

# Feature Overview

Cloud cost management, Cloud Ops, Cybersecurity and security scans across AWS, Azure, and Microsoft 365.

- Features

# Features

## Cloud FinOps

Managing financial operations within cloud environments, enabling cost optimization, budget monitoring, and efficient resource allocation.

- **AWS & Azure Cost Analyzers** - Provides detailed insights into cloud spending patterns, cost trends, and optimization opportunities to improve financial visibility.
- **AWS Saving Opportunities** - Identifies potential cost-saving recommendations by analyzing current resource usage and highlighting opportunities such as Reserved Instances and resource optimization.
- **AWS Costmap** - Visualizes daily AWS service costs and usage distribution across services, helping teams understand spending behavior and identify high-cost services.

## CloudOps

Efficient management and monitoring of cloud infrastructure to maintain operational efficiency and resource utilization.

- **Resource Manager** - Provides a centralized inventory of cloud resources across multiple services, enabling users to track and manage infrastructure components from a single interface.
- **Unutilized AWS Resources** - Detects idle or underutilized AWS resources that can be optimized or removed to reduce unnecessary cloud spending.
- **AWS Resource Optimizer** - Identifies opportunities to right-size resources across services such as EC2, EBS, and other compute or storage components to improve performance and reduce costs.
- **CloudOps Automation (IaC Automation)** - Automates the provisioning and management of cloud infrastructure using Infrastructure-as-Code modules such as Terraform for services like VPC, ECS, EC2, RDS, CloudFront, and IAM.
- **Azure WAR** - Evaluates Azure cloud architecture against Microsoft's Well-Architected Framework best practices. The review analyzes workloads across key pillars such as reliability, security, cost optimization, operational excellence, and performance efficiency, helping teams identify architectural risks and improvement opportunities.

## Cyber Security

Identify and mitigate risks associated with cyber threats across integrated systems and applications.

- **OSINT Analysis** – Monitors publicly available information to detect potential security risks, exposed assets, and vulnerabilities related to domains or applications.
- **DAST (Dynamic Application Security Testing)** – Performs security testing on web applications to identify vulnerabilities such as misconfigurations, injection flaws, and insecure endpoints.
- **Network Security Analysis** – Identifies exposed ports, security group risks, and network configuration weaknesses that could allow unauthorized access.

## Cloud Security

Identify security vulnerabilities and maintain compliance with industry security standards and regulatory frameworks.

- **AWS CIS v5.0** –Evaluates AWS account configurations against CIS security best practices.
- **AWS PCI DSS v3.2.1** – Maintains a secure environment for cardholder data.
- **AWS GDPR** – Strengthens compliance with data protection regulations.
- **AWS SOC2** – Provides assurance of security controls.
- **Azure ISO 27001** – Addresses information security management requirements.
- **Azure SOC2** – Enables security auditing and monitoring.
- **Azure CIS v2.1.0** – Implements best practices for secure configurations.
- **Microsoft 365 Security** – Ensures compliance and secure collaboration.
- **Entra ID Security** – Enhances identity security and compliance.

## Workload Security

Secure workloads deployed across various cloud platforms.

- **AWS AMI** – Identifies vulnerabilities in AMIs to improve security.
- **AWS ECR** – Detects vulnerabilities in ECR container images.
- **Azure ACR** – Ensures secure containerized applications in Azure Container Registry.

## Agentic AI

Provides an intelligent AI-powered assistant that helps users analyze cloud data, generate reports, and receive recommendations through conversational interaction.

- **AI for Finops** – Produces detailed cybersecurity analysis reports by evaluating vulnerability scans, compliance data, and security insights.
- **AI for Cybersecurity** – The AI Assistant will begin generating the Cyber Security report based on the provided details.

## Issues Board

The **Issues Board** provides a centralized interface for tracking and managing operational and security issues identified across the platform. Users can monitor issues based on **severity levels, status, and service categories**, enabling teams to prioritize remediation tasks and track progress across cloud environments.