CEQUENCE SECURITY

Better Together: API Sentinel and Amazon API Gateway

Continuous Visibility and Risk Monitoring of Your APIs

Introduction

APIs represent a core development component for today's modern applications deployed on AWS. However, APIs are a double-edged sword, accelerating development while introducing security challenges such as:

- **Deprecated, hidden and shadow** APIs that fall outside of security teams' visibility.
- **Hidden parameters** for privilege escalation that can lead to theft or fraud.
- **Inadvertent exposure** of confidential data in error messages.
- **Application business logic** flaws that lead to automated bot attacks.

Amazon API Gateway provides developers with an avenue to create, publish, maintain, monitor, and secure APIs at any scale. API Sentinel from Cequence Security complements Amazon API Gateway volumetric and user authentication security features with runtime visibility, risk analysis and conformance assessment to help your team gain a complete understanding of your API footprint and reduce the associated risks that APIs may introduce.

API Sentinel on AWS

Deployed as a modern application on Amazon Elastic Kubernetes Service (EKS) from AWS Container Marketplace, API Sentinel integrates with Amazon API Gateway to create a runtime inventory of your APIs, analyze them for potential security risks, and assess their conformance levels against OpenAPI specifications.

Amazon API Gateway logs can be filtered in Amazon CloudWatch and forwarded to an Amazon S3 Bucket using Amazon Kinesis Data Firehose. API Sentinel will then monitor your APIs to uncover potential security gaps that can be mitigated before they become incidents.

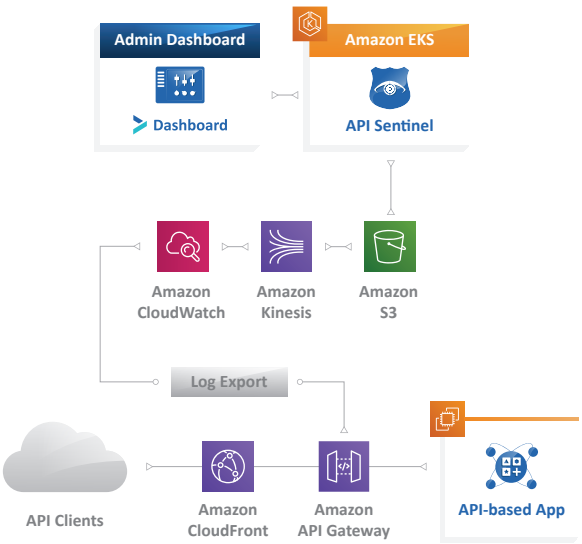
To help ensure that all of your APIs are discovered and monitored, API Sentinel can integrate with other API Gateways as well as common proxies (HAProxy, Envoy, NGINX).

aws partner network

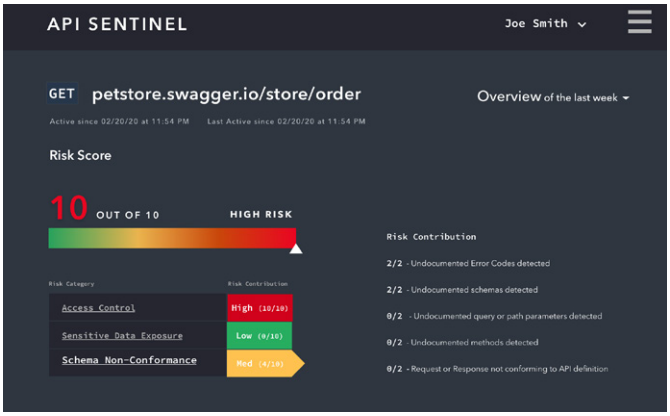
Advanced
Technology Partner

About Cequence Security

Cequence Security is an AWS Advanced Technology Partner and was one of the launch partners for the APN Global Startup Program. Together, we help protect our customers' APIs and web applications from cyberattacks with a cloud-native, container-based application architecture. Customers include F500 organizations across multiple vertical markets, and our solution has earned numerous industry accolades.



API Sentinel Features



Continuous Risk Scoring

API Sentinel continually analyzes your APIs to provide a risk assessment based on security best practices including:

- **Strength** of access control.
- **Sensitive data** in error messages or payload.
- **Use of encrypted** communication.
- **Conformance** to your OpenAPI specifications.

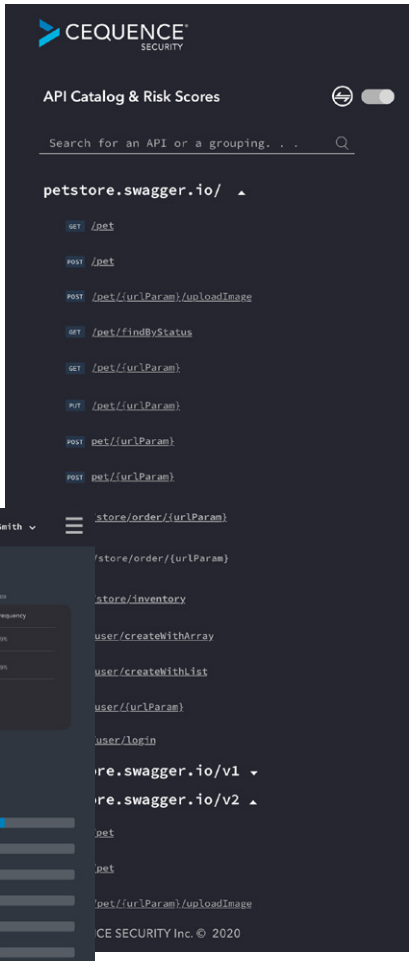
Each API endpoint (e.g., a single HTTP GET endpoint or a POST endpoint) is analyzed continually with the result displayed visually on a scale of 1-10, allowing you to quickly target and address any potential security gaps before they are published. For example, API Sentinel can flag an API that is transferring PCI data without encryption, helping you maintain compliance.

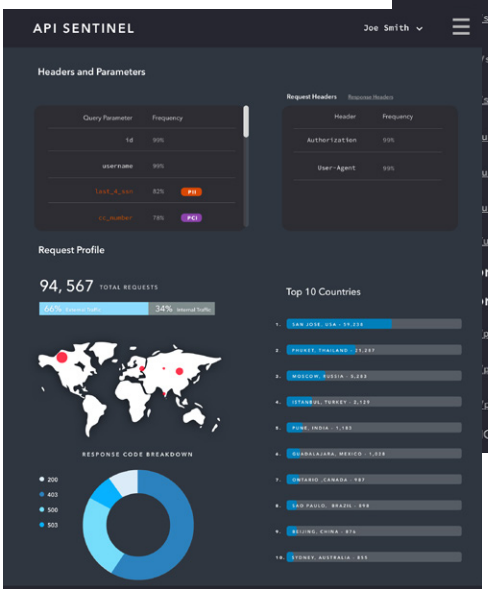
Schema Non-Conformance Detection

API Sentinel allows you to perform a runtime comparison of your inventoried APIs against your OpenAPI specification to surface any potential security gaps. Any API endpoints, headers, parameters and response codes that may not be listed in the specification are flagged as non-conformant and can be addressed by development, effectively mitigating security risks before they reach production.

Runtime API Inventory

Integration with your API Gateway or Proxy allows your security team to automatically discover your entire API footprint including those knowingly published as well as shadow APIs. Discovered API endpoints are graphically displayed in the management dashboard using default or user-defined groupings.





API Usage Analysis

The Runtime API Inventory is complemented by a rich set of usage data including the countries, IP addresses and organizations that your API requests are originating from. Predefined filters allow you to view the geographic distribution of API usage during specific time periods while additional visibility into the headers, parameters and response codes discovered provides real-time API usage patterns.