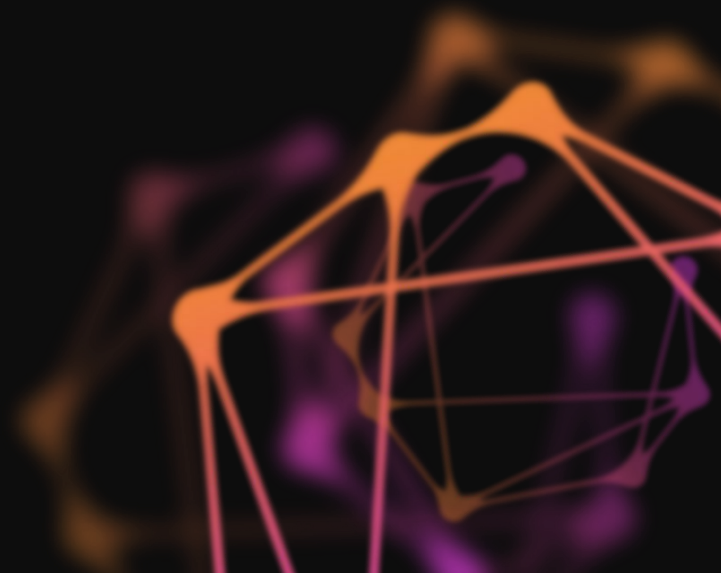




ZITADEL

ALWAYS RUN A
CHANGING SYSTEM



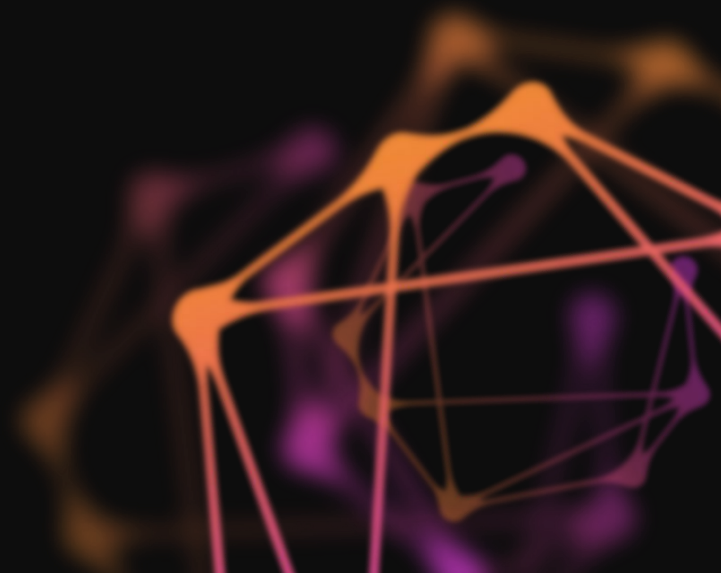
Agenda - Why we built a cloud-native open source IAM

- Who is “we”
- Why did we start the project
- What make it (so) special
- What else can it do for you



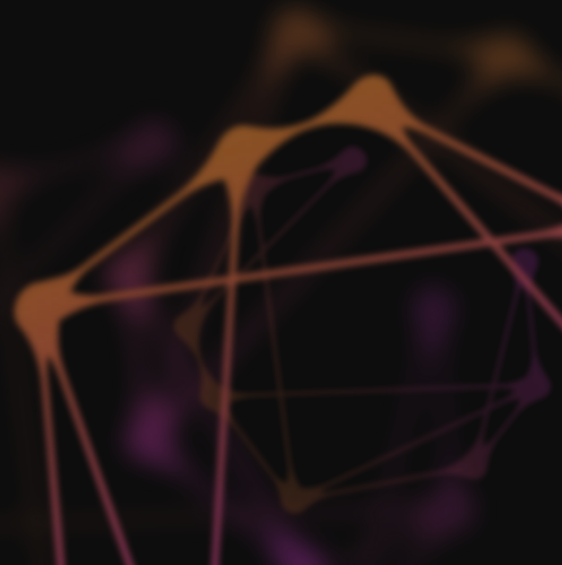
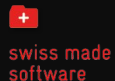


Who is “we”



CAOS - the “we”

- Founded early 2019
- 11 Employees specialized in IAM and GitOps
- Open Source Company
- Member of Swiss Made Software & CH Open
- OpenID Foundation Sponsor



The People



Christian Jakob
DevOps Enthusiast



Stefan Benz
Software Engineer



Florian Forster
Head of CAOS



Silvan Reusser
Software Engineer



Maximilian Peintner
Software Engineer



Michael Wäger
Software Engineer



Livio Amstutz
Software Engineer



Jürg Rinaldi
UI/UX Designer



Fabienne Gerschwiler
Software Engineer




Elio Bischof
Automation Advocate



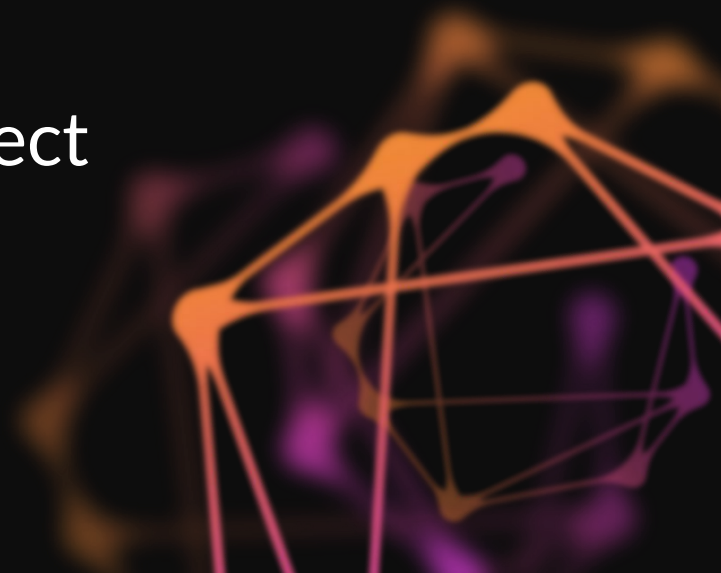
Maximilian Panne
Chief Operating Officer

What we do

1. Develop two open-source projects
 - **ZITADEL**: Cloud-native Identity & Access Management (IAM)
 - **ORBOS**: Container Runtime Platform (CRP) based on GitOps
 2. Offer Europe's only cloud-based **IAM-as-a-Service** → [ZITADEL.ch](https://zitadel.ch)
 3. Operate our products or provide support services for clients
 4. Provide consulting and engineering regarding IAM and DevOps
- 
- An abstract graphic in the bottom right corner consisting of a network of interconnected nodes and lines. The nodes are represented by small, glowing orange and purple spheres, and the lines are thin, light-colored lines connecting these nodes, creating a complex, web-like structure.



Why did we actually start the project



2019 - The Start

- We built and operated an IAM for a (X)aaS provider
- Deficiencies of existing solutions were clear from prior evaluations
 - More on this later ;-)
- It was clear to us that a IAM built for (X)aaS cases could gain traction



The basic requirements of most (X)aaS project today

- Authentication
 - Including 2FA / MFA / Passwordless
 - SSO with Identity Providers
- Authorization
 - (Role Based) Access Control
 - Delegation (of Roles) for Self-Service Access Management
- Self Service in general



What generally felt wrong or was missing

Features

- Long Term Audit Trail (not just logs)
- Self-Service
 - Customer (User Profile)
 - Partner (User & Access and SSO management)
- Delegation of access management
- No real focus towards a “platform IAM”

Market

- US Companies dominate the market
 - SaaS
 - Product
 - Open Source
- No IAM-as-a-Service provider from Europe

Technology

- Often times dated technology stack
- Hard to run and scale
 - Especially multi Datacenter or Regions
- Oftentimes no great API's

Pricing

- Security features hidden behind a paywall (e.g 2FA)
- Pay by user or session pricing
- Differentiate employees, customers, partner, machines

Regulatory

- GDPR
- Broken Privacy Shield and Safe Harbor
- Own your data (portability)

What functions each project needs - sooner or later

SSO

Conveniently login to every possible service with one account



Secure Authentication

Use multiple factors and passwordless to authenticate



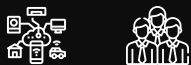
Identity Brokering

Allow users to reuse existing identities such as their business or social account



Identity Management

Store digital Identities of Employees, Customers, Partners, or IoT



Access Management

Let customers assign roles to manage access

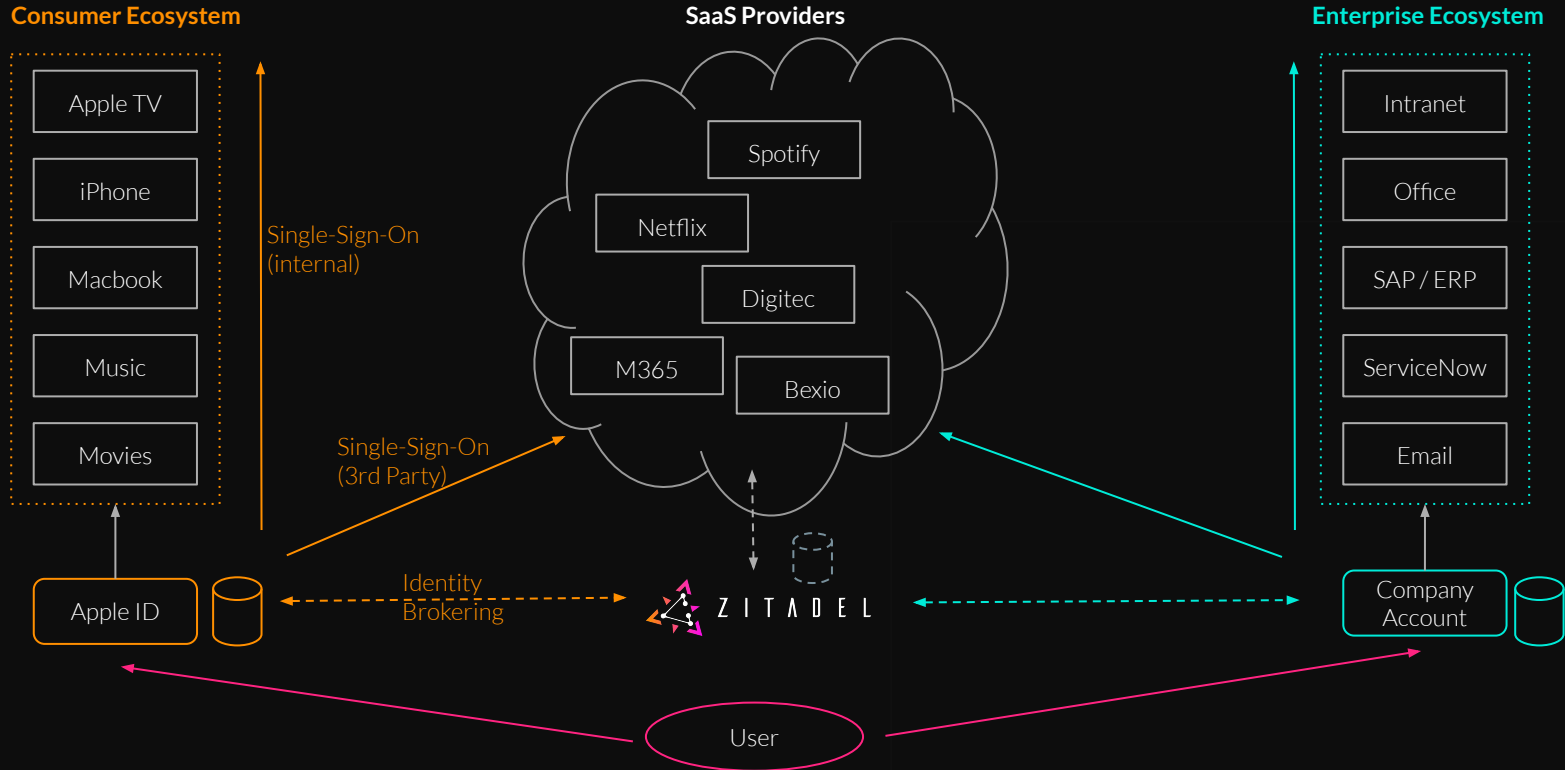


APIs

Manage workflows, integrate with any application

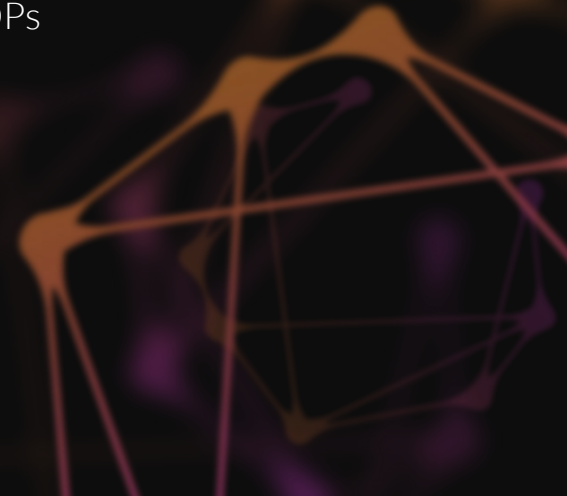


The Challenge 1 - Identity Brokering with self service

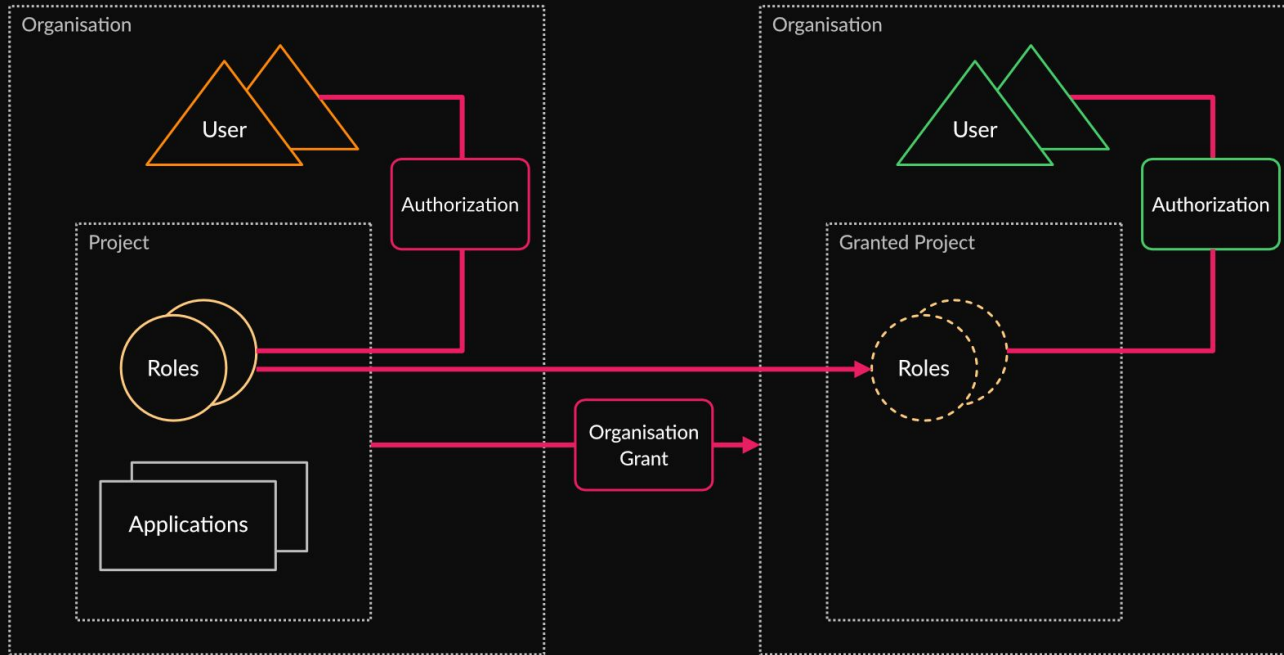


The Challenge 1 - Identity Brokering with self service

- Self-Service Management of IDPs (identity providers)
 - Close to non-existent with today's IAM solutions
- Primarily a problem for business customers who want to reuse existing IDPs
- Private customers will face this problem too in the future
 - Government ID, Social ID, Self-Sovereign (SSI),...

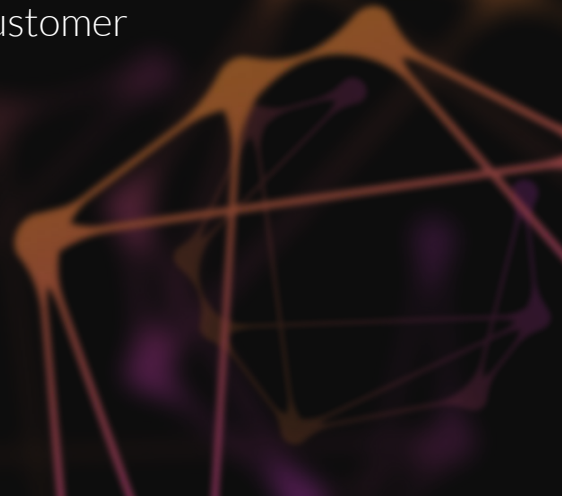


The Challenge 2 - Delegation of roles to other organizations



The Challenge 2 - Delegation of roles to other organizations

- Existing solutions do not easily allow for delegated access management
 - When building a SaaS project, this is a key feature
 - You want to own your services and delegate some roles to an customer



The Challenge 3 - Audit Trail

- Change to settings / permissions also need to be “auditable” over a long time > 12 Months
 - If a breach happens you want to be able to reproduce that exact situation in the past
- Efficient storing of audit data necessary to scale well
 - The “let’s create an audit DB does not solve this problem”



The Challenge 4 - Analytics & Reporting

- Threat intelligence
 - Use the historical data to create accurate threat models
 - Prevent attacks and malicious changes (privilege escalations)
- Business reports from historic data
 - Allow for great reports over long time periods for analytical purpose



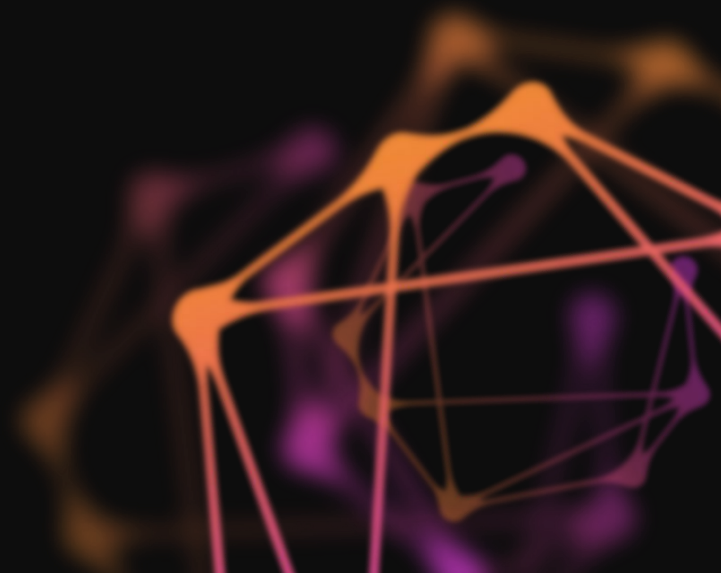
Influential products to our vision



Cockroach Labs



What make ZITADEL (so) special



Vision for the project ZITADEL

- Security features are always included and not a paid add-on
- Has a long-term audit trail built natively into the data model
- Make no difference in account types
- Cloud-native architecture
- Optimised for easy day 2 operations and scalability
- Multi Region operations possible out of the box
- Easy to integrate with modern API's
- Open Source with a Apache 2.0



Made for (X)-as-a-Service Providers

Time to market



Self-Service

Delegate the authorisation management to your customers for self-administration

Portability



Cloud Native

Deploy ZITADEL on Kubernetes on-premise, in a private instance, or use ZITADEL Cloud

Automation



API first

Administrate all aspects programmatically and manage workflows

Security



Build for analytics

Threat Analytics and Breach Assessment (“Time Travel”)

Trust



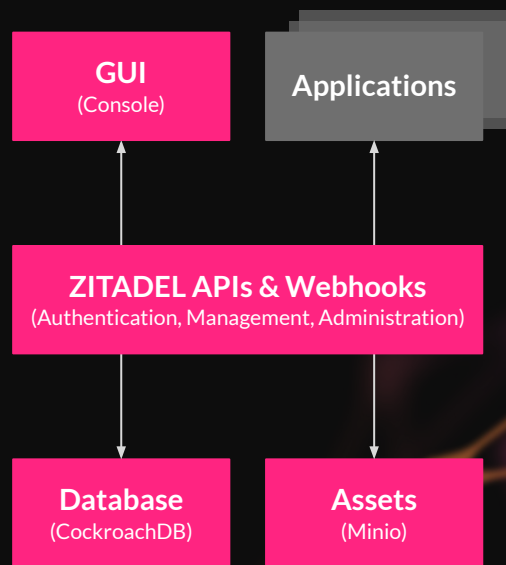
Open Source

Contribute, fork, examine or use the ZITADEL Project

Architecture & Technology

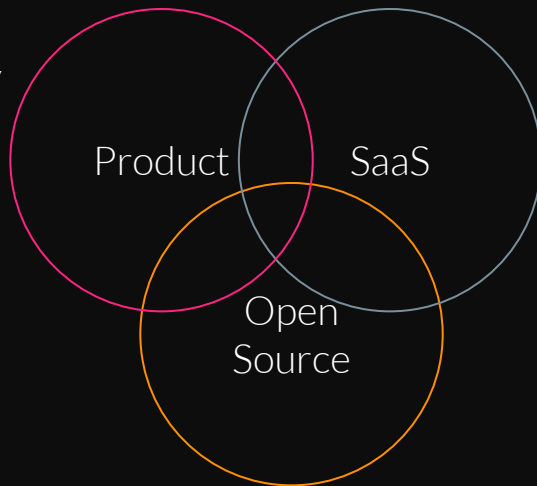
- Golang, Angular, CockroachDB and Minio
- Scalable app & storage from one server to geo-redundant multi-DC/Cloud
- API-first design
- Runs on CNCF compliant Kubernetes
- Low footprint
- Event-sourcing for unlimited records and analytics

More? [ZITADEL Architecture](#)



Where ZITADEL aims at

- Gain control of your data by using a dedicated instance
- All features available
- Flat fee pricing



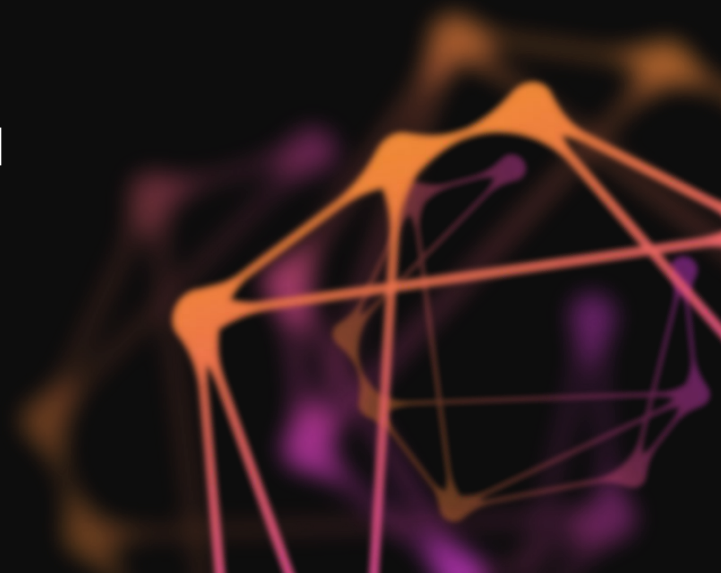
- Trust and Transparency
- Proven and Open Standards
- All security features included

- Faster time to market
- Always up to date
- Flat fee pricing





What else can ZITADEL do for you



ZITADEL platform integrates with your identities and applications

SSO

Conveniently login to every possible service with one account



Secure Authentication

Use multiple factors and passwordless to authenticate



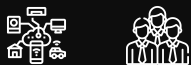
Identity Brokering

Allow users to reuse existing identities such as their business or social account



Identity Management

Store digital Identities of Employees, Customers, Partners, or IoT



Access Management

Let customers assign roles to manage access



APIs

Manage workflows, integrate with any application



Key features

Authentication

- Passwordless (FIDO2)
- 2FA with FIDO U2F, OTP
- OpenID Connect 1.0 / Oauth 2.0
- Federation
- SSO

Access Management

- Role based access management
- Delegation of role management to third-parties

Identity Management

- Self-registration incl. Verification
- User self-service for password, authenticators, and profile
- Service Accounts for machines

IAM Administration

- Policies (eg, password strength)
- Private-Labeling (Login, Mails)
- Event-based audit log of changes

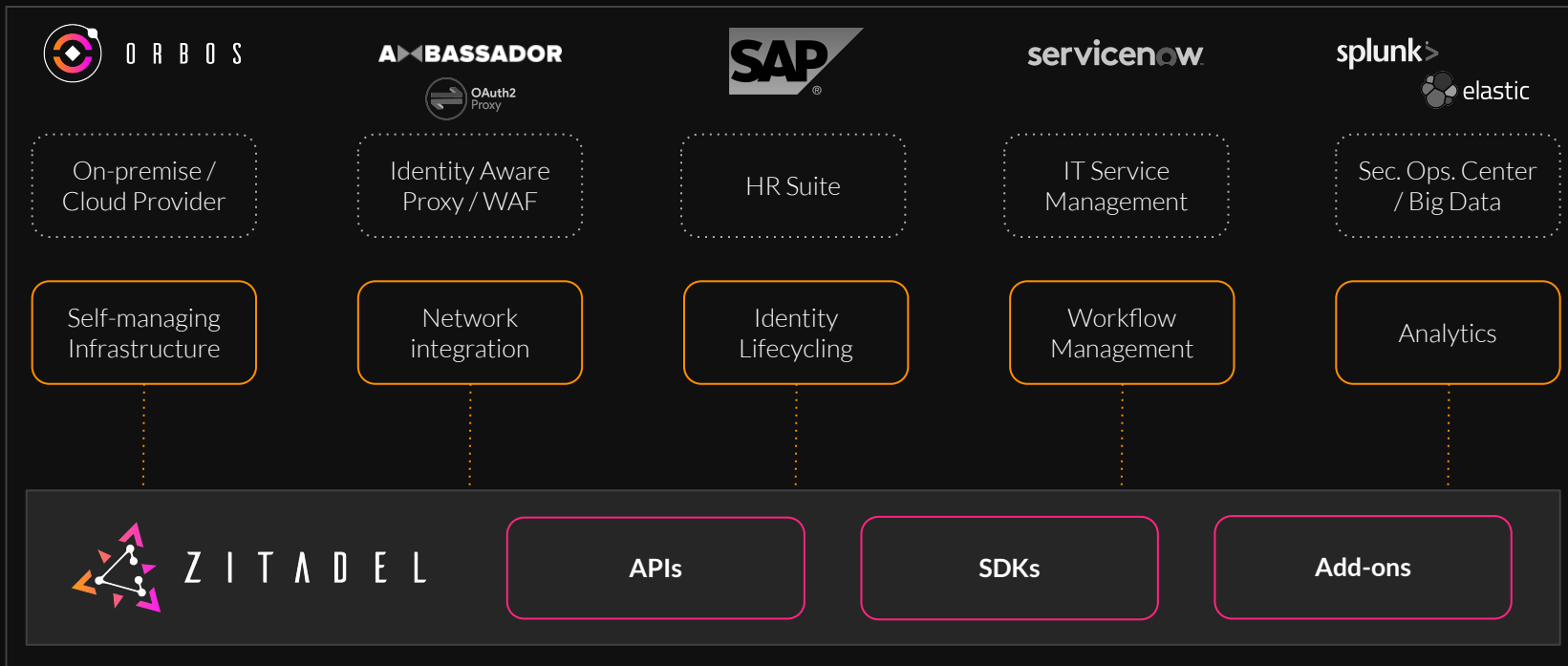
Interoperability

- Opaque, JWT Access / ID Tokens
- Authentication, Management, and Administration APIs
- Outgoing WebHooks

Extensions (add-ons)

- SAML 2.0 (SP/IP)
- LDAP, ADDS, Kerberos
- SMS-TAN
- SCIM2.0
- Event Archive Export

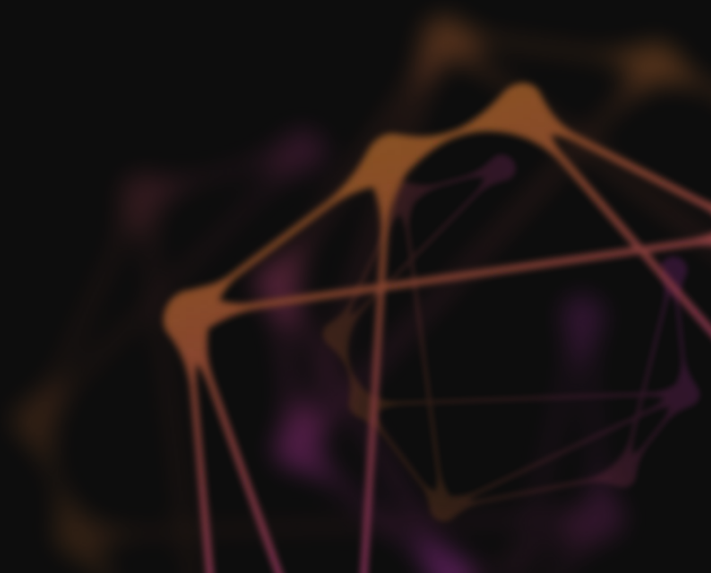
Build your use cases on a solid IAM platform



Resources around ZITADEL

- [GitHub Repo](#)
- [.net Library](#)
- [Dart Library](#)
- [Go Library](#)
- [Elixir Client](#)
- [Documentations](#)

Contributions welcome!



Questions?

ZITADEL.ch/contact

hi@caos.ch



[Github](#)



[LinkedIn](#)



[Twitter](#)

Try out ZITADEL for free, no strings attached
ZITADEL.ch