



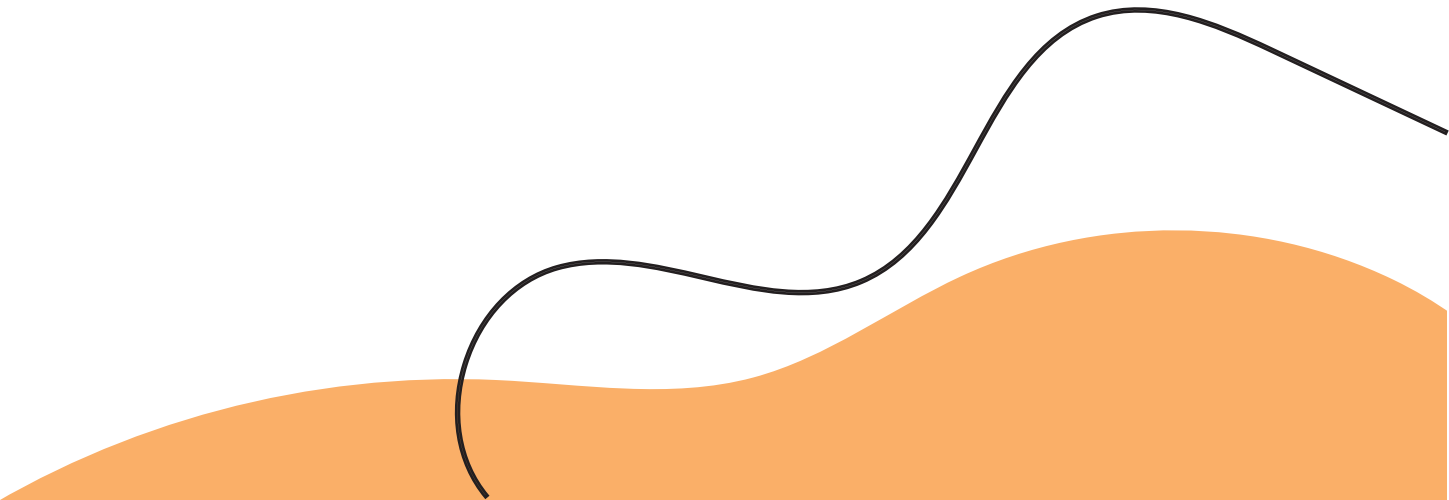
# ZLURI SECURITY

Whitepaper



# Table of Contents

Introduction .....	1
Principles .....	1
Organization & People .....	1
Infrastructure Security .....	2
Platform Security .....	2
Authentication & Role-based access control .....	2
Customer Metadata .....	2
Secure Internet Connectivity .....	2
Secrets Management .....	2
Zluri Architecture .....	6
Product Development: .....	5
Data Retention & Removal .....	5
Penetration testing .....	5
Conclusion .....	6



# Introduction:

Our valuable customers are our first priority, and we take utmost care to protect your data & sensitive information. We are keen on earning your trust and working towards offering the best in class privacy and security configurations. Also, we deem to provide transparency into our security programs to gain and maintain your trust throughout. This whitepaper explains how we store & secure your sensitive information.

## Principles:

The following principles guide us when designing the product:



### 1. Minimum data collection

We collect as little metadata as required to provide accurate insights to the administrators about the SaaS usage in their organization.



### 2. Transparency

We clearly illustrate the data we collect and how we use them.



### 3. Security:

We constantly try to secure all sensitive data through best-in-class technology infrastructure & processes.

## Organization & People

Zluri has a security team led by a CISO which constantly monitors the security health of the platform. The CISO reports directly to the CEO. All employees are hired after a thorough background verification process. Also, each employee undergoes mandatory security training.

# Infrastructure Security

Zluri platform is exclusively hosted on AWS. This enables us to take advantage of Amazon's world-class infrastructure & ensures high availability. We also use AWS KMS & Secrets Management services to protect your sensitive data at rest.

For more information about Amazon Web Services' security, please go through their security documentation at <https://aws.amazon.com/security/>.

## Platform Security

### Authentication & Role-based access control

Zluri enables you to set up SAML-based authentication for access into Zluri with other popular providers such as Okta, Microsoft Azure, and G Suite. Also, it uses the industry-standard platform - Auth0 for authentication and authorization services. Apart from this, the sign-on to Zluri is protected by 2-factor authentication.

Zluri is pre-configured with several roles that enable different levels of access to different aspects of the platform. This includes control of financial data, specific apps, or user management.

### Customer Metadata

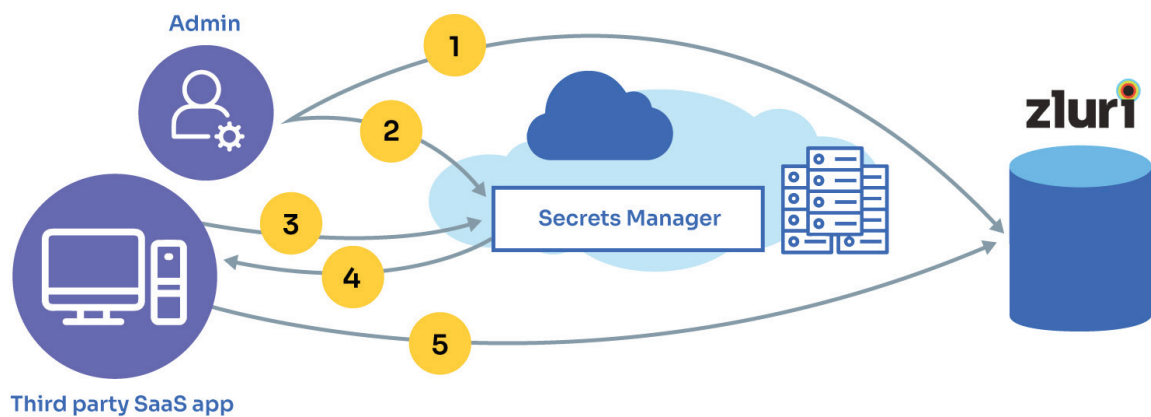
An important point for our customers to understand is what data elements we process. We collect basic metadata about your organization's employees & their SaaS usage. It comprises their email ids, groups, departments, sign in & sign out activities, etc.

### Secure Internet Connectivity

All Zluri's externally-facing services use HTTPS TLS version 1.2 or higher to ensure encryption in transit of all customer information, irrespective of where that connection is established.


### Secrets Management

Zluri's platform helps our customers store sensitive information such as API keys, access tokens, scopes, usernames & passwords required to connect to third-party applications. We store & protect these using AWS Secrets Manager. The diagram below illustrates how a basic secrets manager works.





As an organization administrator, when you connect to a Third-Party SaaS App through OAuth, we generate the access token & refresh token, which we store in the AWS Secrets Manager. Whenever we need to run the sync, we fetch the secrets from the Secrets manager to connect to the application. You can also choose to store the secrets in your own Secrets Manager account.

#### Your secret store


Zluri Secret Store (Default)

#### Migrate

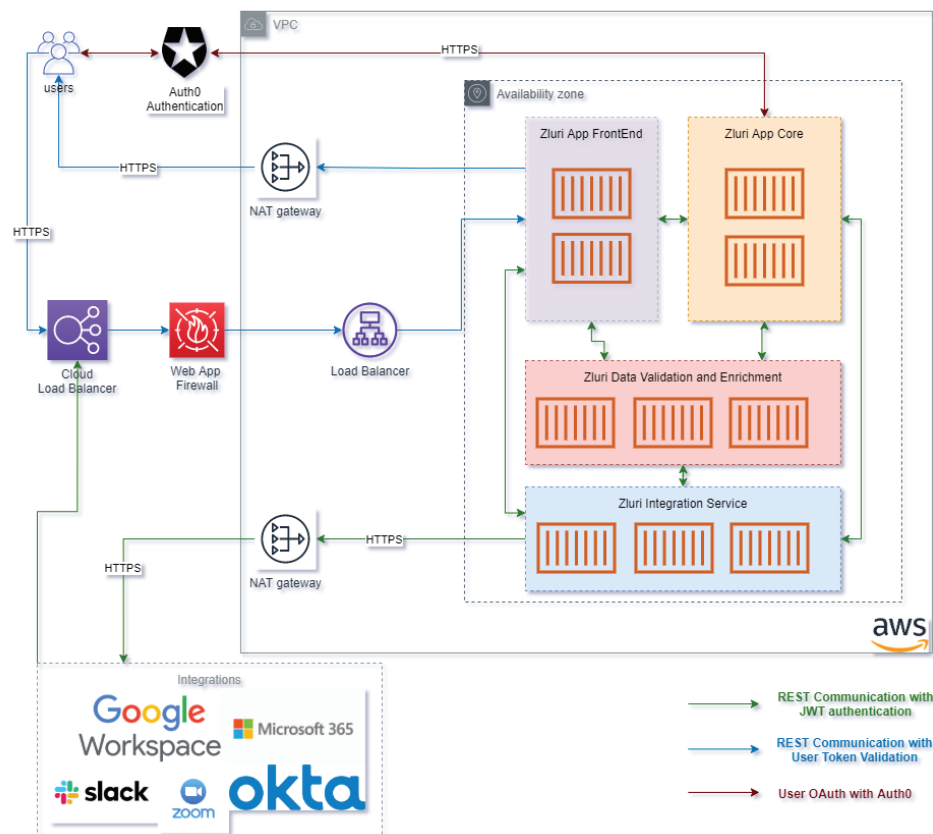

Your AWS Secret Manager


GCP Secret Manager

The flow is similar to the one described above.

In this case, you can store your secrets in your own Secret store. Whenever Zluri requires the credentials to connect to your account in the 3rd party SaaS application, Zluri will request secrets from your own secret store.

# Zluri Architecture



The above image provides an overview of our architecture.

We restrict the data flow using AWS Web Application Firewalls & other technologies like Subnet & security gateways. The data flows are permitted using only specific rules in AWS using NAT gateways & security groups. AWS services also protect the data on disk with encryption at rest.

The communication between the application & the user's browser is secured with HTTPS using TLS v1.2 or above. Auth0 handles user's authentication with SSO identities provided by Google, Microsoft Office 365, etc.

The incoming traffic goes through an AWS load balancer which can scale to handle any loads. The traffic then goes through the AWS Web application firewall. This protects the data flows, which looks into allowing traffic from authorized sources and blocks any malicious traffic. It also blocks cross-site scripting, DDoS attacks, and SQL injection scripts.

All requests are passed through internal load balancers and are authenticated with Json Web Tokens (JWT). Network connections from internal hosts to external resources leave the environment via the NAT gateway, where all traffic is inspected.

## Product Development:

We put security at the center of our product development process. From conceptualization to designing, implementation & ongoing operations - security is embedded into the product feature at every stage. We ensure that any new feature does not create unnecessary privacy implications for our customers. Also, Security testing is performed with every release, both in an automated and manual fashion.

## Data Retention & Removal

You can control the data that your employees can access through Zluri. To attain maximum value from Zluri's data analytics, it requests access to your employee PII data like employee first name, last name, corporate email address, office location, and phone number, etc. You may request us to remove any pieces of information about your organization. All your data is stored in an encrypted state, backed up to 60 days. All the collected customer data, such as SaaS-app usage metrics, will be retained indefinitely unless requested to be removed by you. You can read more details in our Privacy Policy and Data Retention Policy Documents (<https://www.zluri.com/privacy-policy>).

Zluri presents you with comprehensive and auditable logs of key activities to keep you informed.

## Penetration testing

We constantly engage in third-party audits for conducting penetration tests, which are done by replicating the most malicious hacking attacks and strategies.

Please reach out to our support team for the latest security reports.

## Compliances

Zluri's MSA and DPA norms are supported by the people, processes, and technology necessary to protect customer personal data in compliance with legal and contractual obligations for regulations such as GDPR and CCPA.



## GDPR:

Zluri complies with all requirements outlined by the General Data Protection Regulation & is certified by them. As we have provided in our Data Processing Addendum, the parties acknowledge that as per articles in GDPR, Zluri is either Controller (responsible for the processing of personal data of its employees or personal data and related information, including profiling of data subjects using its platform) Or Zluri is the Processor for personal data (personal data and related profiling information of customer's employees) on behalf of its customers who are here with designated as controllers. The performance of the services will require the processing of personal data by the supplier as a Processor where Zluri is designated as Controller or Sub Processor where Zluri is designated as Processor. Zluri can assist customers in fulfilling their obligations as data controllers by

- Supporting customers in complying with requests from Data Subjects
- Aggregating applicable personal data for customers replying to requests from Data Subjects.
- Replying to investigations and inquiries from supervisory authorities concerning processing activities on behalf of a customer.
- Conducting Data Protection Impact Assessments.

Our Data Protection Addendum can be found [here](#).

You can review our GDPR Certificate [here](#).



## SOC 2:

Zluri maintains an annual SOC 2 - Type 2 report performed by an independent third party, certifying that our platform meets all the requirements for security and confidentiality as defined by AICPA.

Detailed SOC2 Report can be shared on request to our support team.





### ISO 27001-2013:



Zluri is ISO27001 certified by a third party, providing a platform for discovering, managing, securing, and optimizing SaaS applications. This International Standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the organization's context. This International Standard also includes requirements for the assessment and treatment of information security risks tailored to the needs of Zluri.

You can review our ISO Certificate [here](#).

## Conclusion

We understand that you have come to us to secure your SaaS environment. And, Zluri has taken all these steps to protect your sensitive information seriously against modern-day cyber threats.



 2443 Fillmore St, #380-18045,  
San Francisco, CA 94115  
 +1 628 243 5870