allows focused monitoring and protection for critical parts of your cloud infrastructure.

The screenshot shows the Oracle Cloud Targets dashboard. The left sidebar lists navigation options: Overview, Problems, Recommendations, Threat monitoring, Targets (selected), Responder activity, and Responder recipes. The main area displays the 'Targets' section with a sub-header 'Targets identify a compartment to be monitored by Cloud Guard. [Learn more](#)'. Below this are 'Create new target' and 'Delete' buttons, and a search bar 'Filter by target name'. A table with columns 'Target name', 'Compartment', 'Type', 'Recipes', and 'Created' is shown. The table contains no data, with the message 'No items found.' displayed. At the bottom, it says '0 selected' and 'Showing 0 items < 1 of 1 >'.

Target name	Compartment	Type	Recipes	Created
No items found.				



Responder Activity:

Indicates the status of automated responses to security incidents.  
Ensures timely and automated actions are active for improved incident response.

Cloud Guard

Overview

Problems

Recommendations

Threat monitoring

Targets

Responder activity

Responder recipes

Detector recipes

Managed lists

Data masking

Settings

Scope

Responder activity

Responder activity indicates the actions taken or could be taken by Cloud Guard for identified problem. [Learn more](#)

Time create range start

Time created range end

Time completed range start

Time completed range end

Jan 23, 2024

Feb 22, 2024

Filters

Enter search filters

[Reset all](#)

Manage columns

Skip execution

<input type="checkbox"/>	Responder name	Responder activity OCID	Resource	Region	Execution status	Execution type	Problem name	Time created	Time completed
<div><div></div><div></div></div>	No results found with the applied filters								

0 selected

Showing 0 items < Page 1 >

Responder Recipes:

Preset automated actions for specific security incidents.  
Streamlines incident response by automating common security actions.

Cloud Guard

Overview

Problems

Recommendations

Threat monitoring

Targets

Responder activity

Responder recipes

Detector recipes

Managed lists

Responder recipes

To create your own recipe, clone an existing Oracle managed recipe from the root compartment [Learn more](#)

Clone

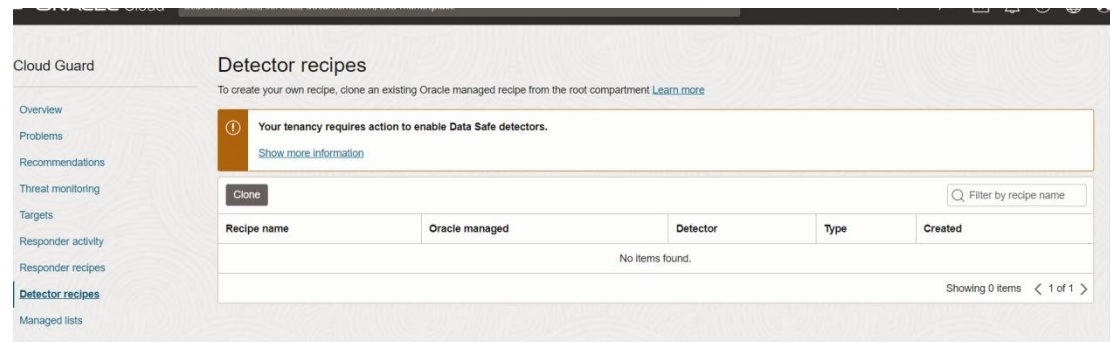
Filter by recipe name

Recipe name	Oracle managed	Created
No items found.		

Showing 0 items < 1 of 1 >

## Detector Recipes:

Predefined configurations for detecting specific security issues.  
Simplifies and standardizes the process of identifying and addressing security threats.

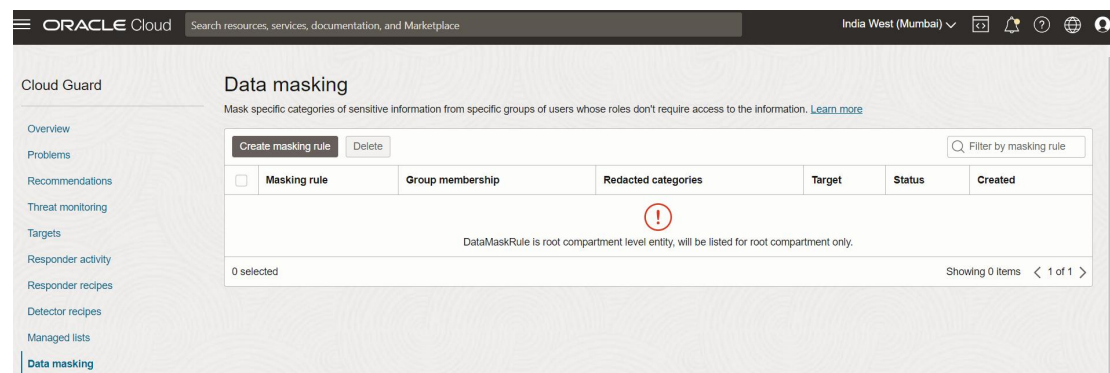


## Managed Lists:

Lists of entities used for defining security policies.  
Facilitates easy management of security policies and configurations.

## Data Masking:

Protects sensitive information by replacing or hiding part of it.  
Safeguards sensitive data from unauthorized access or exposure.



## Settings:

Configuration options for customizing Cloud Guard behavior.  
Allows users to tailor Cloud Guard to their specific security requirements and preferences.