okta

Thinking about building your own login? It could be harder than you imagine!

Peter Fernandez
Principal Developer Advocate

Introduction

Peter Fernandez

Principal Developer Advocate

I'm an Architect, Consultant and Engineer with more than 30 years experience designing and developing secure and robust software solutions.

When not helping folks with the complexities of identity and access management you can usually find me acting in, or directing, a show at my local theater.

peter.fernandez@okta.com

Terminology

ACRONYM / TERM	MEANING
User Authentication	The process of validating user credentials
User Credentials	The security information associated with a user; typically UserID and Password
MFA	Multi-Factor Authentication. Security information provided in addition to user credentials
CIC	Okta Customer Identity Cloud. Also synonymous with Auth0
Auth0	The engine that powers the Okta Customer Identity Cloud
CIAM	Customer Identity & Access Management
B2C	Business to Consumer CIAM
B2B	Business to Business CIAM
B2B2C	Business to Business to Consumer CIAM
No-Code	Configuration only customizations
Low-Code	Minor code-based customizations
Pro-Code	Complex code-based customizations

Agenda

01 Authentication

02 Authorization

03 Summary

04 Q&A

okta

What is Customer Identity?

Customer Identity & Access Management

- The market space that's essentially focused on Consumer users
  - As well as the Access and Management of the identities associated with those users.

okta

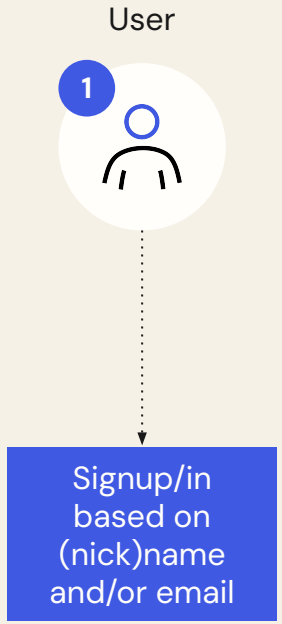
Authentication

okta

Authentication

Typically start with the User Experience

- Create a dialog for Login
  - And a similar one for Signup

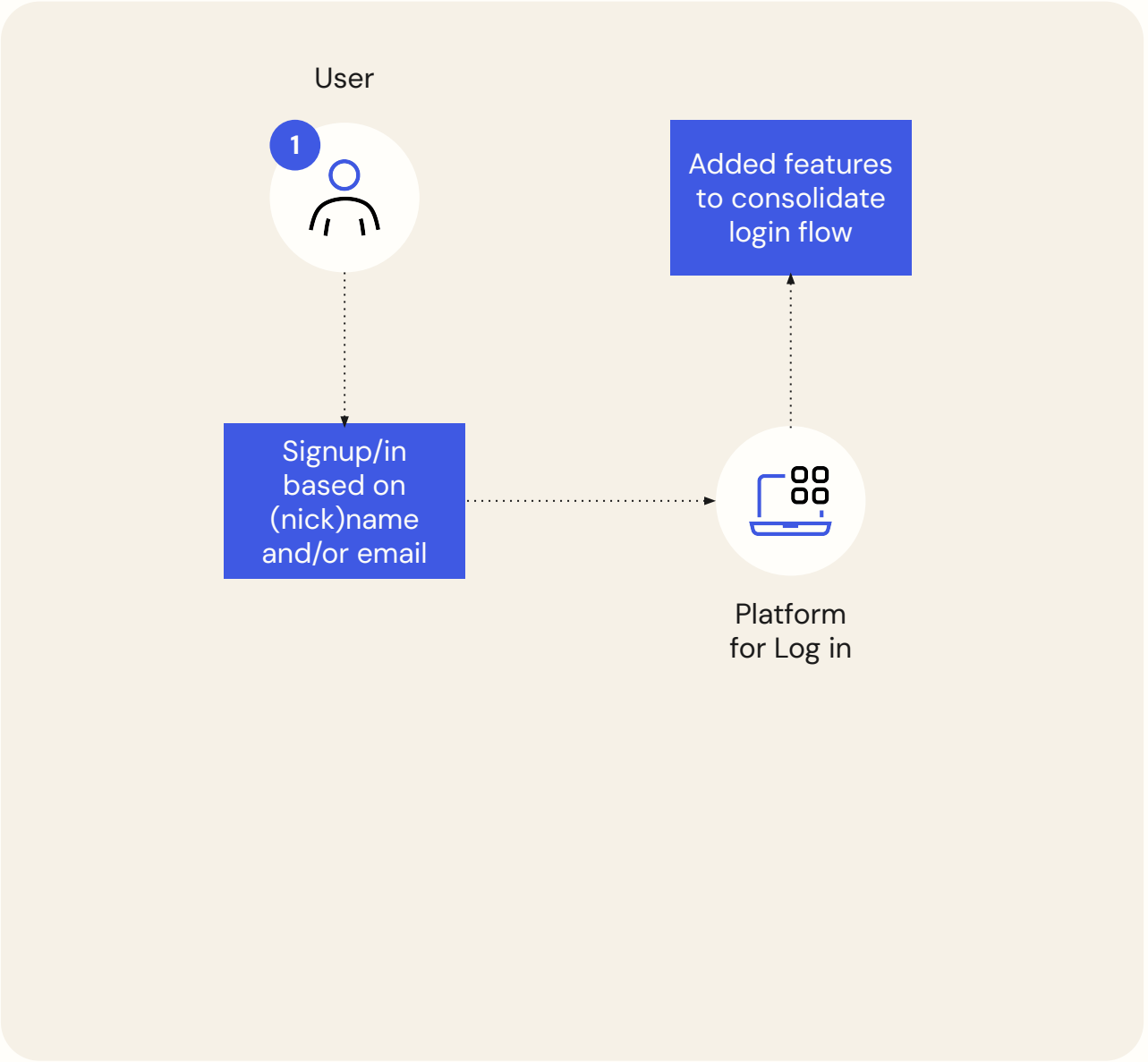


okta

Authentication

Typically start with the User Experience

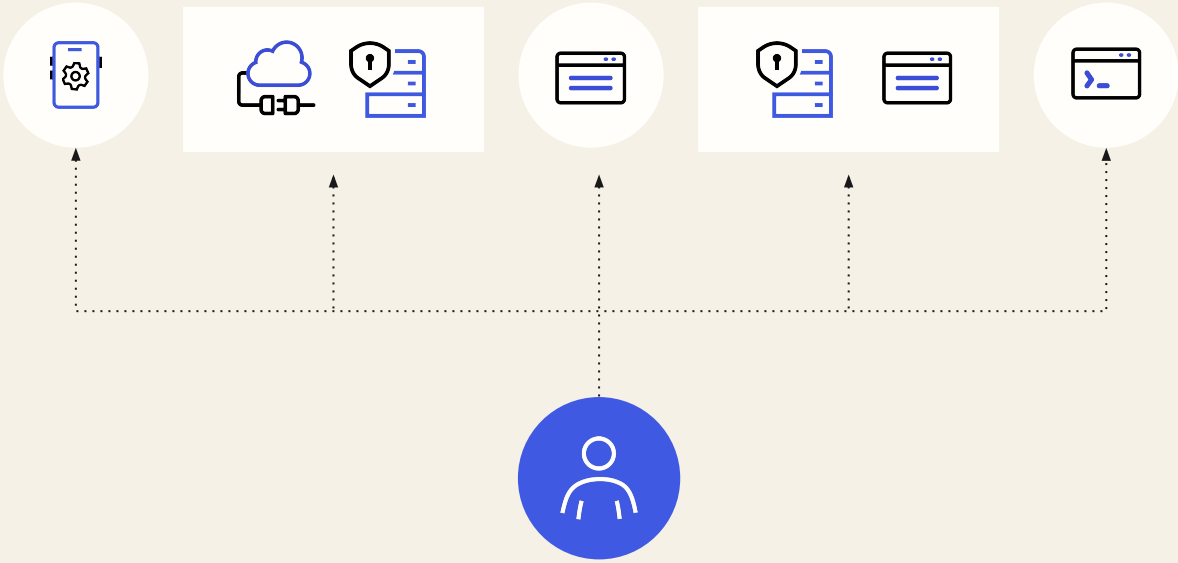
- Create a dialog for Login
  - And a similar one for Signup
- Implement the code to validate credentials
- Consolidate the experience
  - Supporting SSO



okta

Authentication

- Provide a consolidated login experience
- Leveraging the security context of a user

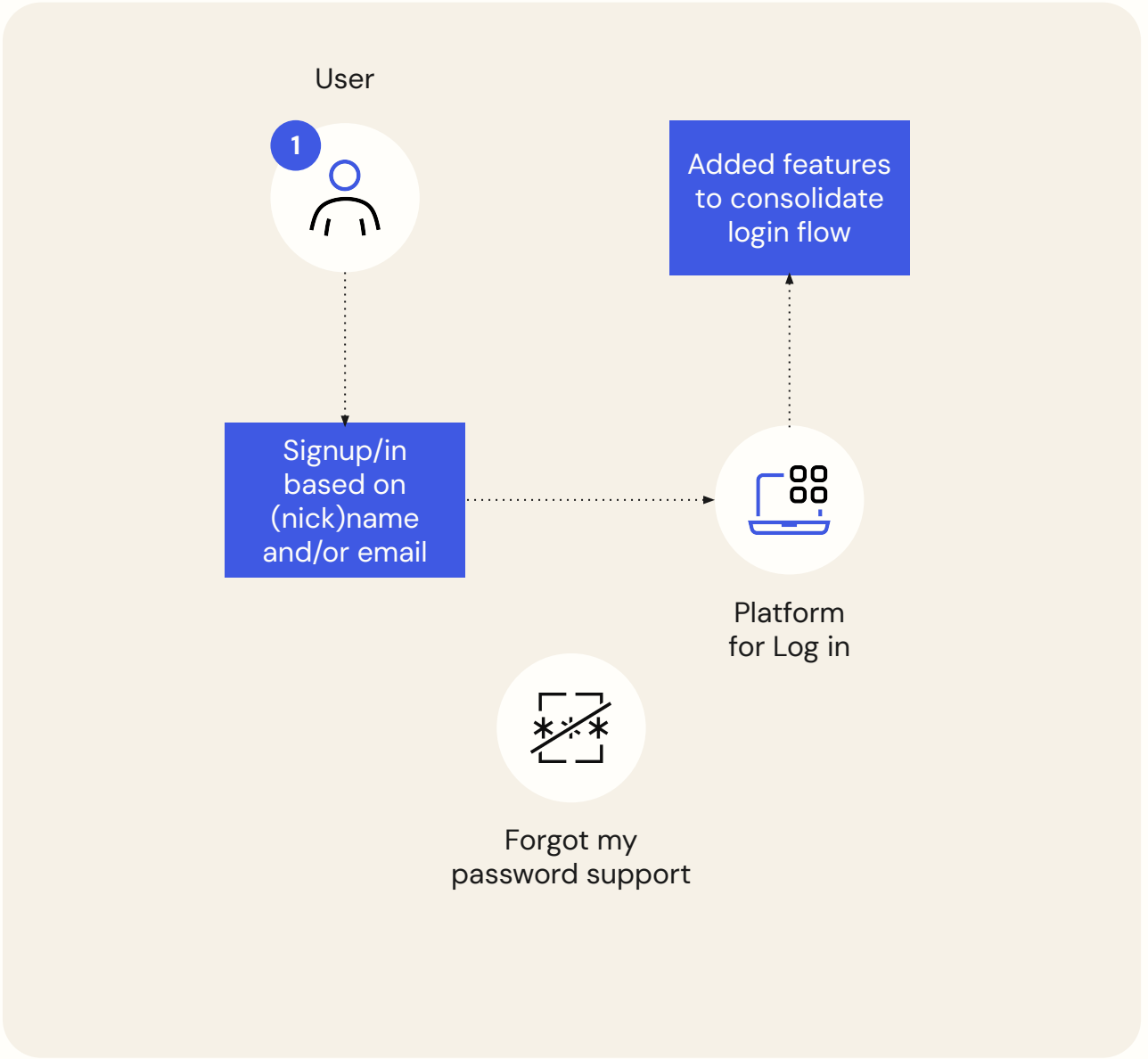


okta

Authentication

Typically start with the User Experience

- Create a dialog for Login
  - And a similar one for Signup
- Implement the code to validate credentials
- Consolidate the experience
  - Supporting SSO
- Iterate through user interface design & testing
- Implement password reset

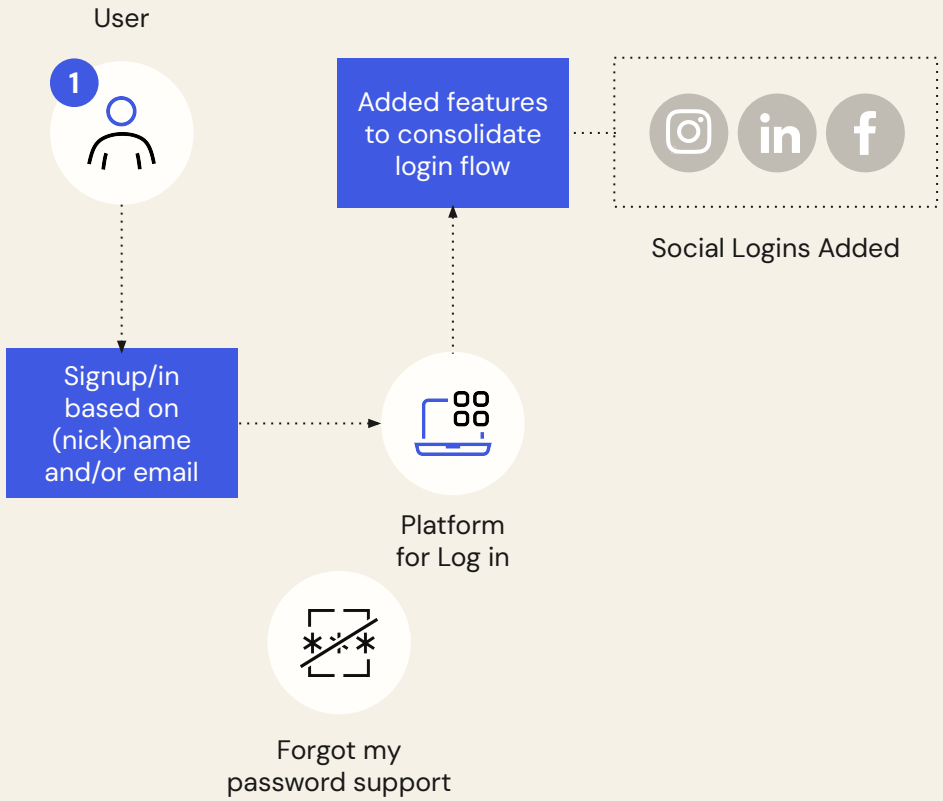


okta

Authentication

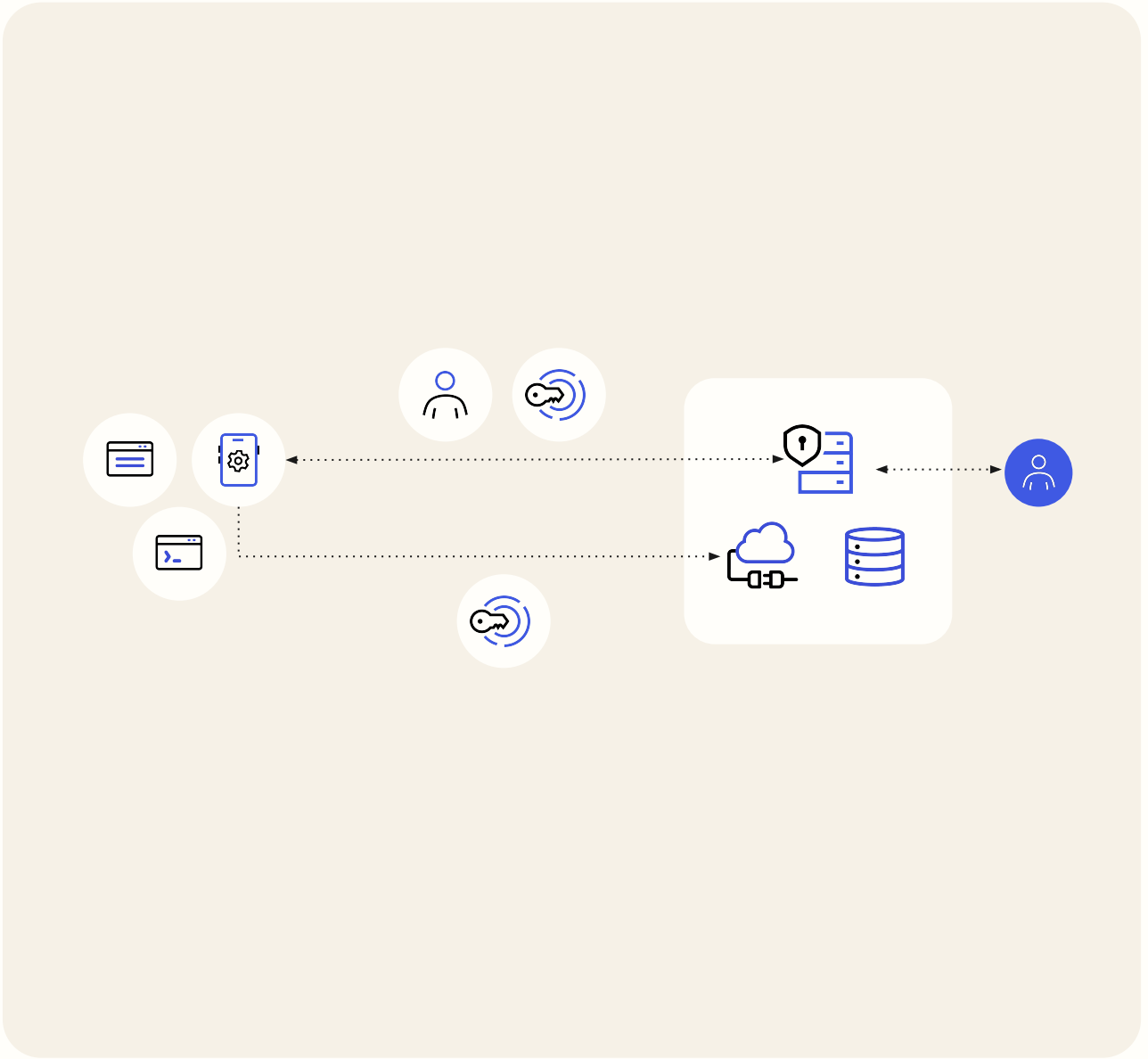
Scaling to provide a more engaging user experience

- Add support for Social Login & Signup
  - Reducing friction in the user experience



Authentication

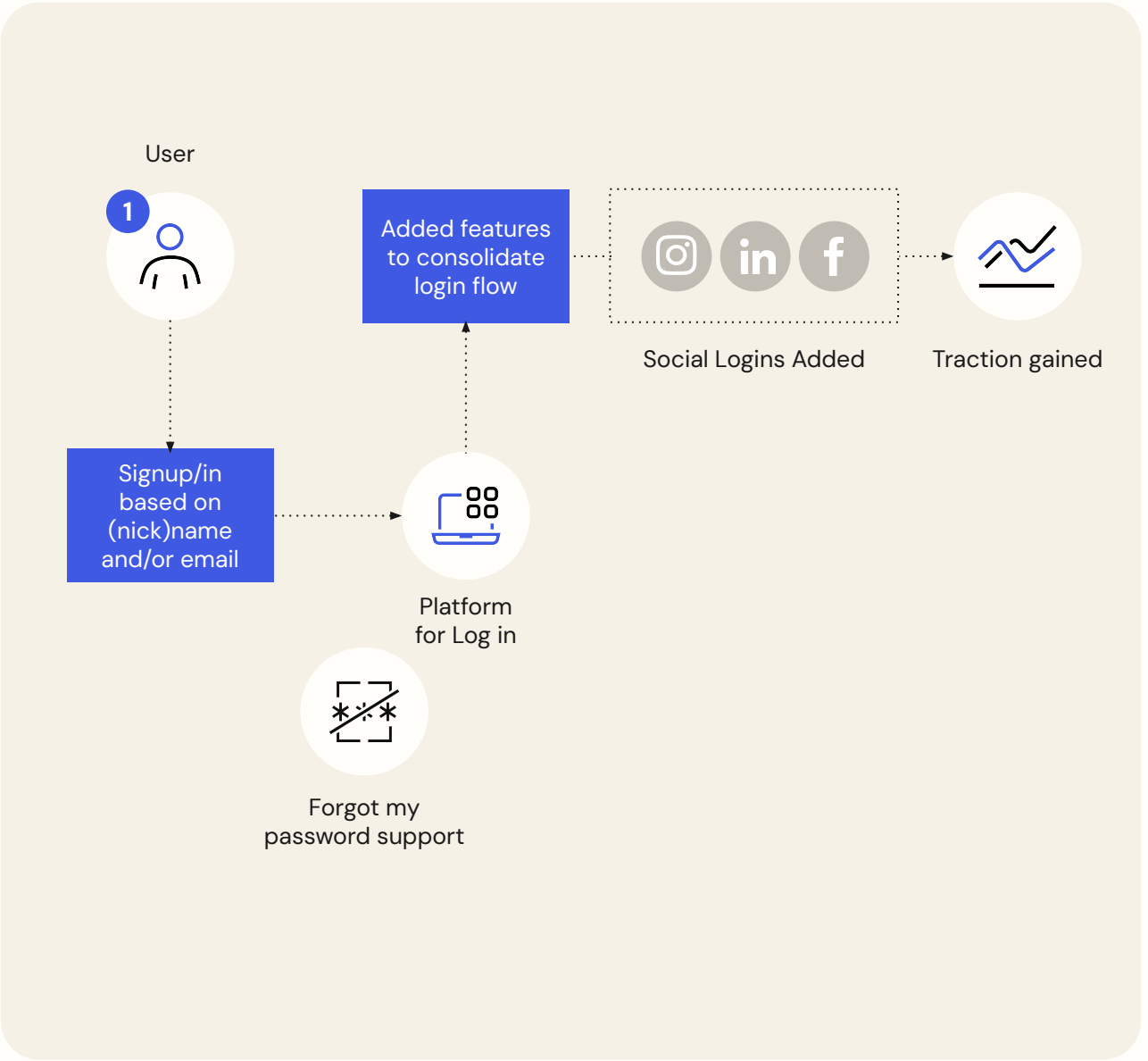
- User Authentication
- Validated by an Authorization Server
- Providing one or more security tokens
- To be consumed by the application



Authentication

Scaling to provide a more engaging user experience

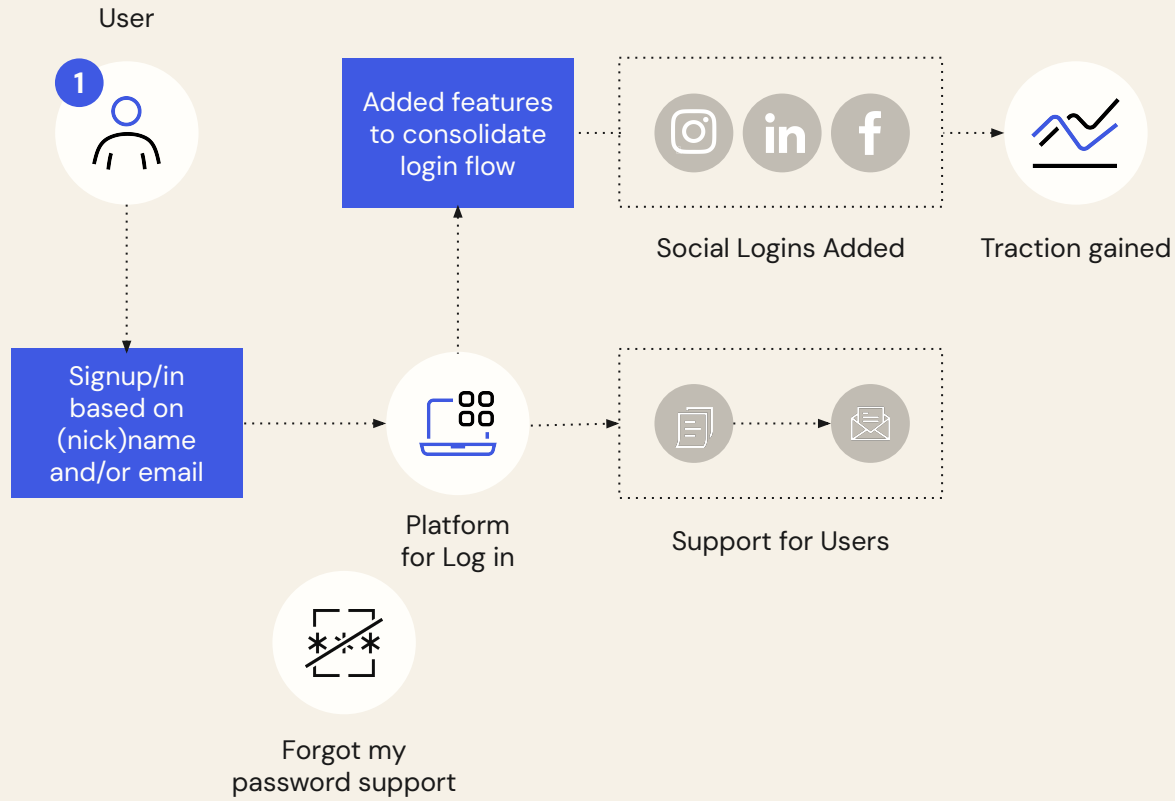
- Add support for Social Login & Signup
  - Reducing friction in the user experience
- Implement code to validate security ID Tokens



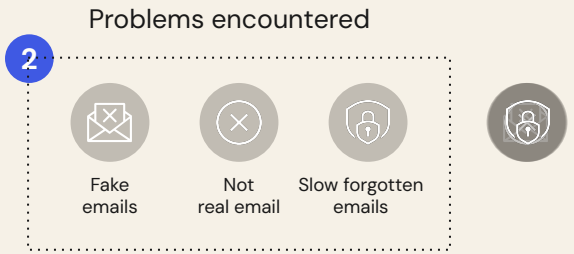
Authentication

Scaling to provide a more engaging user experience

- Add support for Social Login & Signup
  - Reducing friction in the user experience
- Implement code to validate security ID Tokens
- Provide better user support
  - Linked Accounts



Authentication



Issues that could lead to vulnerability

- Bot Attacks
  - Automation designed to overload and detect accounts
- Fake Registrations
  - To perpetrate takeover via insecure account linking
- Performance Degradation
  - Clogging identity storage and creating system latency

Authentication

Issues that could lead to vulnerability

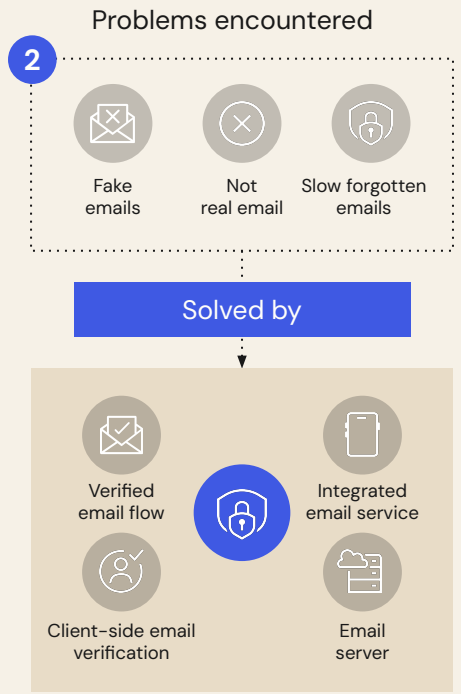
- Unencrypted Passwords
- Insecure Credential Storage
- Insecure User Profile Access
- Insecure User Profile Management
  - Resulting in leaked PII or compromised accounts
- Insecure Change Management policies
  - Resulting in potentially leaked system access information
- etc.

okta

Authentication

Vulnerability mitigation

- User Email Validation
- User Identity Verification
- Secure Communication Workflows...
- Bot Detection
- Brute Force Protection
- Credential guarding
- Suspicious IP management
- et al



Authorization

okta

Authorization

Consent

The operation(s) that a user grants can be performed on their behalf.

Permission

The operation(s) a user is allowed to perform.

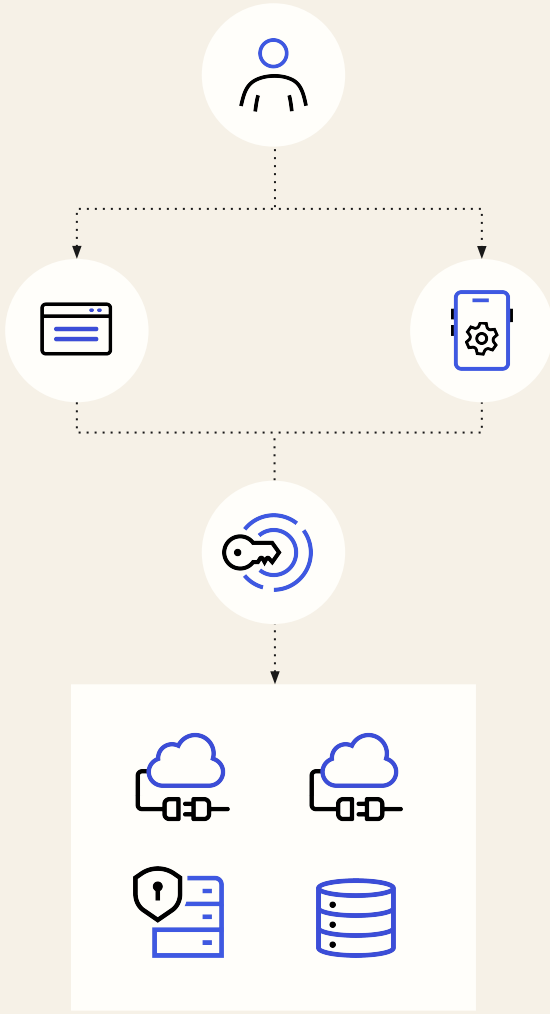
Access

Granularity, centered around RBAC, ABAC, PBAC, etc

okta

Authorization

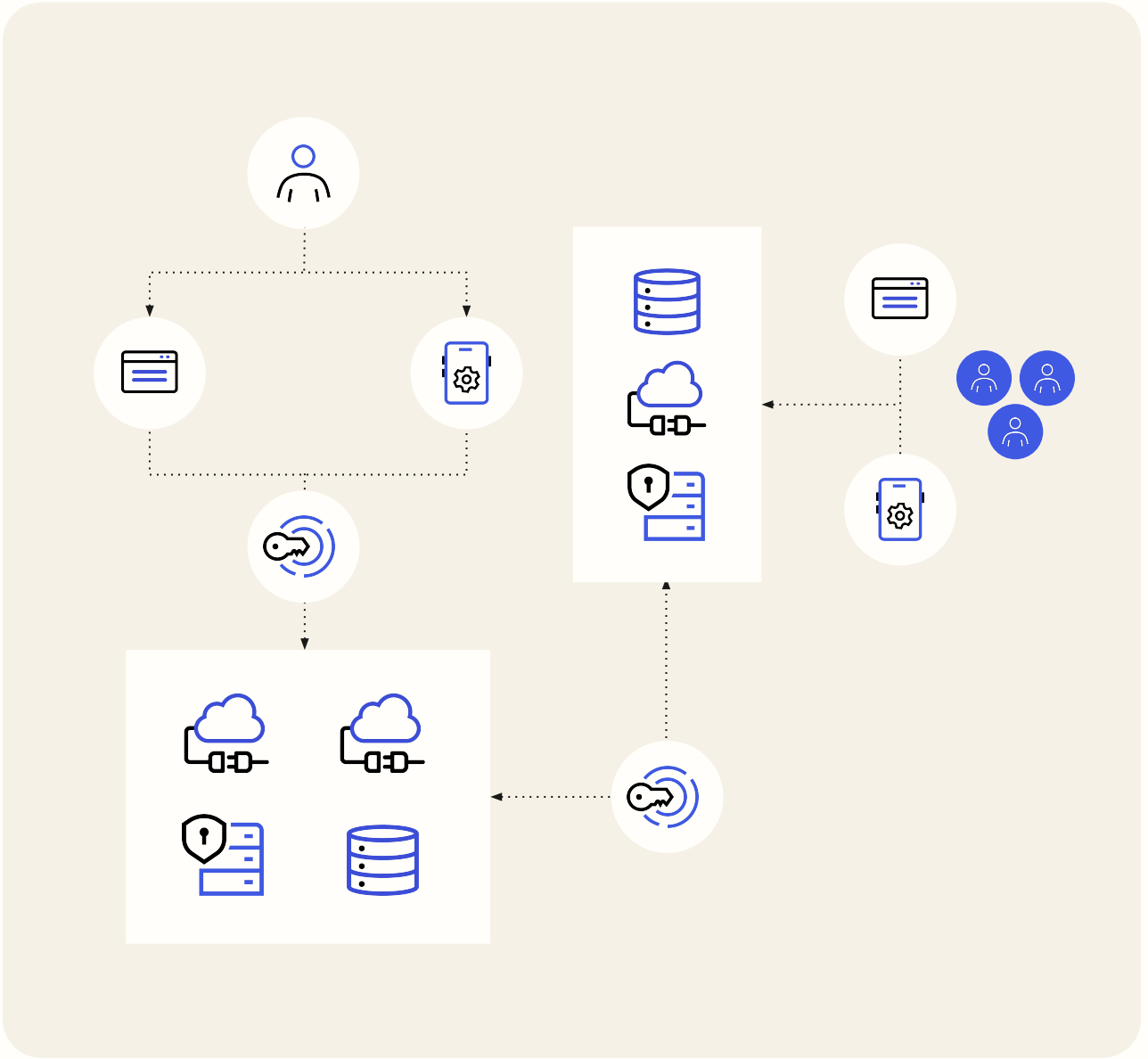
- Resource Servers
- Providing Secure Access
- To User Related Resource(s)
- On Behalf Of A User



okta

Authorization

- Resource Servers
- Providing Secure Access
- To User Related Resource(s)
- On Behalf Of A User

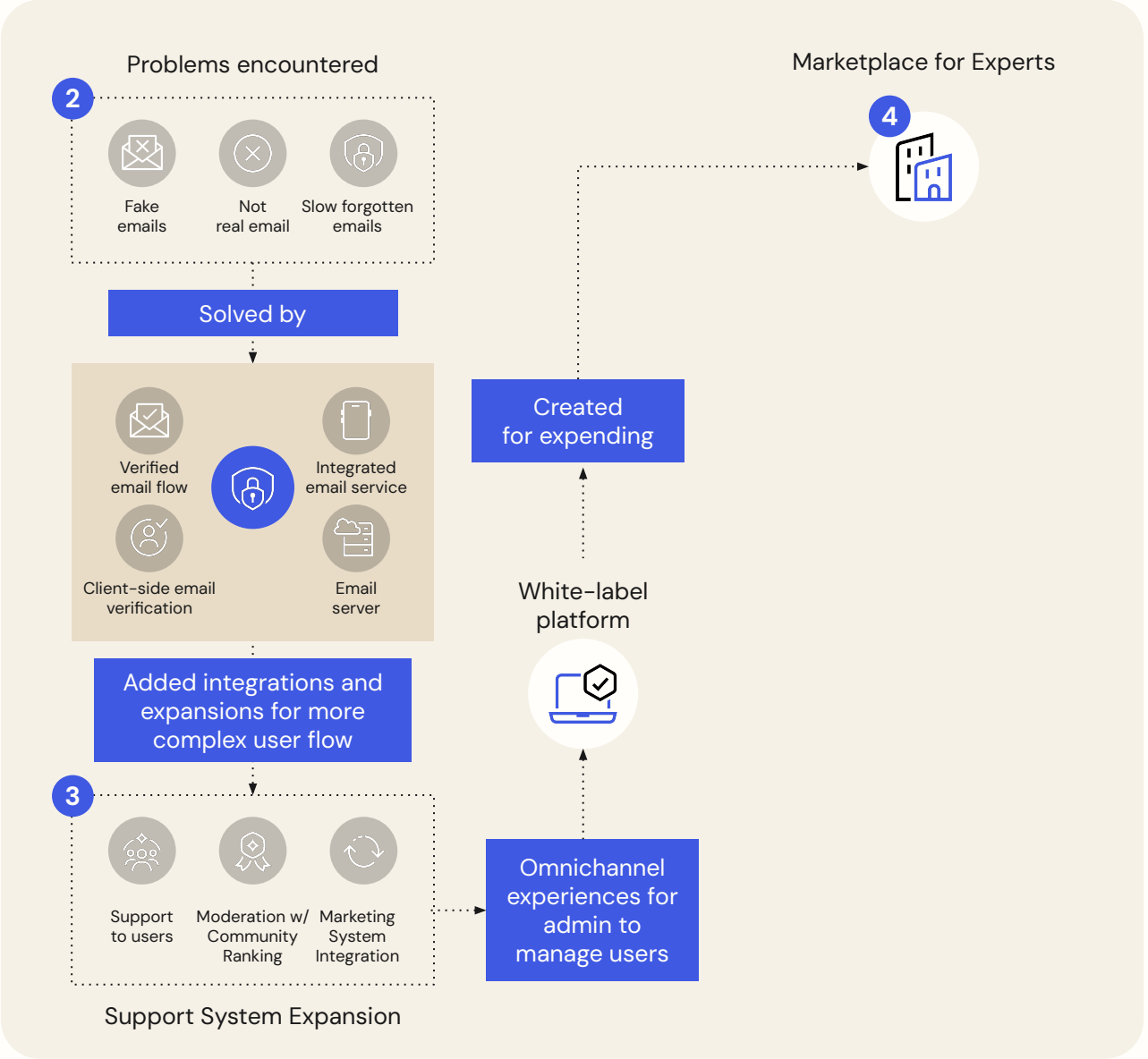


okta

Authorization

Executing at scale

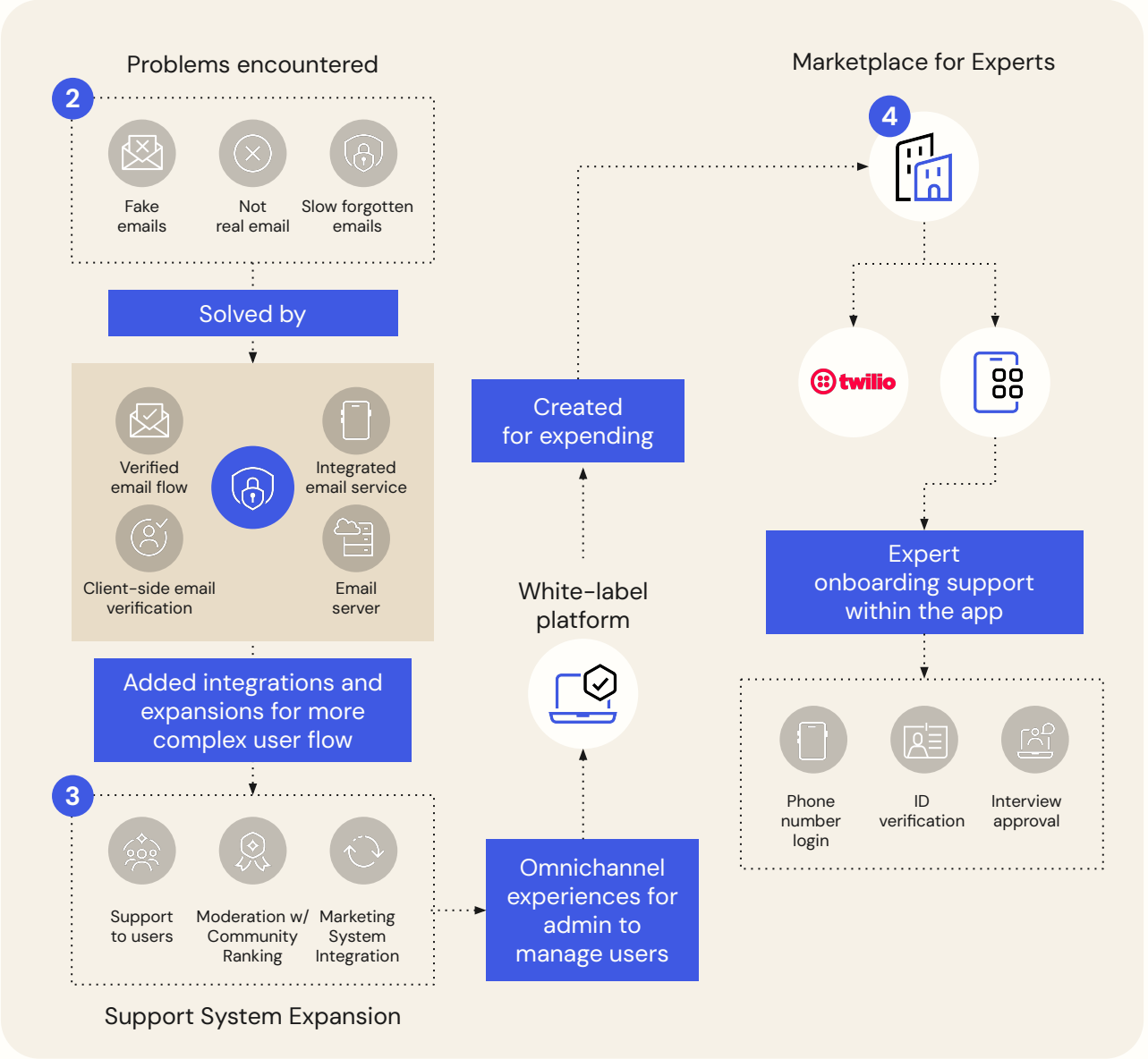
- API Integrations
- API Development
- User Administration flexibility
- Consume Marketplace services



Authorization

Executing at scale

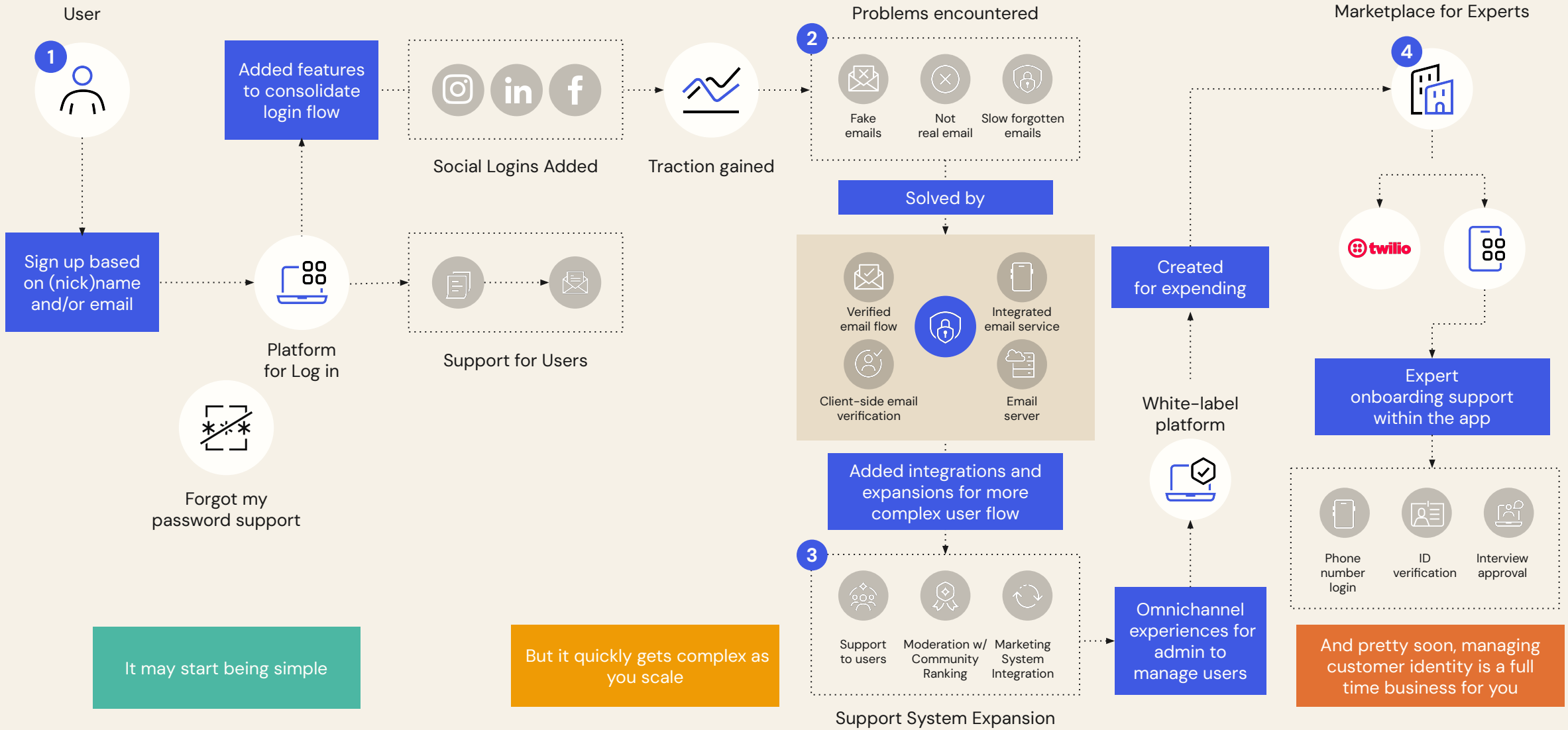
- API Integrations
- API Development
- User Administration flexibility
- Consume Marketplace services
- Build Personalized Consumer Journeys
- Support emerging technologies



Summary

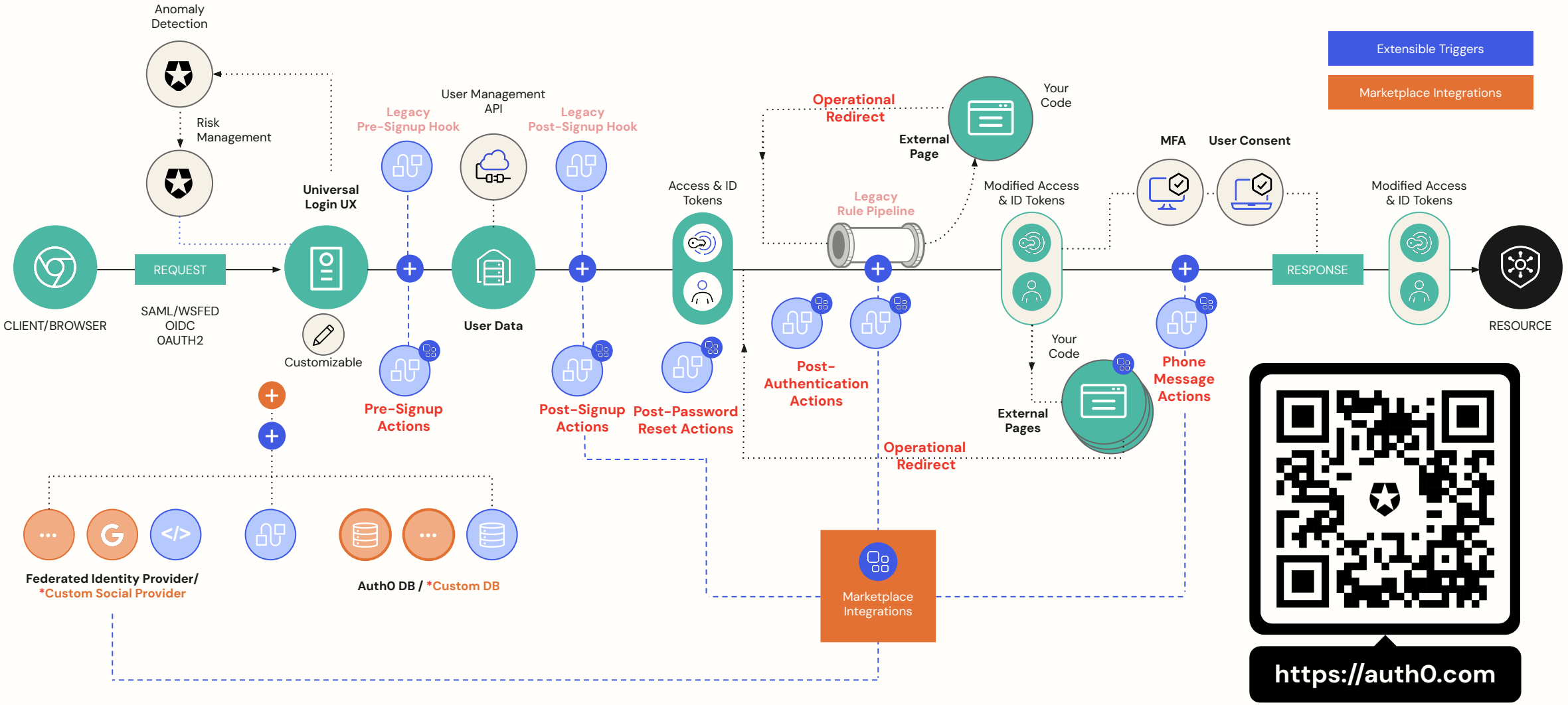
okta

Customer Identity DIY



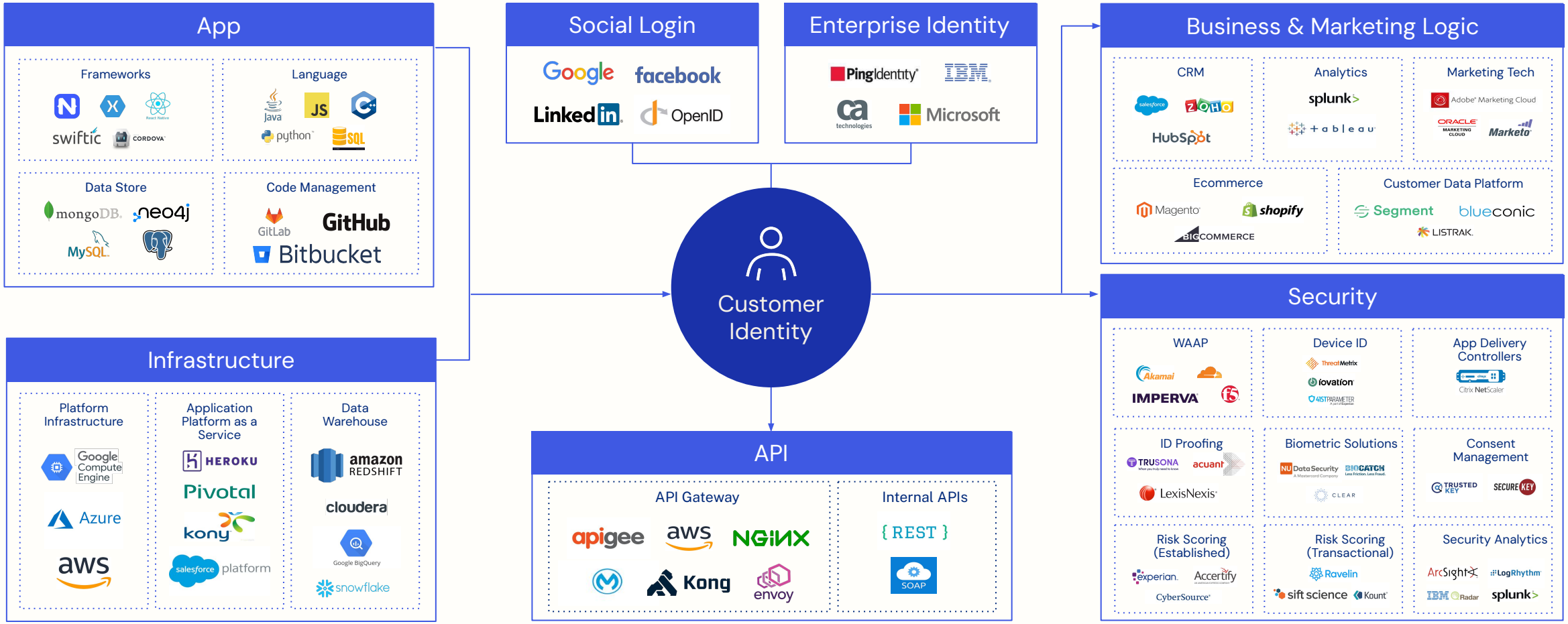
okta

AuthO Authorization Service



https://auth0.com

Today's Technical Ecosystem



okta

Q&A

okta


okta
auth0