gslab | GAVS

CASE STUDY

Robust Security through IDAM
for Customer Experience Automation Platform

Customer Overview

The customer has an AI-powered digital customer experience automation, no-code platform to automate and transform entire customer journeys. The cloud-native, SaaS platform is a complete omni-channel solution delivering intelligent automation with hyper-personalized user experiences. Innovation and faster time to market through rapid solution delivery with little or no code is its USP.

The Context

The customer wanted to establish secure access mechanisms for their automation platform. They had developed an authorization service framework, but it needed adapters to communicate with different Identity Providers (IdPs) such as AWS Cognito, OneLogin, Keycloak, and others.

Type of Service Provided

Identity and Access Management

Technologies Used

MongoDB, Amazon Cognito
Java, Quarkus Framework

The Solution

The GS Lab | GAVS team performed extensive evaluation of leading IdPs based on factors such as security, integration, resource usage, pricing, etc. and followed it with comprehensive planning and implementation to build a cost efficient and productive model. Some key features:

- Detailed requirement specs and integration points for the Identity Service - created using an adapter pattern and as a wrapper for other IdPs
- Single tenant architecture that supports multiple applications, organizations
- Recommended use of the Identity Service only for authentication and the customer's platform for authorization – for adherence to IAM standards and zero trust policy
- Identity Service enables management of users, applications, organizations, and performs application-wise user authorization; Auth Service performs role-based user authorization
- Highly secure service provisioning APIs (user management, onboarding, auditing, reporting) using enterprise JWT tokens
- Defined interface that every IdP adapter needs to implement
- Implemented adapters for AWS Cognito, OneLogin, Okta, Keycloak
- AWS Cognito used as IdP; underlying IdP can be changed to any of the above by implementing services of the provider
- Users can be given access to multiple applications, organizations
- User data is only stored on the IdP
- Supports authentication using federated applications such as Google, OneLogin, Okta, or any IdP that supports SAML or OIDC authentication flows

To find out how GS Lab | GAVS can help your organization, please visit **www.gavstech.com**

Challenges

- Lack of a robust service for user authentication and authorization
- Absence of adapters for different IdPs
- Several issues moving from the previous multi-tenant architecture on customer request

Solution Highlights

- Requirement specs and integration points for Identity Service
- Single tenant architecture that supports multiple applications, organizations
- Services for management of users, applications, organizations
- Identity Service used for authentication and automation platform for authorization
- Highly secure service provisioning APIs
- Definition of interface to be implemented by IdP adapters
- Implementation of adapters for AWS Cognito, OneLogin, Okta, Keycloak
- Support for authentication using federated applications

Solution Impact

- Rapid TAT – implemented solution much before accepted timelines
- Improved operational efficiencies
- Highly flexible solution providing choice of multiple IdPs

gslab | GAVS

CASE STUDY

Robust Security through IDAM
for Customer Experience Automation Platform

Solution Architecture