Authorization Governance Automation

Cloudentity provides the most flexible and scalable solution for authorization governance automation to increase development velocity and secure digital business across hybrid, multi-cloud and microservices infrastructure.

Innovation and Business Impact

Delivering new and enhanced services is a top imperative, but authorization governance inefficiencies continue to impact application delivery, innovation, and security. Why? Developers typically hardcode authorization logic within apps and APIs – an inefficient 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.

While federated identity authentication facilitates session access, it does not address access and data exchange exposures between services and APIs, nor does it provide transactional security or data privacy control. These shortcomings leave the business exposed to cyberattack and data leakage. Ultimately, application rollouts are delayed due to prolonged security verification effort. It's time to "left shift" DevSecOps.
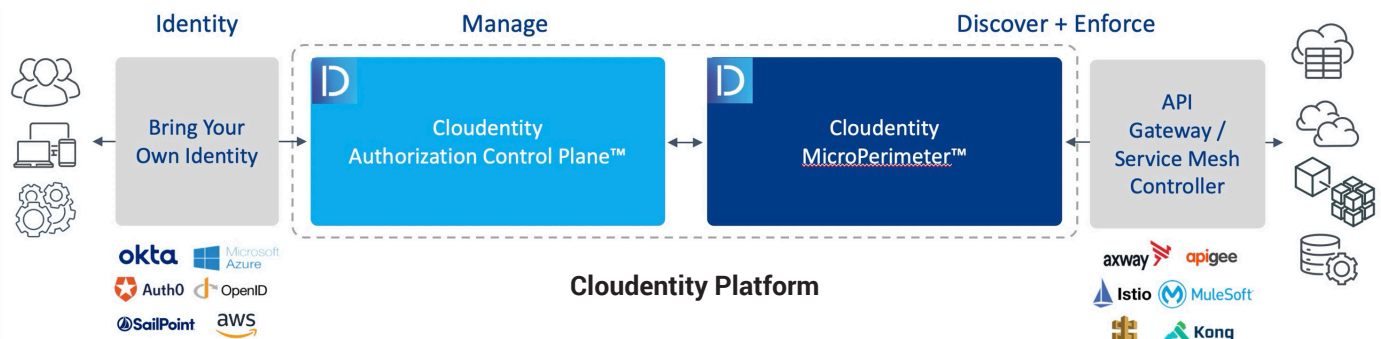
Cloudentity Solution

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

Delivered as an external declarative authorization solution, our flexible, scalable Authorization Governance Automation 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, and gain real-time enforcement at hyperscale – assuring Zero Trust access and data protection at millions of service requests per second. As a result, our enterprise customers have increased development velocity and service agility while mitigating privacy consent, API security 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 drag and drop 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 consent workflows and applies to services/API OAuth scope, data exchange guiderails, and complete audit log

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 Authorization Governance Automation 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.

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

✓ End-to end data lineage & policy analytics

Cloudentity MicroPerimeter™

✓ Dynamic, high-speed transaction-level 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, a broad range of popular Identity Management / IdP sources, as well as broad range of popular API Gateway and Service Mesh platforms. Organizations can also use our optional Identity Control Plane and open-source API Gateway solutions.

Unique Platform Capabilities

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

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

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

Interoperability and 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. The solutions are distributed as a lightweight Linux package or as a Docker container via container orchestration platforms. Operating within a Kubernetes cluster, the sidecar 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.
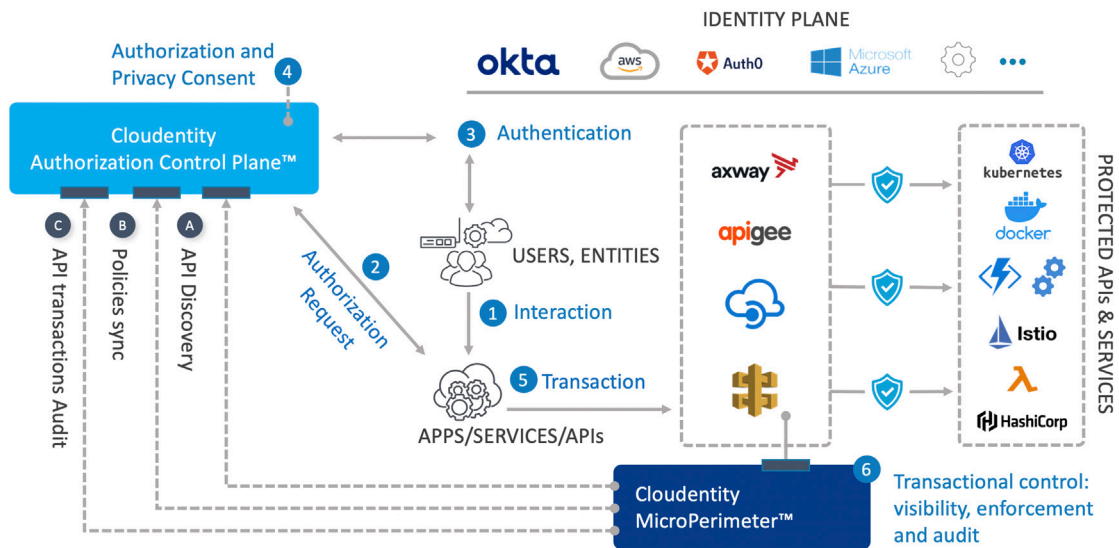
CLOUDENTITY
206.483.2255
info@cloudentity.com
2815 2nd Ave.
Seattle, WA 98121 • USA