CSPM with Single-Pane-of-Glass visibility & control

Client

Our Client is headquartered in CA with the goal of empowering security teams in enterprises adopting the Cloud with the capabilities to design, implement and continually ensure the effectiveness of their security and compliance controls. The Product is designed to help enterprise security teams assess current security, compliance risks and expedite remediation workflows.

Objective

Objective is to build a robust product to take care of Cloud Security Posture Management (CSPM) with Single-Pane-of-Glass visibility & control across public clouds.

This Product provides unparalleled visibility into security posture and offers the ability to take immediate action to remediate issues.

It enables the enterprise security teams with the capabilities to design, implement, manage, and ensure the effectiveness of their security and compliance controls.

Basically, designed specifically for InfoSec and SecDevOps teams and provides continuous security monitoring for public cloud infrastructure.

Challenges

These are the following challenges faced:

- Single holistic view to look at the Enterprise cloud resources with all details such as Resource meta data and the Violations.
- Filter Capabilities to look at specific areas like Production systems or particular resource types like Bucket /Container resources etc.
- No Inbuilt Hierarchy available in the Native Clouds to see the Parent /Child relationship of the resources.
- Any additions /deletions of the Cloud resources has to surfaced immediately.
- Filter only Subset of the Enterprise resources based on Tags.

Solution

Extracted the resources and built the Hierarchy to show like exact Tree view with all the info of Parent /Child and the respective children's along with the details of the resources and the number of violations exists for each resource. This view will aid the Customers to figure out the problematic area and take quick remediation. From this view, they can filter based on various parameters like Resource types, Names, Region wise, Violation only etc. We have extensively used all the features of D3JS to arrive the tree view. Also, the users can Zoom in /Zoom out particular nodes /resource types.

Benefits

- Customers can install this product inside Kubernetes Cluster, running within their environment and no need to traverse the data outside of their Enterprise.
- Overlaid the Cloud Security Posture into Resource Hierarchy, it starts with Organization node, Projects, folders etc. and in-turn provides the information related to which part of the Organization has issues /Violations (Vulnerabilities /Threats /Misconfiguration)
- Keep Track of the Security Posture across Times and compare what has been changed.

Technology Used

Angular 9 with Material, Python, Postgres, Falcon Framework, Redis and Docker CE, Terraform