



Building Cloud Confidence

Compliance, Security
Standards, and Regulations



Table of contents

Kissflow introduction	01
Platform architecture overview	01
a. Kissflow features	
b. Multi-tenant SaaS architecture	
Infrastructure security	04
a. Backup and recovery measures	
Data management and security	06
a. What data are managed in Kissflow?	
Application security and functionality	08
a. Extensive integration capabilities	
b. Identity management policies	
c. Access control management	
Organizational security	15

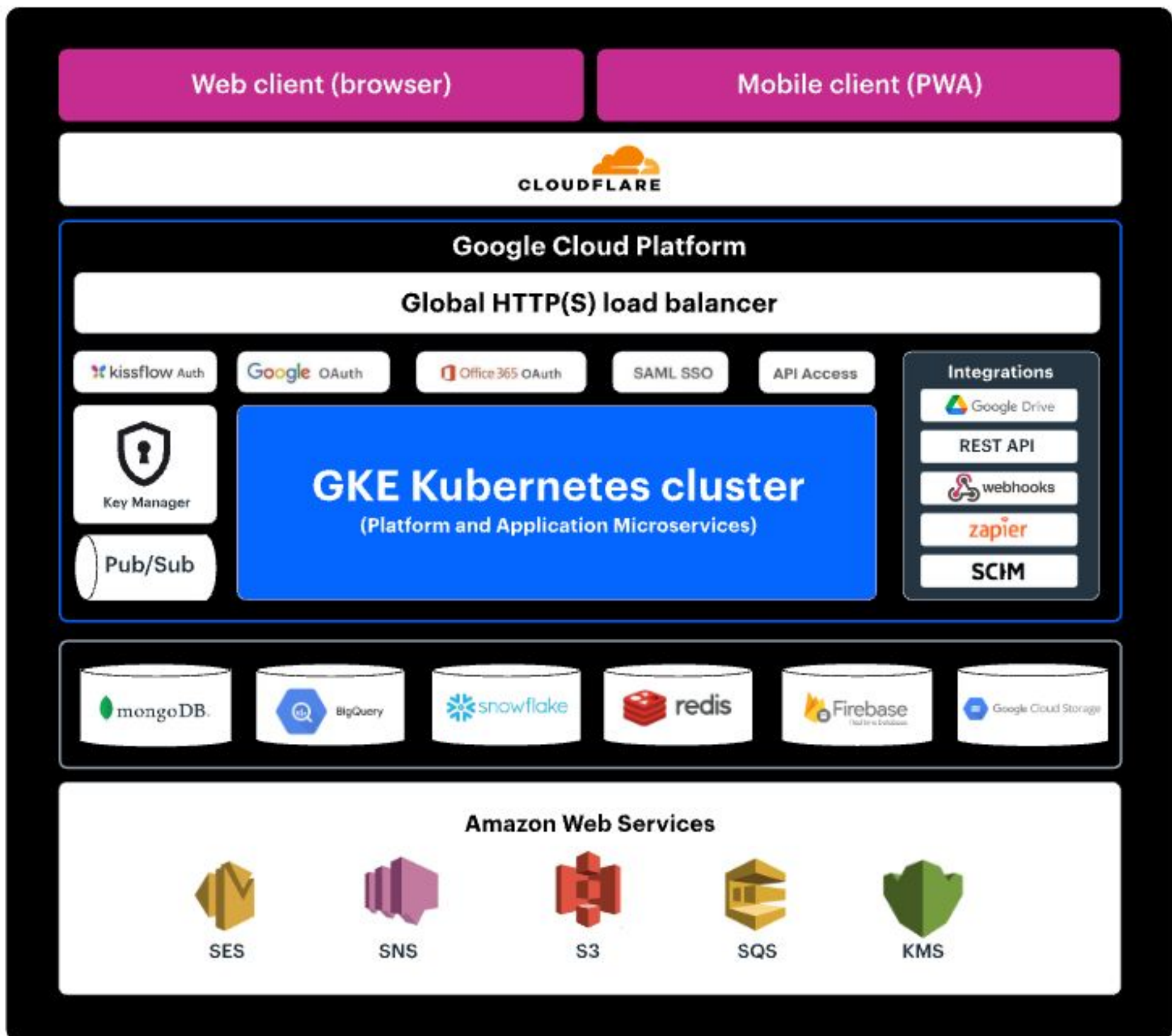


What is Kissflow?

Kissflow is a low-code, no-code platform that solves the problem of custom application development for internal business processes. The platform helps enterprises build fully functional low-code apps, automate processes, and enable citizen development. Development is faster on Kissflow than on any other platform because of its simplicity, speed, and flexibility, which makes it perfect for both tech-savvy and non-tech-savvy users.

Platform architecture overview

Kissflow's technical architecture is built on a scalable, flexible foundation and adapts to your business's evolving needs.



Platform technology

Code Language
Python

Frontend
React

Microservices Architecture
Docker & Kubernetes

Data Streaming
Google Pub/Sub

Data and analytics

Database
MongoDB

Analytics
Snowflake

AI integration and SDKs

Integration
**Integrated
AI services**

SDKs
**Client-side & server-
side SDKs on GitHub**

The perfect blend of simple and powerful features



App Builder

Create fully functional and secure apps with low-code, no-code tools



Generative AI

Build an entire process with AI-suggested fields based on user-inputs



Boards

Get complete visibility into projects and cases with flexible boards



Analytics

Bring in data from across the platform to identify areas for improvement



Process Builder

Build and deploy human-centric workflows with no-code and Gen AI



Integrations

Keep data moving inside and outside of Kissflow with custom connectors

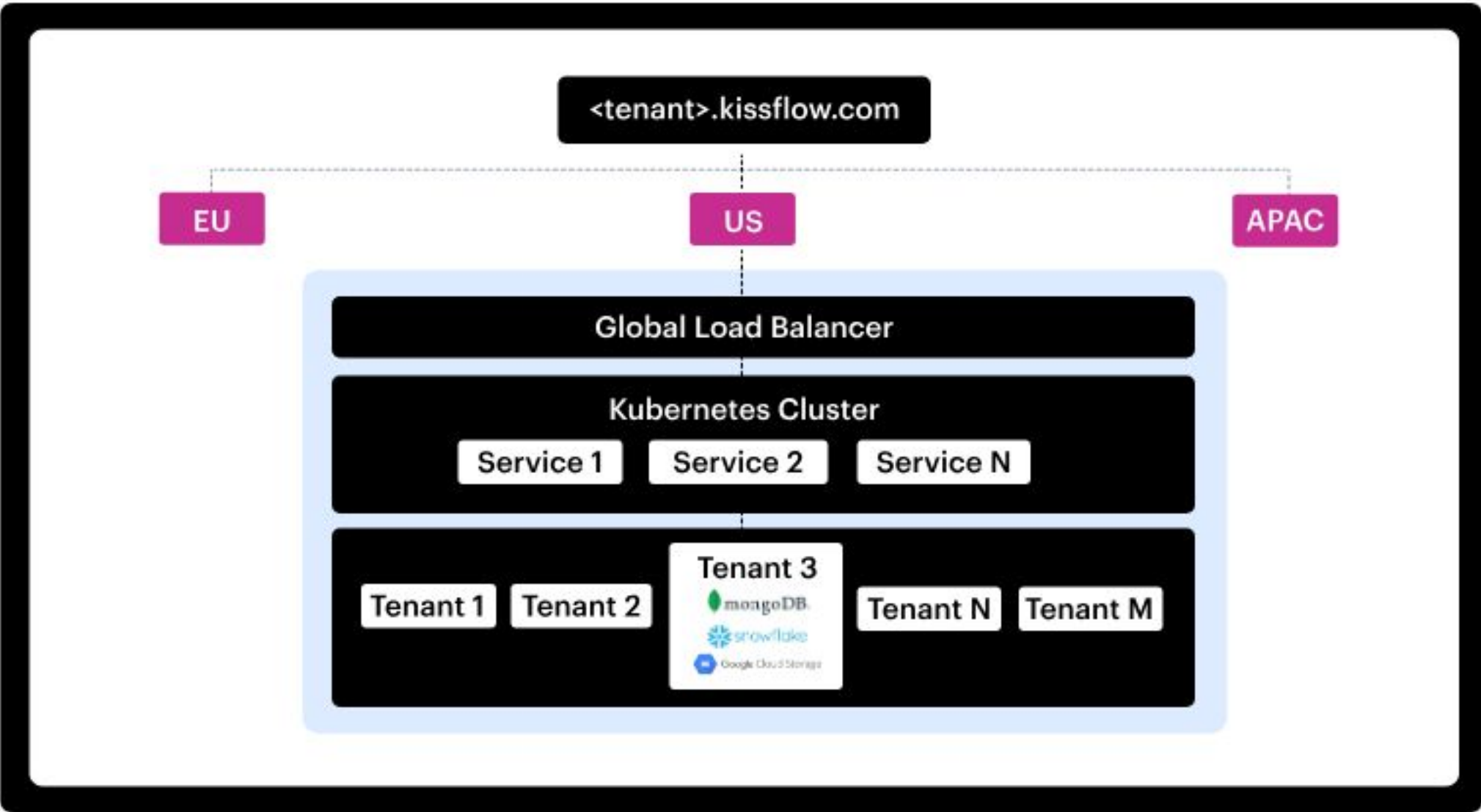
Kissflow multi-tenant SaaS architecture

Kissflow’s SaaS architecture isolates and protects each customer's data and access. It operates in well-partitioned environments that can be scaled according to needs.

Cloud hosting options		
Primary hosting Google Cloud Platform	Other hosting providers AWS	Hosting options Multi-tenant hosting and private clusters

Geographical location

Kissflow has three instances of the platform that meet the needs of different customers.



US instances	EU instances	APAC instances
US-Central-1 Iowa data centers of GCP	EU-West Frankfurt data centers of GCP	Mumbai data centers of GCP

Kissflow offers a private cluster on GCP and AWS for all major regions.

Infrastructure security

Infrastructure security measures include



Network security features such as firewalls and IP whitelisting to safeguard against unauthorized access



Account-level rate limiting to prevent localized attacks and ensure system integrity and performance



Implementation of OWASP guidelines to prevent web application attacks and potential data breaches



Encryption of API calls using TLS 1.2 to secure data transmission between systems



DDoS protection

Kissflow employs a robust DDoS protection service using CloudFlare and reCaptcha that shields against Layer 3, Layer 4, and Layer 7 attacks.



Ongoing DAST and annual VAPT measures

Kissflow ensures platform security through regular Dynamic Application Security Testing (DAST) and annual Vulnerability Assessment and Penetration Testing (VAPT) to proactively identify and address vulnerabilities.

Backup and recovery measures

Kissflow has enforced defined Backup and Recovery Policies in case of disasters.

Recovery Point Objective

Kissflow backups are run every 24 hours, restoring the latest daily backup for stability

Recovery Time Objective

Kissflow recovery time is 48 hours, depending on the nature of the disaster

Backup Availability

Data is backed up every 6 hours and retained up to a maximum of 90 days

★ Disaster recovery

Kissflow has Infrastructure as a Code (IaC) scripts that enable quick deployment of new environments. We also have a strong Disaster Recovery (DR) plan in place, tested annually to ensure business continuity and minimize downtime in the event of disruptions.

🔒 Uptime commitment

Kissflow guarantees 99% uptime for our platform and offers service credits for any downtime. Track our current and historical availability at <https://status.kissflow.com/> Every change to data is meticulously audited and logged for complete transparency.

Data management and security

Encryption

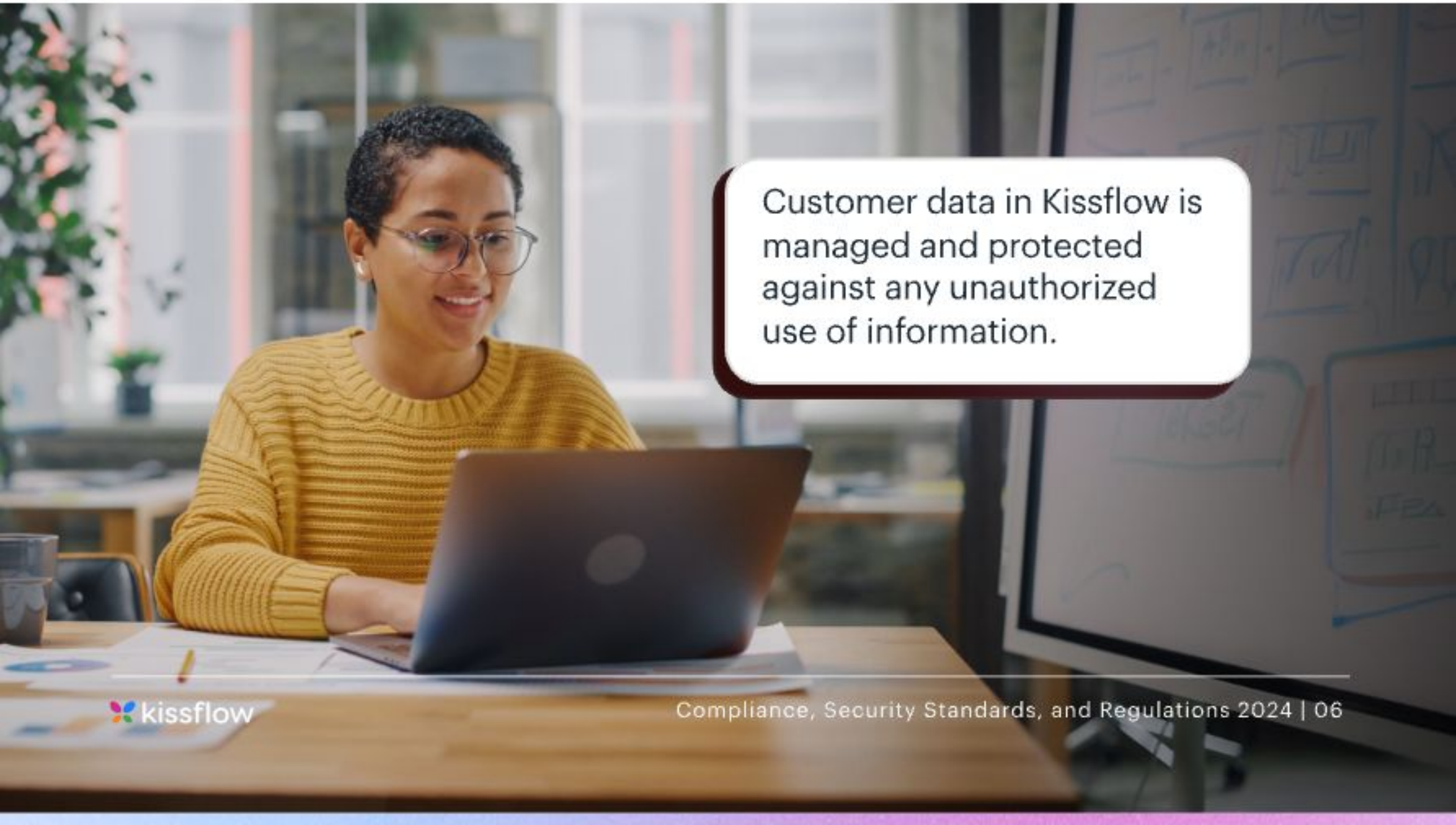
- All files are securely encrypted and stored in Google Cloud Storage, ensuring high availability across multiple regions
- AES 256, the industry standard for encryption, is utilized to encrypt all data at rest on our platform
- The data in transit, either within our network or over the internet, is protected via secure HTTPS using TLS 1.2+ protocol at all times

Retention and deletion of data

Kissflow maintains customer data during service use, but upon termination, all data will be deleted from the production environment within 30 days and from backups within 90 days.

Data portability

Customers can request to export their data in a machine-readable format, ensuring smooth data portability after service termination.

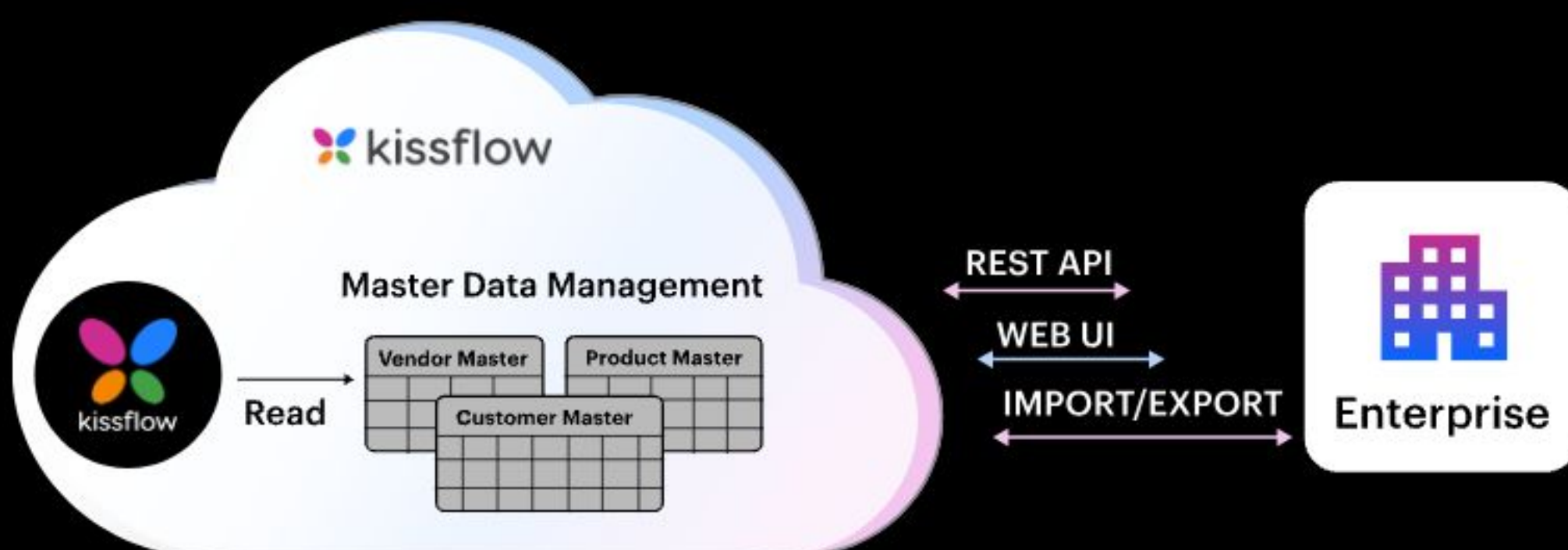


Customer data in Kissflow is managed and protected against any unauthorized use of information.

What data are managed in Kissflow?

🛡️ Master data management

Certain Kissflow apps rely on master data for their functionality. Users can easily create these essential master datasets within Kissflow and organize them into integrated tables that seamlessly work with their apps.



🔗 External data objects

Access the data stored in external platforms like MySQL and MSSQL, eliminating the need to store it within Kissflow. This process simplifies data integration and ensures real-time, secure access to information.

Application security and functionality

The Kissflow application security model is restrictive in nature and enables you to set up application security with the level of granularity needed to meet your requirements.

Secure software development

We follow a strict change management process where all code changes are authorized, tested, and verified before deployment to production.

Source code review

We adhere to secure coding practices and implement rigorous quality checks, including static code analysis, to maintain the highest code integrity.

Automated code deployment

Our CI/CD pipeline automates secure code deployment and eliminates the need for manual intervention.



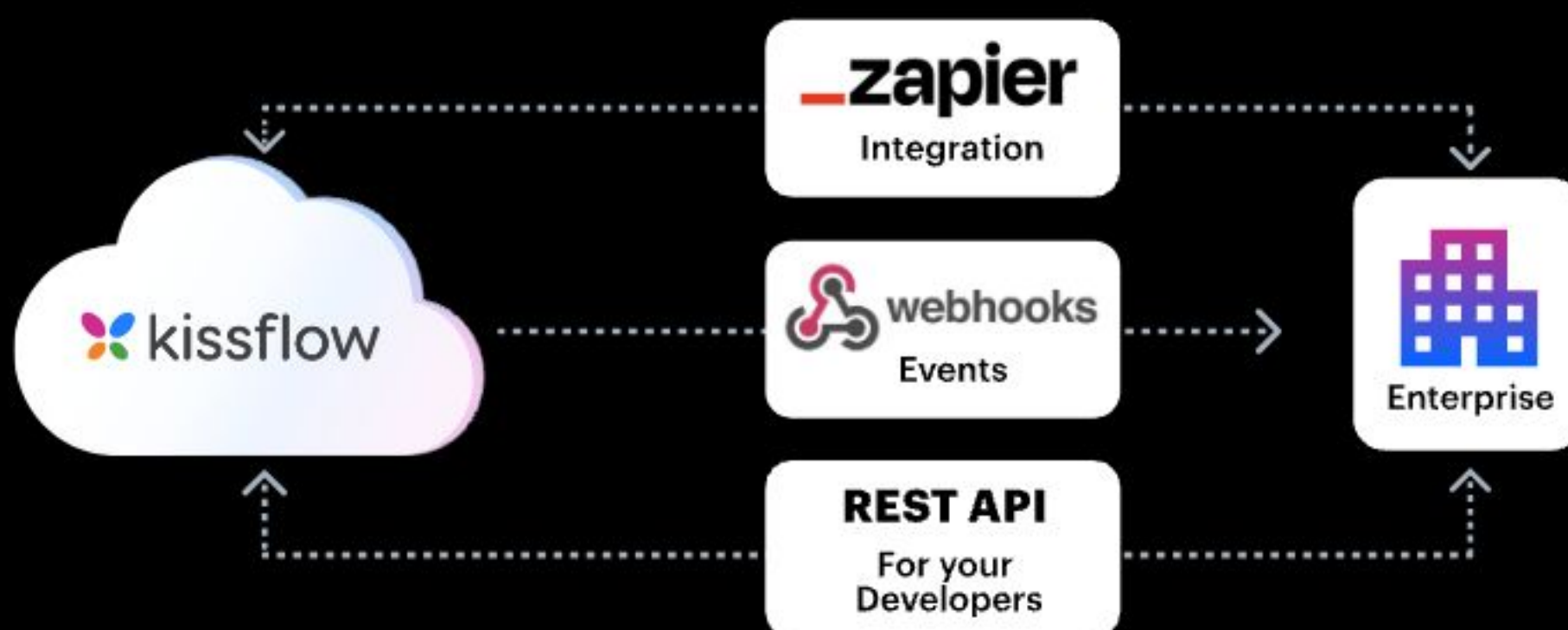
Application security has 3 elements

- Integration capabilities
- Identity management
- Access control management

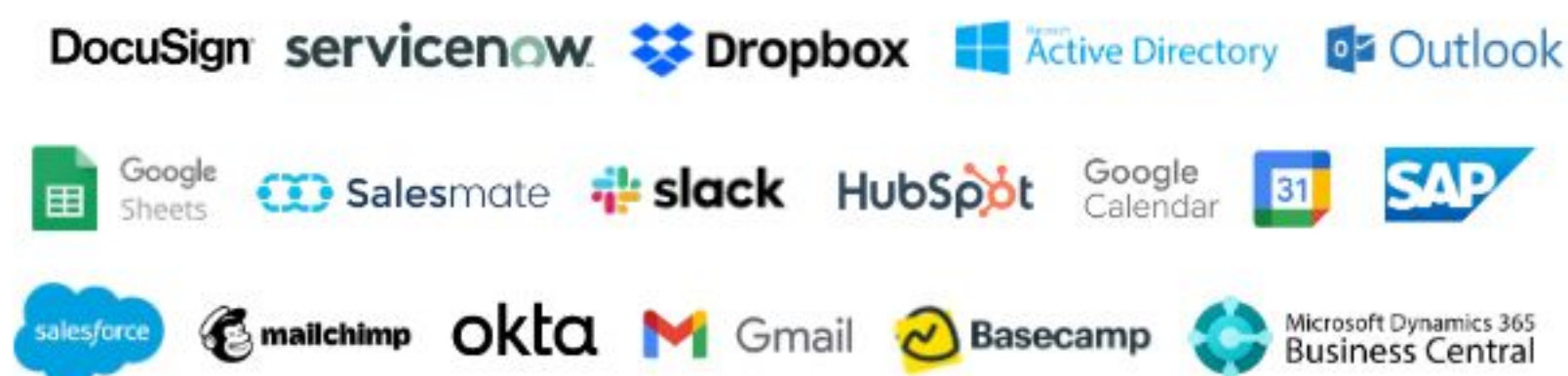
1. Extensive integration capabilities

Kissflow provides various integration options with other SaaS applications and enterprise systems.

- Use a secure REST API to act and access your data in the Kissflow system
- Webhooks events are provided to receive events from Kissflow
- Kissflow uses both Pull/Push integration approaches:
 - Push for generating and consuming events during workflows
 - Pull via REST API for external system details



Kissflow has over **40 internal event triggers** and over **36 no-code connectors** to external systems.



2. Identity management policies

Identity and access management

Govern user-level activities to ensure adherence to organizational policies and regulations

- | | |
|---|--|
| ✓ The identity and role of a user is established during the authentication process | ✓ At any point in time, the identified user is confined to only one Kissflow role |
| ✓ Data access controls are implemented through flow-level roles | ✓ Users can't access data unless it is shared with them by adding them as flow members |
| ✓ Admins have the flexibility to set the file upload source according to their requirements | ✓ Admins can also control file print and download permissions |



Authentication methods

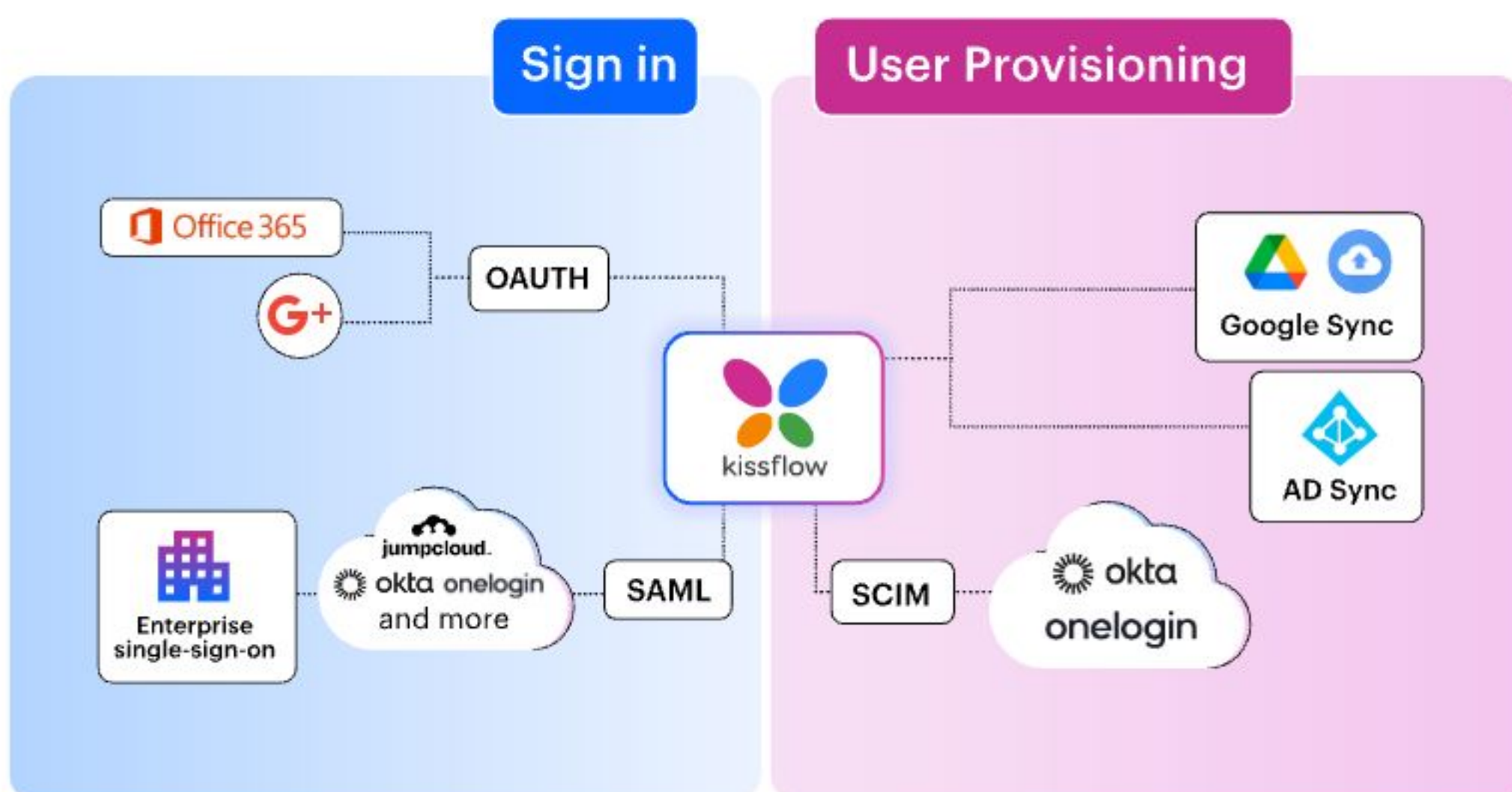
Kissflow provides the following authentication choices for customers:

a. Password policy

- Passwords are managed only by the respective users
- For SSO, Kissflow does not store Google or Office 365 passwords
- Kissflow authentication stores encrypted passwords in the database
- Two-factor authentication can be set up for users for an extra layer of security

b. Single-sign on (SSO)

- Integrate your existing authentication mechanism with Kissflow
- Kissflow delegates the authentication process to the SSO provider using the SAML
- Kissflow supports SAML v2 Protocol integration with your SSO, such as Okta, OneLogin, etc.
- Enforce SSO for Kissflow login via existing GSuite or Office365 credentials using OAuth



c. Role-based access control

- Kissflow users have defined roles based on access control
- Associated privileges are configured by a Kissflow Super Administrator role
- The role management is completely managed by your organization

d. API keys management

User API keys

Users have their own API key for accessing available resources based on their roles and associated permissions.

Service Account API keys

Create bots with configurable access to resources to view common resources from outside the user account or to act on behalf of a user.

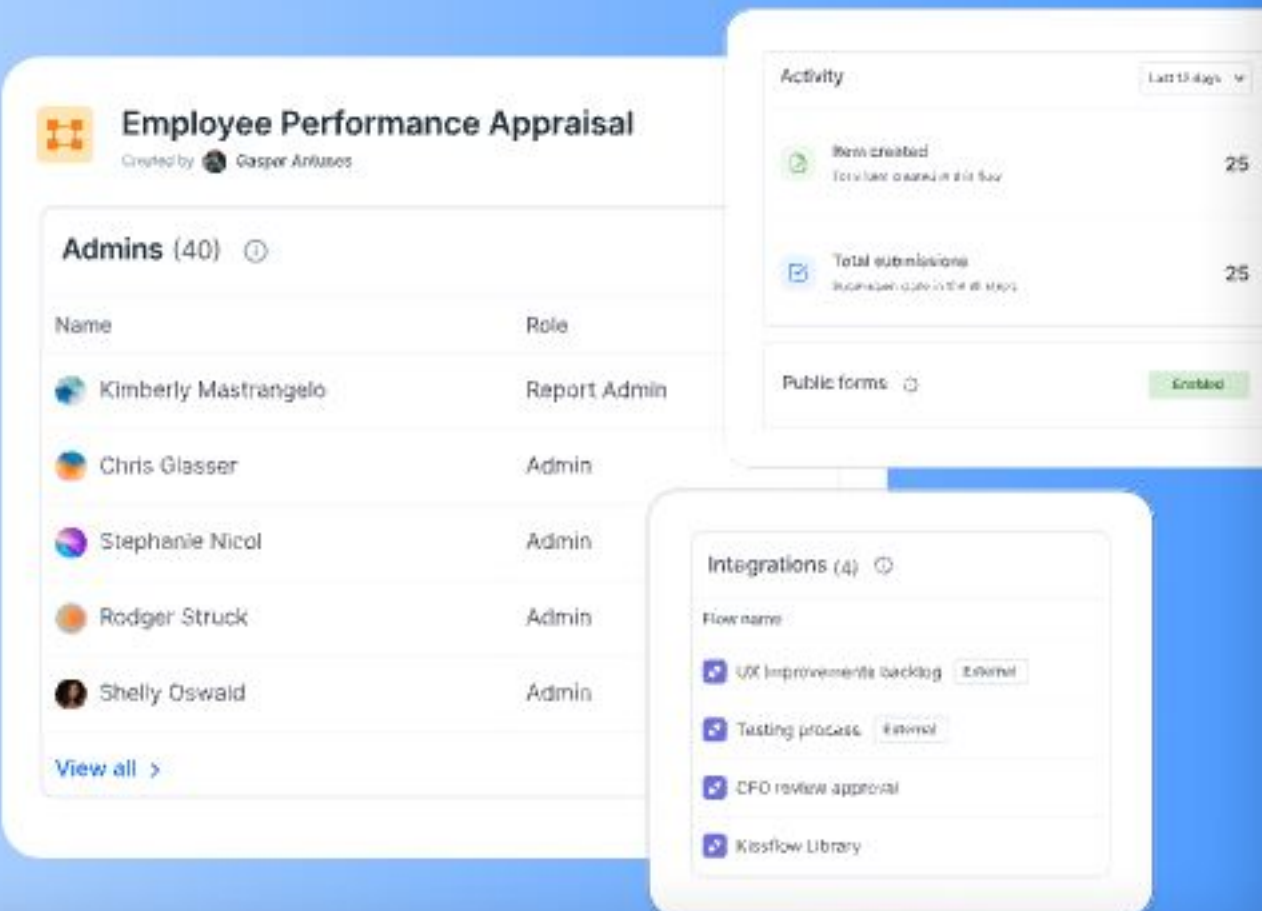
3. Access control management

User-level permissions

- Users can only be added to the platform after approval by an Admin
- Upon user deletion, all associated Personally Identifiable Information (PII), roles, and access to data are removed to minimize security risks
- Users can be temporarily suspended or deactivated without deleting their accounts, providing flexibility in managing user access
- Users can't access data unless it is shared with them by adding them as flow members
- Admins have the flexibility to set the file upload source according to their requirements
- Admins can also control file print and download permissions

Kissflow governance layer

Govern your apps with complete visibility to ensure smooth operations and heightened security.



Employee Performance Appraisal
Created by Gaspar Antunes

Admins (40)

Name	Role
Kimberly Mastrangelo	Report Admin
Chris Glasser	Admin
Stephanie Nicol	Admin
Rodger Struck	Admin
Shelly Oswald	Admin

[View all >](#)

Activity (Last 15 days)

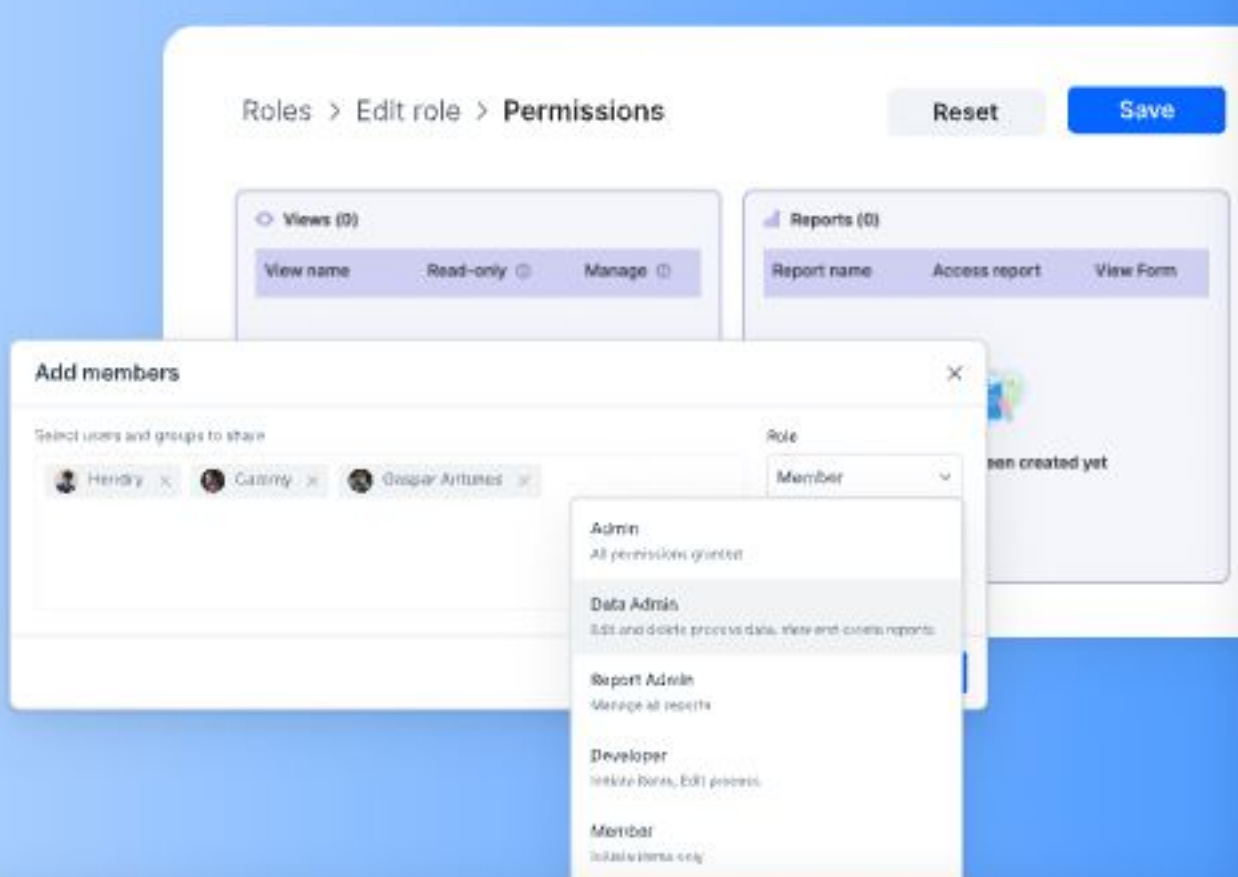
- Item created (Form has been created in 10 days) 25
- Total submissions (Business days in the 15 days) 25

Public forms [View](#) [Enabled](#)

Integrations (4)

- UX improvements backlog [External](#)
- Testing process [External](#)
- CFD review approval
- Kissflow Library

Monitor and keep your apps secure with heightened security protocols and encryption



Roles > Edit role > Permissions [Reset](#) [Save](#)

Views (0)

View name	Read-only	Manage
-----------	-----------	--------

Reports (0)

Report name	Access report	View Form
-------------	---------------	-----------

Add members

Select users and groups to share

- Henry
- Carly
- Gaspar Antunes

Role

Member

Admin
All permissions granted

Data Admin
Edit and delete process data, view and create reports

Report Admin
Manage all reports

Developer
Create forms, Edit process

Member
Submit forms only

Grant controlled access to apps and data by assigning users to specific roles

Emma Schrute Active

Super Admin

Flows (4)

Name	Role	Status
UX Improvements backlog	Admin	Live
Testing process	Admin	Draft
CFO review approval	Member	Live

View all >

Flows created

Processes

35

Boards

27

Apps

32

Gain insights into user behaviour and detect and address any suspicious activity

Access a detailed history of every action and event within your account

Audit logs New audit logs

Last 30 days

Object

Event category

Actor

+4 more

Export

Audit ID	Timestamp	Actor	Event name	Object	Event category	Acc	IP
AUD1234378	19/03/20, 7:52 am	John doe	Approved an Item	Design review	Flow administration	Interactive	123.45
AUD1234377	19/03/20, 7:40 am	John doe	Modified an Item	Design review	Flow administration	Interactive	123.45
First name Jackkk → Jack Last name + Sparrow Email + sparrow@pirates.com Nick name - Jack Manager - Barbossa Group - CTC							
AUD1234376	19/03/20, 7:33 am	Randy	Submitted an item	Design review	Flow administration	Interactive	123.45
AUD1234375	19/03/20, 7:32 am	John doe	Created a process	Design review	Flow administration	Interactive	123.45

Organizational security



Third-party security assessment

We assess third-party vendors' security, review their contracts and obtain compliance audits or certifications. We manage associated risks and promptly address any security incidents.



Business continuity

Kissflow's robust Business Continuity Planning (BCP) ensures uninterrupted service, mitigates risks and enables swift recovery from disruptions or unforeseen events.



Security awareness

All employees receive mandatory security and privacy awareness training, reinforced by posters and regular messages. We help foster a vigilant culture of adherence to best practices.

Looking for more
information?

Contact Us