CEQUENCE SECURITY

API Sentinel

Continuous API Visibility, Monitoring and Protection

Introduction

APIs are enabling a digital transformation for enterprises on a global scale. As a proof point, Gartner states that by 2023 over 50% of B2B transactions will be performed through real-time APIs versus traditional approaches[1]. At the same time, APIs introduce a range of security challenges:

- **Shadow, hidden, deprecated, and 3rd party APIs** published outside of a defined process and left unprotected.
- **Exposure of confidential or sensitive data** resulting in data loss and compliance violations.
- **Coding errors** that lead to privilege escalation and result in data loss or fraud.
- **Application business logic flaws** that enable bad actors to execute business logic abuse and automated bot attacks.

To address these security challenges, organizations need more than just developer-side testing tools or silo-based API visibility tools. What's needed is a tool that provides 360-degree visibility into your web APIs, from the edge to your data center, to your ingress controllers, and helps you improve and maintain your API coding efforts.

Cequence API Sentinel

Runtime visibility, monitoring and threat protection. Key benefits include:

- Eliminates API Discovery "Surprises" with 360 degree API visibility, inventory and risk analysis.
- Prevents data leakage-related compliance violations with sensitive data discovery.
- Embeds security into your API lifecycle with REST-based API framework.

API Sentinel Overview

API Sentinel helps security teams, API centers of excellence, and data governance officers address their most pressing API problem – visibility and monitoring of their internal and external APIs. It extends that visibility into risk and conformance analysis to discover and remediate gaps that can result in data loss or fraud. Deployable in a matter of minutes, API Sentinel integrates with your API management infrastructure and CI/CD tools to provide immediate value to both security and developers alike by finding all the APIs for visibility, discovering potential security gaps, and alerting development teams for rapid remediation.

API Sentinel Features

Reign in Your API Footprint With 360 Degree Visibility

The #1 API security challenge most organizations face is finding all of their APIs. API Sentinel solves this problem by integrating with a broad range of infrastructure components, including API gateways, proxies, load balancers, and ingress controllers to deliver 360-degree visibility into public-facing and internal APIs including shadow, 3rd party, and managed. A Discovery API allows you to proactively push API metrics to API Sentinel as an alternative to an inline deployment. The API Inventory Dashboard graphically displays APIs based on risk, with drill-down metrics that include the geographic distribution of API usage by country, IP address, and organization with additional visibility into the headers, parameters, and response codes discovered.

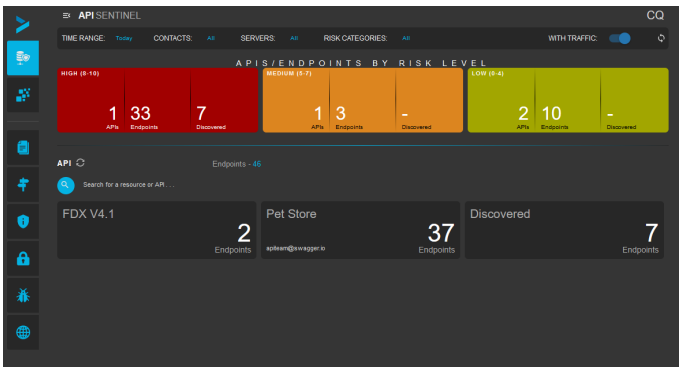

Image 1: Continuous discovery, inventory tracking, and risk categorization help you reign in your API footprint.

Prevent Sensitive Data Leaks & Compliance Violations

Data governance and security teams can eliminate potential compliance violations using the Sensitive Data Exposure dashboard to quickly identify and remediate APIs and endpoints using sensitive data based on predefined (credit card and social security numbers, Stacktrace codes) and custom data patterns. The Dashboard provides fingertip access to details, including the API source or response codes leaking the data, the pattern found, and the underlying IP address details. Notifications can be sent to development teams for speedy remediation using predefined alerts for tools such as Slack, PagerDuty or email.

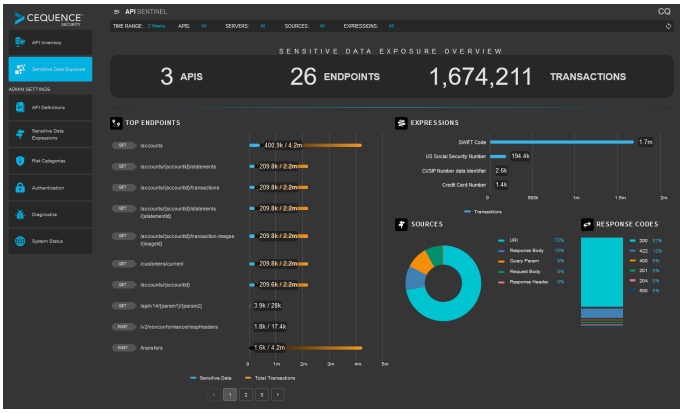

Image 2: The Sensitive Data Dashboard displays APIs that are using sensitive data and could jeopardize compliance.

Improve and Maintain Coding Consistency

API Sentinel fosters collaboration between security and development teams by quickly uncovering potential API security gaps for remediation. Using predefined and custom risk assessment rules, API Sentinel analyzes your public-facing and internal APIs to uncover those deemed high risk. Flexible alerting capabilities allow you to initiate update requests to the development team via Slack, PagerDuty, email, and other tools. An added assessment layer is available for those that have adopted the OpenAPI specification framework. Using a specification definition pushed from CI/CD framework tools or uploaded directly, API Sentinel performs a conformance comparison, sending an alert to development for those APIs found to be non-conformant.

Embed Security into the API Lifecycle

A broad set of REST-based APIs allows you to embed runtime security into your API lifecycle. The Spec Management API enables you to push new specifications and updates to API Sentinel directly from CI/CD framework tools. The Discovery API allows you to proactively push API metrics from other network sources to API Sentinel as an alternative to an inline deployment. An export API enables you to send findings to external tools for analysis and fraud remediation.

Deploys in Minutes

API Sentinel can be deployed as a Kubernetes application in your data center, as a SaaS, or in managed environments like Amazon EKS and GCP GKE. It integrates with your API management infrastructure, including API gateways, proxies, load balancers, and ingress controllers to ensure that all your public-facing and internal APIs are discovered, inventoried, and analyzed, regardless of deployment location or which network infrastructure management infrastructure component they flow through.

[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