Enterprise AWS Cost and Security Optimization Framework
Author: Adedayo
Specialization: Cloud Security & Cloud Governance
Platform: Amazon Web Services (AWS)

1. Introduction

This document describes the analysis and implementation of a cost and security optimization framework in an AWS environment.

I conducted this engagement to reduce unnecessary operational spending while maintaining strong security controls and governance standards.

The initiative focused on identifying redundant services, unused resources, and inefficient configurations, and applying risk-based optimization strategies.

2. Objectives

The primary objectives were to:

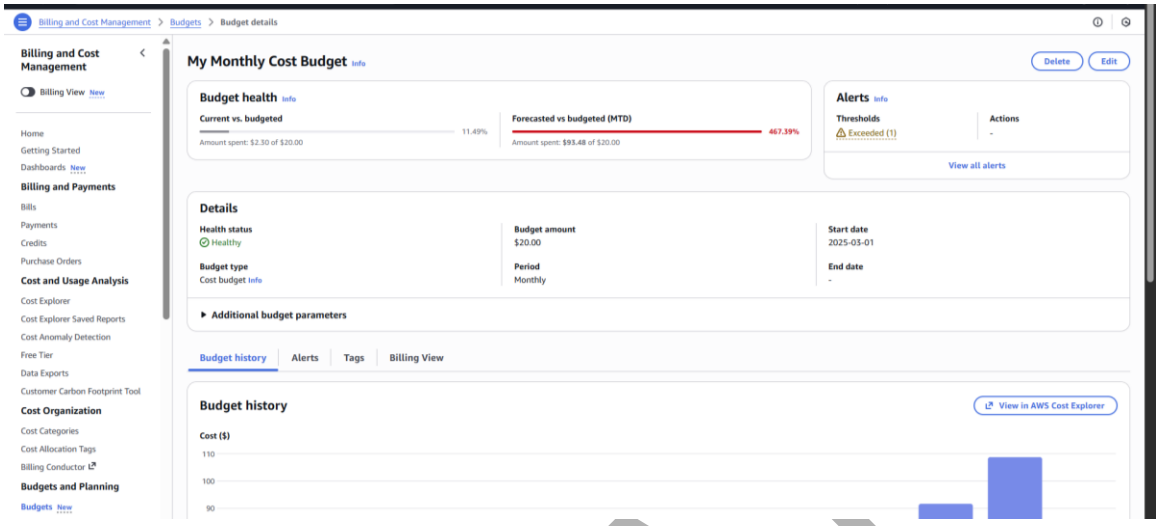
- Reduce cloud operational costs
- Eliminate unused and redundant resources
- Optimize security service usage
- Maintain regulatory and security requirements
- Improve financial governance
- Support sustainable cloud operations

3. Environment and Scope

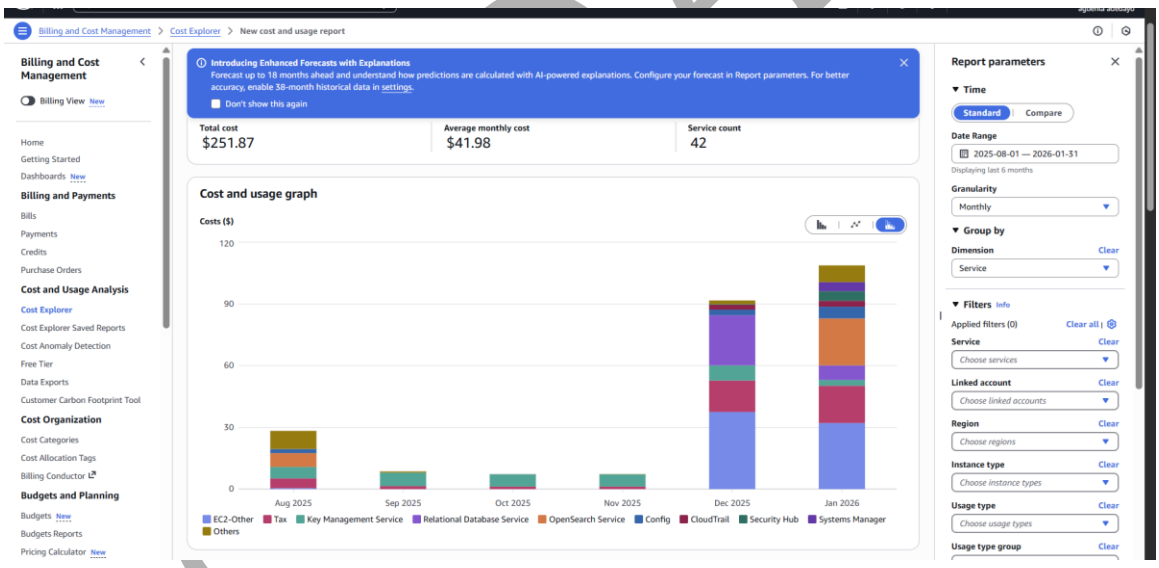
The AWS environment included multiple security and monitoring services:

- Amazon GuardDuty
- AWS Security Hub
- Amazon Inspector

Billing alerts and budgets were configured to monitor spending and enforce financial controls.



Cost Explorer was used to analyze service-level and resource-level expenditures.



4. Security Service Optimization

4.1 Redundant Tool Analysis

An assessment was performed to identify overlapping security capabilities across services.

Threat detection, vulnerability scanning, and compliance monitoring tools were reviewed for redundancy.

Optimization actions included:

- Retaining core services (GuardDuty, Security Hub, Inspector)
- Eliminating unnecessary overlaps
- Streamlining monitoring configurations

4.2 Regional Optimization

GuardDuty and Inspector coverage was reviewed across regions.

Unused regional deployments were disabled to reduce unnecessary charges.

5. Unused Resource Identification

A comprehensive audit identified unused and underutilized resources, including:

- Elastic IP addresses
- NAT Gateways
- Load Balancers
- EBS Snapshots
- Orphaned KMS keys

These resources were evaluated for business and security impact.

6. Cost Optimization Actions

The following remediation actions were implemented:

- Deletion of unused Elastic IPs and snapshots
- Removal of inactive load balancers
- Replacement of NAT Gateway with VPC endpoints where appropriate
- Cleanup of unused KMS keys

- Consolidation of monitoring configurations

All changes were reviewed to ensure no impact on security posture.

7. Financial Monitoring and Governance

AWS Budgets and billing alarms were configured to provide early warning of abnormal spending.

Cost Explorer dashboards were used for ongoing cost tracking.

Optimization activities were documented to support financial audits and governance reviews.

8. Risk-Based Optimization Strategy

All cost reduction decisions followed a risk-based approach.

Critical security services were preserved.

Cost savings were prioritized in low-risk and non-production areas.

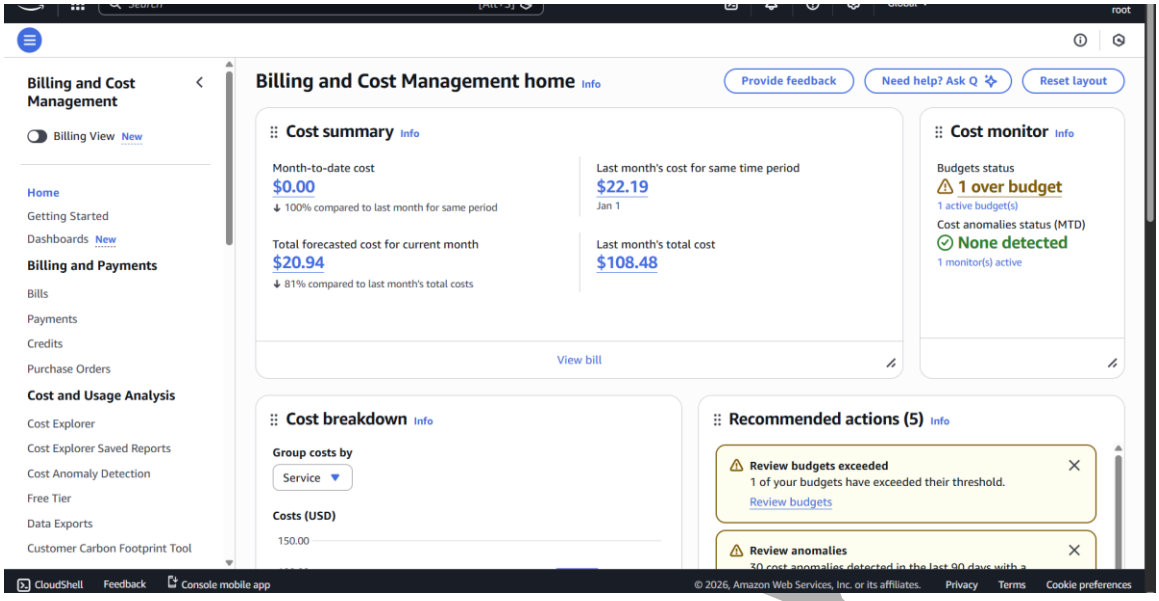
This ensured that optimization did not weaken security defenses.

9. Post-Optimization Review

After optimization, spending patterns were reviewed.

Cost trends showed consistent reduction across major service categories.

No degradation in monitoring or security visibility was observed.



10. Outcomes and Impact

This implementation delivered:

- Significant reduction in monthly cloud costs
- Improved visibility into spending patterns
- Stronger financial governance
- Optimized security service deployment
- Reduced waste and inefficiency

Estimated savings ranged between 40% and 50%.

11. Conclusion

I designed and implemented an enterprise-grade AWS cost and security optimization framework.

Through structured analysis, targeted remediation, and continuous governance, this solution balances operational efficiency with strong security controls and long-term sustainability.