CLOUDENTITY

Ensuring API Access Security and Data Privacy

to Enable API First and Open Data Initiatives

Abridged Edition

Open Data promises to revolutionize business intelligence and the customer experience, introducing endless possibilities for growth and innovation. The dynamic sharing of data within large organizations and among business partners enables a vast array of new insights and services that not only enhance the customer experience, but also help organizations better understand and serve their customers.

This sharing of data serves as the foundation for digital transformation and is almost all done via Application Programming Interfaces (APIs), introducing massive scale, security, data privacy and compliance issues. 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. To fully realize the promise of the Open Data economy in a way that earns the trust of customers and partners while managing risk, companies must ensure the utmost security of sensitive data as it flows between users, applications, services, and APIs. This imperative has sparked an API First approach to progress API security designed to enable fluid service and API accessibility with added controls that reduce cyber threat exposures and ensure data privacy and protection.

Cloudentity's authorization governance automation platform serves to advance API First programs to mitigate cyber attack and data privacy risks, but also accelerates digital business by modernizing legacy apps, meeting Open Data B2B2C privacy consent requirements, and increasing developer velocity for service delivery and enhancement.

What is Open Data?

Open Data refers to the practice of organizations aggregating and sharing customer data among distinct corporate divisions and with third-party service providers, while adhering to granular data protection controls and permissions managed through explicit customer consent. Open Data programs, such as Open Banking and the Financial Data Exchange (FDX), healthcare's ePHI exchange programs, and Customer 360 projects, aim to facilitate a secure exchange of often sensitive data across lines of business, supply chains and partners with the purpose of enhancing application and service capabilities, customer insight, and user engagement.

The advantages of Open Data sharing are realized by customers and organizations alike. Customers gain better and faster access to services offering transparency and streamlined customer journeys. Companies gain greater insights about classes of customers and services as part of KYC (Know Your Customer) initiatives. Firms can use a data-driven approach to provide other useful information or to facilitate access to other services at customers' fingertips. Open Data protocols that leverage APIs, such as PSD2 and FDX for Open Banking and FHIR for Open Healthcare, also set the stage for powering up new and future B2B2C applications by providing a mechanism from which to drive third-party services into a standards-based and secure data exchange ecosystem.

A complex array of distributed APIs work together to enable this sharing, underpinning modern transactions. APIs provide protocols that determine how systems communicate with each other, allowing data to flow between apps, services, platforms and providers. For example, APIs are seeing dramatic adoption in the retail sector, where they are being utilized to augment and supplant EDI (Electronic Data Interchange), which has for decades been the standard.

Open Data drivers

A number of factors are spurring on the Open Data transformation. In the Open Banking realm for example, a major impetus is compliance and regulation. To stimulate innovation and competition, Europe's PSD2 initiative directed banks to give third party payment service providers access to the information of customers who have consented to sharing that data. Since its 2018 issuance, this initiative has reverberated across the globe, taking different incarnations in different countries.

Market factors are another driving force. Customer behavior is changing. Consumers are no longer geographically limited to the offerings of local companies and organizations, whether banks, healthcare providers, or retail stores. Whether being a part of the "iPhone generation" or just being stuck at home during a pandemic, users have become accustomed to digital transactions replacing physical ones and seek frictionless, seamless interaction.

Overall, there is a desire for enhanced orchestrated user experiences that merge data from different sources to provide insightful information and enhanced customer experiences. Organizations who can offer this sort of holistic digital engagement will be in a better position to serve the expectations of a modern customer base.

Risks and Requirements

Security and compliance

A lack of proper means of authentication and authorization within a company's API and service portfolio could allow threat actors to perform account takeover or identity theft. In an Open Banking context, criminals could make unauthorized financial transactions or apply for fraudulent loans in the name of a bona fide customer. In the healthcare field, they could leverage accessed health data as a means of extortion. Even inadvertent data leakage can result in data protection obligations and penalties in violation of privacy regulations such as GDPR, CCPA, PIPEDA, LGPD, and PDPA. Other risks include exploitation of API-specific vulnerabilities as listed in the OWASP API Top 10.

Privacy Consent

Another consideration in Open Data is incorporating customer privacy consent - a requisite for modern B2B2C applications and services. Organizations, whether to meet data privacy regulations or to boost user trust, must provide customers the ability to stipulate how their sensitive personal data is to be used. However, conventional approaches to applying fine-grained access policy according to privacy consent across distributed applications, services and APIs are currently inefficient, inadequate and not scalable.

Open Data security requirements:

- Capturing and managing consent and authorization scope from users, customers, applications and APIs
- Discovering, identifying and on-boarding a multitude of apps, services and APIs into the identity and authorization ecosystem
- Managing fine-grained authorization policy to ensure conditional access and compliant data exchange
- Enabling internal and third-party "tokenized" access via Open Authorization (OAuth), rather than passing actual entity credentials, with granular permissible data scope
- Enforcing granular access and data exchange controls at the transaction-level between entities, apps, APIs and services
- Orchestrating authorization control provisioning across identity, microservice, security and fraud systems

Current challenges

App and API security exposures

A major challenge with securing apps, services and APIs today is that organization lack service and API visibility, centralized policy control, and transactional enforcement processes. The responsibility of access and security controls for each app, service and API often lies with engineering, which can result in controls that are difficult to manage and audit.

Additionally, the sheer volume of APIs and service gateway connections has grown. Developers are contending with increased application access demand and complex multi-cloud workloads, making it an unwieldly process to discover and identify new or shadow services and APIs, as well as include them in standardized, granular access and data protection modes.

The limits of authentication

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. The use of federated authentication mechanisms, such as single sign-on (SSO) and multi-factor authentication (MFA), are commonplace for session-based system access. However, session-based authentication does not provide the breadth of fine-grained policy, nor depth of transactional data exchange enforcement. Most identity-based authentication solutions do not typically extend granular controls down to service and API data exchange in a uniform manner and at real-world performance requirements.

Inefficient authorization

Authorization verifies that an entity, be it a user, machine, application or API, has permission to access a resource. In most organizations, developers hard-code authorization rules and privacy controls into each application. This inefficient, bespoke process is prone to human error, policy drift and blind spots that opens the business up to attack and compliance exposures.

Prolonged service delivery

The lack of a streamlined authorization method yields variations in app and API authorization controls. This results in more prolonged security validation cycles, delaying application release.

Cloudentity authorization governance for API First and Open Data initiatives

Cloudentity provides a flexible, scalable and proven solution for authorization governance automation to enable API First and Open Data initiatives within an enterprise's existing hybrid, multi-cloud and microservices infrastructure.

The approach ensures continuous access control and data privacy for the high-value, sensitive information shared internally and among business entities and their customers.

Through Cloudentity's authorization governance automation solution, organizations can decouple identity and authorization, orchestrate service and app on-boarding, enable fine-grained authorization policy as code, and gain transaction-level enforcement at hyperscale.

On-boarding, fine-grained policy management and privacy consent - at scale

Developers can make use of Cloudentity's automated onboarding to bring apps and APIs into the identity and authorization ecosystem. As new services are identified, they can be incorporated into existing policy-based enforcement controls.

Instead of deciphering hard-coded authorization policy for each application and API, Cloudentity enables the creation of fine-grained authorization policies through a graphical editor, so even non-developers can understand, create and provision policies without coding or configuration expertise.

Cloudentity has built-in self-service consent workflows and dynamically applied data governance guiderails to prevent unpermitted information leakage while capturing user permissions and API/service transaction activity logs.

By placing access and data exchange enforcement as close to the service or API as possible, Cloudentity provides Zero Trust controls to prevent north/south perimeter and east/west lateral attack, unauthorized access, and data leakage risks.

Development at the speed of business
With authorization and consent management decoupled from the application and by encompassing this management as a service, the need for prolonged security verification for new apps is removed, increasing developer velocity.

Fast, easy, infrastructure-agnostic deployment
Cloudentity 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 visibility, tracking and policy enforcement.

Cloudentity enables customers to seamlessly integrate authorization governance into their existing identity, API, container and security management ecosystem. The solution offers pre-built connectors that work with popular identity management and IdP sources, as well as a broad range of popular API gateway platforms. Beyond built-in analytics, all system and transaction events are recorded and can be forwarded to logging, fraud and SIEM system.

Unique, enterprise-class capabilities

Cloudentity offers unique, enterprise-class features that align to API First, Open Data program requirements.

Automated user, app, API onboarding into AuthN/AuthZ ecosystems
Enables developer app/API registration, inventory and discovery.

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
Applies data exchange guiderails for each request to negate or redact unpermitted information while capturing data lineage in tamper-proof Privacy Ledger™.

Consent governance workflow
Manages full customer privacy consent process and enforces at the transaction level to meet PII data security obligations.

Transaction enforcement at hyperscale
Enforces millions of requests per second - 60x OAuth token minting and eval performance at 90% lower latency.

Perimeter and lateral microservice Zero Trust
Provides Continuous Zero Trust control at all service ingress and egress decision points to address OWASP API vulnerabilities and attacks.

With Cloudentity, you can...

- Streamline on-boarding apps and APIs into the identity ecosystem
- Integrate seamlessly with existing IdPs and API gateways
- Aggregate context data across IAMs, IdPs, apps and other sources
- Expedite Open Data management with consent, API security, authorization analytics and reporting
- Satisfy business, industry and regulatory compliance leveraging built-in and extensible policy packs, as well as end-to-end data lineage
- Dynamically enforce all app and API access / data exchange at the transaction level
- Gain high-performance control that negates OAuth token examination and re-tokenization latency
- Meet Open Data security and privacy compliance mandates

Conclusion

Authorization governance is a cornerstone technology to enable API First and Open Data initiatives. Cloudentity automates the necessary fine-grained authorization policy management and provisioning, privacy consent management, and transaction-level enforcement across hybrid, multi-cloud and microservice environments. It cost-effectively “left shifts” development and DevSecOps for the benefit of application modernization and expedited service delivery.

Learn how Cloudentity Authorization Governance Automation solutions can expedite and further your API First and Open Data programs by visiting www.cloudentity.com.

CLOUDENTITY

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

206.483.2255

info@cloudentity.com

2815 2nd Ave
Seattle, WA 98121 • USA