Financial Services

Refactoring API Management with Gloo Gateway for Saving Costs, Gaining Multi-Cloud Capabilities, Achieving Zero Trust, and Increasing Revenue

Industry
Data Analytics

Revenue
$1.4 Billion

Location
North America

A data analytics company is focused on credit scoring services. In their pursuit of providing accurate reporting and analytics, the company is on the cutting edge of predictive analytics, business rules management, and optimization.

Business Objective

The company aims to grow online revenues from $1.5 billion to $10 billion annually, a nearly 10-fold increase. To accomplish this, they are building a platform to serve both internal and external API marketplaces, from which a developer can log in to explore and consume internal and external partner APIs.

To aid in the discovery, modern portal technologies need to be implemented. While the company primarily operates on AWS, the business is driving toward multi-cloud in order to fuel growth as well as requirements of their customers.

In order to operationally scale to expected demand, the re-designed platform requires improved support for Cloud Native CI/CD and automation tools, including ArgoCD and Crossplane.

$1.5B — Today
$3B — 2024
$10B — 2030

solo.io
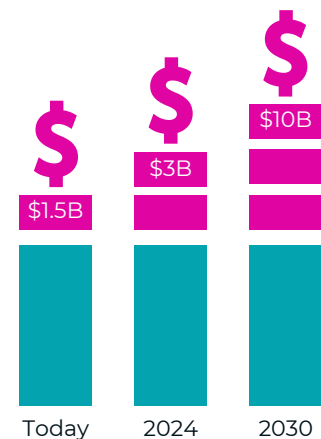
Solution

Our customer's transformation journey involves a shift from a monolith to a microservices architecture, including the adoption of Amazon's Elastic Kubernetes Service (EKS), Elastic Compute Cloud (EC2), and the future use of AWS Lambda functions. As a financial services company, our customer is hyper-focused on ensuring the security of their applications, and they are driving towards a "secure-by-default" approach and zero trust security model.

The company aims to create a unified networking platform, integrating gateway, portal, and mesh components into a single platform, which will reduce the operational overhead of managing disparate networking elements. This unified solution will include both north-south and east-west traffic with authentication and authorization using OIDC and OPA and service-to-service communication with mTLS enforcement for all services.

Why Choose Solo.io?

Gloo Gateway is the foundation for all cloud networking capabilities in the customer's new SaaS platform built on AWS and ready to scale to a multi-cluster, multi-cloud deployment.

Our customer's goal is to provide developers with self-service capabilities for APIs and service meshes, and this solution will allow developers to manage security policies, critical infrastructure, core observability, and multi-tenancy themselves.

Gloo Gateway allows our customer to unify management of north-south and east-west traffic to gain operational efficiencies by unifying the API gateway and service mesh functions together.

solo.io
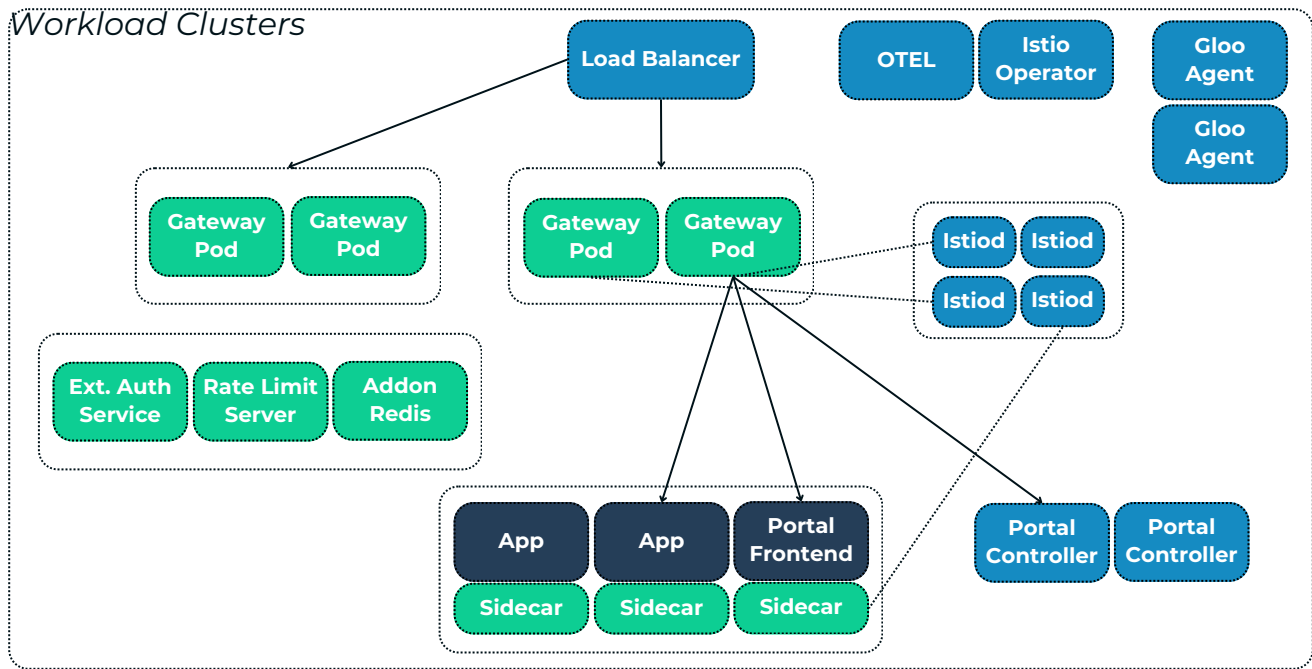
Gloo Gateway enables our customer to better manage their APIs to connect with their external users as they control access to their paying customers. One of the requirements was to use OPA to determine which APIs a developer has access to.

Finally, the implementation of a zero trust security model is a key outcome. Security for north-south traffic with Gloo Gateway is using OPA to provide a standardized approach to secure traffic coming through the gateway. **Gloo Mesh** adds key east-west security with features such as workspaces and workspace isolation and shared root trust for mTLS across clusters.

The developer self-service aspect will also extend to defining operations teams' policies, aligning with the principle of "least privilege" that underpins the zero trust model. These changes will enhance security and operational efficiency, while empowering developers.

About Solo.io

Learn More