CLOUDENTITY

Solution Brief

Mitigating OWASP API Threats with Cloudentity

Cloudentity provides continuous Zero Trust control across APIs and services that mitigate OWASP API vulnerabilities and prevent unauthorized access, data leakage and privacy compliance risks.

APIs are the underpinnings of app modernization and digital transformation, connecting users and systems to a network of services, applications, and databases. As the fabric of modern service delivery and compartmentalized app development, the application logic and sensitive data APIs expose has made them a high-value target of threat actors. Many noteworthy breaches, such as those at Facebook, USPS, Venmo, JustDial (India) and Federation of Industries (Brazil), were consequences of poor API oversight and authorization. Recognizing the risk to users and applications, the Open Web Application Security Project (OWASP) published a list of the top API vulnerabilities to inform security practitioners of the exposures of unprotected APIs and how they can be exploited. Left unchecked, these threats can yield identity theft, breach, data leakage, and compliance violation risks.

> “By 2022, API abuses will be the most-frequented attack vector resulting in data breaches for enterprise web applications.”
>
> - Gartner Research*

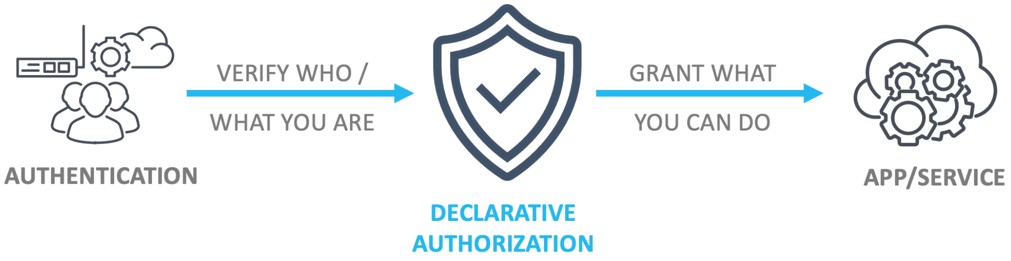
API Security Gaps

How have API threats manifested to become a leading attack vector? The responsibility of access and security controls for each API often lies with software engineering – where increased release cycle frequency, single function module development, and use of third-party APIs have contributed to varying security controls that are difficult to manage and audit. Developers must contend with complex multi-cloud workloads and API service connections, as well as a cumbersome array of identity, security and compliance requisites. In most organizations, authorization rules are typically hardcoded for each application and API. This inefficient, bespoke process is prone to errors, policy drift, and blind spots.

Beyond coding and configuration complications, just discovering and classifying services and APIs is an unwieldy process. The volume of APIs and service gateway connections has grown, even more so amid the pandemic. Incorporating applications and APIs in standardized, granular access and data protection modes has become even more difficult to manage. While organizations have adopted federated authentication mechanisms for session-based access, this identity-centric method does not typically extend granular controls down to service and API data exchange in a uniform manner, nor at real-world performance requirements. In the microservices world, APIs send and receive massive amounts of service requests, which can reveal sensitive information and take in unwanted data – opening the door for attacks.

Authorization Governance

Cloudentity overcomes these enterprise challenges by decoupling identity and authorization from applications and APIs, and enabling declarative authorization with real-time enforcement and full data lineage for reporting, forensics and auditing.



With our authorization governance automation platform, organizations can simply and effectively orchestrate API/service discovery and onboarding; centralize, manage and provision fine-grained policy; and gain transaction-level protection. Through declarative authorization, every service and API request is enforced against standardized policies as close to the app or service as possible. This provides comprehensive, adaptive access and data exchange security with granular OAuth scope and object level control mechanisms to meet a wide array of PII and sensitive data privacy obligations. The solution can enforce millions of requests per second – 60 times the OAuth token minting and eval performance at 90% lower latency compared to other approaches. As a result, organizations gain continuous Zero Trust control at all service ingress and egress decision points to mitigate OWASP API vulnerabilities, data leakage and east/west lateral threats.

*Source: Gartner Inc. “API Security: What You Need to Do to Protect Your APIs from Attacks and Data Breaches” webinar (G00404900)

How Cloudentity Mitigates OWASP API Threats

API1:2019 Broken object level authorization – Cloudentity provides fine-grained, object-level authorization to APIs with policy enforcement as close to the services as possible to negate data misuse.

API2:2019 Broken user authentication – Cloudentity can be used to authenticate APIs using OpenID Connect and OAuth 2.0.

API3:2019 Excessive data exposure – Cloudentity provides built-in data classification that enables you to identify which APIs are processing sensitive data and offers additional access control policies to keep them secure.

API4:2019 Lack of resources and rate limiting – Cloudentity provides API rate limiting for token and access requests to protect against brute force attacks.

API5:2019 Broken function level authorization – Cloudentity ensures that all entities (users, services, and APIs) are identified and authorized leveraging our ML-based contextually-aware risk engine.

API6:2019 Mass assignment – Cloudentity provides JSON schema enforcement and API schema validation at each policy enforcement point.

API7:2019 Security misconfiguration – Cloudentity provides automated API discovery and cataloging and allows for standardized providing of authorization policy as code.

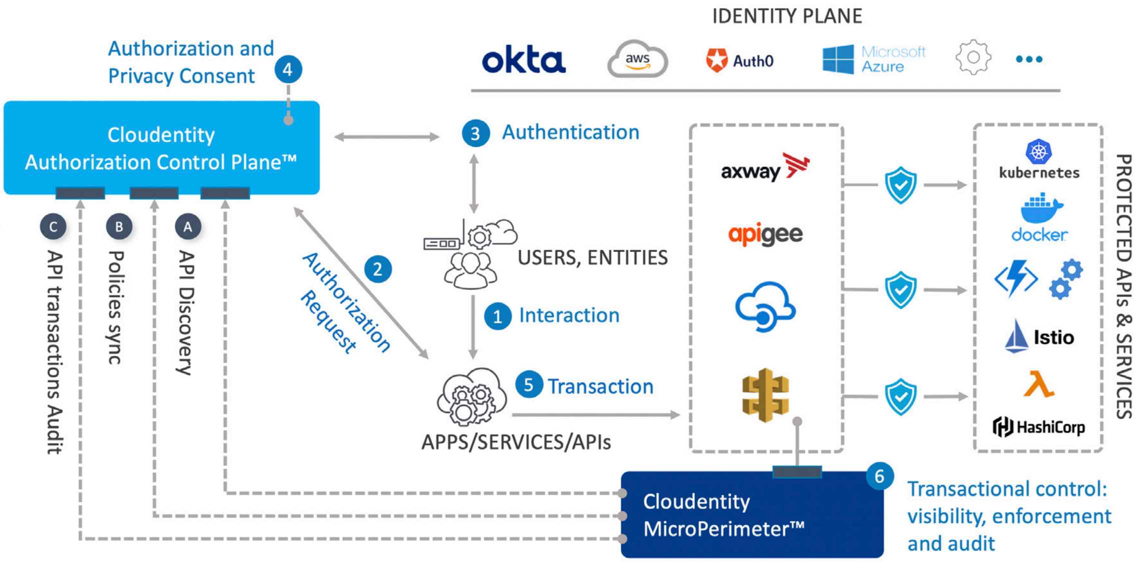
API8:2019 Injection

API9:2019 Improper assets management

API10:2019 Insufficient logging and monitoring – Cloudentity works natively with leading WAF providers to protect against injection, improper asset management and insufficient logging and monitoring. Beyond built-in analytics, all system, user consent, policy management and transaction events are recorded and can be forwarded to logging, fraud and SIEM systems.

Native Microservices Control

Enterprises can seamlessly integrate and scale Cloudentity solutions into their existing identity, API gateway, service mesh controller, and container 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 granular policy enforcement.



Cloudentity is a pioneer and innovator in authorization governance automation. Through our 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.

CLOUDENTITY
206.483.2255
info@cloudentity.com
2815 2nd Ave.
Seattle, WA 98121 • USA