CEQUENCE SECURITY

API Sentinel

Continuous Visibility and Risk Monitoring of Your APIs

Introduction

APIs are enabling the digital transformation for enterprises around the globe. According to Gartner, by 2023, over 50% of B2B transactions will be performed through real-time APIs versus traditional approaches[1]. However, APIs are a double-edged sword, accelerating development while also introducing a range of security challenges:

- **Deprecated, hidden and shadow** APIs published outside of security teams' visibility and left unprotected.
- **Hidden parameters** that allow privilege escalation and lead to theft or fraud.
- **Exposure** of confidential or sensitive data in response codes or error messages.
- **Application business logic flaws** that enable bad actors to carry out account takeover fraud, scraping and fake account creation.

To address these security challenges, security teams currently need to deploy multiple point products to address exploit prevention, non-conformance, or shadow APIs, all of which managed separately.

API Sentinel takes a different approach, providing enterprises with unmatched visibility into API usage, specification conformance and security risk. Armed with an understanding of API usage and potential risk, security and development teams can efficiently prioritize fixes at a per-API level to mitigate security risks.

API Sentinel Overview

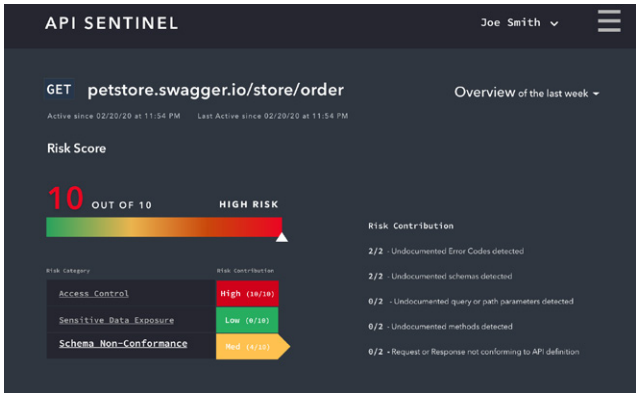
API Sentinel helps your security and development teams eliminate API security risks before they are published with runtime API inventory for visibility, continuous risk analysis and specification conformance assessment. Armed with a complete picture of your API security posture provides your team with the information they need to eliminate potential risks before they become incidents.

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.

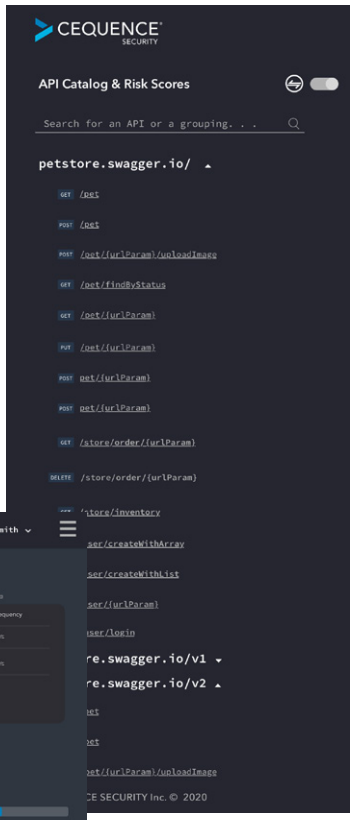


Cequence API Sentinel

Enables your team to regain control over your API footprint, regardless of deployment location. Key benefits include:

- Provides real-time visibility and monitoring of all your public-facing APIs with a runtime inventory.
- Enables you to prioritize API security fixes by identifying risk factors of sensitive data leakage or fraud.
- Helps maintain PCI or HIPAA compliance with complete API visibility and sensitive data discovery.
- Closes potential security gaps that may result from API implementations not conforming to OpenAPI specification.

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.

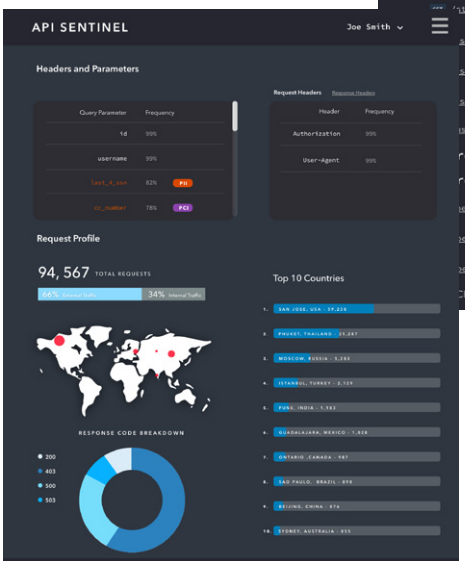


Schema Non-Conformance Detection

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.

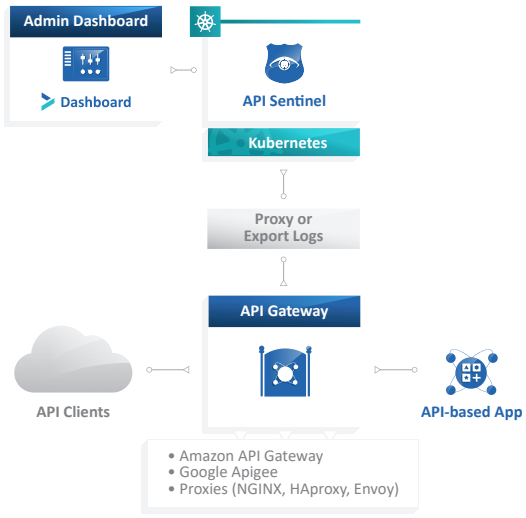


API Usage Analysis

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 pattern

Deploys in Minutes

Deployed as a Kubernetes application, API Sentinel uses an intuitive, widget-based interface to natively integrate with popular API management tools including Amazon API Gateway, Apigee API Management and Proxies (Envoy, NGINX and HAProxy). Within in a matter of minutes, you can begin tracking, monitoring and reducing the risks your APIs may introduce.



API Sentinel and the Application Security Platform

API Sentinel complements Bot Defense and the Application Firewall with continuous visibility and risk monitoring of your API footprint. Findings surfaced by API Sentinel can be used by your development teams to block the publication of potential vulnerability exploits that may result from a non-conforming API. API Sentinel can be deployed in conjunction with Bot Defense and App Firewall to provide organizations with the only multi-threat API security offering on the market.

[1] Source: Gartner - Gartner's API Strategy Maturity Model, October 2019

CEQUENCE SECURITY
100 Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai