JioCloud

Identity Lifecycle Management

Overview

JioCloud Identity Lifecycle Management gives you complete oversight and control over every identity in your environment—human and non-human. It automates core processes like provisioning, deprovisioning, access reviews, and validations, so you do not have to rely on error-prone manual tasks. The solution prevents orphan accounts, enforces identity policies, and makes sure validations don’t get skipped. With real-time monitoring and a central dashboard, your teams can catch risks early, streamline audits, and ensure that the right people have the right access at the right time. From onboarding new systems to enforcing policies across clouds, JioCloud simplifies identity governance—without slowing down operations.

Key Features

- **Multi-cloud and hybrid support**
  Manage identities across multiple cloud providers and on-prem platforms from one place.
- **Centralised dashboard**
  Enforce policies, track usage, and flag risky accounts—all through a single interface.
- **Automated provisioning and deprovisioning**
  Set up and revoke access automatically, reducing delays and minimising human error.
- **Orphan account prevention**
  Identify and clean up unowned or unused accounts to reduce security risks.
- **Periodic validations and reviews**
  Run scheduled access checks to meet compliance and avoid privilege creep.
- **Role-based access (RBAC)**
  Restrict dashboard access based on user roles to maintain control and reduce exposure.
- **Broad technology support**
  Compatible with RHEL, Ubuntu, SUSE, Windows, Kubernetes, Azure, GCP, Postgres, and MySQL.
- **Custom workflows and integrations**
  Adapt the platform to your internal processes with configurable workflows and connectors.

Benefits

- Stronger compliance with automated validations, access reviews, and orphan account detection.
- Centralised identity visibility across clouds, apps, and teams.
- Fewer errors and delays with fully automated provisioning and deprovisioning.
- Simplified audits with continuous monitoring and policy enforcement.
- Secure onboarding and access governance for non-human identities.
- Reduced risk from over-provisioned or stale accounts.
- Faster integration with custom apps and Active Directory tenants.
- Lower operational effort with self-service and service desk automation.

Technologies Supported

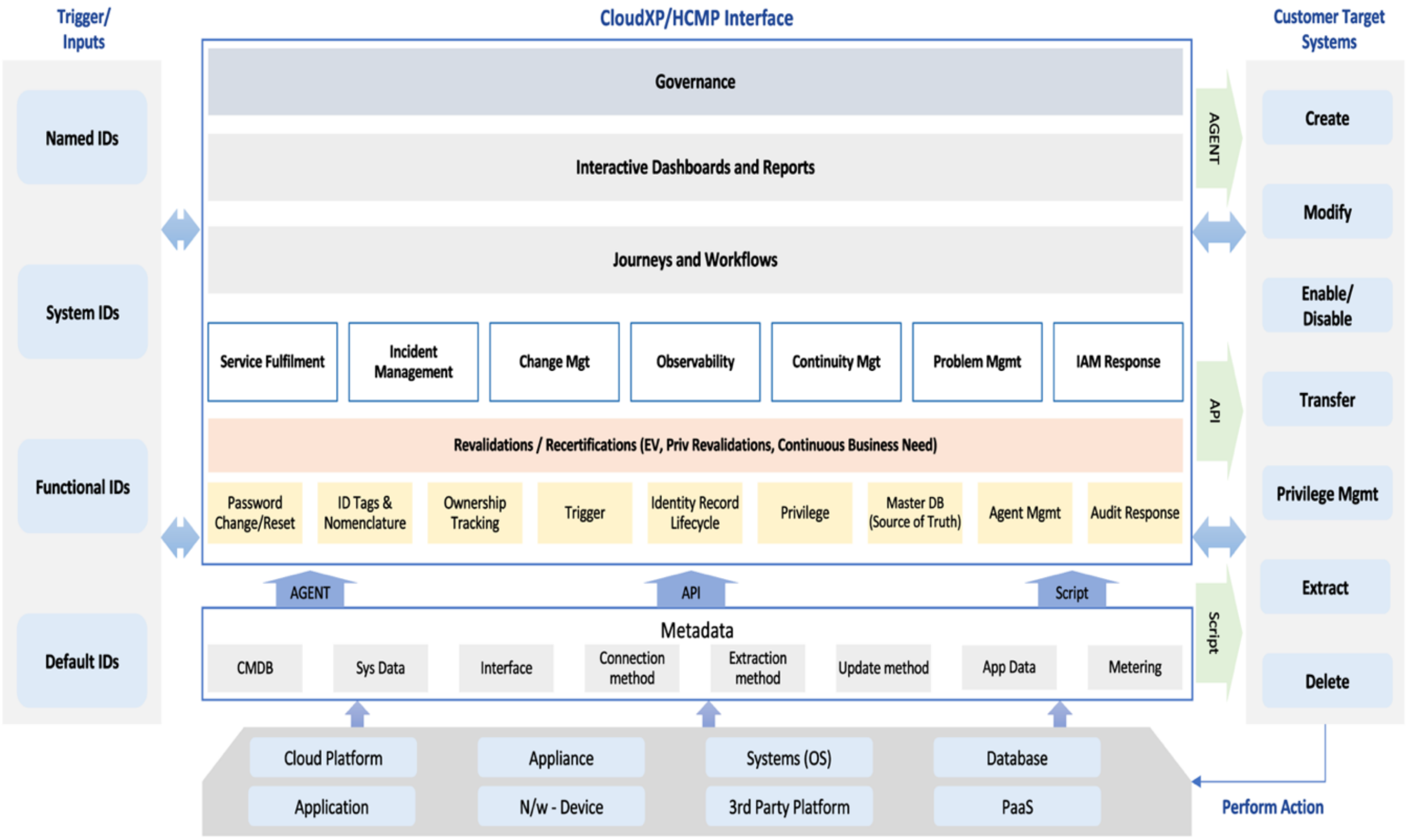
Operating System	**Developed**
	RHEL
	Ubuntu
	SUSE
	Windows
Cloud Platform	**Roadmap**
	RHOS
	Azure (Data extraction)
	GCP (Data extraction)

Databases	**Roadmap**
	MySQL
	PostgreSQL
	MSSQL
	Oracle
	MongoDB
	Cassandra
Other	**Roadmap**
	Kubernetes
	Windows AD
	CyberArk

Technical Specifications

Specification	Details
SLA	99.9% uptime
API Support	[REST]
Data Storage Options	[SQL, NoSQL, etc.]

Architecture Diagram



Use Cases

- **Enterprise IT**
  Centralised identity control across hybrid infrastructure.

- **Public sector and governance**
  Enforce secure, auditable access policies for government platforms.

- **Financial and healthcare sectors**
  Automated access reviews for compliance-driven environments.

- **DevOps and automation teams**
  Manage non-human identities and service accounts at scale.