CLOUDENTITY

Authorization Governance Automation

What, Why, How

Executive Overview

App modernization, big data, and service integration serve as the foundation for digital transformation, and are almost always done over APIs - introducing massive scale, security and data privacy issues. While delivering new services and enhanced applications are a top imperative, authorization management deficiencies continue to impact security audits and application rollout, and open the business to security and compliance risks.

Cloudentity increases development velocity, improves audit efficiency, and mitigates risk by advancing fine-grained authorization policy management and delivering continuous, transaction-level enforcement across hybrid, multi-cloud and microservice environments.

One of the major challenges with securing apps, services and API access and sensitive personal data exchange today is that organizations lack visibility, centralized policy control, and transactional enforcement processes. The responsibility of access and security controls for each app, service and API often lies with development, where decentralized rule oversight and increased release cycle frequency has resulted in varying security controls that are difficult to manage and audit.

Developers are contending with increased application access demand, complex multi-cloud workloads and API service connections, and a cumbersome array of identity, security and compliance requisites. Beyond coding and configuration complications, just discovering and classifying services and APIs is an unwieldy process. Incorporating applications and APIs in standardized, granular access and data protection modes is even more difficult to manage. The volume of APIs and service gateway connections has grown, even more so amid the pandemic. At the same time, cyberattacks are also on the rise, with threat actors exploiting web, app and access exposures as enumerated in the latest OWASP API vulnerabilities.

While organizations have adopted federated identity authentication mechanisms to protect session access, essential authorization management remains fragmented, limited, and lax. In most organizations, authorization rules are typically hardcoded by engineers for each application. This inefficient, bespoke process is prone to human error, policy inconsistency, and operational blind spots.

OWASP API Vulnerabilities

As APIs have become the fabric of modern service delivery and compartmentalized app development, their exposure of application logic and sensitive data has made them a high-value target of threat actors. The OWASP foundation has published a set of top API exposures, such as:

- Broken object-level authorization
- Excessive data exposure of object properties
- Broken function-level authorization
- Security misconfiguration
- Injection flaws
- Improper asset management
- Insufficient logging or monitoring

Through authorization governance, enterprises can mitigate these and other security risks.

The lack of cloud-native, authorization management proficiency also slows down application modernization, business integration and service improvement projects. An organization's ability to ensure timely service and application enhancements is often stymied by inefficient and inconsistent authorization management due to these variations in app and API visibility, access and authorization controls, as well as gaps in data lineage. Ultimately, this results in more prolonged security validation cycles, delaying application delivery and service innovation.

DevSecOps needs to shift left. Modernizing application development and setting security at the pace of business requires:

1. Moving user, machine and service access and data exchange authorization to the edge as an externally managed authorization service
2. Streamlining entity onboarding to the identity and authorization ecosystem
3. Removing the coding and configuration complexity to enable granular policy control
4. Achieving transaction enforcement and auditability of apps, services and APIs on premises and in cloud

Cloudentity overcomes these enterprise challenges by decoupling identity and authorization from applications and APIs, and enabling declarative authorization policy as code. With our modern application authorization solution, organizations can simply and effectively orchestrate app, service, API and user on-boarding; centralize, manage and provision fine-grained policy; gain privacy consent control; and achieve continuous transaction-level enforcement at hyperscale with full data lineage - enabling expedited security verification.

Authentication Limitations

Authentication is the process of verifying the identity of a user, device, or service, often based on factors of what the entity knows or has to regulate access to a system.

- Federated authentication mechanisms, such as single sign-on (SSO) and multi-factor authentication (MFA), are primarily used for session-based system access
- Identity-centric, session-based authentication does not offer fine-grained policy at a necessary breadth to address the scope of access conditions for all entities and resources
- Identity management solutions do not typically extend granular controls down to service and API data exchange in a uniform manner, nor at real-world performance requirements.

As a result, engineering and security teams gain increased development velocity and service agility while mitigating privacy, API security and compliance risks. Furthermore, organizations can accelerate digital transformation business opportunities that require crucial data protection and privacy consent controls.

Cloudentity Modern Application Authorization

Cloudentity makes cloud-native authorization management flexible and scalable, ensuring secure, compliant and confidential access and transactions across hybrid, multi-cloud and microservices infrastructure. Our solution enables organizations to manage, monitor and audit data exchange control between users, systems, applications and APIs with declarative authorization and real-time transaction enforcement.

Before Cloudentity

- Delayed application delivery and service enhancement
- Impacted Open Data initiatives
- Authorization policy inconsistency and inadequacy
- Development and DevSecOps complexity and inefficiency
- Increased web, app and API attack surface
- Privacy, audit and compliance exposures

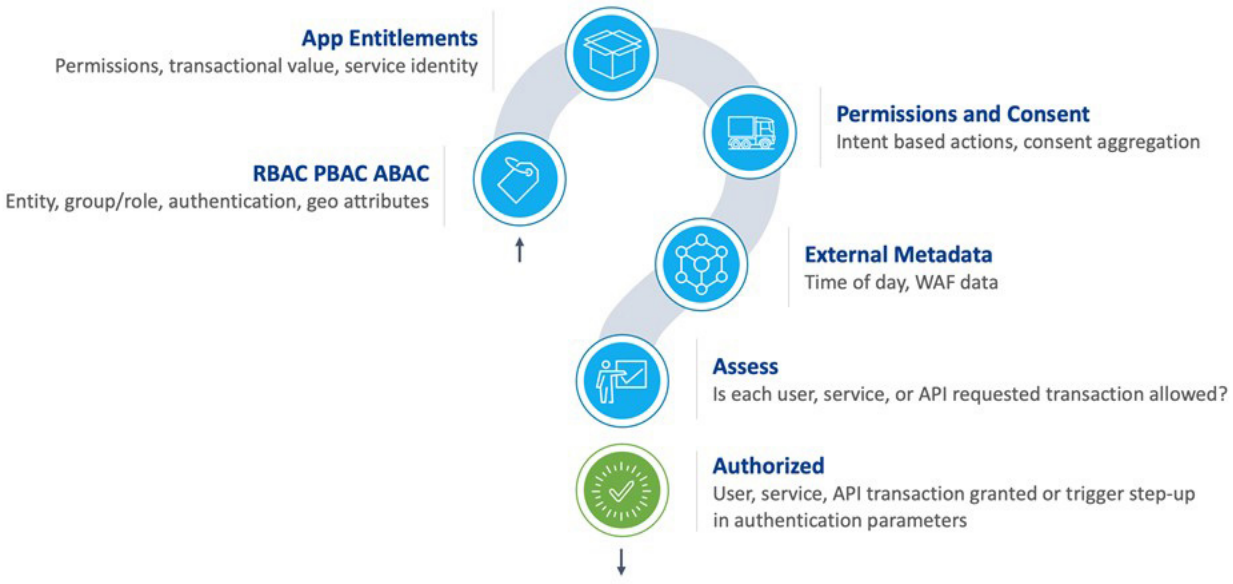
After Cloudentity

Fine-grained declarative authorization

Cloudentity Dynamic Authorization extends nominal identity-based authentication with fine-grained authorization incorporating extended context that complies with NIST authorization and privacy standards.

Policy development is facilitated through a graphical, natural language rules editor, multi-source context normalization, and pre-defined compliance policy packs. 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.

Through declarative authorization, a companion Cloudentity security app, running as a Docker container sidecar within a Kubernetes cluster or a lightweight installable Linux package for legacy applications, enforces every app, service and API requests against the pre-defined policy as close to the app or service as possible. The approach provides comprehensive, adaptive access control with granular OAuth scope and transactional data protection mechanisms, as well as end-to-end data lineage for reporting, forensics and audit. In addition, Cloudentity Privacy Ledger™ provides a tamper-proof audit of the who, what, where, when and why that consent was granted or rejected.



Governance automation in action

Through Cloudentity's modern application authorization platform, operating as on-premises software or as a cloud-based SaaS service, developers can readily on-board apps and APIs into the identity and authorization ecosystem. Services, API gateways and APIs are discovered and classified to expedite cataloging authorization context to be normalized and extended. Fine-grained authorization policies are developed through a graphical editor, allowing even non-developers to understand and create policy without coding or configuration expertise. This provides policy-as-code agility where granular policy packs can be standardized, centrally managed, and readily provisioned across distributed applications and services. Built-in privacy consent workflows allows users/entities to manage sensitive information sharing permissions to be applied to data protection controls.

Once activated, authorization enforcement occurs at the transaction-level and at hyperscale as close to the app, API or service across hybrid, multi-cloud and microservices environments, such as Kubernetes. High-performance processing of millions of transaction requests per second occurs close to each service component, with full data lineage to extend policy monitoring, reporting, auditing, and forensics. This provides Zero Trust controls for all service ingress and egress decision points to prevent unauthorized north/south perimeter and east/west lateral access and data leakage risks.

Cloudentity Platform Advantages

- Decouples authentication and authorization as an external service
- Streamlines on-boarding apps and APIs into the identity ecosystem
- Integrates seamlessly with existing identity, API, microservices and security systems
- Aggregates context data across IAMs, IdPs, apps and other sources
- Advances governance: fine-grained authorization policy, API security, auditing and analytics
- Satisfies business, industry and regulatory compliance leveraging built-in and extensible policy packs, as well as end-to-end data lineage
- Dynamically enforces all application and API access and data exchange at the transaction level
- Delivers high-performance control that negates OAuth token examination and re-tokenization latency
- Expedites privacy consent management to adhere to compliance and Open Data specifications

Simple, flexible and scalable deployment

With Cloudentity, there is no need to rip and replace existing technology. Our microservice delivery model and infrastructure-agnostic approach allows customers to seamlessly integrate authorization governance into their existing identity, API, microservice (e.g. Kubernetes) and security management ecosystem. The solution offers pre-built connectors that work with popular identity management and IdP sources, such as those from Okta, Google and Microsoft, and is standards-based, supporting protocols such as OAuth 2.1, FAPI R/W, OIDC and SAML2. Since Cloudentity separates authentication sources from app authorization, IdPs can be readily switched or aggregated for added flexibility.

The solution also works with a broad range of popular API gateway platforms, such as those from Axway, Google, Amazon, Microsoft and Kong, to identify, catalog and on-board APIs and enable dynamic authorization. Cloudentity solutions are 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 solution provides east/west connection visibility, tracking and policy enforcement. Beyond built-in analytics, all system changes, user consent and end-to-end transaction events are tracked and can be forwarded to logging, fraud and SIEM systems.

Allow IT to operate at the speed of business

Authorization management is a cornerstone technology for app modernization and digital business transformation. Cloudentity modern application authorization enables enterprises to increase developer velocity and service agility, and through policy as code and transaction-level enforcement, reduce operational complexity and mitigate security exposures. The solution delivers continuous authorization across hybrid, multi-cloud and microservices infrastructure with single-pane-of-glass visibility, management and auditability.

Cloudentity satisfies fine-grained authorization and privacy consent governance requirements necessary to meet today's privacy compliance (e.g., GDPR, CCPA) and open data initiatives (e.g., Open Banking and Open Healthcare). Furthermore, this evolutionary approach also offers the extensibility needed to address ongoing business, architecture and privacy compliance change.

Learn how Cloudentity cost-effectively "left shifts" development and increases DevSecOps proficiency to allow IT to operate at the speed of business; resulting in faster, more efficient and more secure service delivery.

CLOUDENTITY

Cloudentity is a pioneer and innovator in modern application authorization. Through its externalized, declarative authorization solution, enterprises can take advantage of digital business and open data opportunities, increase development velocity, and mitigate API access and personal data privacy risks. For more information, visit www.cloudentity.com.

206.483.2255

info@cloudentity.com

2815 2nd Ave
Seattle, WA 98121 • USA