CLOUDENTITY

Scalable B2B and Partner Authorization

Enable Onboarding, Collaboration, Privacy and Transaction Controls

Abridged Edition

For many B2B enterprises, partner and supplier networks are an essential part of business, providing the power to reach new markets, capitalize demand, close opportunities, and fulfill orders. Whether by using off-the-shelf solutions or building specialized applications, organizations are employing digital collaboration, portals, sales enablement, and supply chain solutions to engage with their partners. More advanced approaches are tying together disparate internal and external systems, services, and data to share business intelligence, manage inventories and deliveries, streamline workflows, and expedite customer success.

This sharing of data between entities is almost all done via Application Programming Interfaces (APIs). 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. More so, as an organization's partner and supplier network grow, administration and operational gaps increase as well. To enable fluid onboarding, collaboration, management and accountability while mitigating unauthorized access, data privacy and compliance risks, organizations must extend identity-based authentication and access with fine-grained, contextual authorization and enforcement between parties, applications, services and down to the API object level – at scale.

Cloudentity's modern application authorization platform provides the secure accessibility, delegated administration, protected data exchange, privacy consent, and analytics required to securely accelerate B2B partner and supplier relationships. More so, it provides organizations the means to simplify, efficiently manage, and enforce authorization policy across the distributed applications, services and APIs that power this ecosystem connectivity.

Risks and Requirements

Security and compliance

A lack of proper authentication and authorization across a company's internal and third-party web applications, APIs and service portfolio could allow threat actors to perform account takeover or identity theft. It also may allow terminated parties, even competitors, to gain unauthorized access, intelligence and app usage. Even inadvertent data leakage to partners and suppliers has business and privacy consequences, including penalties associated with GDPR, CCPA, PIPEDA, LGPD, PDPA and HIPAA violations.

Privacy Consent

Another consideration for partner and supplier authorization is incorporating customer privacy consent – a requisite for modern B2B2C applications and services. Organizations, whether to meet data privacy regulations or to boost third-party trust, must provide customers, partners and suppliers the ability to stipulate how their sensitive personal data is to be used. Conventional approaches to applying fine-grained access policy according to privacy consent across applications, services and APIs are currently inefficient, inadequate and not scalable.

Modern CIAM features:

Customer Identity and Access Management (CIAM) solutions are designed to transfer a customer's digital identity and access parameters to different applications. Key features to consider of modern CIAM solutions include:

- Ease to develop and apply privacy consent workflows
- Flexibility to support a wide range of identity and entitlement sources
- Simplified delegated administration for third-party and corporate services
- Broad authentication support including passwordless and MFA
- Use of identity standards, such as SAML2, OAuth, OIDC, SPIFFE
- Granular authorization policy, enforcement and logging
- Centralized service and microservice-native transaction level control

Current challenges

App and API security exposures

A major challenge with securing apps, services and APIs today is that organizations lack service and API visibility, centralized policy control, and transactional enforcement processes. The responsibility of access and security safeguards 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, identity-centric authentication does not provide the breadth of fine-grained policy, nor depth of transactional data exchange enforcement required for B2B and B2B2C programs. 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, which includes other services, APIs and data, and applies a stateful policy to determine the scope of allowed transactions. In most organizations, developers hard-code authorization rules and privacy controls into each application. This inefficient, bespoke process is prone to human error, policy inconsistency and operational blind spots, opening the business up to attack and compliance exposures.

A more effective, automated approach

The B2B and B2B2C security and privacy requirements for partner and supplier management make it clear that a new approach to authorization is needed to retain business trust and to fulfill compliance requirements.

Cloudentity solution for B2B and Partner authorization

Cloudentity provides a flexible and scalable solution for modern application authorization to enable B2B and partner proficiency initiatives within an enterprise's existing hybrid, multi-cloud and microservices infrastructure. The approach ensures continuous access control and personal data privacy for the sensitive information shared internally and among business entities and their customers.

Through Cloudentity's modern application authorization solution, organizations can decouple identity and authorization, orchestrate app, service and API on-boarding, enable fine-grained authorization policy as code, gain privacy consent control, and achieve 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 and create policy 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 for all ingress and egress decision points to prevent unauthorized north/south perimeter and east/west lateral attack, 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 applications and service enhancements 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 modern application authorization 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, SIEM and other systems.

Unique, enterprise-class capabilities

Cloudentity offers unique, enterprise-class features that align to B2B and partner authorization requirements.

Automated user, app, API onboarding into AuthN/AuthZ ecosystems

Enables developer app/API registration, inventory and discovery.

Multi-tenancy and delegated administration

Scale out partner management with a single instance to serve multiple business and multi-tenant applications, as well as delegated user administration.

Authorization policy orchestration

Simplifies policy management with expedited GUI policy editor, natural language code, pre-defined policy packs and dynamic provisioning.

Secure, traceable data sharing

Dynamic authorization based on business agreements between parties and to authorize attribute flows between partner and customer organizations.

Application and service data governance
Applies data exchange and consent governance guiderails for each requests to negate or redact unpermitted information, while capturing the transaction lineage in a tamper-proof Privacy Ledger™.

Consent governance workflow
Manages 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.

Conclusion

Organizations seek to reduce operational costs and overhead with regards to engaging and scaling their partner relationships. Authorization management is a cornerstone B2B technology to advance partner and supplier business while mitigating security, privacy and compliance risks. Cloudentity automates fine-grained authorization policy management and provisioning, administrative delegation, consent management, and transaction-level enforcement necessary to secure application and API access and data exchange between a business and its partner and supplier ecosystem.

Learn how Cloudentity Modern application authorization solutions can increase your partner network advantages, and extend your B2B and partner security capabilities by visiting www.cloudentity.com.

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 flexibly and across IAMs, IdPs, databases, apps, tokens and other sources
- Incorporate privacy consent through built-in workflows across apps and APIs
- Satisfy broad compliance mandates with 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
- Scale as needed with delegated administration, multi-tenancy and multi-tenant application support
- Ensure use of open standards (OAuth, OICD, SPIFEE, OPA) to facilitate rapid deployment

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 B2B2C opportunities, increase development velocity, and mitigate API access, security, 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