CLOUDENTITY

Modern Application Authorization

Real-Time Data Visibility, Access Control, and User Consent Management.

Innovation and Business Impact

Enterprises are accelerating digital business to enhance competitiveness, service capabilities and the customer experience. Application modernization, compartmentalized development, big data, cloud computing, and service integration are happening via APIs and microservices, introducing significant security and data privacy issues. Delivering new and advanced services is a top imperative that requires improving software development agility without sacrificing security. To mitigate risk while advancing digital transformation initiatives, companies must ensure Zero Trust access and data protection with fine-grained authentication policy applied across their distributed infrastructure encompassing internal and external-facing APIs.

Unfortunately, modern application authorization and privacy management inefficiencies continue to impact application delivery, innovation, and compliance. Why? Developers typically hardcode authorization logic within apps and APIs – a decentralized process prone to errors, policy drift and blind spots. Complex multi-cloud workloads with diverse API components and service connections, and a cumbersome array of identity, privacy and compliance requisites amplify the problem.

Cloudentity Solution

Cloudentity aggregates IdP authentication sources and decouples authentication and authorization from applications and APIs to simplify, centralize, and automate authorization management. This ensures continuous, compliant and audit-able access and data exchange protection for all transactions across legacy, multi-cloud and microservices environments.

AUTHENTICATION — VERIFY WHO / WHAT YOU ARE → DECLARATIVE AUTHORIZATION — GRANT WHAT YOU CAN DO → APP/SERVICE

Delivered as an external declarative authorization solution, via SaaS or software, our flexible, scalable modern application authorization platform streamlines the onboarding of users, apps and APIs into the identity and authorization ecosystem, and enables developers to manage fine-grained policy as code, orchestrate provisioning, assure privacy consent, and achieve real-time enforcement at hyperscale – assuring Zero Trust access and data protection at millions of service requests per second. With Cloudentity, enterprises now have visibility and control over where application programming interface (API) data is shared and how it flows between APIs and distributed services on premises or in the cloud. As a result, our enterprise customers have increased development velocity and service agility while mitigating API access, privacy, and compliance risks.

Faster Time to Market: Automate app, service and API inventory, policy standardization, and declarative authorization provisioning to expedite release security verification

Fine-grained Policy: Go beyond nominal authentication with granular authorization leveraging a graphical policy editor, pre-defined policy packs, and extended rule context

Agnostic Orchestration: Centrally manage, activate and monitor governance with seamless integration into existing identity, app, service and security infrastructure

Hyperscale Enforcement: Gain real-time, transaction-level enforcement, close to the app, service or API, delivering high performance control at real-world volume workloads

Privacy and Data Compliance: Manages user privacy and consent workflows and applies them to OAuth scopes consumed by applications, APIs, services - providing data exchange guiderails and a complete audit record

Complete Data Lineage: captures and presents data origin, what happens to each piece of data, and who or what has access to the data in real-time for immediate control validation, policy adjustment, compliance verification and remediation

Zero Trust API Security: Reduced attack surface through continuous perimeter and lateral monitoring and enforcement to prevent OWASP API vulnerabilities, unauthorized access, and data leakage risks

Cloudentity's modern application authorization platform makes policy creation, provisioning and enforcement effective, extensible and scalable. Key software components are the Cloudentity Authorization Control Plane™ and Cloudentity MicroPerimeter™, as well as Identity and API Gateway integration options.
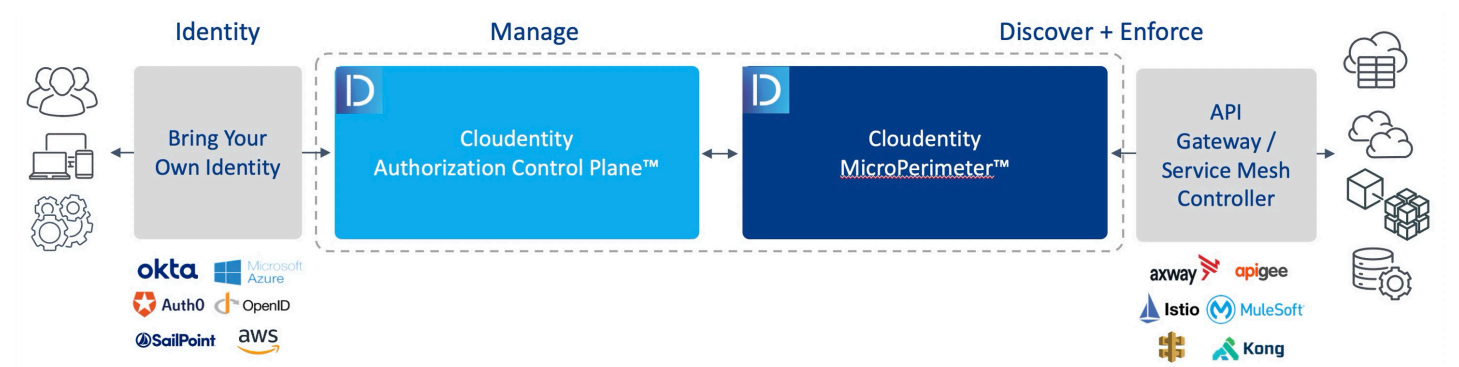

Policy Management, Consent Workflow, and Data Lineage Visualization - Simplified

Fine-grained authorization policies are developed through a graphical, natural language rules editor, allowing even non-developers to understand and create policy without coding or configuration expertise. Services, API gateways and APIs are readily discovered and classified to expedite cataloging authorization context to be normalized and extended. The policy then generates authorization-as-code that describes the rules to be applied to an entity, be it user, machine, app, API, or service, for each access and data exchange transaction.
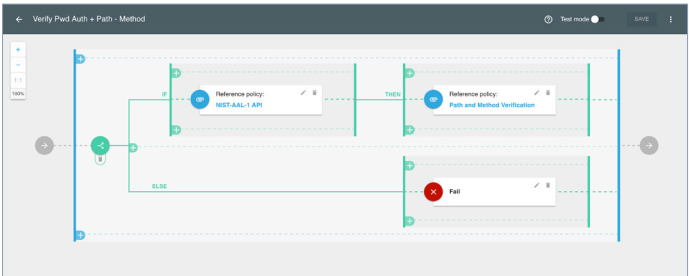

Graphical Policy Editor
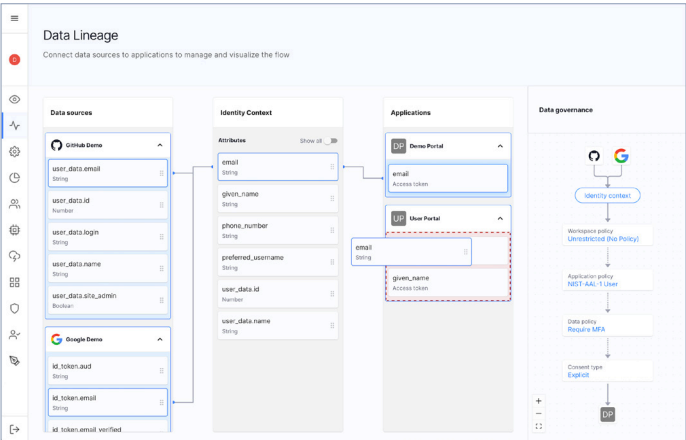
Data Lineage Visualization

A graphical, drag-and-drop interface that is used to view and govern the mapping and distribution of user data from identity providers to applications. The simple user interface, with built-in guided tours and examples, allows even non-technical users to easily understand, administer and validate authorization governance policy. The visual representation of the policies, that are applied to the applications and the data they consume reduces administrative complexity and compliance risks.

Privacy consent allows entities to manage their privacy by asserting control over who and what personal information can be shared with a company and third parties conducting business with that company. Cloudentity's built-in privacy consent workflows manage entity onboarding and on-going sharing permissions. These are dynamically enforced down to the API transaction-level to adhere to bounds defined by the entity.
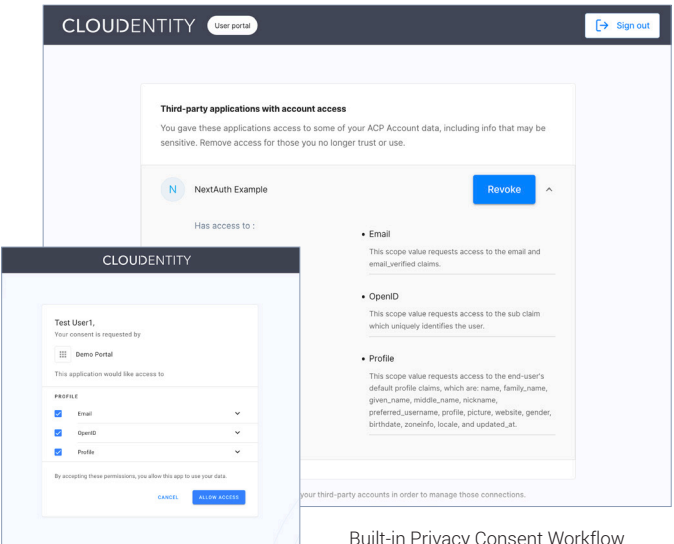
Built-in Privacy Consent Workflow

Key Benefits

• Faster service delivery • Simplified policy orchestration • Increased developer productivity • Verifiable compliance
• Privacy consent adherence • Zero Trust microservices • Reduced attack surface • Rapid time to value

Cloudentity Authorization Control Plane™

✓ App / service registration with API catalog and authorization context mapping

✓ Fine-grained policy creation via graphical editor and natural language policy-as-code

✓ Declarative authorization management

✓ Scope governance and privacy consent workflow

✓ End-to end data lineage & policy analytics

Cloudentity MicroPerimeter™

✓ Dynamic, high-speed transaction-level edge enforcement at hyper-scale

✓ Service/API discovery, visibility

✓ Continuous Zero Trust control: mitigate perimeter and lateral attack/data leakage

✓ Cloud-native defense k8s, ECS

✓ API Edge Gateway and WAF integration

Bring Your Own: Identity and API Gateway / Service Mesh Controller

Integrates with, and can aggregate data from, a broad range of standards-based identity providers, bespoke identity, and entitlement data sources. Provides dynamic edge enforcement for most industry standard API Gateway and Service Mesh platforms, as well as direct decision point access for bespoke, non-standard API, and Service deployments. Organizations can also use our optional Identity Provider capabilities and open-source API Security Gateway solution.

Platform Advantages

Automated Entity Onboarding: Enables developer app/ API registration and inventory. As new services and APIs are identified, authorization policy is dynamically applied and enforced

Intelligent Identity Provider (IdP) Discovery: recommends initial IdPs and enables subsequent IdP auto-routing at end-user login to improve user experience and eliminate custom IdP routing mechanisms

Authorization Policy Orchestration: Simplifies policy management with expedited GUI policy editor, natural language code, pre-defined policy packs, and dynamic provisioning

Transactional Multi-factor Authentication (MFA): ties MFA to application and data governance policies to conditionally trigger an MFA challenge before authorization access to an app or data is permitted to ensure security with least use experience friction.

Application and Service Data Governance: Data exchange guiderails for each request to negate or redact unpermitted information while capturing data lineage in tamper-proof Privacy Ledger™

Complete Privacy Consent Workflow: Manages full privacy consent self-service workflow and enforces at the transaction level to meet PII and sensitive data protection obligations

Transaction Enforcement at Hyperscale: Enforces millions of requests per second - 60x OAuth token minting and eval performance at 90% lower latency compared to other approaches

Perimeter and Lateral Microservice Zero Trust: Continuous Zero Trust control at all service ingress and egress decision points to mitigate OWASP API vulnerabilities and east/west lateral threats
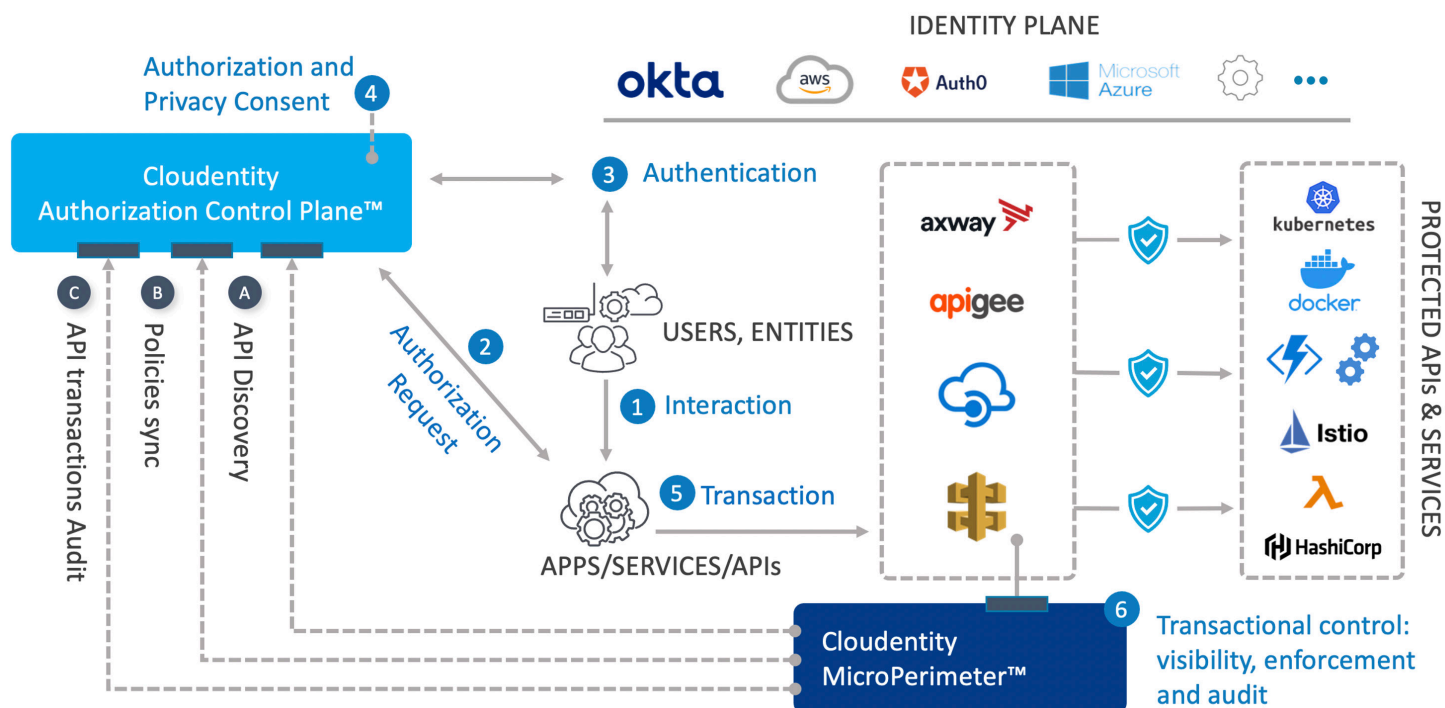
API Open Standards Compliance Certification

Cloudentity has achieved certifications across an array of API standards to ensures future-proof integrations and allow enterprises to comply with evolving global open standards specifications. These certifications include:

Financial-grade API (FAPI) advanced - Open Banking Brazil - Client Initiated Backchannel Authentication (CIBA)

Deployment, Interoperability, and Scale

Cloudentity's Authorization Control Plane is offered as a built-for-cloud, multi-tenant SaaS platform that elastically scales to meet demand for unlimited scale. Enterprises can seamlessly integrate and scale authorization governance into their existing identity, API gateway, service mesh controller, container, legacy app, and security management ecosystem leveraging pre-built connectors, as well as APIs for bespoke integration. The MicroPerimeter™ edge enforcement solution is distributed as a lightweight Linux package, platform specific serverless component, or as a Docker container via container orchestration platforms. Operating within a Kubernetes cluster, the Microperimeter provides east/west lateral connection visibility, tracking and policy enforcement. Beyond built-in analytics, all system changes, user consent, policy management and transaction events are tracked and can be forwarded to logging, fraud and SIEM systems.