Knowledge Brief

Quadrant Knowledge Solutions

How Cloudentity Modern Application Authorization and Consent Fortifies Digital Business Transformation

A Case Study Perspective on:
API-First Security
B2B/B2C Service Privacy

Quadrant
Knowledge Solutions

Case Study Review

CLOUDENTITY

How Cloudentity Modern Application Authorization and Consent Fortifies Digital Business Transformation

Driven by digital business transformation fueling growing demand for cloud computing and application modernization, organizations across industry verticals and geographical regions have adopted a cloud-first/API-first strategy. A large number of global companies have accelerated their cloud infrastructure, microapp development, and service integration projects. Most of an enterprise's legacy applications have traditionally been based on a conventional monolithic architecture, which allowed organizations to implement more centralized authentication and authorization management. However, considering current dynamic business and partner ecosystem scenarios along with demand for increased accessibility and big data intelligence, industry leaders are moving away from monolithic to cloud-native with microservices-based architecture for application deployments.

Microservices-based applications with internal and external-facing APIs enabled organizations to gain the agility and application capabilities necessary to be competitive. However, organizations are facing a greater difficulty to maintain robust authentication and authorization policies across microservices-based applications and distributed services in a multi-cloud environment. Organizations are struggling with inconsistencies across security verification, various levels of permissions, authentication, authorization, privacy, and the enforcement of these policies. With decentralized management and provisioning complexity, organizations are facing challenges in implementing uniform yet granular policies across applications and services.

Authorization management and policy governance across microservice and multi-cloud environments are increasingly becoming cumbersome for development and security teams. The permission and verification requirements vary between different users, systems, applications, and access scenarios. Additionally, due to broad demand for anywhere-accessibility driven by the pandemic necessitating remote workplace usage, as well as the Internet of Things phenomenon, organizations are exposed to greater security and privacy risks. Enterprises are looking at implementing robust API security and governance while maintaining compliant to internal, regulatory, and business agreement requirements – which must be reflected in policies pertaining to data protection, privacy, and access management. Organizations are required to improve user experience; provide users, systems, and services the right level of access to various enterprise applications and data; and streamline their development and security operations.

Quadrant Knowledge Solutions has recently evaluated Cloudentity's Modern Application Authorization and Consent platform, an external declarative authorization solution available as SaaS or as software. Cloudentity's solution helps organizations streamline the onboarding of users, applications, and APIs into the identity and authorization ecosystem. The platform simplifies and centralizes authorization and data privacy policy management and automates provisioning in order to provide customers control standardization across services and APIs.

Cloudentity's platform offers two major functions: Authorization Control Plane™ (ACP) and Cloudentity MicroPerimeter™. To facilitate deployment, the platform also has Identity and API Gateway integration options. The ACP provides centralized policy management, provisioning, analytics, and logging functionalities. It helps organizations streamline user and application onboarding, manage fine-grained authorization policies, manage consent workflows, generate policy-as-code, and track APIs and services data exchange. Highlight features include a graphical policy editor, data lineage visualization, privacy consent integration, and high-performance, object-level transactional enforcement. Cloudentity ACP helps organizations implement Zero Trust security principles by ensuring a context-aware authorization policy management through a control plane that can connect to the MicroPerimeter™, which resides closest to the application or service. The MicroPerimeter™ application provides service and API intelligence, and local policy and data privacy enforcement.

The analyst team at Quadrant conducted a detailed analysis of Cloudentity's approach and platform, and evaluated customer implementations. This Knowledge Brief provides a brief analysis of two customers provided by Cloudentity and verified by Quadrant's team.

Modern Application Authorization and Consent in Action to Support High Tech – B2B and Partner Authentication

A large high-tech company needed to advance capabilities and controls regarding how business agents, systems, and users access the institution's portals and applications across different business entities. At the application and service integration level, ongoing security requirements became cumbersome and costly through multiple engineering, validation, and maintenance stages. The company wanted a more uniform, scalable, and secure approach to control access to data their partners can see and to data used across in-house containerized apps as well as through externally-connected services. Since their business and agent network will expand and evolve, they required a solution that offers identity and entitlement flexibility, delegated administration, and robust privacy controls. As a large business entity seeking to optimize IT capabilities, the solution must be able to provide multi-tenancy and support multi-tenant applications.

Solution

Cloudentity provided its Modern Application Authorization and Consent solution to extend the firm's Partner Identity and Access Management (PIAM) capabilities with granular authorization controls that could be applied to various partner types, hybrid and cloud applications, identity, and entitlement sources. The solution integrates with a wide range of partner IdP platforms and allows for self-service, automated registration, and delegated administration. Built-in privacy consent workflows allow the firm to integrate registration and privacy safeguards more rapidly to meet B2B2C data exposure controls. This authorization management solution is offered as a multi-tenant service, allowing each engineering team to more easily develop and repurpose fine-grained security policies and take advantage of more automated provisioning within their respective Kubernetes and microservice controller environment – whether on-premises or cloud infrastructure.

Result

The initial test project, conducted by one of the largest divisions within this tech company, was successfully completed in weeks and was put into production within months. Cloudentity met all architectural and functional requirements and exceeded the engineering, DevOps, and security team's expectations. The teams took advantage of the platform's data lineage to extend partner oversight and management. Overall development, provisioning, integration, and testing resources were significantly reduced – justifying a phased expansion into additional applications, business units, and applications. The expectation is to offer the platform as a service for its businesses. Moreover, it has allowed the parent company's business architect to satisfy requests to enhance partner access, system integration, and data sharing.

Modern Application Authorization and Consent in Action to Financial Services – API-first

A large financial institution needed to adhere to the NYDFS cybersecurity regulation's data privacy and audit specifications, one of which, for example, was adaptive multi-factor authentication for sensitive transactions. Decentralized management with disparate authorization and authentication coding, as well as complex business logic, made fulfilling compliance requirements a cumbersome and costly task. The company needed to aggregate user data across directories and domains while supporting IAM platforms and advancing DevSecOps initiatives.

Solution

Cloudentity provided its Modern Application Authorization and Consent solution and rapidly onboarded hundreds of modern cloud and on-premises legacy applications. The new unified system offers a way to centrally govern identity and authorization, and apply policy as code. It aggregates multiple sources of identity data, normalizes authorization context, and integrates with numerous existing IAM and access technologies. Cloudentity's built-in, standards-based policy sets simplify policy implementation, including support for NYDFS controls. The solution also delivers rigorous consent management services at the data object level, and provides robust and immutable auditability.

Result

The project was completed in four months, at a fraction of the time and cost compared to the previous approach. The firm achieved application modernization with a common user experience across cloud apps and a fortified microservice security approach to enforce data exchange policy for every transaction. The reduction of development coding, configuration, ongoing maintenance, and overall streamlining of app security verification amounted to less than one year's payback and a longer-term economic benefit. Moreover, this API-first project serves as a key foundation to advance the financial institution's future Open Banking business endeavors.

Quadrant's Perspective on Cloudentity

Global industry leaders are migrating at various stages to cloud-native applications with microservices-based architecture. While organizations are increasingly focusing on gaining IT agility and application modernization, a lack of robust API access security, data privacy, and governance controls has become a delaying factor, if not roadblock, to their digital business initiatives. Specifically, without the means to uniformly see and manage access, privacy and data protection controls across APIs and connected services, developers and security teams take longer to test, resolve, and validate compliance. By externalizing authentication, authorization, and data privacy controls, Cloudentity, through its innovative Modern Application Authorization and Consent solution, is helping organizations gain real-time data visibility, streamline fine-grained policy management, and ensure continuous enforcement. By placing policy-based enforcement near to the application, API and service, granular enforcement can be achieved with nominal latency.

Cloudentity, with its cloud-native, integrated, and automated platform, is well-positioned to help organizations realize Zero Trust advantages across hybrid, multi-cloud, and microservices environments at scale.

The Knowledge Brief, prepared by Quadrant Knowledge Solutions, was sponsored by Cloudentity and is based on independent analyst research and assessment.