Best in Class API Protection with Signal Sciences and Cloudentity

Summary

Driven by digital transformation and the API economy, businesses are increasing their reliance on APIs to transmit data across services and applications. Application Programming Interfaces (APIs) enable organizations to share data with authorized customers, partners, developers and even other business units who leverage that valuable data in their own applications.

As a component of modern business innovation and software development, APIs enable applications to exchange data and, in effect, "talk to" one another. But the risk of exposing valuable data via APIs is real: Gartner1 estimates that by 2022, API abuses will be the most-frequent attack vector for enterprise web application data breaches. Clearly, API security must be part of any API development plan.

Companies seeking to secure their applications from security risks and attacks such as business logic attacks, API data leakage, Layer 7 DDoS, and API misuse must place a greater emphasis on their API authorization, governance and security. In addition, scrutiny caused by the introduction of data privacy laws such as the GDPR in Europe and CCPA in the United States, provides an even greater burden for companies to securely inspect, authenticate, and authorize the data being transmitted by APIs. Recognizing these emerging threats, Gartner has created a new category bringing web application security and API security together, calling it a WAAP (Web Application and API Protection)

OWASP Top 10 API Vulnerabilities

Recently, the Open Web Application Security Project (OWASP) created the initial list of the most critical API threats, which span both traditional attacks like SQL injection and modern attacks like object-level authorization and broken authentication.

To combat these growing number of API threats the integration between Signal Sciences and Cloudentity provides a best in class solution combining real time layer 7 protection with data-context aware authentication, authorization and governance at the API endpoint for cloud-native and hybrid cloud applications.

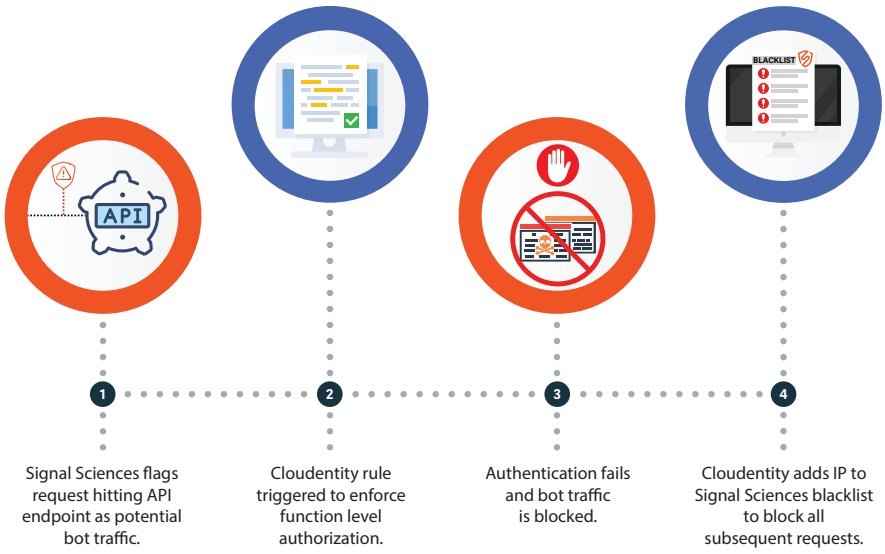
As the leading next-gen WAF and RASP solution on the market, Signal Sciences leverages its patented architecture and highly accurate detection methodology to defend against a wide array of API attacks.

Cloudentity's API MicroPerimeter™ solutions provides visibility, protection, and enforcement at the API level, focused exclusively on the transactional data and providing object level authorization. This affords a level of control and security not currently available in the market or provided by traditional API security solutions like an API gateway.

Solution Overview

As today's adversaries increase the sophistication and scale of their attacks, it's more important than ever to protect your apps using a defense in depth approach. By combining the powerful detection and blocking capabilities of Signal Sciences with the granular and contextual enforcement capabilities of Cloudentity, this integration provides the ultimate protection against threats facing your API landscape.

Use Case : Blocking a Bot Attack



How Does Signal Sciences + Cloudentity Protect Against the OWASP API Top 10?

Vunerability	Mitigation
1. Broken object level authorization	• Implement identity and privacy aware object-level authorization checks using Cloudentity's Authorization Control Plane (ACP). • Utilize the secure token service built into Cloudentity's API MicroPerimeter™.
2. Broken authentication	• Authenticate API using a certified Auth 2.0 provider through Cloudentity's ACP. • Authenticate applications using SPIFFE standard through Cloudentity's ACP.
3. Excessive data exposure	• Audit and review data responses and integrations with data classification vendors. • Built-in service classification for PII, PCI, and sensitive data processing using Cloudentity's ACP.
4. Lack of resources and rate limiting	• Signal Sciences monitors for resource abuse and utilizes rate limiting as an enforcement action. • Cloudentity's API MicroPerimeter allows rate limiting for token and access requests.
5. Broken function level authorization	• The ACP provides externalized function level authorization enforced at the API perimeter. • All entities (user, service, thing, data) in a transaction are authenticated and authorized. • ML based insights for policy usage based on live traffic and data sensitivity.
6. Mass assignment	• Cloudentity provides JSON schema enforcement and API schema validation at the MicroPerimeter.
7. Security misconfiguration	• Signal Sciences monitors and blocks attacks against unpatched or outdated third party frameworks or libraries. • Cloudentity discovers and protects APIs through authorization as code and governance.
8. Injection	• Signal Sciences protects against injection style attacks including SQL, XSS, command execution, and others.
9. Improper assets management	• Signal Sciences and Cloudentity together provide complete visibility and protection across all web, mobile, and API properties.
10. Insufficient logging and monitoring	• Both Signal Sciences and Cloudentity provide robust logging and monitoring of security related API events along with seamless integration with leading SIEMs and DevOps tools.

About Signal Sciences

With its award-winning next-gen WAF and RASP solution, Signal Sciences protects more than 40,000 applications and over a trillion production requests per month. Signal Sciences' patented architecture provides organizations working in a modern development environment with comprehensive and scalable threat protection and security visibility. The company works with some of the world's most recognizable companies, as indicated on the company's website, including Duo Security, DataDog, Under Armour, Twilio SendGrid, and Doordash. Signal Sciences is also named a Forbes Next Billion-Dollar Startup and received the 451 Firestarter award, InfoWorld's Technology of the Year, and Computing's DevOps Excellence Award for Best DevOps Security Tool. For more information, visit Signal Sciences website or follow @Signal Sciences.

About Cloudentity

At Cloudentity we understand that the world of API Security and Application management is rapidly changing and requires new tools to ensure companies are not only protecting infrastructure, but complying with a growing complexity of privacy and security regulations while increasingly sophisticated customers are demanding assurances from the companies they do business with. We build those tools!