CEQUENCE

Datasheet

API Attack Surface Discovery

API Spyder

As organizations evolve, their networks are constantly changing – new applications are deployed, existing applications are updated, and new hosting providers are engaged through organic growth or mergers and acquisitions. All these actions promote the addition of new APIs, increasing an already extensive attack surface. Most organizations simply don't know how many APIs they have and where they are, and that knowledge is foundational for any successful security program.

At each organization, API Spyder discovers an average of:

326	197	37
API Hosts	**Domains**	**Hosting Providers**

This ever-expanding attack surface has led to new requirements for security teams:

- Complete visibility into and monitoring of public-facing API hosts and hosting providers
- Identification of API-specific security issues such as publicly-exposed OpenAPI or GraphQL endpoints
- Persona-tailored reporting on external attack surface discoveries

It's critical to have visibility into existing publicly-accessible APIs as well as to monitor for new APIs, especially those that may have been made public accidentally, such as non-production servers or applications in testing.

API Spyder at a Glance

- **External attack surface discovery** including API hosts and hosting providers
- **User-configurable algorithms** for API discovery and classification
- **API risk identification** with actionable insights
- **Persona-centric reporting** and detailed data export

API Spyder Overview

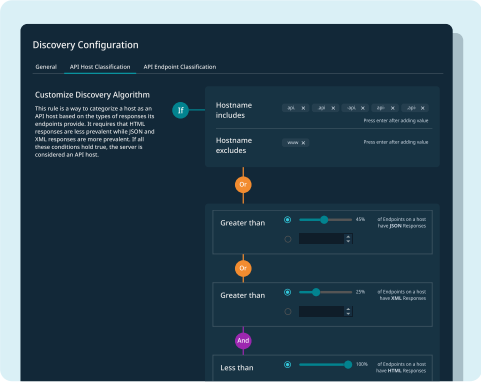
Cequence API Spyder is SaaS-based discovery tool that provides an attacker's view into an organization's public-facing resources. It discovers external API hosts, unauthorized hosting providers, API-specific security issues, and provides executive-level and full data stream reporting.

API Spyder Features

Comprehensive External Attack Surface Discovery

Requiring no installation or agents, API Spyder performs discovery crawls based on domains or IP addresses to discover API hosts and associated hosting providers. This method enables API Spyder to identify API hosts even if they aren't transacting data, a critical capability for finding API hosts made public by accident, such as those misconfigured or leftover from testing. Discovery crawls can be performed on-demand or scheduled, and can also be configured from a particular geography as needed for speed, geo-fencing, or data privacy purposes.

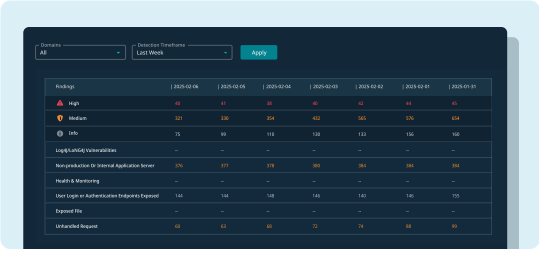
User-Configurable API Discovery and Classification Algorithms



Resources discovered by API Spyder are classified through user-customizable algorithms. Every organization and vertical is different, and this capability enables users to tune the discovery and classification algorithms to match their business and reduce false positives. For example, users can tune the algorithms based on the number or percentage of JSON, XML, or HTML responses to improve identification accuracy for unique or heavily modified endpoints.

API Risk Identification

During the crawl process, API Spyder discovers API hosts with known issues including publicly-exposed Swagger, OpenAPI, or GraphQL endpoints or non-production servers. API Spyder will categorize these findings by function and severity with the full context of the request and response. Findings are also user-configurable, enabling organizations to focus on those risks they deem most relevant.



Reporting for Executives and Security Teams

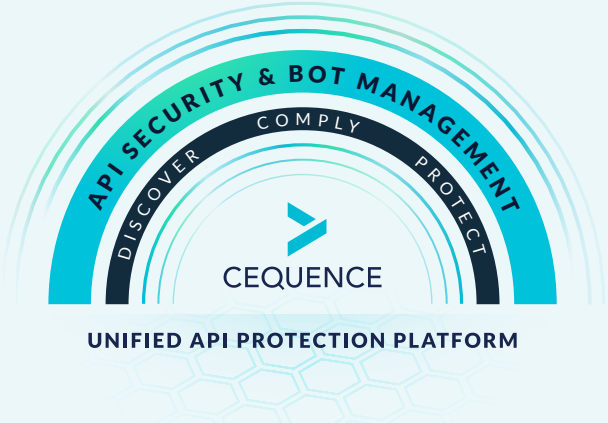
API Spyder provides graphical, PDF executive summary reports for a high-level summary view. Detailed technical data can be exported in Excel format including all hosts discovered by API Spyder about each API host including IP address and security findings.

Works with Cequence AI Gateway

The Cequence AI Gateway enables agentic AI access to any internal, external, or SaaS application, in minutes, without coding. API Security can automatically create API specs that the AI Gateway uses to create MCP servers, eliminating significant manual effort.

API Spyder is Part of the Cequence Unified API Protection Platform

The Cequence Unified API Protection platform unites discovery, compliance, and protection to defend an organization's applications and APIs against attacks, business logic abuse, and fraud. Demonstrating value in minutes rather than days or weeks, Cequence offers a flexible deployment model that requires no app instrumentation or modification. Trusted by the largest and most demanding private and public sector organizations, Cequence protects more than 10 billion daily API interactions and 4 billion user accounts.



CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai