Gartner

Cool Vendors in API Strategy

Published 18 May 2020 - ID G00720429 - 13 min read

By Analysts Shameen Pillai, Paolo Malinverno, Mark O'Neill, Jeremy D'Hoinne

Initiatives: Application Architecture, Development, Integration and Platforms

Explosive demand for APIs and innovative use cases require application leaders to have an effective API strategy in place. This report highlights three vendors offering innovative solutions that tackle emerging API governance, design and security challenges.

Additional Perspectives

- Summary Translation: Cool Vendors in API Strategy (10 December 2020)
- Invest Implications: Cool Vendors in API Strategy (01 June 2020)

Overview

Key Findings

- Unmanaged or unmonitored “shadow APIs” are the source of increasing security risks and governance challenges.
- The growing need for API-enabled self-service data access requires the use of new non-REST design approaches.
- Complex and unpredictable API usage patterns require novel approaches to API security without which, distinguishing between legitimate usage, anomalies and potential threats is difficult.

Recommendations

Application leaders responsible for API strategies should ensure that their teams:

- Use the appropriate tools and processes to discover which APIs their organization provides and consumes in order to implement suitable governance policies.
- Meet API creation and design demand by utilizing emerging design frameworks such as GraphQL. These can provide viable alternatives to traditional API design and development methods for API-enabled self-service data access.

- Improve the security of your APIs by exploiting innovative solutions that use artificial intelligence to identify suspicious API usage and prevent security incidents before they happen.

Analysis

This research does not constitute an exhaustive list of vendors in any given technology area, but rather is designed to highlight interesting, new and innovative vendors, products and services. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

What You Need to Know

APIs have become such integral parts of mission-critical business systems, application architectures and customer-facing user experiences that an API platform is a very common part of a digital transformation. Findings from Gartner's 2020 CIO Survey show that more organizations now cite modern architectures that support APIs and microservices for internal and external use as key differentiators in their ability to execute new business strategies (see "The 2020 CIO Agenda: Winning in the Turns").

In addition, Gartner's 2019 Survey on API Usage and Strategy found that while the use of internal APIs is reaching saturation point at 88% of surveyed organizations, a majority (68%) reported the use of private/B2B APIs with their business partners. Usage of third-party APIs such as Google Maps or Twilio is also common (52%). Almost half (46%) say they now provide their own public APIs.

Such growth creates implementation challenges for application leaders responsible for API strategies, particularly in the areas of design, governance and security. Gartner's research continues to show that lack of skills, standards, roles, tooling and security remain top concerns for API strategies. The most successful application leaders exploit new technologies and solutions to prevent or mitigate risks and to optimize architectures and governance processes to fuel innovation. They also continue to invest in raising their API strategy maturity across all dimensions (see "Gartner's API Strategy Maturity Model").

This report features vendors that captured the Gartner research community's attention with their potential to offer viable solutions to meet these challenges and to help application leaders responsible for API strategies improve their API programs:

Data Theorem

Palo Alto, California (datatheorem.com)

Analysis by Mark O'Neill

Why Cool: Data Theorem discovers what it calls "shadow APIs," which are APIs built or used by an organization but not currently managed.

Data Theorem's API Secure product has a continuous discovery capability that identifies shadow APIs by examining sources such as mobile apps, web apps, public internet sources, cloud PaaS environments and information from API gateways. It also has a continuous inspection capability that provides vulnerability assessments of the APIs that have been discovered. For cloud-delivered APIs, the two features of continuous discovery and inspection work with APIs deployed in Amazon Web Services, Google Cloud Platform and Microsoft Azure. API specifications (including Swagger/OpenAPI) are supported in addition to enterprise API gateways (such as Google Apigee, MuleSoft and Kong).

Unlike other vendors, Data Theorem discovers not only the APIs that an organization provides itself, but also the APIs that the organization consumes and utilizes from third-party developers and open-source libraries. This additional capability better protects customers, since the unmanaged consumption of third-party APIs can result in governance issues (see "Managing the Consumption of Third-Party APIs").

Data Theorem was founded in California in 2013, by Himanshu Dwivedi, who previously was a cofounder of iSEC partners and was the technical director of @stake's San Francisco practice. Initially, Data Theorem began by building products focused on mobile app security. Realizing the threat brought to organizations by shadow APIs, Data Theorem has released products to discover and inspect APIs.

Challenges: Organizations are getting better at discovering and cataloging their own APIs, including through the work of API product managers and API platform teams (for more on API platform teams, see "Federate, Rebrand and Recharter Your API Center of Excellence to Enable an API Platform Team").

API management is already in place in many organizations, but these products typically lack an API discovery capability and require administrators to manually register APIs (for example, by loading Swagger/OpenAPI definitions). However, over time, the addition of API discovery as a feature in general purpose API management products is a threat to Data Theorem's API discovery capability. In addition, API security inspection is increasingly provided by API testing tools.

Data Theorem's focus on API discovery and shadow APIs makes it cool, but it could be vulnerable to other vendors adding the same functionality.

Who Should Care? Application leaders responsible for API programs must know which APIs the organization uses, including those not officially provided by the organization. In addition, API product managers can benefit from API discovery, as can API platform teams. Chief information security officers and security teams also benefit from API discovery, because, as security professionals know well, "you can't secure what you don't know about."