CEQUENCE SECURITY

Tracking and Enforcing API Contracts for Partner Ecosystem

Customer Challenge: API Contract Violations

This (anonymous) customer uses unique APIs to deliver tracking and logistics services to hundreds of retail partners. Each API is unique, and is written to exacting specifications, which are then used as an API contract between the two parties. The growth in partners, and the risk of API errors that could lead to vulnerability exploits or sensitive data leakage, led the customer to investigate API security platforms. Their requirements were visibility into all of their APIs, a mechanism to confirm APIs were conforming to specifications and not leaking sensitive data.

Customer Profile

Returns and tracking logistics provider for retailers.

Outcomes with API Sentinel

- **Discovers and prevents sensitive data leakage** that may jeopardize partnership status and compliance
- **Graphically displays an inventory** of all external and internal APIs
- **Provides comprehensive risk assessment** based on predefined and custom risk categories

The Solution: Runtime Specification Conformance Enforcement

Using Cequence API Sentinel as a complement to Cequence Bot Defense, the customer is able to track all of their partner APIs in real-time. The runtime visibility into API traffic source, destination, ISP and organization allows them to uncover shadow APIs, possible misuse, and anomalous behavior. Each API is analyzed for potential risk such as authentication, non-conformance or data leakage risks – those deemed high risk are flagged for development review. Each partner API has an associated specification that is used to establish an API contract between the customer and the retail partner. The API specifications include details on what data should be included in the API requests and responses.

The agreed upon specification is uploaded to API Sentinel, where it is used to compare each API to the specification for conformance and potential sensitive data leakage. Using the API Sentinel Sensitive Data Dashboard, the customer will be able to quickly see any non-conformant APIs that may be leaking sensitive data such as a social security, credit card number or even a custom data pattern. Predefined connectors to DevOps tools will allow them to initiate an alert and quickly remediate the security gap. In addition to sensitive data analysis and enforcement, API Sentinel will assess each of the APIs to confirm they are using the defined authentication mechanism.

Results: Complete API Security

API Sentinel deployed in conjunction with Bot Defense provides this customer with an end-to-end API security solution that helps them meet their contractual obligations. Starting with the ability to see all APIs, and ensure they are all adhering to the specification contract helps to ensure no security gaps are published that may result in an exposed vulnerability. Bot Defense complements API Sentinel with the ability to see all the APIs and web apps, then analyze the respective transactions to uncover (and prevent) malicious bot activity and business logic abuse.