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 of these actions bring additional APIs to light, 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
API Hosts

197
Domains

37
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

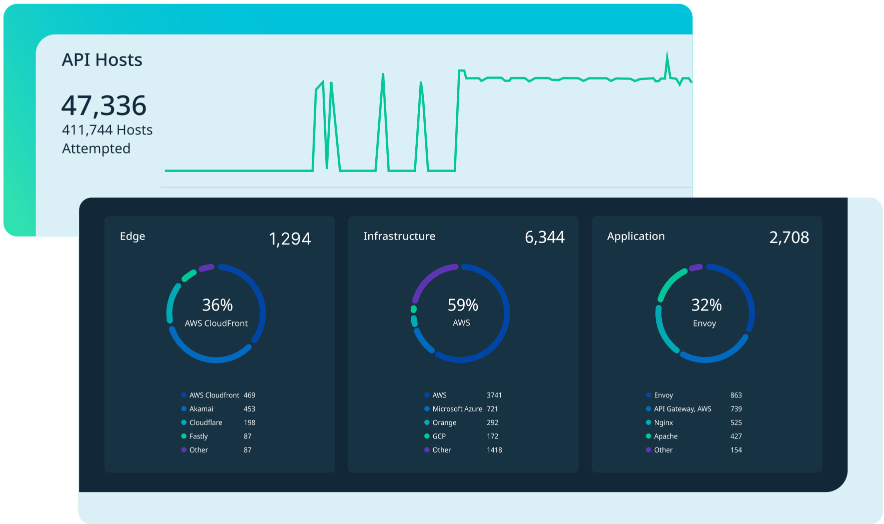
It's critical to have visibility into existing publicly-accessible APIs as well as to monitor for new APIs, especially those that may have been made public accidentally, such as non-production servers or applications in testing.

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.



AWS Cloudfront	469
Akamai	453
Cloudflare	198
Fastly	87
Other	87

AWS	3741
Microsoft Azure	721
Orange	292
GCP	172
Other	1418

Envoy	863
API Gateway, AWS	739
Nginx	525
Apache	427
Other	154

API Spyder Features

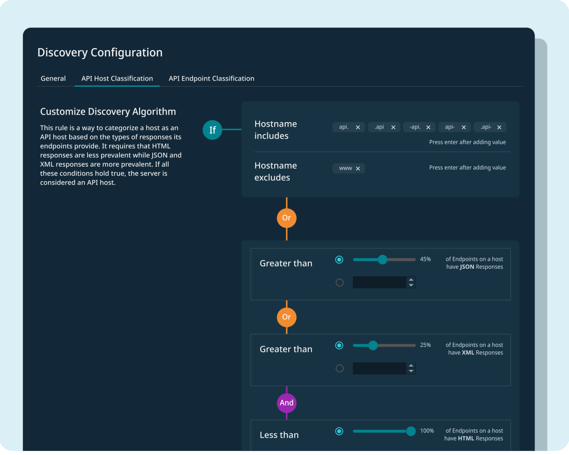
Comprehensive External Attack Surface Discovery

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 on a schedule, enabling continuous monitoring of the external API footprint as well as one-off crawls configured to look for something specific, such as an API host that may be affected by a zero-day vulnerability. Crawls 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 dramatically 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.



Discovery Configuration

Customize Discovery Algorithm

This rule is a way to categorize a host as an API host based on the types of responses its endpoints provide. It requires that HTML responses are less prevalent while JSON and XML responses are more prevalent. If all these conditions hold true, the server is considered an API host.

If

Hostname includes: api. ✕ .api ✕ -api. ✕ api- ✕ .api- ✕

Press enter after adding value

Hostname excludes: www ✕

Press enter after adding value

Or

Greater than ● 45% of Endpoints on a host have **JSON** Responses ○

Or

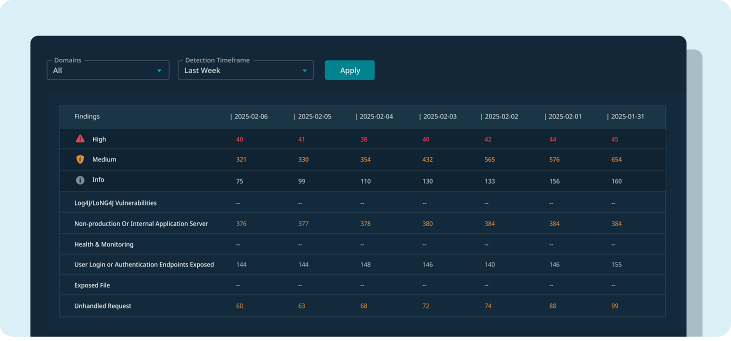
Greater than ● 25% of Endpoints on a host have **XML** Responses ○

And

Less than ● 100% of Endpoints on a host have **HTML** Responses

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, providing full visibility into how issues were detected and categorized. These risks are also user-configurable, enabling organizations to focus on those risks they deem most relevant.



Domains: All

Detection Timeframe: Last Week

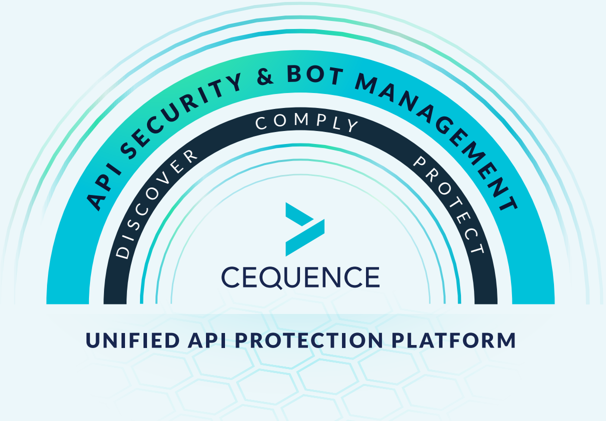
Findings	2025-02-06	2025-02-05	2025-02-04	2025-02-03	2025-02-02	2025-02-01	2025-01-31
High	40	41	38	40	42	44	45
Medium	321	330	354	432	565	576	654
Info	75	99	110	130	133	156	160
Log4J/LoNG4J Vulnerabilities	--	--	--	--	--	--	--
Non-production Or Internal Application Server	376	377	378	380	384	384	384
Health & Monitoring	--	--	--	--	--	--	--
User Login or Authentication Endpoints Exposed	144	144	148	146	140	146	155
Exposed File	--	--	--	--	--	--	--
Unhandled Request	60	63	68	72	74	88	99

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. This format enables security teams to share and delegate to other stakeholders such as application owners.

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. Cequence solutions scale to meet the demands of the largest and most demanding private and public sector organizations, protecting billions of user accounts and billions more daily API interactions.


API SECURITY & BOT MANAGEMENT
DISCOVER
COMPLY
PROTECT
CEQUENCE
UNIFIED API PROTECTION PLATFORM

CEQUENCE