CEQUENCE SECURITY

DATASHEET

# Cequence API Sentinel

## Continuous API Visibility, Monitoring and Protection

## Introduction

APIs are at the heart of nearly every digital transaction we execute and they 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.

## API Sentinel at a Glance

Cequence API Sentinel provides runtime visibility, monitoring and threat protection. Key benefits include:

- **Integration with a broad range of network infrastructure components** ensures complete discovery of your API footprint.
- **Customizable, ML-based sensitive data analysis** helps prevent data leakage-related compliance violations with sensitive data discovery.
- **Continuous risk assessment** uncovers coding errors for remediation and a stronger security posture.

## 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 continuous risk and conformance assessment to help you discover and remediate coding errors 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 pipeline tools to provide immediate value to both security and developers alike.

## 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 network infrastructure components, including API gateways, CDNs, proxies, load balancers, and ingress controllers to deliver 360-degree visibility into public-facing and internal APIs including managed, unmanaged and 3rd-party. A Discovery API allows you to proactively push API metrics to API Sentinel as an alternative to 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.

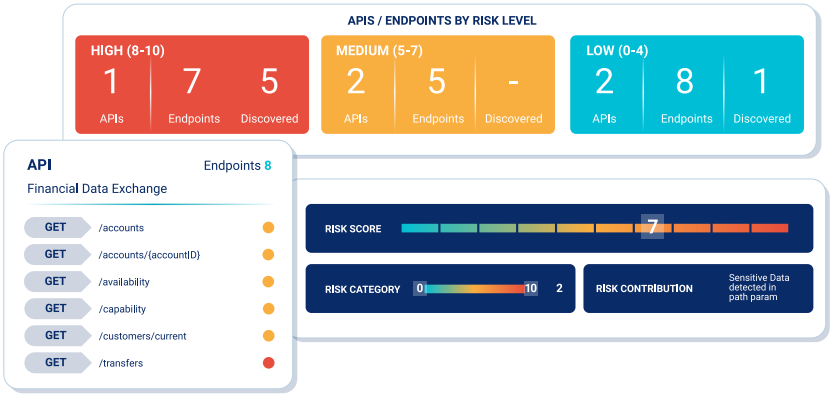



Image 1: Continuous discovery, inventory tracking, and risk categorization help you reign in your API footprint.

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

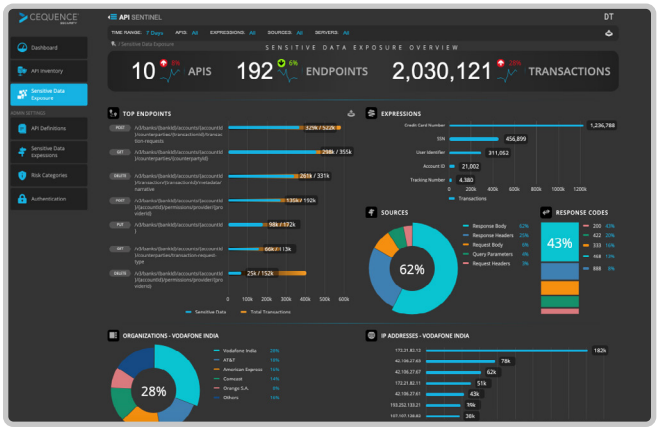


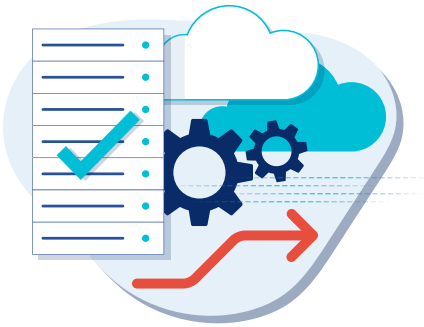

*Image 2: The Sensitive Data Dashboard displays APIs that are using sensitive data and could jeopardize compliance.*

## 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 customizable data patterns. Context-aware sensitive data detection using a Natural Language Processing (NLP) machine learning technique complements predefined patterns and reduces false positives by allowing you to find sensitive data exposure using contextual clues (e.g., presence of keywords close to the actual detected value). The results are graphically displayed in the dashboard for fingertip access to details such as 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 rapid remediation using predefined alerts for tools such as Slack, PagerDuty or email.

## Improve and Maintain Coding Consistency

API Sentinel fosters collaboration between security and development teams by quickly uncovering potential API coding errors for remediation. Using predefined and custom risk assessment rules, API Sentinel continuously 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. To help accelerate API specification framework adoption, you can automatically generate an OpenAPI 3.0 specification for any discovered API that is not based on an OpenAPI specification.



> "Cequence Security exceeds our requirements for runtime API visibility and protection.
>
> VP of Security,
> Large Global Telecom Service Provider

## Broad, API-based Ecosystem Integration

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 SaaS, in the public cloud, in your data center and as a hybrid. 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, cataloged, and analyzed, regardless of deployment location or which network infrastructure management infrastructure component they flow through.

# API Sentinel and the Cequence Unified API Protection Solution

API Sentinel is an integral component of the Cequence Unified API Protection solution, complementing API Spyder, API Security Testing and API Spartan with continuous visibility and risk monitoring of your API footprint. Findings surfaced by API Sentinel can be used by your development teams to avoid the publication of vulnerability exploits caused by API coding errors. Organizations that have fully embraced an API-first methodology or are just getting started, trust Cequence Security to protect their APIs and scale their business with the only solution that addresses every phase of their API protection lifecycle. The Unified API Protection solution brings together runtime API visibility, security risk monitoring, and patented behavioral fingerprinting technology to consistently detect and protect against ever evolving online attacks. The solution has proven to be effective in preventing online fraud, business logic attacks, exploits and unintended data leakage, scaling to process over 6B API calls per day while protecting 2B+ user accounts and more than $1.3T in asset value across our F500 customer-base.

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