July 2023

Datos Insights Vendor Evaluation: API Security Solutions

Report Author: Tari Schreider

Report Excerpt Compliments of:

CEQUENCE

July 2023

Datos Insights Vendor Evaluation: API Security Solutions

Report Author: Tari Schreider

Table of Contents

© 2023 Datos Insights or its affiliates. All rights reserved.

List of Figures

List of Tables

© 2023 Datos Insights or its affiliates. All rights reserved.

© 2023 Datos Insights or its affiliates. All rights reserved.

Summary and Key Findings

This Datos Insights Vendor Evaluation is an in-depth analysis and voice of the customer of API security solutions. Participants of this report represent startup and scaleup vendors that submitted their API security solutions to 100 points of evaluation scrutiny. This report is a buyer's guide for organizations seeking a standalone API security solution. The report also discusses the market history, size, investment, API threats, and standards.

Vendors participating in this report include Cequence Security (Cequence), FireTail Inc. (FireTail), TeejLab Inc. (TeejLab), and Salt Security Inc. (Salt Security). The key findings from this report follow:

- **API sprawl is shockingly pervasive:** Today, organizations use an average of 20,000 APIs. A lack of API management and oversight leads to many APIs being promoted to production with known security issues. API sprawl's target-rich attack surface motivates hackers to develop an increasing number of zero-day API attacks.
- **Compromised APIs have led to over one billion compromised records:** The exploitation of APIs is growing in frequency and sophistication, accounting for many compromised records. Zero-day attacks have led to single-event compromises of hundreds of millions of records.
- **Modest market size, despite healthy compound annual growth rate (CAGR) growth:** The API security solution market size is projected to reach US$289 million in 2023. The market is estimated to grow at 24% CAGR, reaching nearly US$700 million in 2027.
- **Managed API security solutions grow in popularity:** Customers and prospects show a preference for solutions where the provider assumes the bulk of API protection. Many organizations lack API security expertise and access to API threat intelligence. Customers must recognize they still own the risk.
- **Solutions are pricey but offer substantial value:** API security solutions are a six-figure decision for most organizations. Entry-level pricing can begin below US$100,000, but the ARR can quickly grow based on use and adoption by other organizational programming groups.

© 2023 Datos Insights or its affiliates. All rights reserved.

Introduction

To understand API security is first to understand APIs. In its most basic form, an API is a software interface that connects two or more applications. The benefit of the API extends past connectivity; APIs perform functions or exchanges of information without human intervention. They standardize how organizations extract and share data without writing hundreds of competing application interfaces.

Today, the average number of APIs organizations use is in the range of 15,564 to 25,592.[1] It has been reported that there could be 1.7 billion APIs in use by 2030, making APIs one of the largest known software components of an enterprise attack surface.[2]

Imagine not knowing what functions many of those APIs perform, how many versions exist, or that they even exist. On the one hand, APIs give application development teams great power, but on the other, they introduce potentially significant vulnerabilities. Hackers increasingly target APIs as the gateway to an organization's sensitive information. The growing threat introduced by such widespread API use is one of the reasons Datos Insights made API security its **number two top ten cybersecurity trend of 2023**.[3]

This Impact Report serves as a primer for CISOs on API security. It provides API vendors with a view of the market not previously disclosed by cybersecurity market research and advisory firms.

This report is part three of a four-part series on API security. Part one was an aerial view of the API security product landscape; part two was an in-depth analysis of several WAAP products and the market landscape. Part four will provide insight and analysis into customer sentiment gathered during the product reference checking portion of the Datos Insights Vendor Evaluation.

---

1 Dan Kennedy, 451 Research, "The 2022 API Security Trends Report," Noname Security, April 2022, accessed February 21, 2023, https://nonamesecurity.com/resources/api-security-trends-report/.

2 Rajesh Narayanan, Mike Wiley, "Continuous API Sprawl," F5, November 2, 2021, accessed February 23, 2023, https://www.f5.com/pdf/reports/f5-office-of-the-cto-report-continuous-api-sprawl.pdf.

3 See Datos Insights' report Top 10 Trends in Cybersecurity, 2023: A Sea of Change for the Industry, January 2023.

© 2023 Datos Insights or its affiliates. All rights reserved.

Methodology

This Datos Insights Vendor Evaluation examines the state of API security solutions through various stages of overall product and vendor maturity. Secondary research for this report was first conducted to identify API security solutions that, by design, provide API lifecycle protection. This aspect of research yielded 17 solutions that when analyzed, provided a broader understanding of the market, solution providers, and projected growth.

Desk research of white papers, API security standards, and industry publications was analyzed to understand the market definition, growth, challenges, and present state. Primary research involved interviewing API security vendors, receiving demonstrations to validate product claims, and interviewing solution customers.

Four vendors, Cequence , FireTail, Neosec, and Salt Security, provided technical assistance in validating the Datos Insights Vendor Evaluation scoring criterion to ensure the evaluation criteria were relevant. Neosec opted not to participate in the report after its acquisition by Akamai.

Inclusion in the report required API security solutions to provide lifecycle API security and have commercial availability for at least one year. Open-source solutions were excluded. Eleven vendors met this criterion and were invited to participate in the Datos Insights Vendor Evaluation. Seven vendors agreed to participate; however, three dropped out, one by acquisition and two for time constraints and lack of available references. The research performed for this report occurred from February through June 2023.

The four API security vendors representing startups to scaleups completed a comprehensive 200-point company, customer, and product questionnaire, provided a product demo, and submitted customer references. That said, given the size and structure of the research data, the information presented within this report is considered a directional indication of the state of API security products.

© 2023 Datos Insights or its affiliates. All rights reserved.

Brief History of API Security

The first API vulnerabilities were logged in Common Vulnerability Enumeration (CVE) when Salesforce introduced the first commercial API in 2000. API security was predominately addressed through existing application security testing tools in the late 1990s. However, in 1999, a new class of software called WAF emerged, providing some but limited protection for APIs. By 2003, the WAF market was well on its way to becoming the US$1.4 billion (about $4 per person in the US) market it is today.[4] In 2010, API gateways appeared, providing API security functionality, but were limited in scope.

An increasing number of API exploits and attacks would drive the development of new products focused on protecting APIs. The API security product market as we know it today emerged from 2013 to 2014 when vendors such as Cequence, Curity, ThreatX, and Wallarm launched standalone products designed specifically to secure APIs. Over the next eight years, dozens of products claiming to secure APIs flooded the market. Now, the market is crowded with over 80 direct and adjacent vendors vying for a share of the CISO's wallet in securing APIs.

[4] Ricky, "Web Application Firewall (WAF) Market CAGR of 19.2% 2021," Firewall Authority, December 26, 2021, accessed February 22, 2023, https://firewallauthority.com/web-application-firewall-market-cagr-of-2021/.

© 2023 Datos Insights or its affiliates. All rights reserved.

The Market

Table A is a high-level presentation of market trends and implications.

Table A: The Market

Market trends	Market implications
API vulnerabilities largely unaddressed by organizations	• A growing number of significant security breaches owing to poor API visibility and security occur and will continue for the foreseeable future. • The race toward digitizing organizations will put more rushed and poorly designed APIs into production. • Many organizations will attempt to solve API vulnerabilities through better design and coding, only to realize the same security failings as applications in general.
Technology trends reshaping the API security solution market	• Increasing recognition of API protection limitations in WAFs is moving people toward standalone API Security and WAAP solutions. • Application refactoring changes application security requirements, introducing new threat vectors. • The growth of microservices increases the complexity of API discovery.
Macro market trends shaping how API security solutions are marketed and acquired	• API security awareness in 2021 and 2022 is giving way to budgeted API security projects in 2023 and 2024. • High-profile API security breaches create a land rush toward API solutions where solution awareness wins over solution efficacy. • The financial market's uncertainty is forcing firms to deprioritize legacy security projects in favor of API security solutions.

© 2023 Datos Insights or its affiliates. All rights reserved.

Market trends	Market implications
Customers pushing the envelope in desire for advanced API security functionality	• Integration with cloud-native application protection platforms and cloud workload protection platforms to detect and remediate detected API security issues. • Security information, event management (SIEM), and security orchestration automation and response (SOAR) product integration to detect and respond to API security incidents. • Evolution to API security posture management.
Crowded API security vendor market	• A cybersecurity market segment with over 80 entrants is unsustainable by any measure. Customers will face an onslaught of confusing product messaging and claims by vendors looking to stand out from the crowd. • Smaller vendors will be forced to burn investment funding on marketing versus development to be noticed in the market. • Larger vendors will acquire smaller vendors with unique API security approaches to broaden legacy solutions' appeal.

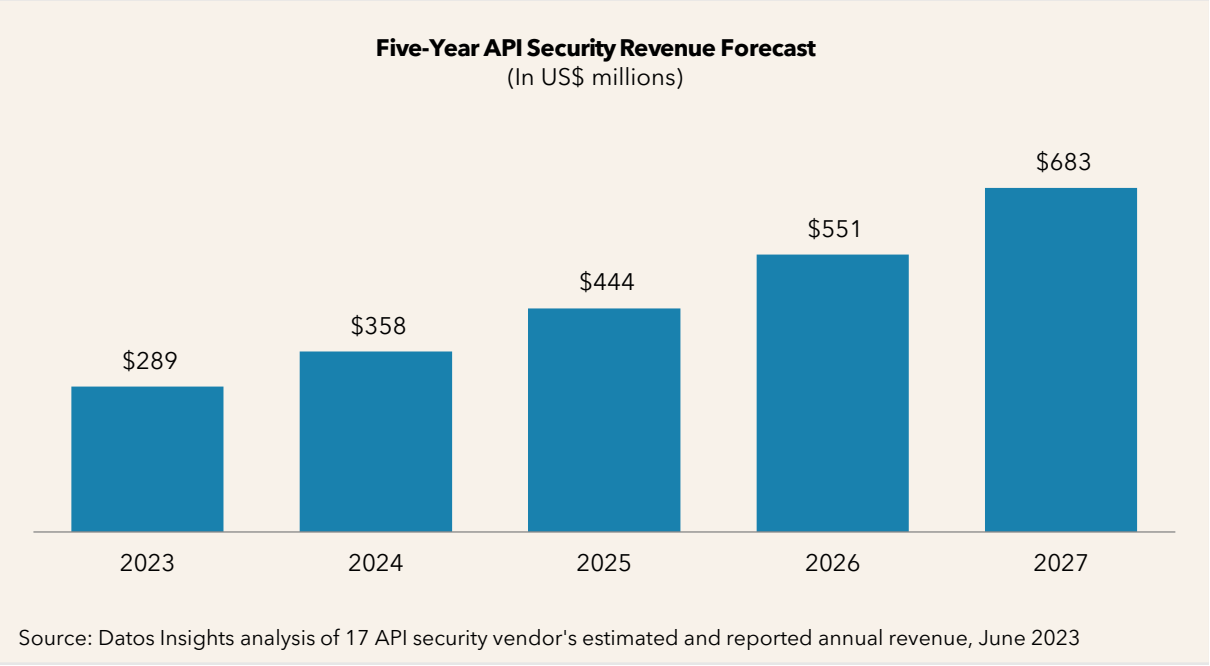
Source: Datos Insights

Market Size

Datos Insights estimates the 17 known API standalone security solution vendors will generate US$289 million in 2023. The market will reach nearly US$700 million in 2027, growing at a CAGR of 24%. The five-year period of 2023 to 2027 total sales will cumulatively reach US$2.3 billion. Figure 1 presents the API security solution market's projected growth from 2023 through 2027.

© 2023 Datos Insights or its affiliates. All rights reserved.

Figure 1: Five-Year API Security Solution Market Forecast



Source: Datos Insights analysis of 17 API security vendor's estimated and reported annual revenue, June 2023

Datos Insights arrived at this market estimate by analyzing the actual and estimated annual revenue of 17 vendors offering singular API security solutions. Additionally, a proprietary formula for estimating revenue per employee for security software vendors was used to cross-check the revenue forecast.

VC Investment

The VC community has invested US$1.44 billion in 15 API security solution vendors. The average amount invested in each company is US$96.3 million, the smallest investment was US$125,000, and the largest was US$632 million. Datos Insights sees a slowing of new VC investments for startup API security solutions. Still, investments for market consolidation and later-stage growth will lead.

Table B presents the 15 VC investments in the API security solution market.

© 2023 Datos Insights or its affiliates. All rights reserved.

Table B: API Security Solution VC Investments

Company	Investment (in US$ Millions)	Current Status
42Crunch	US$20.6	The company remains private after its US$17 million Series A round led by Energy Impact Partners. 42Crunch partnered with Cisco to collaborate on an open-source API discovery and security tool, APIClarity.
Akto.io	US$4.5	The company remains a small independent software company focused on developing its open-source continuous integration and continuous deployment (CI/CD) API security solution accessing its Seed round funding led by Accel.
Cequence	US$101.5	The company has become one of the market's most respected API security vendors. In April 2023, it had a venture raise round by the HP Pathfinder venture fund and Propersity7 Ventures.
Fire[illegible]		The private company uses its early-stage funding from Paladin Capital to rapidly elevate its products and expand its customer base in North America.
Gho Secu		The company emerged from stealth in August 2022 with a Seed round from 468 Capital, DNX Ventures, and Munich Re Ventures.
Gravitee.io	US$41	This French private company has grown to over 150 customers; its 2022 Series B round of US$30 million was used to grow the company to the ninth fastest-growing open-source startup.
Impart Security Inc.	US$7.7	With origins as a WAF vendor, the private real-time API security company is leveraging its US$6 million Seed round funding from CRV to evolve its original WAF product to a complete API security solution.
Metlo	US$0.125	The private bootstrapped company is focused on developing an open-source API security solution. The company received minimal Pre-Seed funding from Y Combinator, a startup accelerator.
Neosec	US$20.7	The company was acquired by Akamai Technologies in April 2023, including its 40 employees, to complement its application and API security portfolio.

© 2023 Datos Insights or its affiliates. All rights reserved.

Company	Investment (in US$ Millions)	Current Status
Noname Security	US$220	The company rapidly achieved unicorn status with only US$5 million in revenue in December 2021. Prestigious VC investors Georgian, Insight Partners, and Lightspeed Venture Partners back the company. In 2023, the company partnered with Wiz, a cloud security platform.
Orca Security	US$632	This private company entered the API security solution market in October 2022. Its principal business remains cloud security.
Salt Security	US$271	This unicorn company has successfully raised eight venture rounds to expand product functionality and global expansion to become a leading API security vendor.
Traceable AI	US$80	The company remains private after its Series B round of US$60 million in May 2022, led by IVP. In June 2023, the company introduced the first API security reference architecture for zero-trust.
Wallarm	US$10.8	Since its Series A funding in October 2018, this private company has been able to fund growth and operations through product ARR.
Wib Security	US$16	This Israel API security company secured its Seed round in November 2022 to expand its position as a holistic API security solution. In February 2023, the company launched API Pen-Testing-as-a-Service.

Source: Datos Insights analysis of public disclosures.

© 2023 Datos Insights or its affiliates. All rights reserved.

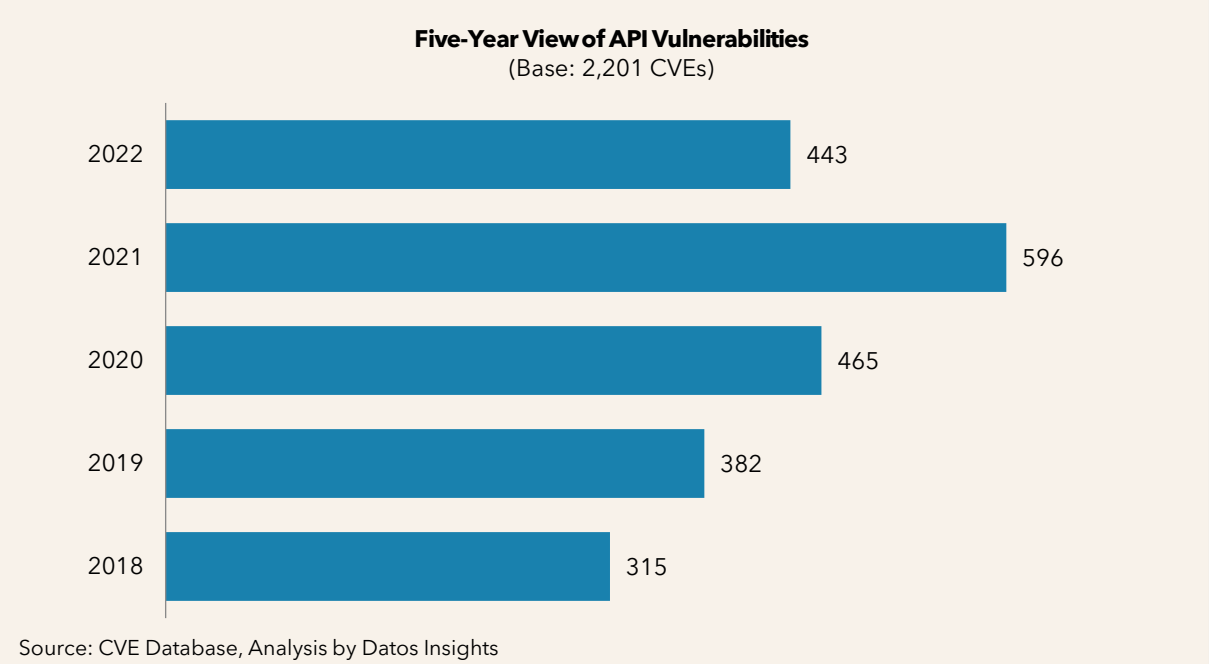
API Vulnerabilities, Threats, and Breaches

APIs are essential for software development and integration to fuel the digital economy. Unfortunately, they pose significant security risks. APIs expose application logic and sensitive data to external parties, creating a large attack surface for malicious actors.

API Security Vulnerabilities

When famous bank robber Willie Sutton was asked why he robbed banks, he quipped, "Because that is where the money is." This quip became known as "Sutton's Law" and is apropos when applied to hackers compromising APIs to access sensitive information. Why? Because APIs provide the keys to the kingdom. Hackers are continually looking for ways to exploit API vulnerabilities, of which there is no shortage. Since 1999, there have been over 3,600 vulnerabilities involving APIs. 2023 is shaping to be a banner year in API vulnerabilities, with 342 API CVEs reported through April 2023. Figure 2 shows the growth of API vulnerabilities over the past five years, according to the CVE database.[5]

Figure 2: Five-Year View of API Vulnerabilities



Source: CVE Database, Analysis by Datos Insights

[5] "CVE List Downloads," CVE, accessed November 16, 2022, https://www.cve.org/downloads.

© 2023 Datos Insights or its affiliates. All rights reserved.

OWASP Top 10 API Vulnerabilities

In 2019, Open Web Application Security Project (OWASP) released the first top 10 list of API vulnerabilities; since then, hacker approaches have evolved, as evidenced by the six changes in the top 10. OWASP released the 2023 top 10 API security risks. According to a threat research report issued by Cequence, the definition of API6 states API security that isn't functioning properly ends up with attack automation being utilized against it.[6] Table C provides a summary of the original and changed top OWASP API threats.

Table C: Top 10 OWASP API Vulnerabilities

2019 Top 10	2023 Top 10 Release Candidate	Primary Concern
API1:2019 Broken Object Level Authorization	Broken Object Level Authorization	Attackers can exploit API endpoints vulnerable to broken object-level authorization by manipulating the ID of an object sent within the request.
API2:2019 Broken User Authentication	**Change:** Broken Authentication	API authentication is complex and often confusing. Misconceptions about API boundaries of authentication and how to implement it correctly often occur.
PI3:2019 Excessive Data Exposure	**Change:** Broken Object Property Level Authorization	Attackers can exploit API endpoints vulnerable to broken object property level authorization by reading or changing values of object properties they are not supposed to access.
API4:2019 Lack of Resources & Rate Limiting	**Change:** Unrestricted Resource Consumption	Lack of monitoring and improper monitoring can allow malicious activity to pass unnoticed.

[6] API Protection Report, March 2023, Cequence Security, Accessed on July 19, 2023, https://pages.cequence.ai/rs/490-RQF-960/images/CQ-APIProtectionReport-H1-2022-vF.pdf

© 2023 Datos Insights or its affiliates. All rights reserved.

2019 Top 10	2023 Top 10 Release Candidate	Primary Concern
API5:2019 Broken Function Level Authorization	Broken Function Level Authorization	Attackers could send legitimate API calls to the API endpoint. Endpoints might be exposed to anonymous users or regular, non-privileged users.
API6:2019 Mass Assignment	**Change:** Server-Side Request Forgery	Server-Side Request Forgery flaws occur when an API fetches a remote resource without validating the user-supplied URL. Attackers can coerce the application to send a request to an unexpected destination, even when protected by a firewall or a virtual private network.
API7:2019 Security Misconfiguration	Security Misconfiguration	Missing security hardening across the API stack, improperly configured permissions on cloud services, missing security patches, and out-of-date systems.
API8:2019 Injection	**Change:** Lack of Protection from Automated Threats	Attackers operating botnets (for scalping) can bypass rate limiting accessing APIs from thousands of IP addresses worldwide in seconds.
API9:2019 Improper Assets Management	Improper Assets Management	Threat agents can get unauthorized access through old API versions or endpoints left running unpatched and using weaker security requirements.
API10:2019 Insufficient Logging & Monitoring	**Change:** Unsafe Consumption of APIs	Developers tend to trust but not verify endpoints that interact with external or third-party APIs.

Source: OWASP with analysis from Datos Insights

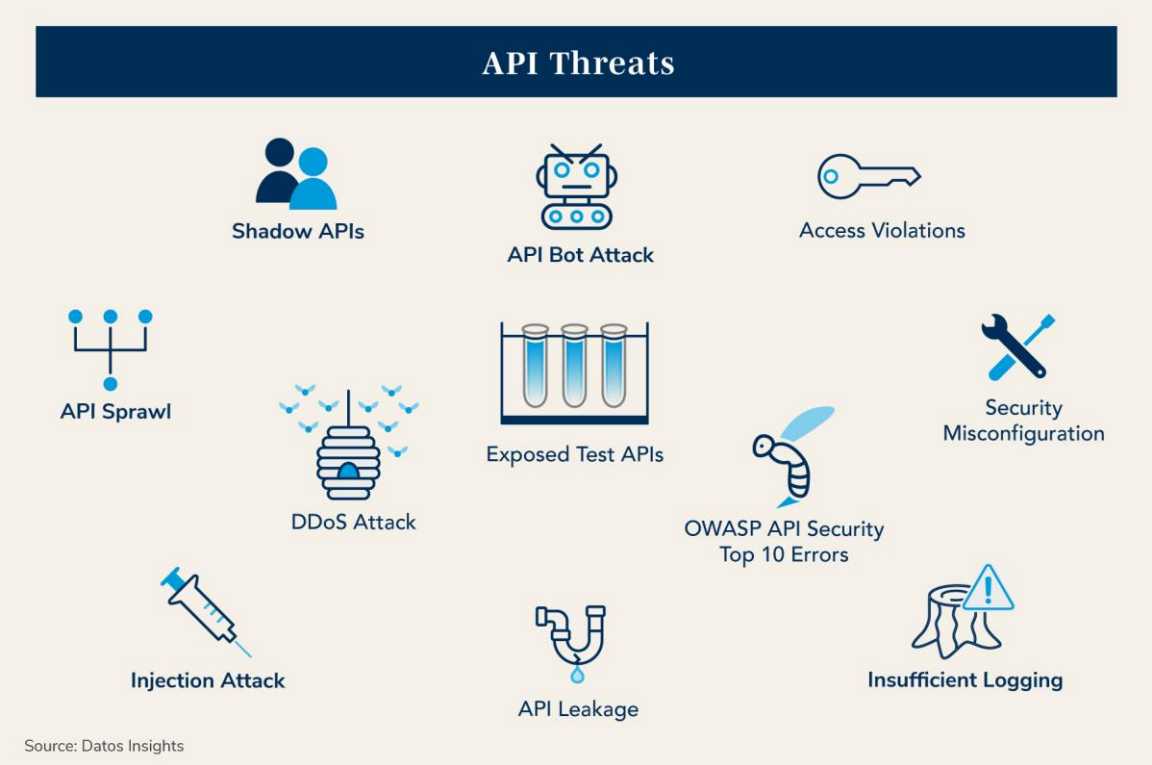
© 2023 Datos Insights or its affiliates. All rights reserved.

API Threats

API security is directly related to application security; subsequently, APIs have many of the same frailties of compromise as applications. APIs are critical because they transfer data between clients and servers connected over public networks. There are many points of potential weakness in that process requiring security safeguards. Dozens of threats exist that hackers can leverage to compromise APIs.

Figure 3 presents the most common API threats.

Figure 3: API Threats



© 2023 Datos Insights or its affiliates. All rights reserved.

API Security Breaches

Table D shows the largest API security breaches since 2021, where over 900 million customer records were compromised.

Table D: Largest API Security Breaches

Company	Industry	Announced	Records Breached	Summary
Twitter	Social media	January 6, 2023	235 million	Zero-day API vulnerability
Optus	Telecomm	September 23, 2022	10 million	Customer data, including addresses, driver's licenses, and passports, through exploited database API
Texas Department of Insurance	Insurance	March 20, 2022	1.8 million	Web service application that allowed access to protected data
LinkedIn	Technology	June 2021	700 million	Data scraping techniques applied by exploiting the site's APIs to collect user information
Peloton	Recreation	May 5, 2021	3 million	A hacker compromised a leaky API after company ignored a vulnerability disclosure from a pen-testing company

Source: Datos Insights analysis of public disclosures.

© 2023 Datos Insights or its affiliates. All rights reserved.

Participants

Four API security solution vendors agreed to participate, made the cut and provided satisfactory reference customers in the Datos Insights Vendor Evaluation. Cequence and Salt Security are entrenched in the API security solution market, whereas FireTail and TeejLab are relative market newcomers. Table E presents high-level information for each participant.

Table E: Firmographics

Criterion	Cequence	FireTail	Salt Security	TeejLab
Growth stage	Scaleup	Startup	Scaleup	Startup
Product	Cequence Unified API Protection	FireTail Platform	Salt Security API Protection Platform	API Discovery and Risk Management
Project category	API life cycle security	API security posture management	API life cycle security	API security posture management
Headquarters	Sunnyvale, California	McLean, Virginia	Palo Alto, California	Vancouver, British Columbia
Founded	2015	2022	2016	2020
Employees	160	12	204	10
Funding (in US$M)	US$101.5	US$5	US$271	Bootstrapped
Product release date	2015	2022	2018	2021
Customers	120	Four	108	Six
Average solution cost	US$100,000 to US$400,000	US$100,000	US$100,000 to US$499,000	Under US$100,000
Revenue	US$40 million to US$75 million (estimate)	Less than US$5 million	US$10 to US$24.9 (est. millions)	Less than US$5 million

Source: API security solution RFI response

© 2023 Datos Insights or its affiliates. All rights reserved.

Datos Insights Vendor Evaluation

Vendors participating in a Datos Insights Vendor Evaluation must complete a 200-point request for information (RFI) covering company, product, and customer dimensions. This section breaks down the individual Datos Insights Vendor Evaluation components, drawing out each area's strongest API security vendors and how they are differentiated in the market.

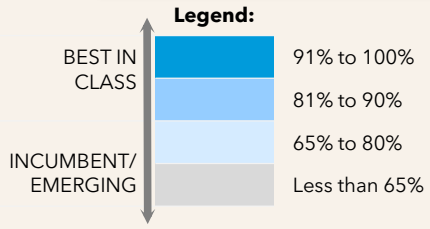
Organizations must carefully consider their needs, risks, and tolerances and map vendor functionality to identify the most appropriate candidates. After the initial paring down, organizations should conduct proofs of concept to measure performance and support and select the right API security solution.

The Datos Insights Vendor Evaluation Components

Figure 4 provides an overview of how each vendor scored in the various areas of importance.

Figure 4: Datos Insights Vendor Evaluation Heat Map

Vendors	Vendor stability	Client strength	Client service	Product features
Cequence	97%	94%	98%	97%
FireTail	83%	81%	77%	63%
Salt Security	89%	94%	91%	95%
TeejLab	81%	90%	79%	81%



Source: Datos Insights

© 2023 Datos Insights or its affiliates. All rights reserved.

Each vendor is rated, in part, based on its data provided when responding to the RFI distributed by Datos Insights and on product demos and follow-up discussions as part of the Datos Insights Vendor Evaluation. Ratings are also driven by the references provided by the customers of the examined vendors, along with analyst knowledge of the API security solution space, to support a multidimensional rating.

Vendor Stability

The vendor stability component evaluates the overall strength of the vendors in terms of financial stability, management reputation, risk management, and global presence. This component determines whether a given vendor has the foundation to compete and sustain its market presence.

In the context of the participating vendors, the vendor stability portion of the Datos Insights Vendor Evaluation is primarily driven by demonstrating market staying power, consistently growing top-line revenue, and aggressively investing in research and development. Participants are relatively small and operating in a startup, pre-revenue mode. Any one of the participants could be acquired by a larger cybersecurity company looking to bolster its API security portfolio. Funding and burn rate should be considered when purchasing private API security solution providers.

Client Strength

The client strength component focuses on the number and diversity of the vendor's customers, the vendor's reputation among the clients, and overall customer turnover. This component measures whether a given vendor has a strong foundation of clients and a robust client pipeline to sustain its growth trajectory.

Sustained growth requires the ability to maintain existing customers and attract new ones. This category evaluates provider strength based on important factors, such as the total number of clients in production, the diversity of those clients, client retention rate, reference checks on the vendor's reputation in the market, and customer feedback regarding their likelihood to replace their solution.

API security solution providers have effectively retained customers. However, further penetrating a highly competitive market can be challenging. Clients are continually looking for solutions with greater efficacy.

© 2023 Datos Insights or its affiliates. All rights reserved.

Client Service

The client services component evaluates the pricing structure, its various attributes, and the comprehensive nature of the vendor's client support and service infrastructure. This component measures whether the vendor provides full service and support to provide real value to the clients.

Strong client service has become necessary to achieve customer satisfaction. It demonstrates a vendor's commitment to ensuring its customers receive the highest standard of products and services. Cybersecurity executives often expect vendors to become strategic partners, collaborating and guiding them on near-term and long-term technology adoption. Customers continue seeking greater visibility and enhanced documentation on product changes and future development. Customers expect quick resolution of defects and issues and continual design, usability, functionality, and performance advancements.

Client ratings of the vendors' service and support, responsiveness, ability to deliver on promises, and cost-to-value ratios were the primary drivers of the ratings in this category. Additional drivers include the vendor's position on key support items, such as providing 24/7 support, having a dedicated point of contact, facilitating customer advisory boards, and offering global/localized support.

Product Features

The product features component analyzes the key features and functionality of vendor solutions and services, including implementation options, user experience, and the strength of the future product roadmap. This component measures whether the vendor offers enough key features and functionality to remain competitive.

Protecting APIs cannot be accomplished piecemeal; a holistic approach is required to protect them throughout their life cycle. Products demonstrating alignment with Datos Insights' 100-point evaluation criteria scored the highest. Customers do not want partial solutions; they desire security testing, discovery, monitoring, and vulnerability detection and remediation in a single platform.

A comprehensive and easy-to-use dashboard with the ability to customize metrics and reports to have confidence in their ability to manage and secure their APIs effectively is required. Many clients also want ready access to all underlying data and the ability to integrate it with other proprietary systems, including SIEM, SOAR, and threat-hunting platforms, for a fuller analysis of their cybersecurity threats.

© 2023 Datos Insights or its affiliates. All rights reserved.

Quality, performance, and service outweigh cost and pricing considerations for most organizations, but the total cost cannot be ignored. Some providers deliver simpler solutions requiring little active management and focus on organizations that want API security that mostly works out-of-the-box with little custom configuration.

The score also considered ease of deployment, integration, reporting, and the provider's ability to understand new threats and quickly deliver detection and mitigation techniques to counter those new API threats.

Datos Insights Vendor Evaluation

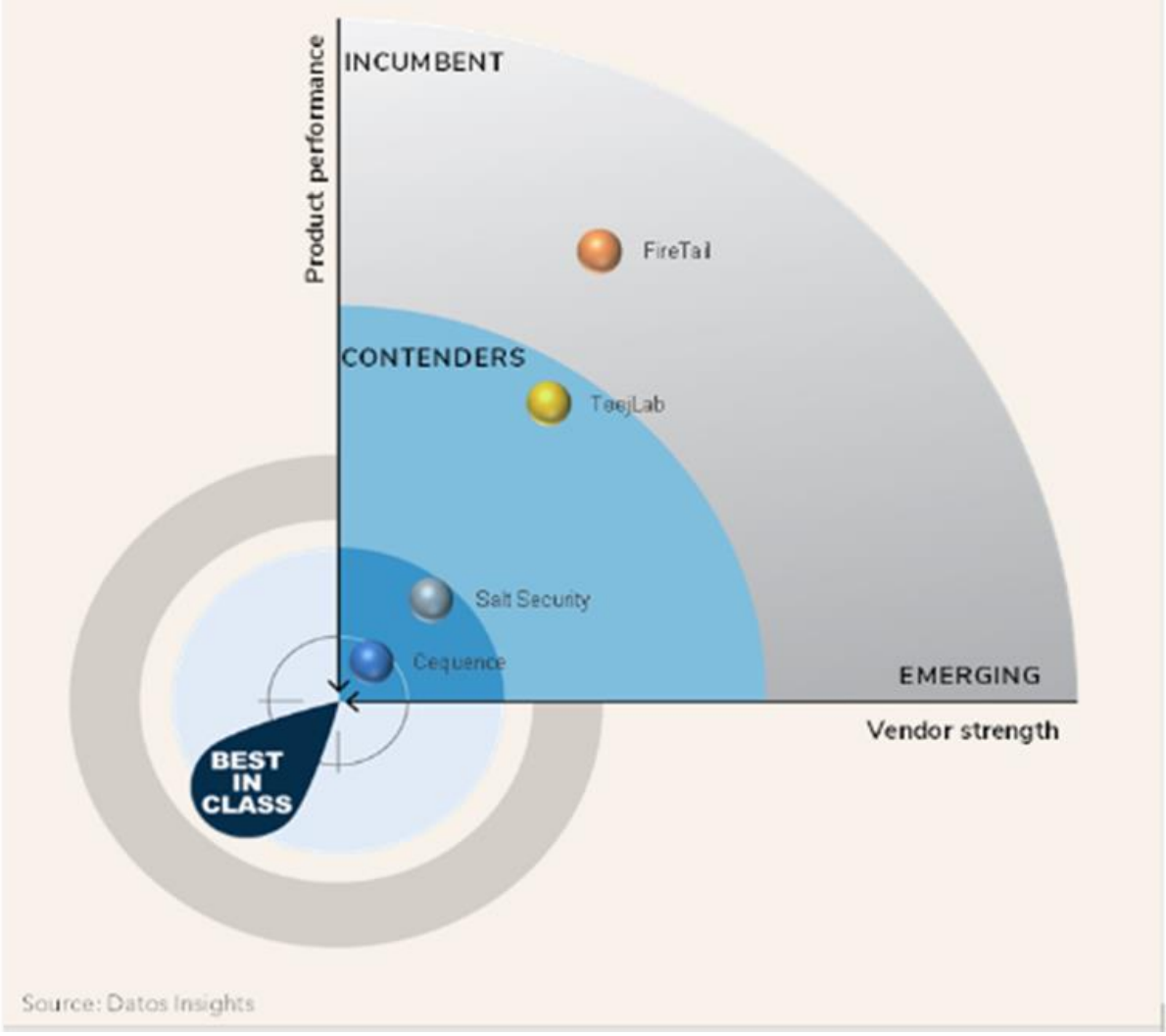
Four major factors drive the results of Datos Insights Vendor Evaluation:

1. Completeness of the response to Datos Insights' RFI.
2. Submission of customer references to be interviewed by Datos Insights.
3. Product demos provided by participating vendors.
4. Datos Insights' knowledge of the API security market and key players.

Figure 5 represents the final Datos Insights Vendor Evaluation, highlighting the market position of the participating API Security standalone solution vendors.

© 2023 Datos Insights or its affiliates. All rights reserved.

Figure 5: Datos Insights Vendor Evaluation of Standalone API Security Solutions



Best-in-Class Vendor

Vendors in this grouping represent the leaders by demonstrating strong financials, diverse client bases, and robust product offerings with industry-leading functionality and reliable client service. These are essentially the leading vendors that everyone else is chasing.

Cequence and Salt Security achieved best-in-class in the 2023 Datos Insights Vendor Evaluation. Both API security solutions scored solidly across all four categories. Cequence (96.3%) edged out Salt Security (92.4%), mainly in the vendor stability category.

© 2023 Datos Insights or its affiliates. All rights reserved.

Contender Vendor

Contenders have created stable businesses, client bases, and competitive product offerings. But they sometimes struggle to identify the next big market trend or product features or lack consistent R&D or IT investment, leading to a failure to update overall performance and infrastructure. Contenders' overall competitive positions will vary a bit, from vendors that are having a tough time keeping up with the best-in-class vendors—due to a lack of resources or stable but outdated technology stacks—to vendors that are just inches away from joining the best-in-class grouping if only they could properly execute on the next release or successfully capture a new client segment.

TeejLab scored 82.5% across the four evaluation categories, teetering on the emerging and contender curve. This newcomer is likely to hover in its present position owing to its unique approach to API security and customer base that desires to monetize APIs.

Emerging and Incumbent Vendors

This last grouping represents vendors with a large potential for future growth or established vendors with stagnating offerings. This group may represent startups or vendors with limited resources. They may exhibit unstable business models, low client count, and limited client service capabilities. However, this group of vendors may also support innovative product features and transformative business models to help them home in on the Datos Insights Vendor Evaluation.

Emerging Vendor

FireTail scored 76% across the four evaluation categories, positioning it as an emerging solution. The vendor shows promise in its early stage of product development but will need to make substantive improvements in solution functionality across all API security capabilities to move from its present position.

Incumbent Vendor

No vendors are presented as market incumbents or legacy providers.

© 2023 Datos Insights or its affiliates. All rights reserved.

API Security Solution Comparison

Datos Insights evaluated API security solutions by 100 product-specific criteria to provide solution buyers with a roadmap of key capabilities to make informed purchasing decisions. Buyers must determine the most important capabilities and deployment approaches to address their specific API protection requirements.

The following tables are designed to call out capabilities buyers typically find important on their solution evaluation journey.

Implementation Model

An organization's IT architecture, network design, and technology standards typically drive how cybersecurity solutions are implemented. API security solutions offer many options when it comes to implementation ranging from on-premise deployment to a fully managed service that would accommodate most implementation requirements.

Table F compares the implementation models of the profiled API security solutions.

Table F: Implementation Model

Capability	Cequence	FireTail	Salt Security	TeejLab
On-premises	■	□	■	■
Inline	■	■	■	■
Managed service	■	■	□	■
Public cloud hosting, e.g., AWS, Azure	■	■	■	■
Software-as-a-Service (SaaS)	■	■	■	■
CDN integration	■	□	■	■
Out-of-band	■	□	■	■
Agentless	■	■	■	□
No code changes	■	□	■	■

© 2023 Datos Insights or its affiliates. All rights reserved.

Capability	Cequence	FireTail	Salt Security	TeejLab
Integrates with SIEM and SOAR solutions	■	■	■	■

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, ☐ = No

API Discovery Capabilities

API discovery is one of the top solution capabilities that should be considered when acquiring an API security solution. The visibility of API traffic is equivalent to successful solution deployments. Table G compares the discovery capabilities of the profiled API security solutions.

Table G: API Discovery Capabilities

Capability	Cequence	FireTail	Salt Security	TeejLab
API discovery via integrations	■	■	■	■
API discovery via traffic monitoring	■	■	■	■
Identify sensitive data types in API, e.g., parameters and payloads	■	■	■	■
Map APIs to endpoints	■	■	■	■
Map APIs to servers	■	☐	■	■
Map APIs to cloud resources	■	■	■	◪
Discover deprecated APIs	■	■	■	■
Discover out-of-date APIs	■	☐	■	■
Discover shadow APIs	■	■	■	■
Tag third-party API consumption	■	☐	■	■

© 2023 Datos Insights or its affiliates. All rights reserved.

Capability	Cequence	FireTail	Salt Security	TeejLab
API Discovery via probe or crawl	■	□	◪	■
API Discovery via source code analysis	■	■	□	■
Discovers HTTP, RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC APIs	■	■	■	■
Discover URL-encoded APIs	■	■	■	■
Discover URL SOAP APIs	■	□	■	■
Discover URL REST APIs	■	■	■	■
Discover URL GraphQL APIs	■	■	■	■
Discover XML APIs	■	□	■	■
API endpoint structure discovery	■	■	■	■
Discover public-facing APIs and associated resources, e.g., cloud services, hygiene state	■	■	■	■
API usage by IP addresses, geo-locations, and organizations	■	■	■	■
Identify API risks based on encryption, authentication, conformance with specifications, production vs. nonproduction, third-party, etc.	■	■	■	■
Risk assessment and categorization	■	□	■	■
Predefined and custom risk assessment rules	■	□	■	■

© 2023 Datos Insights or its affiliates. All rights reserved.

Capability	Cequence	FireTail	Salt Security	TeejLab
Identify APIs with and without OpenAPI Specification (OAS)	■	■	■	■
Automatic generation of OAS for discovered APIs (with or without OAS)	■	☐	■	■

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, ☐ = No

API Security Policies

Providing the capability to set API security policies at the individual or group API level is essential to triggering alerts and enforcing response actions. Table H compares the profiled API security solutions' policy creation and enforcement capabilities.

Table H: API Security Policies

Capability	Cequence	FireTail	Salt Security	TeejLab
Enforce security policy at runtime	■	■	■	◪
Create customer policies by asset groups	■	■	■	☐
Create predefined/customizable security policies	■	■	■	☐
Create security policies based on malicious infrastructure, credentials, and attack behaviors	■	☐	■	☐
Confidence-based policy detection	■	☐	■	☐
Automatic policy modification based on results/changes in behavior	■	☐	■	◪

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, ☐ = No

© 2023 Datos Insights or its affiliates. All rights reserved.

Access Control

The most basic security control organizations require to protect APIs is to control who can gain access to APIs. Table I compares the profiled API security solutions' access control and authentication capabilities.

Table I: Access Control

Capability	Cequence	FireTail	Salt Security	TeejLab
Role-based access control	■	■	■	■
Authentication service	■	□	■	■
Customizable tokens	■	□	■	■

Source: API security solution RFI response

Legend: ■ = Yes, □ = No

API Inventory and Attack Surface

Organizations cannot effectively provide API security until APIs exist in a centralized directory. Once inventoried, an attack surface can be mapped. Table J compares the inventory capabilities of the profiled API security solutions.

Table J: API Inventory and Attack Surface

Capability	Cequence	FireTail	Salt Security	TeejLab
Create API inventory	■	■	■	■
Map API attack surface	■	□	■	■
Tag third-party API consumption	■	□	■	■
Categorize inventory based on assigned risks	■	□	■	◪
Track APIs based on individual APIs and groups	■	□	■	□

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, □ = No

© 2023 Datos Insights or its affiliates. All rights reserved.

Vulnerability Detection

The minimum baseline for API vulnerability detection is the OWASP API Top 10. It is important to view API security as an integral part of the DevSecOps process; subsequently, CI/CD pipeline integration must also be a requirement. Table K compares the vulnerability detection capabilities of the profiled API security solutions.

Table K: Vulnerability Detection

Capability	Cequence	FireTail	Salt Security	TeejLab
Scan for API vulnerabilities in the integrated development environment (IDE) pipeline	■	☐	■	☐
Scan for API vulnerabilities in CI/CD pipeline	■	☐	■	☐
Scan for OWASP API security top 10 issues	■	■	■	■
API leak detection	■	■	■	■
Continuous runtime behavioral scanning	■	☐	■	■
After the scan remediation report	■	☐	■	■
OAS documentation analysis of API specifications	■	☐	■	☐

Source: API security solution RFI response

Legend: ■ = Yes, ☐ = No

Threat Management

Hackers continually improve their tools, techniques, and processes to compromise APIs. API security solutions providers must be able to stay in front of adversaries to offer protection against current threat campaigns. Table L compares the threat management capabilities of profiles API security solutions.

© 2023 Datos Insights or its affiliates. All rights reserved.

Table L: Threat Management

Capability	Cequence	FireTail	Salt Security	TeejLab
Aggregate and correlate API traffic and associate with attacker campaigns	■	□	■	◪
Detect subtle variations in normal consumption patterns	■	□	■	■
Threat intelligence-sharing service	■	□	■	□
Threat-intelligence lab or team	■	□	■	□
Detect and stop attacks based on behavior	■	□	■	◪
Detect and stop attacks based on the confidence score	■	□	■	◪
Detect and Stop attacks based on the infrastructure used	■	□	■	◪
Detect and stop attacks based on malicious tools used	■	□	■	□
Detect and stop attacks based on stolen credentials	■	□	■	■
Response options: block, log, rate limit, geo fence, deception	■	■	■	□
Natively stops attacks	■	■	■	□

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, □ = No

Event Notification

Notification of events is critical to cybersecurity analysts responding to and investigating indicators of compromise or security events of interest. Table M compares the event notification capabilities of the profiled API security solutions.

© 2023 Datos Insights or its affiliates. All rights reserved.

Table M: Event Notification

Capability	Cequence	FireTail	Salt Security	TeejLab
Email notification	■	■	■	■
SMS notification	■	□	◪	□
Intelligent SIEM/SOAR integration	■	□	■	■
Ticketing integration	■	■	■	■
Initiate alerts based on risk metrics	■	■	■	■

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, □ = No

Monitoring

Monitoring API traffic within enterprises ensures zero blind spots. Table N compares the monitoring capabilities of the API security solutions.

Table N: Monitoring

Capability	Cequence	FireTail	Salt Security	TeejLab
Between the client and server (north-south traffic)	■	■	■	■
Between API endpoints (east-west traffic)	■	■	■	■

Source: API security solution RFI response

Legend: ■ = Yes, □ = No

API Security Testing

Discovering and remediating vulnerabilities is sufficient for existing APIs, but comprehensive security testing is necessary for new or revised APIs. Table O compares the API security testing capabilities of the API security solutions.

© 2023 Datos Insights or its affiliates. All rights reserved.

Table O: Testing

Capability	Cequence	FireTail	Salt Security	TeejLab
Use HTTP archive format (HAR) files to generate test cases	■	□	□	□
Collect traffic, analyze, and generate test cases	■	□	■	◪
Create OAS spec, then use it to generate test cases	■	□	■	■
Import existing test cases	■	□	◪	■
Use OAS spec to generate test cases	■	□	■	□
Security test reporting (view, manage tests, compare expected to actual results, compare results for v1, v2, v3, etc.)	■	□	■	■
Collaboration tool integration/initiate remediation tasks	■	□	■	■
Test production APIs for security gaps	■	□	■	■

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, □ = No

Dashboard

User interfaces and dashboards have come a long way; more improvement is needed; however, buyers of API security solutions must find a solution that provides the level of visibility suitable for their needs. Table P compares the dashboard capabilities of profiled API security solutions.

Table P: Dashboard

Capability	Cequence	FireTail	Salt Security	TeejLab
API usage trends	■	■	■	■

© 2023 Datos Insights or its affiliates. All rights reserved.

Capability	Cequence	FireTail	Salt Security	TeejLab
API risk score	■	□	■	■
API threats	■	■	■	◪
Export threat data	■	□	■	■
Threat reporting	■	□	■	■
API risk reporting	■	□	■	■
Executive summary reporting	■	■	■	■
Role-based administration	■	■	■	■
Authentication mechanisms supported	■	■	■	■

Source: API security solution RFI response

Legend: ■ = Yes, ◪ = Partial, □ = No

Auditing

API security begins with the API definition; if the API security constraints (definition) are wrong, its security will be wrong. APIs must be audited against the OAS to validate the definition adheres to user consumption specifications. Table Q compares the auditing capabilities of profiled API security solutions.

Table Q: Auditing

Capability	Cequence	FireTail	Salt Security	TeejLab
Audit API contract	■	■	■	■
Document API contract	■	■	■	■

Source: API security solution RFI response

Legend: ■ = Yes, □ = No

© 2023 Datos Insights or its affiliates. All rights reserved.

Solution Design

Datos Insights has identified six design characteristics solutions must have to scale and adapt to emerging API security requirements. Table R compares the solution design aspects of profiled API security solutions.

Table R: Solution Design

Capability	Cequence	FireTail	Salt Security	TeejLab
Makes use of AI and machine learning (ML)	■	■	■	■
Examines API traffic across an entire enterprise	■	■	■	■
Performs OAS analysis	■	■	■	□
Identify business logic flaws	■	■	■	◪
Identify and block OWASP API Top 10	■	■	■	■
Identify gaps in OAS documentation	■	◪	■	□

Source: API security solution RFI response

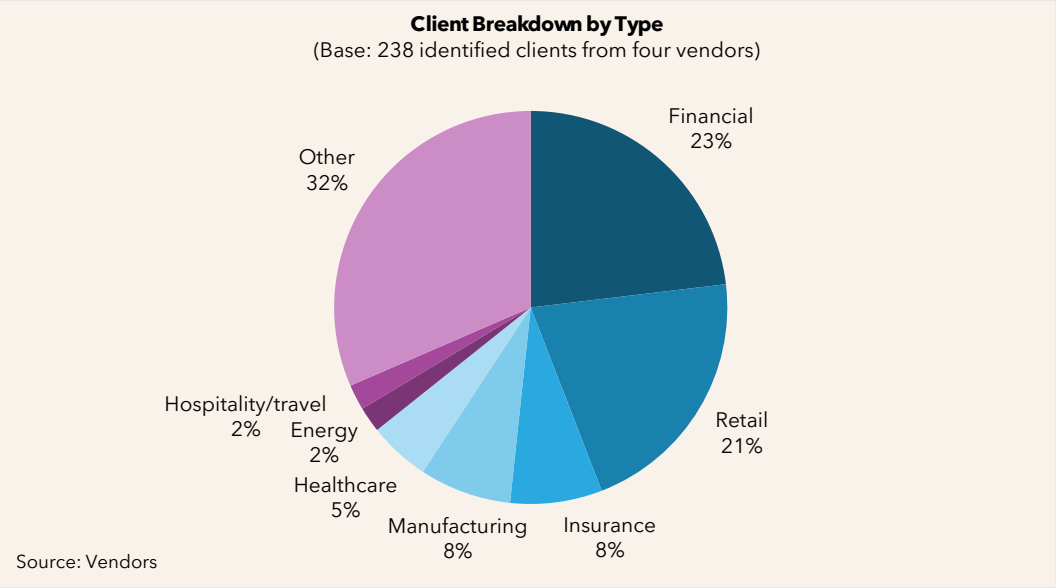
Legend: ■ = Yes, ◪ = Partial, □ = No

Industry Breakdown

Organizations in any industry are consumers of APIs and would benefit from an API security solution. However, some industries, such as financial and retail, are large users of API security solutions. Figure 6 shows the industry breakdown of API security customers for the vendors profiled in this report.

© 2023 Datos Insights or its affiliates. All rights reserved.

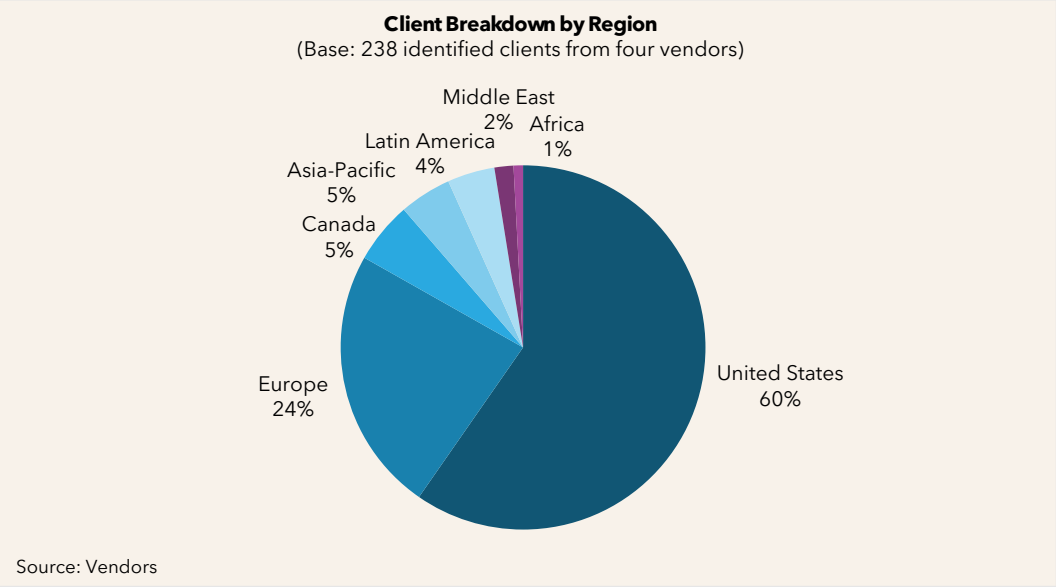
Figure 6: Industry Breakdown



Geographic Breakdown

The U.S. and Europe remain the regions with the most API security solutions installed. Datos Insights believes further global expansion is a product of investment more than need. Investments in global expansion will ensue as vendors receive more funding. Figure 7 shows the geographic breakdown of API security customers for the profiled vendors.

Figure 7: Geographic Breakdown



© 2023 Datos Insights or its affiliates. All rights reserved.

Vendor Profiles

Cequence Security

Cequence Security (Cequence) is a private, California-based software company that provides unified API protection solutions that harness ML-based analysis to defend against sophisticated API attacks. Cequence employs over 150 people across five office locations and has remote workers worldwide. Its latest funding was a December 2021 Series C round, which raised US$60 million, bringing its total investment to over US$100 million. Cequence recently received three strategic inbound investments from the HPE Pathfinder venture fund, Aramco Prosperity7, and KPN Ventures.

Cequence was founded in 2015 by Ameya Talwalkar and Shreyans Mehta, two longtime security veterans of Symantec. The company was founded to solve the growing problem of automated bot attacks increasingly targeting APIs directly. Rather than follow the existing instrumentation with JavaScript and SDK approach, Cequence took an agentless, artificial intelligence (AI)-based approach to find malicious API traffic hiding in plain sight. Cequence's Unified API Protection solution addresses the six phases of the organization's API protection lifecycle: discovery, inventory, compliance, threat detection, prevention, and testing.

Cequence offers three API security solutions:

- **API Sentinel:** Creates an up-to-date API security posture management assessment to understand security risks, obtain compliance, and test for OWASP API Top 10 vulnerabilities in pre- and post-production environments. Assess and remediate sensitive data handling and authentication errors during development.
- **API Spartan:** Prevents automated API attacks and business logic abuse and fraud with unmatched efficacy rates using behavioral fingerprinting that tracks attackers regardless of how rapidly they retool.
- **API Spyder:** Proactively discovers all internal and external APIs that attackers see and categorize based on risk – all without deploying software or traffic flow modifications. Prioritize remediation efforts based on severity.

© 2023 Datos Insights or its affiliates. All rights reserved.

Table S provides basic firm and product information.

Table S: Basic Firm and Product Information, Cequence

Category	Description
Headquarters	Sunnyvale, California
Founded	2015
Revenue	US$40 million to US$75 million (estimate)
Funding	US$101.5 million
Key investors	Dell Technologies Capital, Icon Ventures, Menlo Ventures, and Telcos such as T-Mobile Ventures, KPN Ventures, and Telstra Ventures
R&D percentage	32%
Website	www.cequence.ai
Number of employees	160
Ownership	Private
Key acquisitions	None
Product category	• API Lifecycle Security
Key product name(s)	• Cequence Unified API Protection • Additional products: API Sentinel, API Spartan, API Spyder
Product landing page	https://www.cequence.ai/products/
Product launch date	2015

© 2023 Datos Insights or its affiliates. All rights reserved.

Category	Description
Implementation model	• Hosted (data center) • Hosted (public cloud) • Inline or passive • Integrates with CDNs, gateways, or proxies • Managed service • On-premises • Out-of-band or agentless • SaaS
Number of customers	120
Pricing structure	• Pricing begins at US$10,000; however, the average range is US$100,000 to US$499,000 annually • Multiple enterprise-wide deployments at Fortune 500s with an all-you-can-eat enterprise license agreement costing over US$1 million annually
Annual maintenance	Standard support is included in the price of subscriptions
Product training	• On-site • Remote
Implementation support	• Product self-onboarding • Cequence implementation teams • Third-party deployment partners

Source: Cequence (as of June 20, 2023)

Table T provides detailed product information that will be helpful when making a product selection decision.

Table T: Customer Buying Decision Factors, Cequence

Category	Description
Top five product competitive functions	• Attack surface discovery • API inventory and risk assessment • API security testing • Attack detection • Prevention and native mitigation

© 2023 Datos Insights or its affiliates. All rights reserved.

Category	Description
Top five differentiators	• Protects from every type of attack on the OWASP API Security Top 10, OWASP Web Application Security Top 10, and OWASP Automated Threat list • Enterprise scale across SaaS, on-premises, and hybrid • Automated protection services backed by API security experts • No agents, JavaScript, or SDK, enabling streamlined deployment • Native protection that detects and blocks attacks with unmatched efficacy
Roadmap initiatives (Next 12 to 18 months)	• Productizing various API security testing use cases and integration with discovery, inventory, and threat protection workflows • Advanced notification workflows, allowing customers to define custom workflows when the platform detects API risks or threats • Executive summary reporting and dashboard user interfaces, highlighting the business value of API Protection to the organization
Top three reasons the product is chosen over competitors	• Proven enterprise-scale deployments and customer references in all deployment forms—SaaS, on-premises, and hybrid • Rapid application onboarding without instrumenting the client side (JavaScript, SDK, etc.) or the server side (app plugins, etc.) • Native protection that detects and blocks attacks without needing to rely on an external WAF to block bad IP addresses

Source: Cequence (as of June 20, 2023)

Datos Insights Analysis

Cequence earned the best-of-class designation, earning one of the highest product scores in the history of Datos Insights publishing its Vendor Evaluation reports. Its Unified API Security platform displays the maturity and efficacy customers should expect and receive from cybersecurity investments. Its CQ Prime Threat Research team is at the core of its product development, which keeps up with the latest API threats and attackers. CQ Prime provides actionable intelligence to customers to improve its API security posture through advanced threat hunting.

© 2023 Datos Insights or its affiliates. All rights reserved.

Cequence customers are enthusiastic about its Unified API Security platform and the company. The management team was called out for its transparency and accessibility. Customers also pointed to the vendor's stability, ease of implementation, and overall product effectiveness; all stated the product and vendor experience exceeded their expectations.

Customers noting areas for improvement aligned their recommendations to respective areas versus universal issues across the customer base. One customer wanted a better user interface, and another wanted more multicloud support.

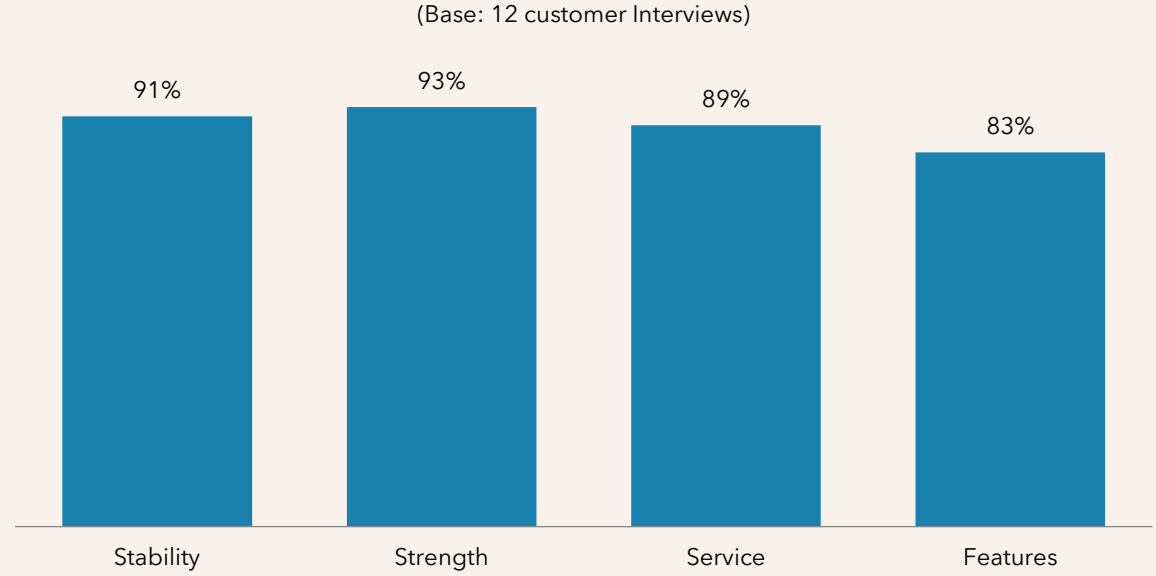
Cequence has an API security solution to match where any organization may be in the API security journey leading to a fully managed unified API protection solution. Cequence's managed API security offering removes the heavy lifting and burden of protecting APIs by organizations that have limited resources and API knowledge. The product's price point positions it at the higher end of midmarket to large enterprises. Datos Insights believes that organizations selecting Cequence will receive the advertised value and more from the product, stay on the leading edge of threat intelligence, and substantially reduce their API risk.

© 2023 Datos Insights or its affiliates. All rights reserved.

Customer Sentiment

Figure 8 shows the composite customer satisfaction scores of the four primary categories of the Datos Insights Vendor Evaluation.

Figure 8: Customer Satisfaction by Category



Source: API security solution customer interviews

Table U outlines the aggregate sentiment offered by the API security solution customers when asked several open-ended questions about their experience acquiring and using an API solution.

Table U: Customer Sentiment

Sentiment Category	Responses
Top-three reasons for acquiring an API security solution	• Discovery and inventory of APIs • Protection from bots designed to attack APIs • Securing APIs in production through runtime protection

© 2023 Datos Insights or its affiliates. All rights reserved.

Sentiment Category	Responses
Top three reasons for selecting the current API security solution	• Ease and speed of solution deployment within IT enterprise • Innovation and efficacy of solution functionality • Demonstrated customer and product support commitment
Key weaknesses of your current API security solution	• Dated user interface and dashboard • Complexity integrating with IT enterprise and solution scalability • Currency with public cloud (AWS, Azure, Google Cloud) versions
API security solutions you replaced or chose not to use after evaluating	• AWS WAF • 42Crunch • Noname
API security feature you would make a priority of development	• Customizable alerting and autonomous actions • Computer-based training • In-depth API threat intelligence
Duration of API security solution deployment	• Ongoing, APIs keep appearing, and departments slow to adopt the solution • Less than one month • Four to six months

Source: API security solution customer references

© 2023 Datos Insights or its affiliates. All rights reserved.

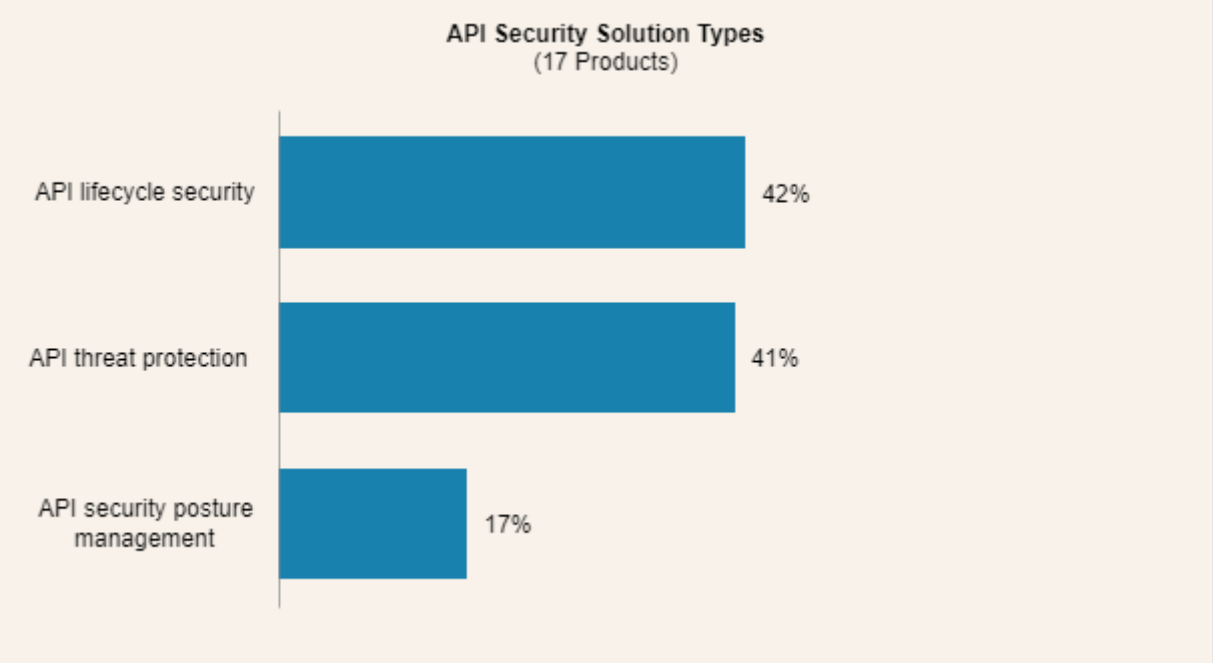
API Security Types

Datos Insights has segmented the API security solution into three types by order of effectiveness:

- **API life cycle security:** Solutions of this type must provide security throughout an API lifecycle beginning with aspects of discovery, analyzing API contracts, and building specifications, policy enforcement, monitoring, detecting, and blocking, runtime security, and testing.
- **API threat protection:** Solutions of this type must include aspects of security testing against the OWASP Top 10, API discovery, detecting and blocking, and runtime protection.
- **API posture management:** Solutions of this type must provide aspects of API discovery, inventory, risk scoring, vulnerability detection, and remediation assistance.

Figure 9 shows the breakdown of API security solutions by type.

Figure 9: API Security Solution Types



© 2023 Datos Insights or its affiliates. All rights reserved.

Conclusion

Buyers of API solutions:

- Understand the requirements of protecting APIs within your environment before evaluating API protection solutions. Solution functionality, the complexity of integration, and the automation of the CI/CD pipeline are essential evaluation criteria.
- Consider cost models and the impact of usage-based price approaches, including cost per API call and API traffic, it is important to understand the total cost of ownership. A low entry-level solution price could quickly increase in its first year.
- Consider managed API protection solutions if you have limited API security expertise on staff and lack API threat insight to create API security policies.
- Ensure vendor stability, M&A activity, employee turnover, and market economics have not impacted API security vendors. The vendor contracted today may look quite different one year later.

© 2023 Datos Insights or its affiliates. All rights reserved.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

Tari Schreider

tschreider@datos-insights.com

© 2023 Datos Insights or its affiliates. All rights reserved. This publication may not be reproduced or distributed in any form without Datos Insights' prior written permission. It consists of information collected by and the opinions of Datos Insights' research organization, which should not be construed as statements of fact. While we endeavor to provide the most accurate information, Datos Insights' recommendations are advisory only, and we disclaim all warranties as to the accuracy, completeness, adequacy, or fitness of such information. Datos Insights does not provide legal or investment advice, and its research should not be construed or used as such. Your access and use of this publication are further governed by Datos Insights' Terms of Use.