CEQUENCE

Datasheet

Cequence API Spyder

Continuous API Attack Surface Discovery and Management

Introduction

Today, nearly every application your employees use is based on APIs. The sales productivity, collaboration, marketing automation and project tracking apps are API-based as are every single app they may use on their mobile device. As organizations continue to expand their use of microservices and create new cloud-native applications, API usage will continue to explode, as will the API attack surface. If not carefully documented and tested, your API attack surface may include publicly accessible production APIs as well as a host of other resources and end points that should not be publicly accessible. Examples include non-production servers, in-development API specifications that include a catalog of internal server endpoints; health monitoring endpoints that return internal application server status, and much more. Not knowing this entire attack surface poses several challenges to security teams:

- **Inability to monitor APIs:** Lack of visibility implies lack of monitoring, which means that the unknown API attack surface could expose your organization to security risks including data breaches, theft, fraud, and business disruption.
- **Incomplete testing:** Penetration or vulnerability testing efforts are incomplete because they do not include the entire attack surface.
- **Out-of-compliance audits:** The unknown attack surface poses a challenge for compliance or audit teams who rely on knowing all the ways in which corporate data can be accessed.

To address these issues, security teams need to be able to discover their entire API attack surface and constantly monitor it for new APIs or domains that are created. They also need to be able to categorize these APIs based on risk and initiate remediation tasks for security and development teams.

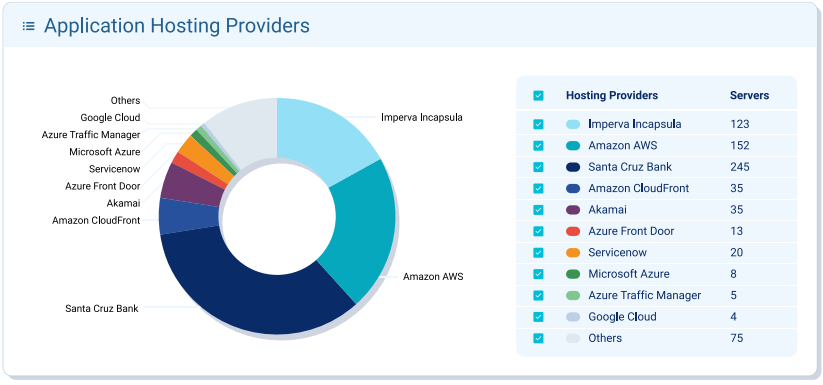
API Spyder at a Glance

You cannot secure or manage the APIs you cannot see. API Spyder helps security and risk compliance teams discover their publicly exposed API attack surface, regardless of where the APIs are deployed.
Key benefits include:

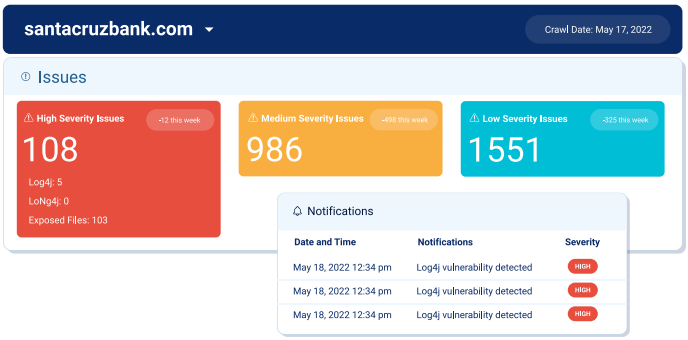
- **Continuous visibility** of publicly exposed production and non-production APIs and endpoints helps security teams keep pace with API development efforts.
- **Up-to-date inventory** of all service gateways and cloud provider deployments that host publicly exposed APIs helps with risk and compliance audits.
- **Exportable reports** and actionable real-time notifications of exposed resources reduces security team remediation response times.protection in minutes, not weeks or years.

API Spyder Overview

API Spyder takes a unique approach to discover your API attack surface. Deployed entirely as a cloud service and requiring no agents or software to be deployed, API Spyder proactively crawls your domains to find all publicly accessible sub-domains. It uses proprietary probing techniques to uncover DNS-listed sub-domains and their underlying API endpoints. Once the sub-domains and the API endpoints are discovered, API Spyder presents the findings in an easy-to-consume dashboard that lists all the service gateways hosting APIs and the types of uncovered API endpoints, classified by function. The dashboard, executive reporting and real-time alerting allow you to quickly translate the findings into remediation efforts.



API Spyder Features

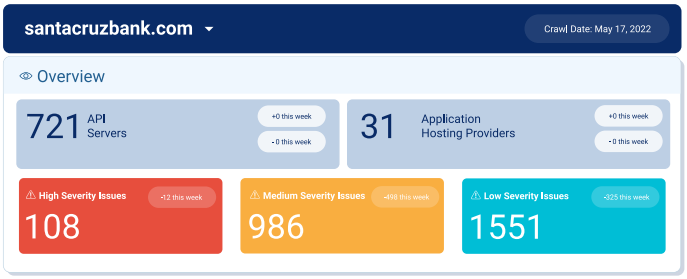


Uncover Log4j and LoNg4j Vulnerable Servers

API Spyder can be used to validate that your Log4j and LoNg4j patching efforts are complete and that no additional vulnerable servers have been added to your digital supply chain. Using predictive crawling techniques, API Spyder discovers public-facing servers that have not yet been patched for the Log4j and LoNg4j vulnerability.

Discover all API Hosting Providers

Accepting a domain as input from the user, API Spyder automatically compiles an inventory of all publicly accessible sub-domains using DNS probing techniques. API Spyder then automatically discovers the hosting service for each sub-domain, such as a CDN or public cloud provider, grouping the sub-domains by hosting service for review, analysis and remediation if necessary.



Discover and Categorize Publicly Accessible API Endpoints

To eliminate the need for API specifications or catalogs as reference points, API Spyder uses a proprietary predictive crawling technology to uncover the publicly exposed API endpoints for each discovered sub-domain. Discovered endpoints are categorized by function (e.g., authentication), API type (e.g., REST or GraphQL), purpose (e.g., health monitoring or Swagger listings) or intended audience (e.g., production vs. non-production). They are also sorted under each discovered sub-domain for easy consumption by security teams.

Notifications

API Spyder continuously monitors your domains, comparing the previous findings with the newly generated results, automatically flagging any changes or deviations for action. Changes to the discovered attack surface are visualized using the dashboard and exported as a file for sharing with other users for remediation. Notifications are generated via email when new Log4j/LoNg4j vulnerable servers are discovered.

Actionable Reporting

A predefined executive report summarizes the findings by domain, the number of discovered API servers and hosting providers. Findings are further categorized by risk levels and the hosting providers broken out by type – ISP, Infrastructure-as-a-Service (IaaS), and CDN – allowing you to uncover potential shadow IT instances. To help you track progress the report wraps up with a week-over-week differences and a set of recommended actions.

API Spyder and the Cequence Unified API Protection Solution

An integral component of the Cequence Unified API Protection solution, API Spyder complements API Sentinel, API Security Testing and API Spartan with continuous API attack surface discovery and monitoring. 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 security journey. The Unified API Protection solution unifies 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 “$9T in customer assets across our F500 customer-base.

CEQUENCE
100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai
© 2023 Cequence Security, Inc. All rights reserved.