

API Security and Management

Alexei Balaganski

October 23, 2023



This Leadership Compass provides an overview of the market for API security and management solutions, along with recommendations and guidance for finding the products which address your requirements most efficiently. We examine the complexity and breadth of the challenges to discover, monitor, and secure all APIs within your enterprise and identify the vendors, their products, services, and innovative approaches towards implementing consistent governance and security along the whole API lifecycle.

Contents

Contents.....	2
Introduction / Executive Summary	5
Highlights.....	6
Market Segment	7
Delivery Models	8
Required Capabilities.....	9
Optional Capabilities	10
Leadership	11
Overall Leadership.....	11
Product Leadership.....	13
Innovation Leadership.....	14
Market Leadership	16
Correlated View.....	19
The Market/Product Matrix.....	19
The Product/Innovation Matrix	20
The Innovation/Market Matrix.....	21
Products and Vendors at a Glance	23
Product/Vendor evaluation	25
Spider graphs	25
42Crunch – API Security Platform.....	27
Airlock by Ergon – Gateway, Secure Access Hub	29
Akamai – App & API Protector, API Security, API Gateway	31
Axway – Amplify API Management Platform	33
Broadcom – Layer7 API Management	35
Cequence Security – Unified API Protection	37
Cerbos	39

Cloudentity.....	41
Cloudflare – API Gateway.....	43
Curity – Identity Server	45
Data Theorem – API Secure	47
ForAllSecure – Mayhem	49
Forum Systems – Forum Sentry	51
Google – Apigee	53
Gravitee – API Management Platform.....	55
Imperva – Application Security Platform.....	57
Nevatech – Sentinel.....	59
Noname Security – API Security Platform.....	61
Perforce – Akana	63
Red Hat – 3scale API Management	65
Salt Security – API Protection Platform	67
Sensedia – API Platform	69
Traceable – API Security Platform	71
Wallarm – Advanced API Security	73
WSO2 – API Manager, API Platform for Kubernetes, Choreo	75
Vendors to Watch.....	77
Check Point	77
Citrix	77
Fastly	77
Kong	78
MuleSoft	78
Orca Security	78
Ping Identity.....	79
Radware	79
Spherical Defence	79
TIBCO Cloud Mashery	79
Tyk.....	80
AWS	80
IBM Cloud.....	80
Microsoft Azure.....	81

Oracle Cloud.....	81
Methodology.....	82
Types of Leadership	82
Product rating	83
Vendor rating	84
Rating scale for products and vendors	85
Inclusion and exclusion of vendors	86

Introduction / Executive Summary

From what used to be a purely technical concept created to make developers' lives easier, Application Programming Interfaces (APIs) have evolved into one of the foundations of modern digital business. Today, APIs can be found everywhere — at home and in mobile devices, in corporate networks and in the cloud, even in industrial environments, to say nothing about the Internet of Things (IoT). The emerging era of Generative AI is also entirely dependent on APIs to implement integrations with existing business applications.

Having followed the market for almost a decade, we have long recognized APIs as one of the most important IT trends. Rapidly growing demand for exposing and consuming APIs, which enables organizations to create new business models and connect with partners and customers, has tipped the industry towards adopting lightweight approaches like representational state transfer (REST). APIs are now powering the logistics of delivering digital products to partners and customers. Almost every software product or cloud service now comes with a set of APIs for management, integration, monitoring, or a multitude of other purposes.

This evolution only continues to accelerate. As new digital transformation initiatives across various industries emerge, diverse business models are reshaping the technical requirements for API development and operations dramatically. New standards, technologies, and development methodologies introduced by the need to support numerous use cases have also introduced additional complexity to existing API management platforms.

REST APIs are still commonly used today, but they are increasingly augmented or displaced with a variety of alternative protocols and standards, such as GraphQL or gRPC. In fact, the industry is evolving so fast that API management solutions in their traditional sense, like API gateways, can already be considered IT legacy products. Modern, loosely coupled cloud-native application architectures demand API management solutions that can handle complicated traffic patterns and deal with ephemeral container-based infrastructures.

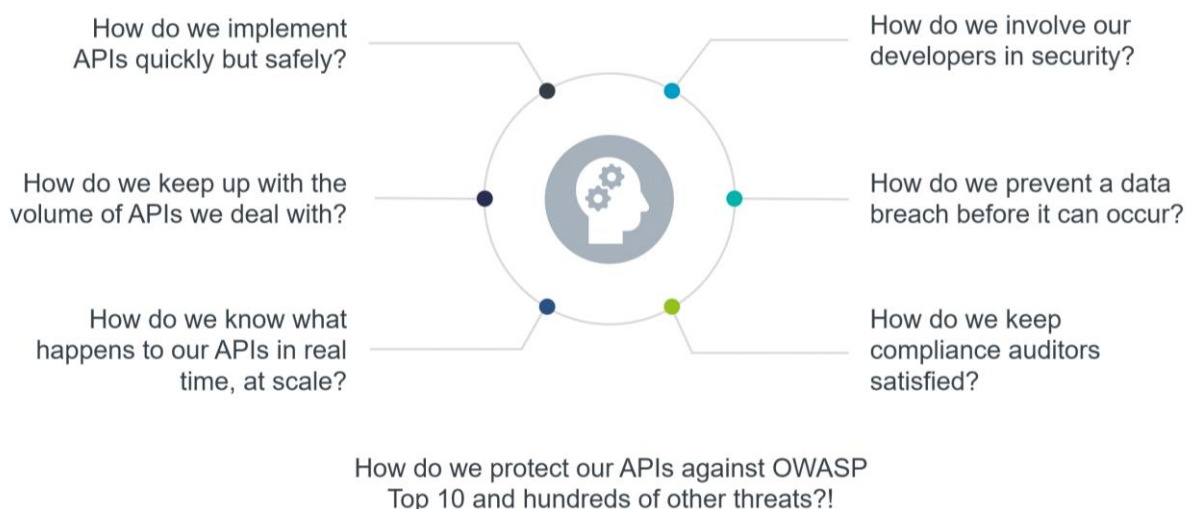


Figure 1: The API challenges organizations are facing

Unfortunately, many organizations still tend to underestimate the potential security challenges of exposing their APIs without a security strategy and infrastructure in place. Although organizations like OWASP are doing a lot to promote the awareness of critical API risks with projects like the recently updated API Security Top 10, this sometimes has an opposite effect – the public tends to forget about the long tail of other problems they have to deal with beyond this essential but definitely not exhaustive list.

Multiple studies have estimated that APIs are already the biggest attack vector for web applications. However, this claim does not even include numerous other potential attack vectors the unchecked proliferation of APIs can expose, including public clouds, distributed applications and microservices, mobile clients, and so on.



Figure 2: API complexity explosion

In a sense, API security has long become an industry of its own; with the scope of risks and challenges the industry confronts growing exponentially, API security solutions have to expand their coverage and grow in complexity themselves. Providing comprehensive protection against the broad range of API-specific threats and doing it consistently throughout the whole lifecycle of an API is complex. Understanding the business logic behind those APIs and adapting the protection accordingly is even more complicated.

Our approach is to emphasize the growing prevalence of API security solutions over traditional (some might say “old school”) API management products. This report covers the current state of the API security and management market.

Highlights

- Both API management and API security markets experienced strong growth in recent years, driven by massive increase in API adoption across all industries combined with an ongoing pressure of security and compliance risks that these APIs are exposed to.
- The tempo of API evolution continues to increase, with multiple standards, protocols and architectures emerging, expanding the scope beyond just the traditional REST

APIs to include GraphQL, gRPC and even asynchronous protocols, such as Kafka or MQTT, that were previously not even considered APIs.

- API security has long become an industry of its own; with the scope of risks and challenges the industry confronts growing exponentially, API security solutions must expand their coverage and grow in complexity themselves.
- Fueled by widely publicized large-scale data breaches and new compliance regulations in various industries, the overall awareness of API security risks and challenges continues to rise. Pure play API security vendors that reach \$1B market valuation are a reality now.
- Market consolidation through acquisitions continues, with not just smaller boutique vendors being incorporated into larger portfolios, but major market leaders as well.
- API discovery and security monitoring solutions continue to be the most popular class of products offered on the API security market, but solutions addressing other phases of the API lifecycle are growing in popularity.
- The notion of “shifting left” can be considered the latest buzzword in the market, with multiple vendors now expanding their portfolios to include API testing solutions. Still, the level of integration of these tools into the existing security and management platforms varies dramatically.
- The Overall Leaders in API Security and Management are (in alphabetical order): 42Crunch, Akamai, Axway, Broadcom, Cequence Security, Curity, Data Theorem, Forum Systems, Google Apigee, Gravitee, Imperva, Noname Security, Red Hat, Salt Security, Sensedia, and WSO2.

Market Segment

With API management capabilities in their traditional sense becoming commoditized, the vendors continue to add sophisticated security capabilities to their products to remain competitive with pure play API security solutions – and their number is growing rapidly as well. API management and API security should no longer be considered as standalone, isolated components of IT infrastructures. On the contrary, choosing the right components of an “API fabric” should cover such aspects as application development and operations, data and infrastructure security, and regulatory compliance, among others.

API discovery and security monitoring solutions continue to be the most popular class of products offered on the API security market, but solutions addressing other phases of the API lifecycle are growing in popularity as well. Most notably, the concept of data-centric security is gaining traction, where the focus is shifting from infrastructure towards protecting the sensitive data exposed by APIs.

Increasingly, vendors incorporate AI and machine learning (ML) into their solutions to enable sophisticated security analytics and real-time detection of malicious or suspicious anomalies in the behavior profiles of APIs, their consumers, and even the endpoint devices. With the growing adoption of generative AI, we can expect that intelligent automation and decision support will play an increasingly important role in API security solutions as well – for forensic analysis, decision support, policy generation and other applications.

On the other end of the API lifecycle, solutions are focusing on “shifting left,” bringing security to the earliest phases of software development and design, providing capabilities like API testing and API specification analysis. Testing early and often makes application code more resilient to attacks and is generally considered a best practice and an essential part of the “secure by design” methodology.

And yet, shifting left alone cannot be considered a panacea for all API security challenges. Consistent and reliable protection of business-critical APIs must not just extend to every other phase of the API lifecycle, but also ensure that this coverage is provided as a holistic, integrated experience.

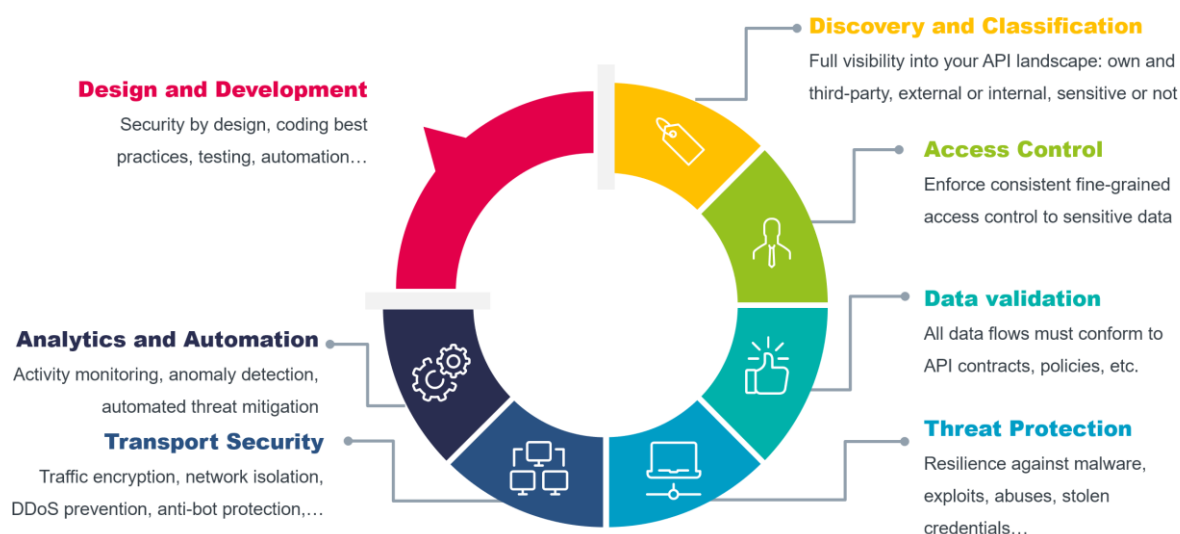


Figure 3: The scope of modern API security

In the end, we are no longer treating API management and security as independent or even mutually exclusive subjects. On the contrary, the ultimate goal is helping organizations identify and deploy solutions that address their business requirements, security risks, and compliance challenges when publishing their own and consuming third-party APIs.

And finally, it’s even more important for companies developing their API strategies to be aware of current security developments and stay agile and flexible to be able to respond quickly to constantly emerging new risks, as well as to incorporate new technologies into their security architectures.

Delivery Models

Most API management platforms are designed to be loosely coupled, flexible, scalable, and environment-agnostic, with a goal to provide consistent functional coverage for all types of APIs and other services. While the gateway-based deployment model remains the most widespread, with API gateways deployed either closer to existing backends or API consumers, modern application architectures may require alternative deployment scenarios like service meshes for microservices.

Dedicated API security solutions that rely on real-time monitoring and analytics may be deployed either in-line, intercepting API traffic, or rely on out-of-band communications with API management platforms. However, management consoles, developer portals, analytics platforms, and many other components are usually deployed in the cloud to enable a single pane of glass view across heterogeneous deployments. A growing number of capabilities are now being offered as Software-as-a-Service (SaaS) with consumption-based licensing.

In short, for a comprehensive API management and security architecture, a hybrid deployment model is the only flexible and future-proof option. Still, for highly sensitive or regulated environments, customers may opt for a fully on-premises deployment.

Required Capabilities

We are looking for solutions that cover at least several of the following key functional areas, either focusing on more traditional API management or specializing in securing existing APIs (ideally, combining both approaches in a single integrated platform).

API Design and Testing – these functions cover the earliest stages of the API lifecycle such as API contract design, transformation of existing APIs, or modernization of legacy backend services, as well as creating and managing policies that govern API performance, availability, and security.

API Discovery, Classification, and Inventory – without a comprehensive, accurate and dynamically updated inventory of all APIs across all corporate IT environments (on-premises, cloud-native, hybrid, Kubernetes, etc.) any security program will not be able to provide consistent visibility, governance, and protection across the entire API attack surface.

Microservice Management – traditional API gateways do not scale well for modern distributed architectures and must be augmented with modern service management capabilities such as the Istio service mesh, which provides native connectivity, monitoring, and security that scale for hundreds and thousands of microservices.

Developer and CI/CD Tools – exposing APIs for consumption, providing documentation and collaboration functions, onboarding and managing developers and their apps are among the functions we are looking for here, as well as integrations into existing continuous delivery pipelines of modern application development projects.

Identity and Access Control – supporting multiple identity types, standards, protocols, and tokens and providing flexible dynamic access control that is capable of making runtime context-based decisions. This does not only apply to the APIs themselves, but management interfaces and developer tools as well.

API Vulnerability Management – discovering existing APIs and analyzing their conformance to API contracts, security best practices, and corporate policies is the only truly proactive approach towards API security. Intelligent prioritization of discovered vulnerabilities by business risk assessment improves both developer productivity and overall security posture.

Analytics and Security Intelligence – continuous visibility and monitoring of all API transactions and administrative activities allow for quick detection of not just external attacks, but infrastructure changes, misconfigurations, insider threats, and other suspicious activities.

Integrity and Threat Protection – securing APIs and services from hacker attacks and other threats requires a multilayered approach to address both transport-level attacks and exploits specific to messaging protocols and data formats.

Strong Internal Security – administrative and developer access to the management console must be secured, with role-based access control implemented across the whole platform and delegated administration capabilities added for scalability and decentralization. Multi-factor authentication and audit trail for all activities are recommended.

Hybrid, Multicloud Deployment – supporting heterogeneous distributed environments including cloud, containers, microservices, and serverless platforms to be able to provide consistent visibility, analytics, and protection across the entire corporate IT is a critical success factor for any API security solution.

Since we do not expect every vendor to be able to provide complete API management and security coverage on their own, seamless interoperability both with the vendor's other own products and with existing third-party products is crucial. A strong focus is put on integration into existing security infrastructures to provide consolidated monitoring, analytics, governance, or compliance across multiple types of information stores and applications.

We expect solutions to support at least some of the following integrations:

- Popular API management platforms, gateways, service meshes, etc.
- Development tools for integrating into DevOps/DevSecOps processes.
- IAM/IAG platforms for identity management and access governance.
- SIEM/XDR platforms for unified monitoring and security intelligence.
- Additional security solutions like data protection, DLP, WAF, Bot Defense, etc.

Naturally, an API management solution also needs to provide its own set of APIs.

Optional Capabilities

Some additional functional capabilities for this Leadership Compass include:

- supporting multiple types of identities, authentication protocols, and tokens.
- providing dynamic access control that goes beyond static roles.
- securing interfaces against hacker attacks and other threats.
- addressing government and industry-specific compliance issues.
- ensuring continued availability and performance of the services.

Each of the features and criteria listed above will be considered in the product evaluation below.

Leadership

The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection requires further analysis and a Proof of Concept (PoC) or pilot phase, based on the specific criteria of the customer.

The Overall Leadership rating provides a combined view of the ratings for:

- Product Leadership
- Innovation Leadership
- Market Leadership

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right.

Overall Leadership

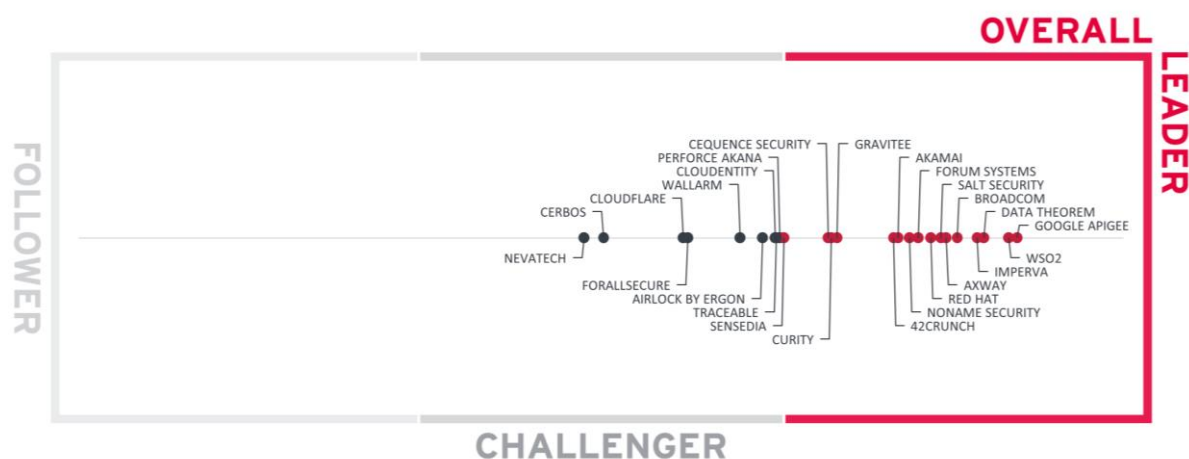


Figure 4: The Overall Leaders in the API Security and Management market

The Overall Leadership rating provides a consolidated view of all-around functionality, market presence, and financial security. However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

This year's list of Overall Leaders are veteran players in the API management and security market, offering comprehensive enterprise-level highly integrated platforms for the most demanding customers, and can easily maintain their leadership positions.

Axway, Broadcom, Google, Imperva, Red Hat, and WSO2 are all large, established vendors with a global presence, strong partner networks, and large customer bases. Forum Systems is still being recognized for its continued “security first” approach in its product design.

Remaining vendors include 42Crunch, Curity, Salt Security, and Sensedia, which are smaller in scale and focus on narrower functionality segments, stay among the leaders as well because of their financial stability, steady innovation, and continued investment into new functionality. Joining them is Cequence Security, which has risen through the ranks from being recognized among Challengers last time.

This year, however, we have several newcomers to our rating, both large and small. Among the former we have Akamai, a veteran edge computing vendor with a global cloud infrastructure footprint and long history of using it to deliver security services, and Nonym Security, the API security’s first “unicorn” company, that has managed to surpass \$1B valuation in just over a year. Among the latter we have Data Theorem, a well-established application security vendor and Gravitee, a startup focusing on unifying synchronous and asynchronous API protocols in a single platform.

Airlock by Ergon, Cloudentity, Perforce Akana, Traceable, and Wallarm are still found among the Challengers but are so close to the leaders that they have strong chances to cross the border next time. The rest of the vendors are found somewhat behind. These include both large companies like Cloudflare that has however just recently started its expansion to the API security market, as well as smaller, highly specialized vendors like Cerbos, which only focuses on solving the authorization challenge for APIs, ForAllSecure specializing in next-generation API security testing, or Nevatech, a boutique API management vendor for the Windows ecosystem.

The Overall Leaders are (in alphabetical order):

- 42Crunch
- Akamai
- Axway
- Broadcom
- Cequence Security
- Curity
- Data Theorem
- Forum Systems
- Google Apigee
- Gravitee
- Imperva
- Nonym Security
- Red Hat
- Salt Security
- Sensedia
- WSO2

Product Leadership

The first of the three specific Leadership ratings is about Product leadership. This view is mainly based on the analysis of the overall capabilities of the various products or services.



Figure 5: The Product Leaders in the API Security and Management market

The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

In the Product Leadership rating, we look specifically for the functional strength of the vendors' solutions, regardless of their current ability to grab a substantial market share. It is

worth noting again that, with the broad spectrum of functionality we expect from a complete data security solution, it is not easy to achieve a Leader status for a smaller company.

Unsurprisingly, all the overall leaders mentioned above are also present among the Product Leaders. These include both large companies like Akamai, Axway, Broadcom, Google Apigee, Imperva, Noname Security, Red Hat, and WSO2, as well as smaller, but capable companies like 42Crunch, Cequence Security, Curity, Data Theorem, Forum Systems, Gravitee, Salt Security, and Sensedia.

Wallarm, Perforce, Ergon, and Cloudentity are also found among the product leaders, while not yet reaching the overall leadership status. Perhaps next time, as their customer base expands further...

Among the vendors occupying the Challengers segment, we can find Cloudflare – a large veteran web security vendor, whose foray into the field of API security is simply too recent to warrant a leadership position. Joining them are smaller companies like Nevatech and Traceable, which offer comprehensive but somewhat more specialized solutions, as well as by Cerbos and ForAllSecure, which only focus on a single functional area of API security.

Product Leaders (in alphabetical order):

- 42Crunch
- Airlock by Ergon
- Akamai
- Axway
- Broadcom
- Cequence Security
- Cloudentity
- Curity
- Data Theorem
- Forum Systems
- Google Apigee
- Gravitee
- Imperva
- Noname Security
- Perforce Akana
- Red Hat
- Salt Security
- Sensedia
- Wallarm
- WSO2

Innovation Leadership

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require to keep up with the constant evolution and emerging customer requirements they are facing. The vertical axis shows the amount of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

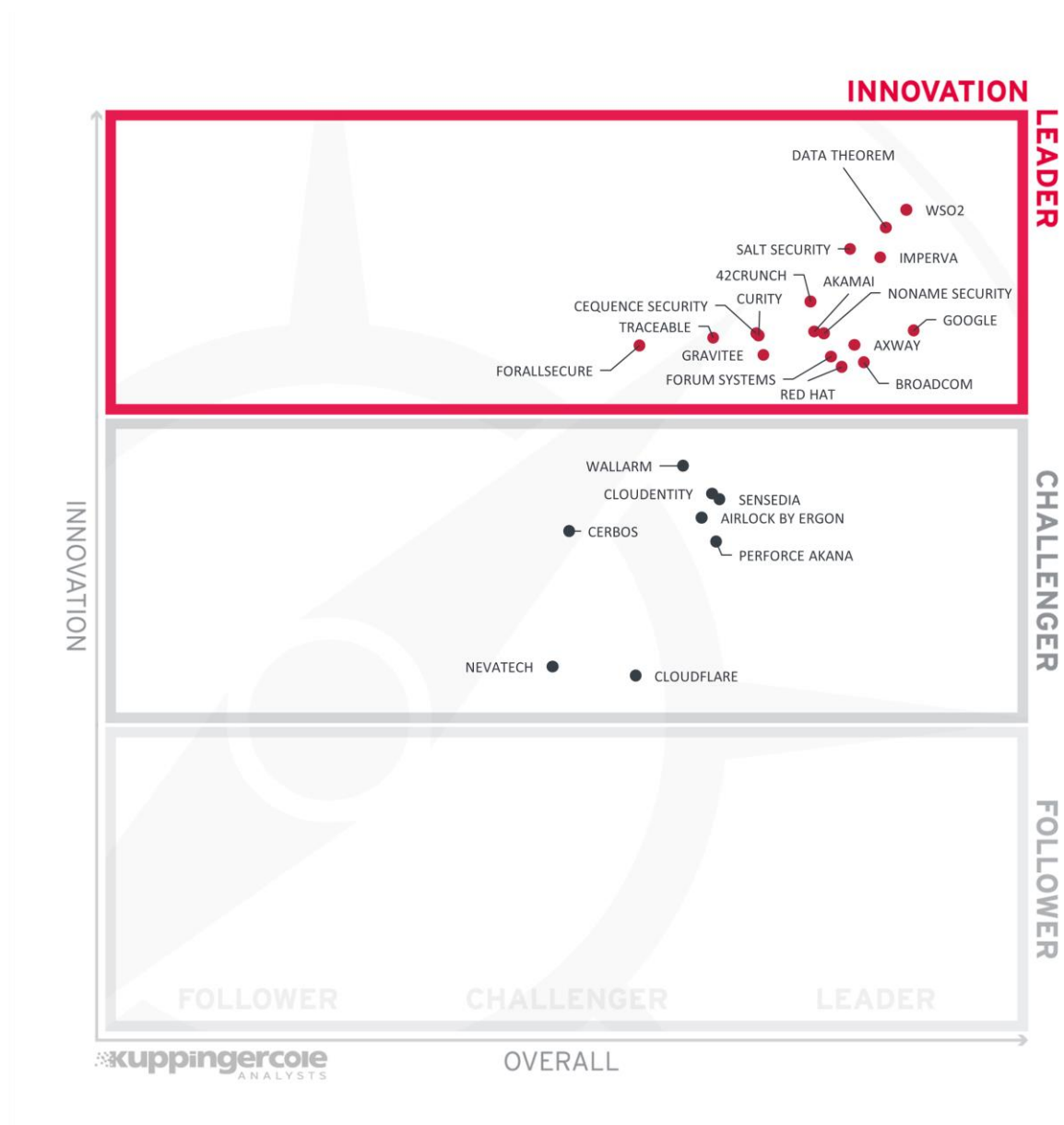


Figure 6: The Innovation Leaders in the API Security and Management market

Our Innovation Leadership shows a mix of both large and small vendors. This clearly indicates, on the one hand, the huge potential for ongoing innovation on various areas of API security and management, but also that by focusing on a relatively narrow functional area, a small development team can achieve impressive results in delivering useful innovative capabilities in their product.

At the same time, we see a major change in comparison to the previous edition of this Leadership Compass. This reflects the major shifts in the current trends and customer requirements that reshape the entire market substantially. With new API standards rising in popularity and also the growing sophistication of securing them, some of the positions in our innovation rating have changed substantially.

We can still see large vendors like Axway, Broadcom, Google, Imperva, Red Hat, and WSO2 among the innovation leaders just like last year. Joining them are smaller companies like 42Crunch, Cequence Security, Curity, Forum Systems, Salt Security, and Traceable. Among the newcomers, companies like Akamai, Data Theorem, ForAllSecure, Gravitee, and Noname Security are recognized as innovation leaders as well.

The remaining vendors are positioned in the Challengers segment, reflecting perhaps the overall maturity of their products that comes with the unfortunate downside of a somewhat slower pace of innovation or simply the fact that their solutions have too narrow a focus to rival their bigger competitors.

Innovation Leaders (in alphabetical order):

- 42Crunch
- Akamai
- Axway
- Broadcom
- Cequence Security
- Curity
- Data Theorem
- ForAllSecure
- Forum Systems
- Gravitee
- Google Apigee
- Imperva
- Noname Security
- Red Hat
- Salt Security
- Traceable
- WSO2

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers and their geographic distribution, the size of deployments and services, the size and geography of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

The vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership chart is rectangular and divided into thirds.

Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section. Please note that this rating does not reflect the overall market presence of large vendors but is only limited to the market shares of their respective API management and security products.

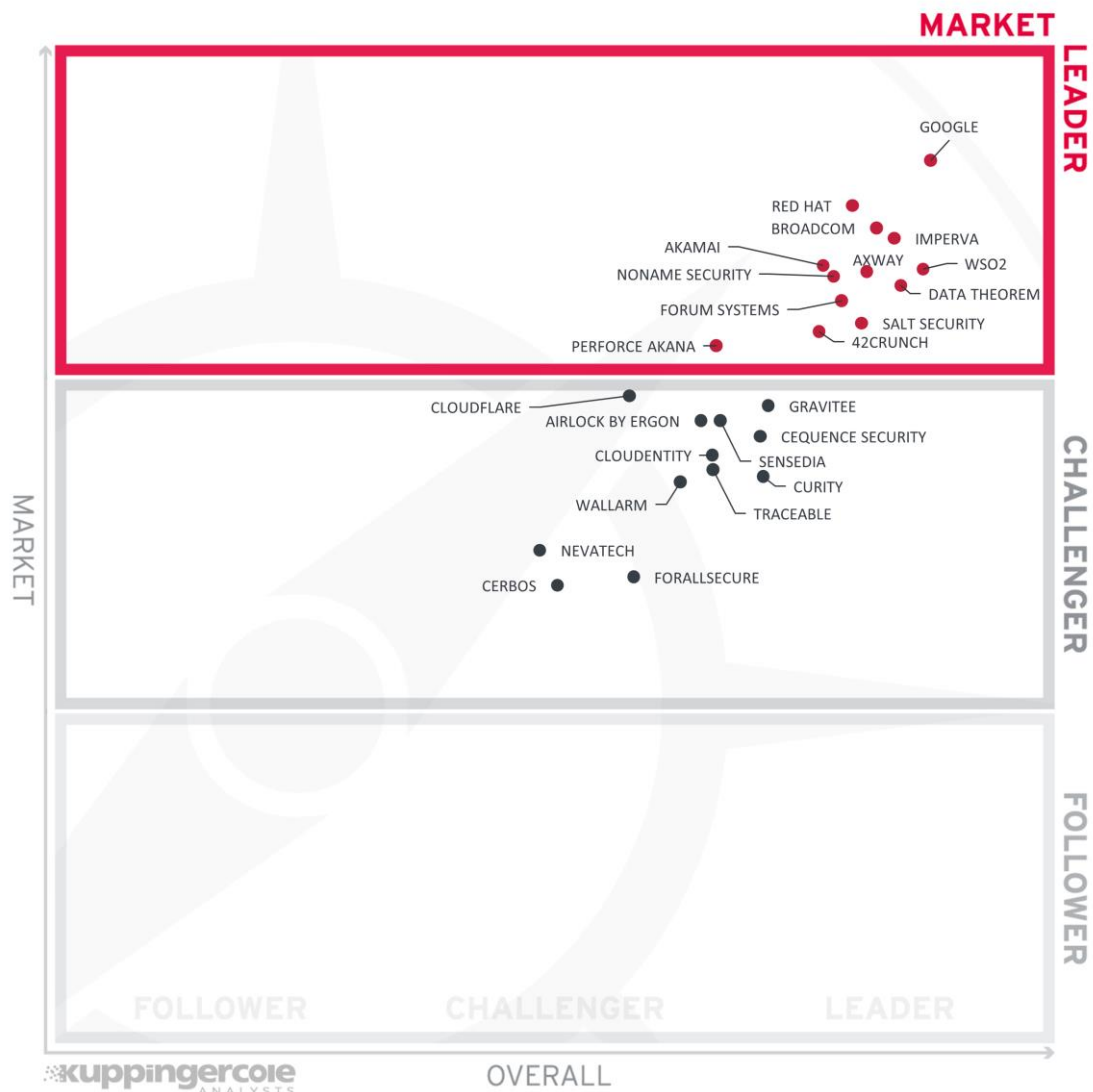


Figure 7: The Market Leaders in the API Security and Management market

Completely unsurprisingly, we find all large veteran players among the Market Leaders, including both API management and API security vendors. This year, we have several new participants among leaders as well, including such industry giants as Akamai as well as Data Theorem and Noname Security having substantial global market presence, too. Even 42Crunch, a much smaller vendor, has managed to massively improve its market presence through strategic partnerships.

The rest of the vendors populate the Challenger segment, reflecting their ongoing journey towards a larger market position. Even large companies like Cloudflare or Perforce are found here despite their strong overall market presence outside the API industry – here they are yet to gain a similar foothold.

Market Leaders (in alphabetical order):

- 42Crunch
- Akamai
- Axway
- Broadcom
- Data Theorem
- Forum Systems
- Google Apigee
- Imperva
- Noname Security
- Perforce Akana
- Red Hat
- Salt Security
- WSO2

Correlated View

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for a product leader, but for a vendor that is delivering a solution that is both feature-rich and continuously improved, which would be indicated by a strong position in both the Product Leadership ranking and the Innovation Leadership ranking. Therefore, we provide the following analysis that correlates various Leadership categories and delivers an additional level of information and insight.

The Market/Product Matrix



Figure 8: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of “overperformers” when comparing Market Leadership and Product Leadership.

Among the Market Champions, we can find the usual suspects – large, well-established vendors like Akamai, Axway, Broadcom, Google, Imperva, Perforce (for the first time!), Red Hat, and WSO2. They are joined by 42Crunch, Forum Systems, and Salt Security, as well as the newcomers Data Theorem and Noname Security. All these companies have mature products that have carved an appropriate niche in the API market.

The vendors in the right middle box are those whose capable products are yet to win them a strong market presence: here we find Cequence Security (also an upgrade!) Cloudentity, Curity, Ergon, Sensedia, joined by the newcomers Gravitee and Wallarm.

Vendors found in the middle segment indicate average results in both product capabilities and market presence. However, they are found there for different reasons. Companies like Cloudflare have only recently entered the API market, they are yet to establish a permanent presence in there. The likes of Cerbos and Nevatech are, in a sense, boutique vendors focusing on a specific narrow capability. ForAllSecure and Traceable definitely have the potential for future growth.

The Product/Innovation Matrix

This view shows how Product and Innovation Leadership are correlated. The vertical axis represents the product strength rating plotted against innovation on the horizontal axis. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a rather low correlation between the product and innovation ratings, with many vendors being far from the dotted line. This is a strong indicator of the turbulent current state of the API market, which is far from being mature, and the overall complexity of comparing solutions focused on totally different functional areas against each other.

Again, among the Technology Leaders, we have a healthy mix of both large established players and innovative solutions from smaller vendors. The usual suspects – large and established vendors – are joined by smaller companies like 42Crunch, Curity, and, for the first time, Cequence Security. Newcomers in this segment are Data Theorem and Gravitee.

Traceable and ForAllSecure can be found in the right middle box, showing that even a highly innovative technology may need more time to be fully implemented into a mature product. Cloudentity, Ergon, Noname Security, Perforce, Sensedia, and Wallarm can be found in the top middle box, showing that their respective solutions have reached a maturity plateau. We hope to see more innovative developments from these company's next time.

Cerbos, Cloudflare, and Nevatech can be found in the middle box, showing a healthy combination of solid product capabilities and a steady, if not amazing pace of innovation. This is typical for smaller companies or vendors that have their primary focus elsewhere.

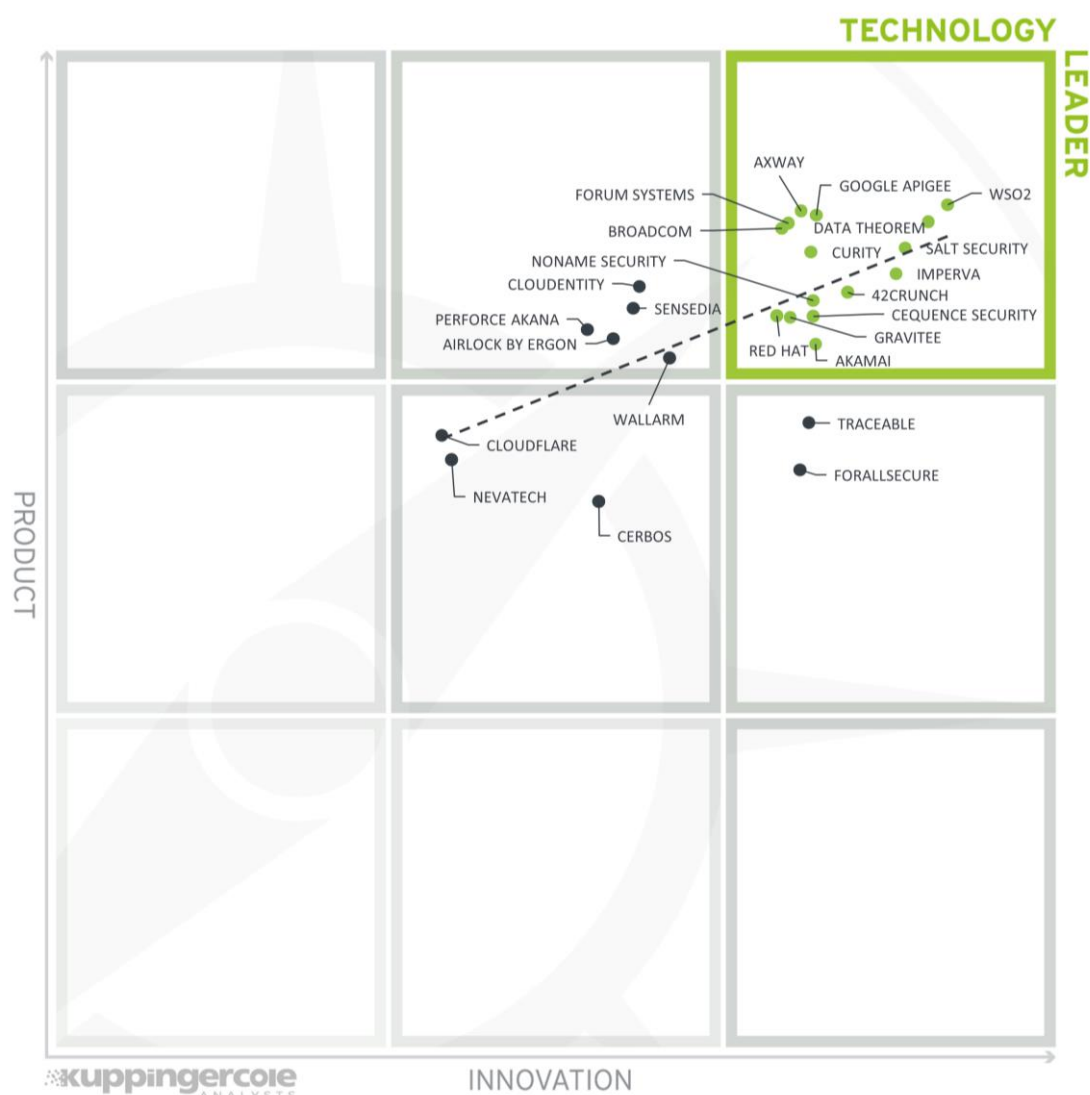


Figure 9: The Product/Innovation Matrix

The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. The vertical axis represents the market position rating plotted against innovation on the horizontal axis. Some vendors might perform well in the market without being Innovation Leaders. This might impose a risk for their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

Vendors above the dotted line are performing well in the market compared to their position in the Innovation Leadership rating. Vendors below the line show, based on their ability to innovate, the biggest potential for improving their market position.



Figure 10: The Innovation/Market Matrix

Compared to the previous edition, the group of the Big Ones has retained the majority of previously recognized vendors as well as added a group of newcomers including 42Crunch, Akamai, Data Theorem, and Noname Security. All these companies combine a strong market presence with a steady tempo of their innovation efforts.

The companies found in the right middle segment indicate their strong potential for improving their market position in the future. These include Cequence Security, Curity, Traceable and the newcomers ForAllSecure and Gravitee.

Perforce is the only vendor found in the top middle box, showing a somewhat slower rate of innovation that does not yet affect its market presence, however.

The rest of the vendors can be found in the middle box, demonstrating average results. They are either still in their startup phase or perhaps focus their primary investments elsewhere.

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on API Security and Management. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other.

These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1. Since some vendors may have multiple products, these are listed according to the vendor's name.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
42CRUNCH	positive	positive	strong positive	strong positive	strong positive
AIRLOCK BY ERGON	strong positive	positive	strong positive	positive	strong positive
AKAMAI	strong positive	positive	strong positive	positive	positive
AXWAY	strong positive	strong positive	strong positive	strong positive	strong positive
BROADCOM	strong positive	strong positive	strong positive	strong positive	strong positive
CEQUENCE SECURITY	positive	positive	strong positive	positive	strong positive
CERBOS	positive	neutral	strong positive	positive	neutral
CLOUDENTITY	strong positive	positive	strong positive	strong positive	strong positive
CLOUDFLARE	positive	neutral	strong positive	positive	positive
CURITY	strong positive	positive	strong positive	strong positive	strong positive
DATA THEOREM	strong positive	strong positive	strong positive	positive	strong positive
FORALLSECURE	positive	positive	positive	positive	positive
FORUM SYSTEMS	strong positive	strong positive	strong positive	strong positive	positive
GOOGLE APIGEE	strong positive	strong positive	strong positive	strong positive	strong positive
GRAVITEE	strong positive	strong positive	positive	positive	positive
IMPERVA	strong positive	strong positive	strong positive	positive	positive
NEVATECH	positive	positive	positive	neutral	positive
NONAME SECURITY	strong positive	strong positive	strong positive	positive	positive
PERFORCE AKANA	strong positive	positive	positive	positive	strong positive

RED HAT	positive	strong positive	positive	strong positive	positive
SALT SECURITY	strong positive	strong positive	strong positive	positive	strong positive
SENSEDIA	positive	strong positive	strong positive	positive	strong positive
TRACEABLE	positive	positive	strong positive	positive	positive
WALLARM	positive	positive	strong positive	Strong positive	positive
WSO2	strong positive	strong positive	strong positive	strong positive	strong positive

Table 1: Comparative overview of the ratings for the product capabilities

In addition, we provide in Table 2 an overview which also contains four additional ratings for the vendor, going beyond the product view provided in the previous section. While the rating for Financial Strength applies to the vendor, the other ratings apply to the product.

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
42CRUNCH	strong positive	positive	neutral	positive
AIRLOCK BY ERGON	positive	neutral	positive	positive
AKAMAI	strong positive	positive	strong positive	positive
AXWAY	positive	positive	strong positive	positive
BROADCOM	positive	positive	strong positive	strong positive
CEQUENCE SECURITY	positive	neutral	neutral	positive
CERBOS	positive	weak	weak	neutral
CLOUDENTITY	positive	neutral	neutral	positive
CLOUDFLARE	neutral	neutral	strong positive	positive
CURITY	positive	weak	neutral	neutral
DATA THEOREM	strong positive	positive	positive	strong positive
FORALLSECURE	strong positive	weak	weak	weak
FORUM SYSTEMS	positive	positive	positive	positive
GOOGLE APIGEE	positive	strong positive	strong positive	strong positive
GRAVITEE	positive	neutral	neutral	positive
IMPERVA	strong positive	positive	positive	strong positive
NEVATECH	neutral	weak	neutral	weak
NONAME SECURITY	positive	positive	positive	strong positive
PERFORCE AKANA	neutral	neutral	positive	positive

RED HAT	positive	positive	strong positive	strong positive
SALT SECURITY	strong positive	positive	positive	positive
SENSEDIA	positive	neutral	neutral	positive
TRACEABLE	strong positive	neutral	neutral	neutral
WALLARM	positive	weak	positive	neutral
WSO2	strong positive	positive	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products, there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass.

API Lifecycle Management – here we evaluate the core capabilities of an API management platform, which cover all major stages of an API lifecycle: from architecting an API strategy to developing, deploying, and refining your APIs to daily management and operations, including API monetization.

Deployment and Integration – with the rapid proliferation of API use cases and deployment scenarios, API management platforms must support a wide range of deployment options, from traditional on-premises appliances and static gateways to modern dynamic microservice-based architectures, serverless applications, and IoT, being able to play well together with popular third-party products.

Developer Portal and Tools – exposing APIs for consumption, providing documentation and collaboration functions, onboarding, and managing developers and their apps are among the functions we are looking for here, DevOps and DevSecOps integrations included.

Identity and Access Control – supporting multiple identity types, standards, protocols, and tokens and providing flexible dynamic access control that is capable of making runtime context-based decisions. This does not only apply to the APIs themselves, but management interfaces and developer tools as well.

API Vulnerability Management – discovering existing APIs and analyzing their conformance to API contracts, security best practices, and corporate policies is the only truly proactive approach towards API security. Intelligent prioritization of discovered vulnerabilities by business risk assessment improves both developer productivity and overall security posture.

Analytics and Security Intelligence – continuous visibility and monitoring of all API transactions and administrative activities allow for quick detection of not just external attacks, but infrastructure changes, misconfigurations, insider threats, and other suspicious activities.

Integrity and Threat Protection – securing APIs and services from hacker attacks and other threats requires a multilayered approach to address both transport-level attacks and exploits specific to messaging protocols and data formats.

Scalability and Performance – maintaining continuous availability of the enterprise services even under high load or a denial-of-service attack is the most crucial requirement for an API infrastructure. A modern API management solution should also address the challenges of lightweight distributed architectures.

These spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some products may have gaps in certain areas while being strong in other areas. These kinds of solutions might still be a good fit if only specific use cases must be addressed. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations across complex, heterogeneous IT environments.

42Crunch – API Security Platform

42Crunch is a privately held API security startup company headquartered in Dublin, Ireland with local offices across the US and multiple European countries. Founded in 2016, the company focuses on proactive discovery and remediation in API contracts (thus, even before any implementation code is written) and runtime protection against API attacks. 42Crunch strives to make API security a commodity by providing developer-focused tools, offering guidance and best practices, and by supporting DevSecOps initiatives.

42Crunch offers an integrated cloud-based platform that works with API Contracts that use standard machine-readable OpenAPI (formerly known as Swagger) format to document any existing or future API structure and operations. The platform can automatically audit the contract for potential vulnerabilities and offer developers the latest best practices and recommendations on hardening their APIs. In addition, it can analyze existing API endpoints for conformance with their contracts. Finally, custom micro-firewalls can be deployed in front of each API to enforce the appropriate security policies on it and to prevent API threats – all without writing a single line of code or configuration.

The company's strong focus on developers means that its platform is designed to be integrated into the API development lifecycle at all stages: available directly in development environments and integrated into CI/CD pipelines. Centralized policy management and full process automation ensure that security becomes an integral part of the API lifecycle and can be applied automatically and at scale – across hybrid clouds or within microservice-based applications. In addition, 42Crunch invests considerable efforts into raising awareness about API security challenges among developers and application security teams. The company maintains APIsecurity.io, an online portal that provides the recent news, guidance, and best practices to developers and security specialists. The free extensions offered for popular integrated development environments, which deliver instant API security feedback to developers, have already attracted over 800 thousand users.

Since our previous review, 42Crunch has substantially increased both its adoption by developers and enterprise customers and the ecosystem of integrations with API management vendors. Technical and commercial partnerships with leading ISVs help the company achieve a global distribution and reach to complement its direct enterprise sales and developer marketplace success. It is also expanding the platform's coverage with new capabilities like API discovery, security testing, and governance. Unfortunately, support for new API standards like GraphQL is still a roadmap item.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



Table 3: 42Crunch's rating

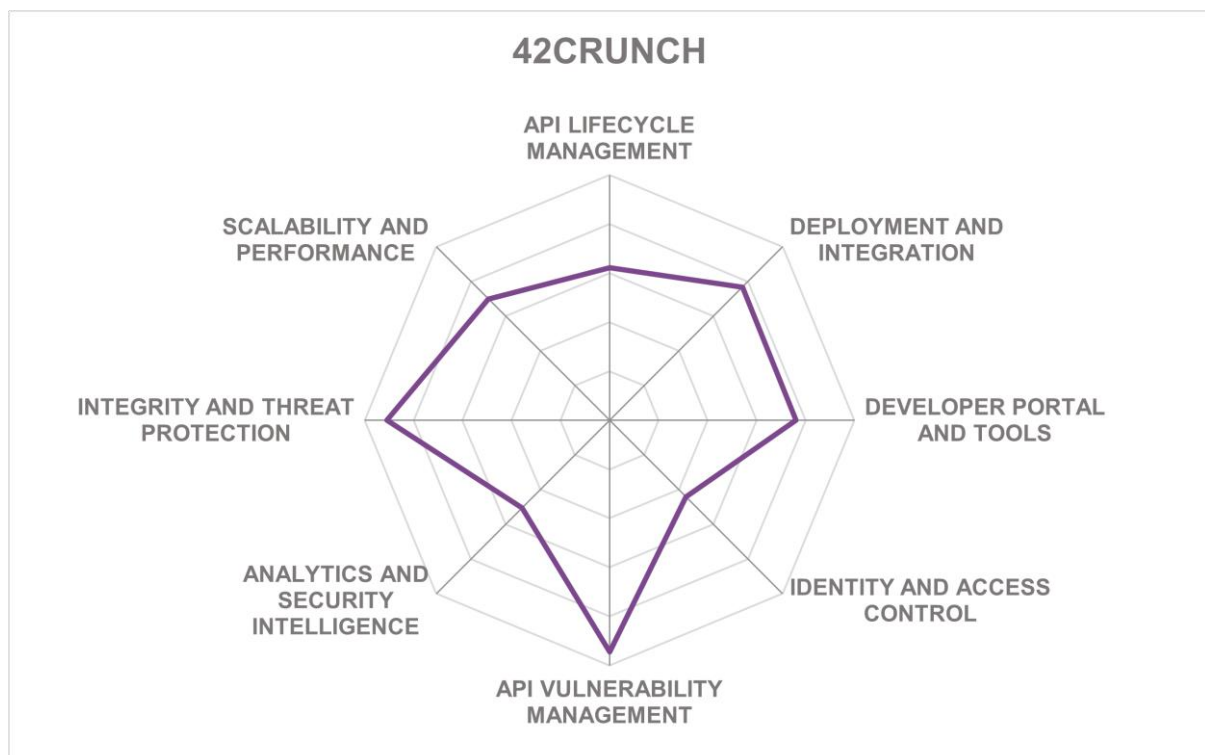
Strengths

- Proactive approach towards API security by design.
- API contract analysis to proactively identify and remediate vulnerabilities and violations.
- Scalable API micro-firewall architecture for policy enforcement and threat protection.
- Comprehensive developer guidance and best practices with the API Security Encyclopedia.
- IDE extensions to provide instant feedback to developers.

Challenges

- Currently, still only supports REST APIs.
- Identity and access controls are fairly basic.
- Runtime security analytics is only available with third-party tool integrations.

Leader in



Airlock by Ergon – Gateway, Secure Access Hub

Ergon is a Swiss-based company established in 1984 with customers primarily in the DACH region and is also growing across EMEA and the APAC regions. Its partner ecosystem is concentrated in DACH but remains small in other areas. Two primary technologies the company has been known for are Airlock IAM (access management and identity federation) and Airlock Gateway (web application firewall and API security). Together, they form the foundation of Ergon's integrated offering, Airlock Secure Access Hub, complemented by a lightweight and configurable Airlock Microgateway for containerized and microservice-based architectures.

The platform supports hybrid policy management by separating shared and local policies to ease the collaboration between developers and security administrators. It incorporates not just IAM and WAF capabilities but offers expanded security functions like DDoS protection and Bot Mitigation as well as includes an API Gateway product with a substantial range of security features. Ergon participates in a bug bounty program to continuously validate and improve the security of all their products. Although Airlock does implement basic API management functions such as monitoring, statistics, or key management, the company positions the product as an API security and access management solution.

Notable API protection features include blocking OWASP API Security Top 10 threats, JSON Schema and OpenAPI specification validation, and Dynamic Value Endorsement, which is Ergon's patented technology that enables dynamic whitelisting of permitted variables within API interactions.

Since our last review, Ergon has added multiple new capabilities to the platform. Notably, support for GraphQL has been recently introduced along with Anomaly Shield, a sophisticated machine learning engine for security analytics. A fully managed SaaS implementation of the Airlock platform is now available as well.

Unfortunately, Ergon is still fairly unknown outside its home market, as the company has only recently started its expansion to other geographies like the Middle East. However, the company's lean and well-integrated product can be recommended for evaluation by any organization looking for an all-in-one solution for enforcing sensitive data protection across multiple channels, beyond just APIs.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	strong positive



Table 4: Airlock's rating

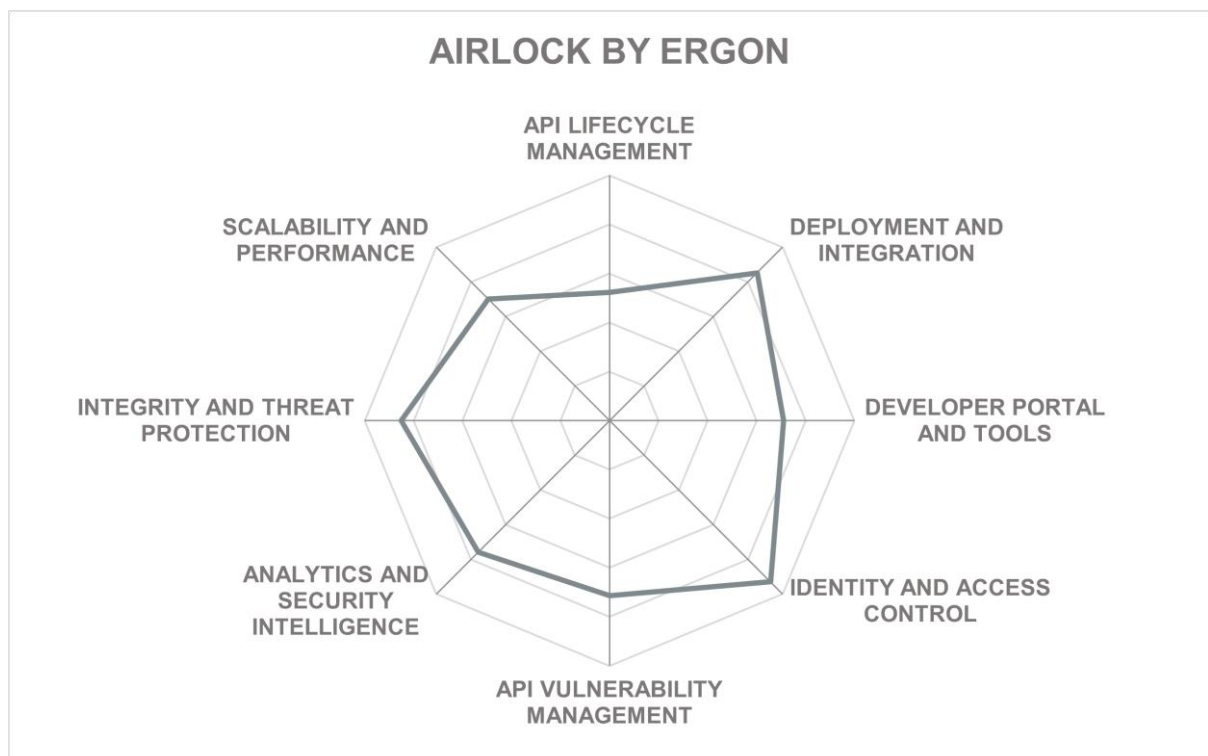
Strengths

- Fully integrated platform for securing access management across web apps and APIs.
- Support for modern containerized architectures.
- Built-in fraud prevention, application, and mobile security functions.
- Secure by default architecture protects from zero-day exploits.
- Dynamic Value Endorsement for data validation without API contracts.
- Comprehensive machine learning capabilities for identifying behavioral anomalies.

Challenges

- API monitoring and management capabilities are limited.
- No public-facing developer portal is available yet.
- Small but growing partner ecosystem and global market presence.

Leader in



Akamai – App & API Protector, API Security, API Gateway

Akamai Technologies is a content delivery network and cloud service provider headquartered in Cambridge, MA. Founded in 1998, the company is one of the veteran players on the market, providing a broad range of performance-, security- and even productivity-related services through their content delivery network (CDN), one of the world's largest distributed edge and cloud platforms with over 4100 points of presence in more than 130 countries.

Over the last two decades, Akamai's platform has evolved into a full-featured Intelligent Connected Cloud Platform that not just competes with established cloud providers in multiple areas like web and mobile application delivery, enterprise security, and strategic services, but in fact complements them with a unified layer of defense capabilities.

Although Akamai's Edge Platform has been offering comprehensive security capabilities for years, including a Web Application Firewall, Bot protection, and DDoS protection, until recently, it was unable to offer comprehensive coverage of such crucial areas as API discovery, vulnerability assessment and abuse prevention. However, with the recent acquisition of Neosec, Akamai has augmented its API security portfolio with comprehensive API security analytics capabilities.

Akamai App & API Protector (AAP) is still the company's core application security offering that harnesses the power and scale of the underlying security cloud to discover and analyze API traffic and use threat intelligence and machine learning to block external threats. An API gateway is also offered, providing capabilities like authentication and authorization, rate limiting, etc.

These "traditional" functions are now complemented by the XDR-style security analytics technology developed by Neosec. Cloud-native and fully managed, the Akamai API Security platform provides true behavioral analytics on top of a security data lake, powering discovery, classification, vulnerability assessment, investigation, and threat hunting capabilities. This solution extends API security coverage to third-party and shadow APIs not hosted on the Akamai platform.

Together, these two solutions aim to provide comprehensive coverage for all aspects of API security including but not limited to the OWASP API Top 10 with the long-term goal of combining them into a single unified platform. Although the products are kept separate by design to avoid vendor lock-in, Akamai now offers a native connector that integrates API security directly with the Akamai Cloud with a press of a button, providing full visibility and automated response integrations with the rest of Akamai's security platform. Shifting left with an API security testing solution is another candidate for future integration.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	positive



Table 5: Akamai's rating

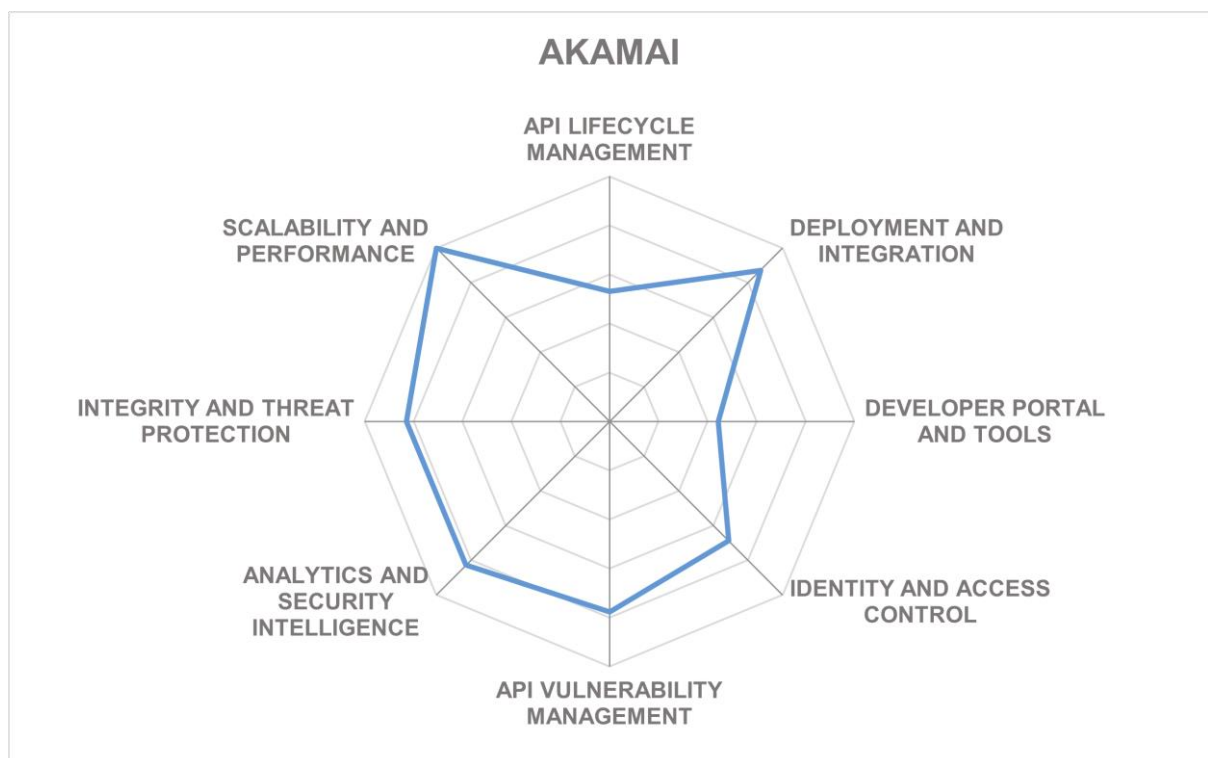
Strengths

- Massive-scale global edge platform enables unprecedented scalability and performance.
- Combines API management, proactive security controls, and reactive monitoring and investigation capabilities with a native connector architecture.
- Comprehensive ML-powered adaptive security engine maps behavioral anomalies to known malicious activities and business risks.
- Security data lake for XDR-like threat hunting and investigations.
- Managed threat hunting services are offered for customers.
- Local API testing to improve developer experience and efficiency.

Challenges

- AAP and API Security solutions are separated, no common UI is offered.
- By design, only offered as a SaaS solution.
- API security testing is not yet integrated with the rest of the suite.

Leader in



Axway – Amplify API Management Platform

Axway, founded in 2001, is a global software company headquartered in Scottsdale, Arizona, USA. The company offers a broad portfolio of solutions for securing organizations' protected resources and extending their operations into the cloud. With the acquisition of Vordel in 2012, Axway has become one of the strong players in the API Management market as well.

Axway Amplify API Management Platform centralizes the discovery and lifecycle management of distributed enterprise APIs across multiple gateways, asset types, patterns, and deployments to facilitate faster innovation and improved business efficiency.

API Lifecycle Management is one of the key components of the company's platform. Amplify API Management Platform comprises the following products: API Gateway for managing and enforcing security and governance policies on a broad range of API protocols; Amplify Enterprise Marketplace and API Portal to enable collaborative, multi-vendor and multi-pattern API provider and API consumer experiences; Amplify Integration and API Builder – graphical low-code tools for SaaS integration and API orchestration; Amplify Analytics – configurable dashboards for API health and usage, as well as consumer engagement monitoring.

A major focus is on automated discovery of all types of programming interfaces across heterogeneous IT environments, including unmanaged APIs. With Axway's integration platform, customers can have full visibility and control not just over REST APIs, but any kind of data exchange internally or externally, thus offering an efficient alternative to shadow IT.

As a part of the company's overall hybrid integration portfolio, Axway Amplify API Management Platform offers a robust set of capabilities for nearly every stage of API lifecycle and can support even the largest enterprise customers with long-term integration strategies going beyond just APIs.

Among notable recent additions to the platform is the Amplify Enterprise Marketplace – a centralized place to curate and monetize all corporate APIs across multiple environments. With discovery, productization, analytics, and security capabilities, it provides a single pane of glass for all API resources.

Amplify Integration, based on the recent DXchange.io acquisition, is another new solution that provides a no-code visual environment for connecting and orchestrating APIs, applications, data sources and other systems accessible even for non-technical users.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



Table 6: Axway's rating

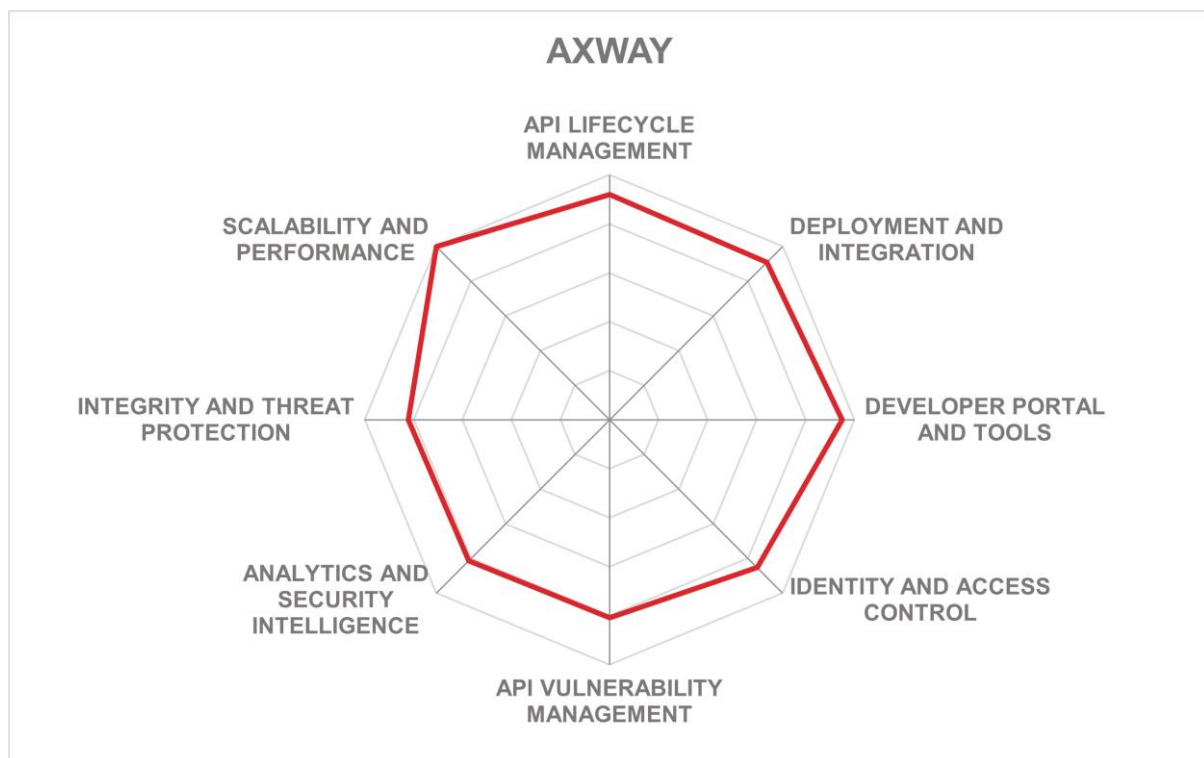
Strengths

- Multiple gateway types (Axway and third-party), including support for microservices and cloud deployments - with a centralized management plane.
- Broad range of supported API standards: REST, SOAP, GraphQL, gRPC, and AsyncAPI.
- Automated discovery of all API types across heterogeneous environments.
- Built-in enterprise marketplace for productization and consumption of APIs.
- Includes a cloud-native integration platform for no-code orchestration and mapping of data flows beyond just APIs.

Challenges

- Targeted primarily towards large enterprise customers, might be too complex for smaller companies.
- Advanced security analytics is only available with third-party tool integrations, but their open approach provides best-of-breed integrations.
- The built-in API firewall is limited, based on open-source code.

Leader in



Broadcom – Layer7 API Management

The Layer7 brand dates back to 2002, when Layer7 Technologies, one of the pioneering API management vendors was founded in Vancouver, Canada. Over the next decade, the company has been providing both on-premises and cloud-agnostic API management solutions to hundreds of enterprise customers.

Since late 2018, Layer 7 is a brand in the portfolio of Broadcom, an American manufacturer of semiconductor and infrastructure software products, belonging to the Identity Security division of Broadcom Software. Layer7 API Management is closely tied to Broadcom's security and DevOps portfolio products such as IAM, PAM, risk analytics, Continuous Testing, Automation, and AIOps.

Within Broadcom, the Layer7 brand now represents the new unified approach towards integration and security for the whole digital infrastructure of a large modern enterprise, with a stronger focus on business-relevant areas such as cyber risk management, digital transformation, or privacy protection rather than individual technology stacks.

The company's entire API management and security portfolio is offered as a single SKU as well as standalone solutions. The solution uses a Continuous API Management model, which is the evolution of the full lifecycle management approach. This single offering replaces hundreds of former SKUs and provides a full range of API development, testing, discovery, management, and monitoring, as well as security capabilities across on-premises, multi-cloud, containerized, and mobile environments. Broadcom's API Academy offers the only industry-agnostic, free API certification program with multiple courses and exams.

The integration of Layer7 API Management with the Broadcom AuthHub also provides greater flexibility in authentication models used as part of the Layer7 OAuth Toolkit. This integration provides the ability for the solution to support advanced authentication concepts such biometric and passwordless authentication leveraging FIDO, YubiKey, as well as risk-based authentication.

Broadcom's API Management portfolio provides a complete solution for practically all API management scenarios imaginable, with a strong focus on enterprise-scale business-driven integration projects, thus making it particularly suitable for large enterprise customers with long-term API strategies.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



Table 7: Broadcom's rating

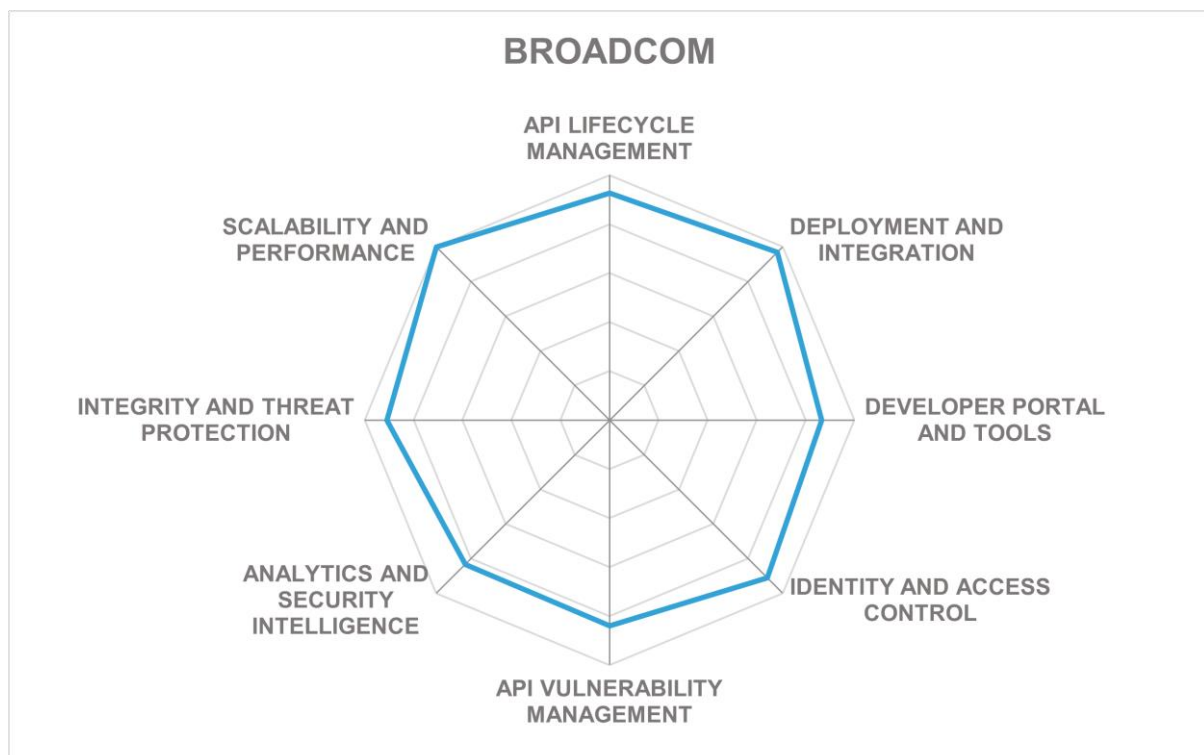
Strengths

- Full range of management tools for API lifecycle management and microservices.
- Part of a larger integrated portfolio of identity, risk management, and security products.
- Unified deployment model for all supported environments.
- Advanced security capabilities through Intelligent automation.
- OpenTelemetry support simplifies third-party observability tool integrations.
- Industry-agnostic API certification program.

Challenges

- Targeted primarily towards large enterprise customers, smaller companies are better served through Broadcom's partner network.
- Advanced API monitoring and analytics relies on additional Broadcom products or requires a third-party tool integration.
- Lack of a single consistent UI across all parts of the platform.

Leader in



Cequence Security – Unified API Protection

Cequence Security is a cybersecurity company headquartered in Sunnyvale, California. Founded in 2015 by a group of security industry veterans, the company focuses on developing a unified ML-based Application Security Platform. This cloud-native, containerized platform powers several security products ranging from web and mobile app protection to API inventory, monitoring, compliance, and risk assessment.

Since the last Leadership Compass, Cequence released its Unified API Protection (UAP) platform which unifies discovery, compliance, and protection across all internal and external APIs to defend against fraud, business logic attacks, exploits and unintended data leakage. A significant increase in scope, the solution is a foundation for their API Spyder, API Sentinel, and API Spartan products setting Cequence apart from other vendors by offering an integrated platform covering the entire API lifecycle.

The core technology that powers the Cequence platform is CQAI – a patented machine learning-based analytics engine that processes the transactional data collected by the platform sensors to discover, analyze, and monitor web, mobile, and API-based applications. By maintaining behavior profiles and fingerprints of each application or API transaction, the platform can then analyze each transaction to identify not just known malicious actions, but anomalies and other suspicious activities as well.

API Sentinel is the company's specialized API security posture management product, a cloud-native, easily deployable solution for performing real-time API inventory and usage analysis, detection of OpenAPI specification non-conformance, and risk assessment according to multiple metrics and policies, helping identify and mitigate API security risks before they turn into data breaches. Thanks to its flexible container-based architecture and breadth of technology integrations, API Sentinel can mix and match both edge and microservice-oriented deployment scenarios.

API Spartan protects APIs in real time from malicious automated attacks that exploit vulnerabilities and enable business logic abuse that can result in fraud or data loss. API Spartan prevents attacks passively or natively inline and requires no JavaScript, Mobile SDK, or web application firewall (WAF) integration. Together with the company's other solutions, Cequence Security can offer its customers a comprehensive, well-integrated platform for addressing API risks at multiple stages of their lifecycles.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	strong positive



Table 8: Cequence Security's rating

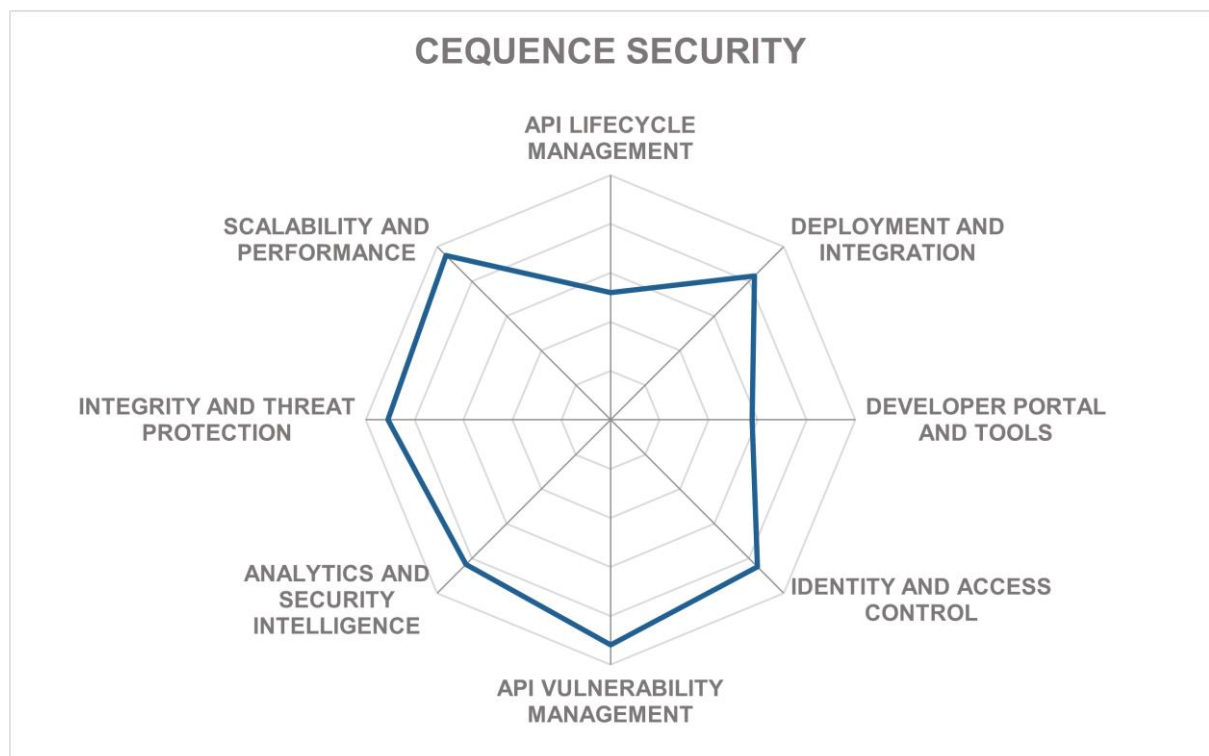
Strengths

- Integrated application security platform powered by purpose-built AI-driven analytics engine.
- Automated API inventory simplifies management and creation of policies.
- Inline deployment enables instant blocking of detected threats.
- Real-time API risk assessment with sensitive data leakage discovery and configurable, extensible risk modeling.
- Built-in generative AI and NLP-based capabilities to increase productivity.
- API attack surface discovery and management capabilities.

Challenges

- Out-of-the-box risk categorization is limited to OWASP, can be extended by customers.
- Customer base is still primarily limited to North America, expanding to Europe and APAC.
- Sell-through motion with partners is relatively new, but getting attention from a growing number of VARs

Leader in



Cerbos

Cerbos is an open-source software vendor focusing on adaptive authorization management. Founded in 2021, the company comprises a highly distributed engineering and management team, while being officially headquartered in London, UK. Since inception, Cerbos has been focusing on developing an open source, language-agnostic dynamic authorization solution that can be integrated into any application with a shallow learning curve.

The company's first product is the open source, off-the-shelf authorization platform that can be deployed in a variety of ways (from bare metal to containers to serverless), supports a broad range of APIs, SDKs and other integrations and can be up and running in minutes. The solution has no external dependencies and is completely agnostic towards existing identity providers or context attribute sources, making it extremely lean and performant.

A YAML-based policy language allows for flexible definition of principal and resource policies, complex conditions, policy inheritance, and versioning to support the GitOps development methodology. Cerbos also includes a sandboxed policy playground and IDE integrations to enable interactive policy development and testing.

As opposed to other projects with similar goals, the solution strongly advocates a stateless approach – it does not implement any integrations with external data sources, delegating this to application developers instead. This ensures constant low latency and seamless scalability in any environment. Using Google's Common Expression Language, it is possible to implement sophisticated logic directly within policies, removing the need to include it into apps themselves. The policy engine also provides a full trace of every decision and why it was made.

The core technology is entirely open source with a strong community. The company is also open to users' questions and requests. The company's business model, however, is to offer a managed cloud environment to make policy deployment, management, and execution even simpler. Cerbos Hub offers a convenient GUI for centralized policy authoring, testing, and analytics. The product is currently available as a closed beta with a waiting list.

In the end, Cerbos is an example of a vendor that only solves one specific problem but does it exceptionally well. The platform's high-performance, low-latency stateless implementation makes it especially suitable for securing access to business-critical APIs, but, of course, it can be used for a variety of other application development scenarios. On the other hand, Cerbos cannot be considered a full-featured API management or security tool, so you should not compare it directly to other solutions mentioned in this report. Still, if you're looking for a universal solution for your API authorization needs, it definitely deserves your consideration.

Security	positive
Functionality	neutral
Deployment	strong positive
Interoperability	positive
Usability	neutral



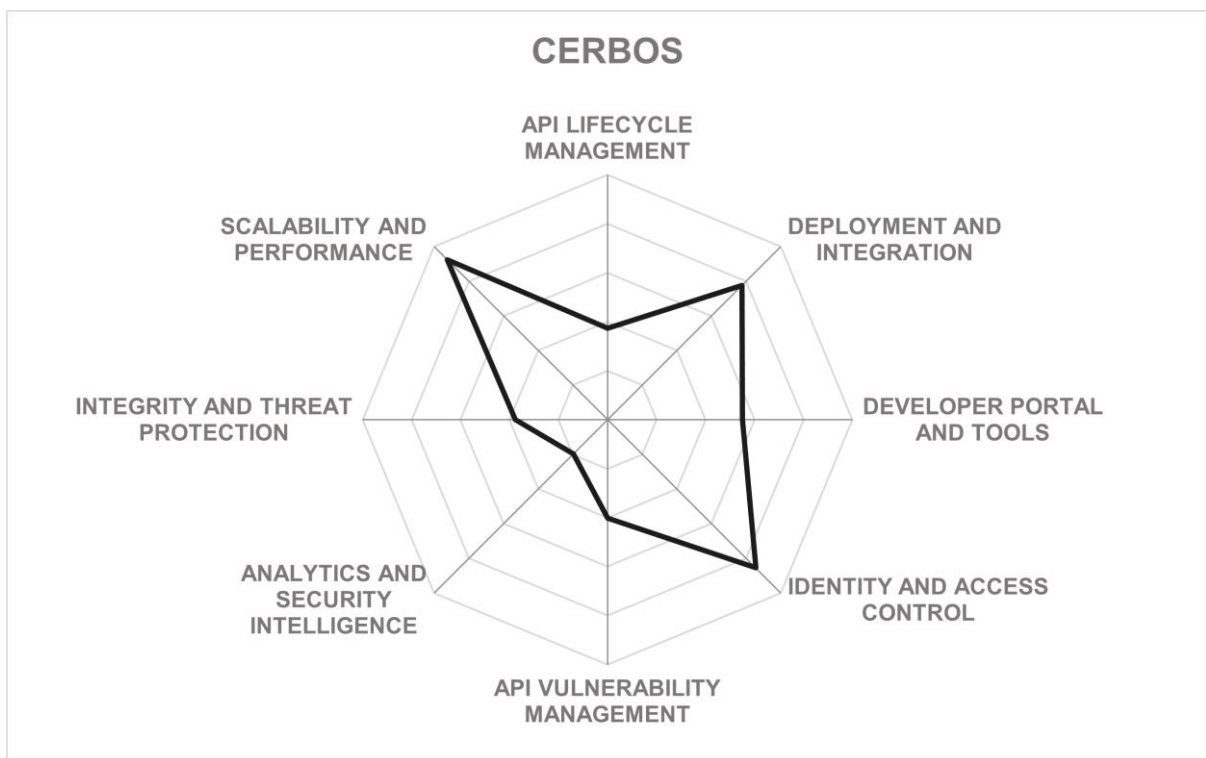
Table 9: Cerbos's rating

Strengths

- Highly scalable, low-latency stateless architecture with a broad range of supported deployment options fit for any application.
- REST and gRPC APIs with SDKs for major languages and development frameworks.
- YAML-based policy language allows expressing complex business logic in an agnostic manner.
- Policy playground and IDE integrations make the solution developer-friendly.
- Open-source codebase with a strong global community.
- Commercial cloud-native offering is available (currently in closed beta).

Challenges

- Solution is only limited to solving authorization needs.
- Stateless architecture forces developers to provide all authorization context data manually.
- Centralized management and other advanced and convenience features are only available in the commercial cloud offering.



Cloudentity

Cloudentity is a privately held identity and access management company founded in 2016 and headquartered in Seattle, WA. In 2021, the company introduced its SaaS CIAM platform referred to simply as “Cloudentity”. This platform is a cloud-native identity, authorization, and consent solution designed to meet the demands of hybrid-cloud services and complex partner ecosystems. Cloudentity focuses on dynamic authorization and authorization as code to secure APIs, microservices, and traditional application workloads.

Cloudentity’s platform provides a broad range of identity and API security services including automated granular authorization and consent capabilities that can be used to secure any application architecture but that excel in hybrid and microservice architectures due to their modern approach. It implements capabilities like fine-grained authorization, API discovery, automated service identity, transactional step-up authentication, privacy/consent management, transactional sessions, data normalization, and data lineage, delegated B2B access control and governance; seamlessly integrating identity providers and externalizing identity and authorization for APIs.

Cloudentity provides a centralized OAuth authorization server and administrative control point along with API discovery and authorization policy decision points deployed at or near the service edges, API endpoints, and workloads that need to be secured. With this approach, traditional perimeter security controls like firewalls or API gateways are replaced with distributed service-level controls for traditional applications, containerized services, embedded devices, and so on, all of which rely on Cloudentity’s ML-based identity/authorization to suggest and apply fine-grained authorization, consent, and entitlement policies uniformly across them.

A major recent development at Cloudentity is achieving full compliance with the FAPI 2.0 security profile (only one of two vendors to reach this milestone so far). This makes the company’s solution especially interesting for highly regulated financial institutions and for organizations looking to level-up their API security standards. Although Cloudentity’s authorization platform is technically not an API management or security solution in a traditional sense, broad its next-generation approach uniformly ties rich authorization and consent policies to API endpoints, significantly reducing the overall complexity of both legacy and modern applications that rely heavily on APIs to exchange sensitive data across hybrid IT environments.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



Table 10: Cloudentity’s rating

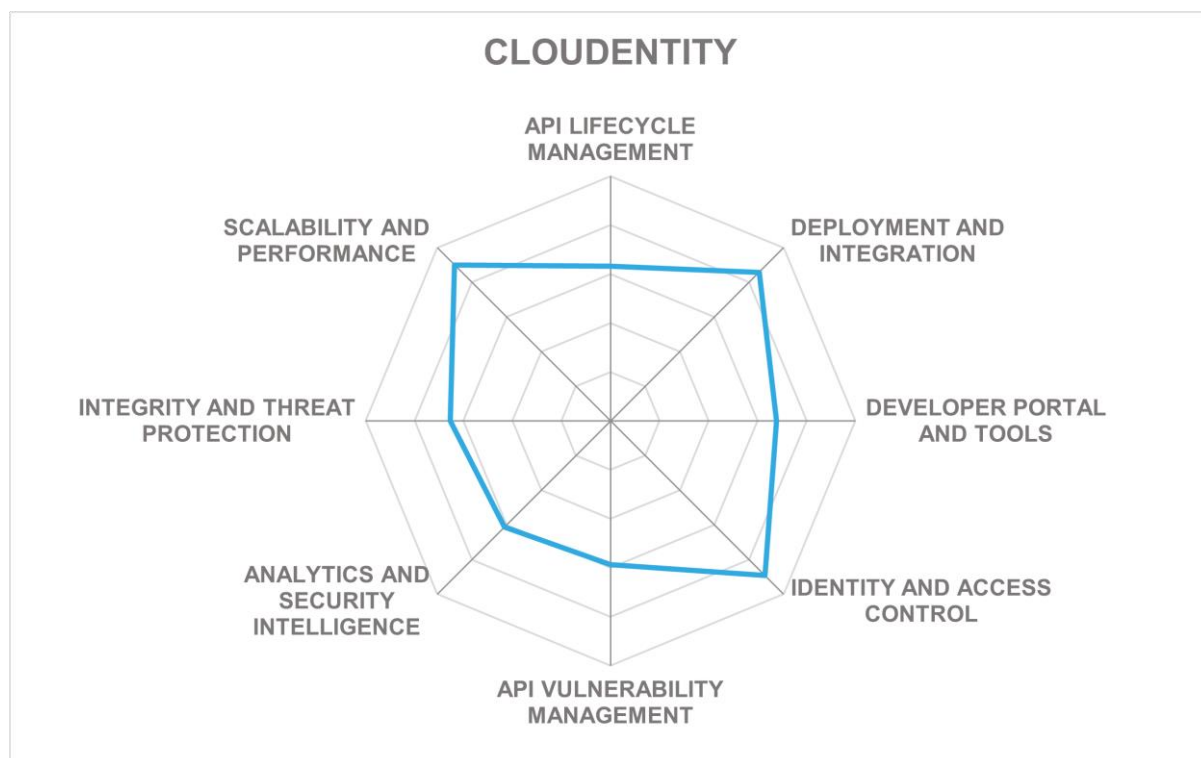
Strengths

- Securely connects APIs to data with fine-grained authorization, consent, and governance.
- Microperimeter security approach pushes policy decision and consent validation to the API edge.
- Broad range of modern and legacy workloads supported across hybrid and cloud infrastructure.
- SPIFFE standard support for unique service identities.
- Data lineage, classification, and governance of usage by API.
- Enables delegated access control for B2B CIAM use-cases which are common in partner ecosystems and supply chains.

Challenges

- Not an API security solution in the traditional sense, focusing primarily on identity and authorization.
- Features are more targeted towards modern cloud-native architectures, less suitable for “legacy” APIs.
- Medium size customer base without the broad reach of large companies.

Leader in



Cloudflare – API Gateway

Cloudflare is a leading Content Delivery Network (CDN) and provider of network security services. Founded in 2009, the company is headquartered in San Francisco, CA. Cloudflare is primarily known for its global security edge infrastructure that is present in over 300 cities worldwide to provide low-latency access for over 95% of the internet population. It has been estimated that nearly a quarter of websites worldwide rely on Cloudflare for network and web security services with over 140 billion threats blocked daily.

According to recent reports, 58% of all data handled by Cloudflare is API traffic. Given that a cloud-scale web application firewall (WAF) has been a core capability of Cloudflare for years and that the company has been expanding into other areas like Zero Trust and the serverless Workers platform for some time, it was only expected that it will foray into API management and security as well. Last year, Cloudflare launched its API Gateway as a standalone product currently exclusively available to its enterprise plan customers, with the long-term goal of developing a complete API lifecycle management solution.

In the new product, Cloudflare is reusing many of its existing capabilities, including the range of inline web security controls, the data loss prevention features previously available in the Zero Trust suite, and Workers to implement bespoke content processing for APIs. Since Cloudflare already has full visibility into customers' traffic for onboarded resources, it can offer efficient multi-level content inspection, consolidated management and analytics, and ML models trained across all customers.

Cloudflare's platform allows for effortless shadow API discovery, automated schema learning and validation based on traffic, and volumetric and sequential abuse detection. However, these capabilities cannot yet be extended to private APIs not served through the Cloudflare platform – this is still planned for future releases.

Currently, the API Gateway offers various security analytics, detection and mitigation capabilities, basic API management capabilities (such as inventory management), and JWT authentication. Notably, the product already supports basic GraphQL protection, with more features coming in the next release. However, other capabilities like classification, risk assessment, more complex authorization scenarios, or developer features are still rudimentary at best.

With Cloudflare's existing strengths in mind, its API security product definitely looks promising, and we will continue closely following its future developments. However, in its current form the product is only suitable for a limited range of scenarios and might be interesting primarily for early adopters looking for massive enterprise-grade scalability.

Security	positive
Functionality	neutral
Deployment	strong positive
Interoperability	positive
Usability	positive



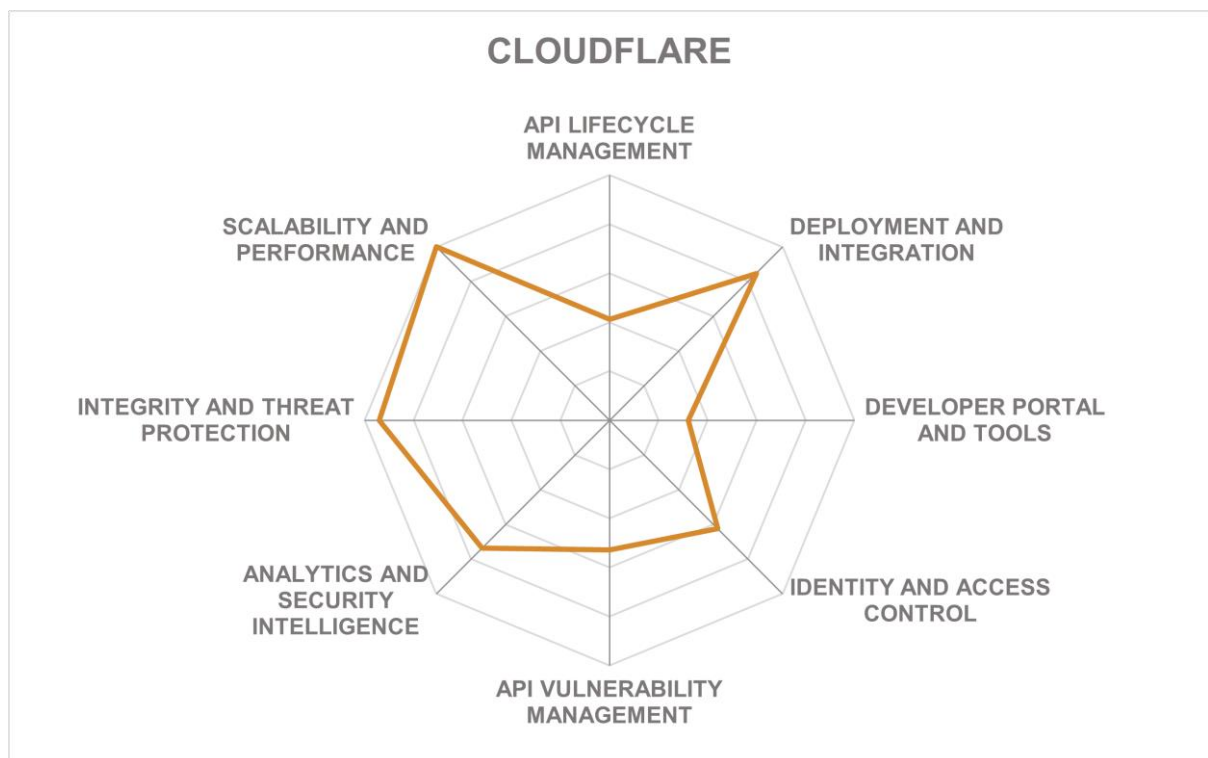
Table 11: Cloudflare's rating

Strengths

- Large globally distributed edge presence, sophisticated traffic acceleration with massive backbone capacity.
- Single processing pipeline that combines multiple access management, security, and analytics functions.
- Transparent deployment and enforcement for resources already exposed through Cloudflare.
- Comprehensive machine learning capabilities with recommendations that can be promoted to rules.
- Basic support for GraphQL security is already implemented, will be expanded soon.

Challenges

- API Gateway is currently only available with the Enterprise plan, severely limiting its visibility to customers.
- Currently does not work with private APIs not onboarded to Cloudflare.
- Several UI shortcomings limit usability, especially for large API inventories.



Curity – Identity Server

Curity is a provider of API-driven identity management solutions based in Stockholm, Sweden. Launched in 2015, the company is focusing on providing identity services for APIs and microservices and removing the complexity by externalizing and centralizing access control across any API.

Using the Curity Identity Server, the company's flagship product, organizations can secure their digital services in configuration and not in code, thus reducing the complexity of development and maintenance.

The Curity Identity Server is a modern solution designed for OAuth 2, OpenID Connect, and SCIM to provide a modern platform for identity and access management for internal and external users and to make it easy to manage very large deployments servicing millions of users. It is composed of three major modules: Authentication Service, Token Service, and User Management Service. The authentication service provides a flexible framework of strong, flexible, multifactor authentication methods, Single Sign-On, and user orchestration workflows.

The fundamental integration point for app and API security is the token service: it implements highly customizable token management, along with scopes, claims, and policies. Using the Curity platform together with an existing API gateway provides a solution to enforce access control centrally on any API, not just standard-aware ones.

A major new feature implemented by Curity is their Hypermedia Authentication API, which allows for the creation of native clients that use OAuth and OpenID Connect flows without relying on a web browser. Thanks to the provided native SDKs, complex authentication scenarios can be implemented without an intermediary user agent, providing a smooth user experience and elevated security using client attestation mechanisms. Among other recent developments at Curity, it's worth mentioning support for decentralized identities and numerous improvements in the DevOps dashboard.

The Curity Identity Server is not an API management solution per se but a component of one. Identity and flexible fine-grained access management are the cornerstones of securing APIs that expose sensitive information. The company provides a reference architecture that combines its identity server with an existing API management product that implements simple and scalable data and privacy protection for API endpoints.

Security	strong positive
Functionality	positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



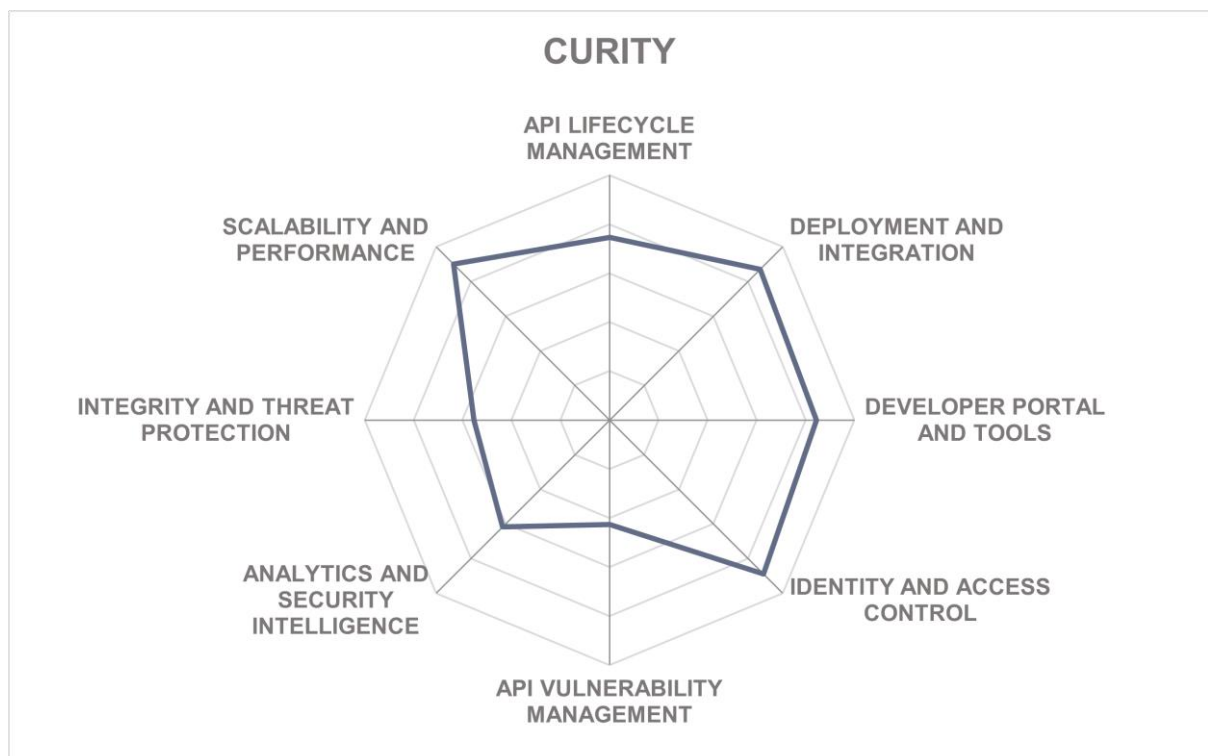
Table 12: Curity's rating

Strengths

- Comprehensive support for OAuth and OIDC open standards.
- Combines flexible authentication with token-based API security controls.
- Hypermedia Authentication API for native clients.
- Comprehensive Open Banking compliance.
- Reference “phantom token” architecture for privacy protection.

Challenges

- Not an API security solution in the traditional sense, focusing only on identity and access management.
- Limited risk engine capabilities.
- Relatively small market presence outside of Europe and the Middle East.



Data Theorem – API Secure

Data Theorem is a company specializing in application security solutions. Founded in 2013 and based in Palo Alto, CA, the company offers a range of automated managed security services for developers of mobile applications and APIs. At the core of the company's entire portfolio is its Analyzer Engine that performs continuous scanning of application vulnerabilities. Through a large ecosystem of technology partners, Data Theorem offers a portfolio of SaaS agentless solutions for mobile, web, API, cloud, and supply chain security.

API Secure, the company's dedicated API solution, is designed to maintain a dynamic inventory of all customer's APIs, perform vulnerability assessments of each one, and remediate security issues within the CI pipeline. The company views API security as an integral part of software supply chain risk management and thus focuses on covering 3rd party APIs as a risk that traditional SCA solutions fail to address.

The product offers a multitude of methods for discovering APIs across various environments, from probing customer's public infrastructure to reverse-engineering web and mobile apps and code analysis to connecting to cloud accounts, CI/CD pipelines, etc. The consolidated API inventory is constantly updated and classified according to multiple criteria like location, purpose, PII exposure, usage, etc. Newly discovered or changed shadow APIs will generate instant alerts.

The analyzer engine performs continuous security testing of each API (using common techniques utilized by hackers) to identify vulnerabilities and exploits, authentication issues, data leaks, compliance challenges and other issues. Customers can use the platform UI at any time to drill through the findings or to generate various reports. However, the primary goal of the solution is to provide active protection automatically.

Data Theorem maintains a large partner ecosystem that not only includes resellers and integrators, but a broad range of technology partnerships with API gateways vendors, cloud platforms, CI/CD solutions, Infrastructure-as-Code operators, WAAP vendors, etc. These integrations enable rich automation capabilities that free security analysts to focus on more creative tasks than responding to each security event manually. Integrating with CI/CD vendors allows for fixing security issues during development, preventing them from migrating to production.

Active protection capabilities include authentication, authorization, enforcement of encryption, common attack prevention, bot and DoS protection and specialized security controls for serverless functions in AWS and GCP.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	positive
Usability	strong positive

datatheorem

Table 13: Data Theorem's rating

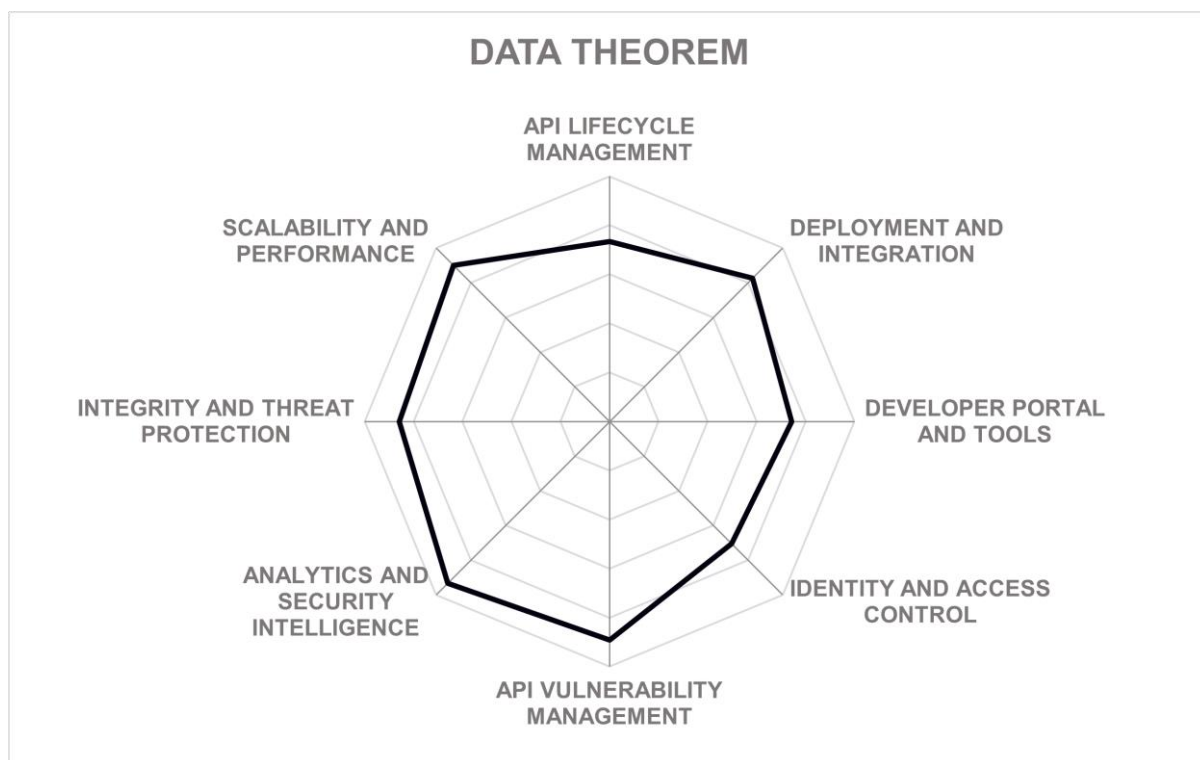
Strengths

- Integral part of a unified application security portfolio designed around a common analyzer engine.
- Comprehensive web app and API discovery capabilities without manual intervention.
- Rich compliance reporting functionality supporting PCI, GDPR, CCPA, HIPAA, OWASP, MITRE, etc.
- Active protection allows for automating response to identified threats either directly or through third-party integrations (CDNs, Infrastructure-as-a-Service operators, API gateways, etc.)
- Supports all major API formats (REST, GraphQL, gRPC, SOAP).
- Strong partner ecosystem, integrations with most major API, WAAP, WAF vendors.

Challenges

- New API UX management workflow is currently being implemented across the entire portfolio, expected to be complete in early 2024.
- Limited market presence outside of North America.
- User interface is not yet consistent across all products.

Leader in



ForAllSecure – Mayhem

ForAllSecure is a cybersecurity company founded in 2012 by a team of security researchers from Carnegie Mellon University. It is headquartered in Pittsburgh, PA. The company's vision is to approach application security testing from the perspective of a real hacker and focus on identifying only real exploitable risks instead of overwhelming developers with too many irrelevant findings.

ForAllSecure's flagship product is Mayhem, a developer-first application and API security testing solution. Mayhem focuses on finding and prioritizing only the risks that can be exploitable by attackers and does not just show the existence of a vulnerability, but also an explanation on how it can be exploited and how to fix it promptly.

For that purpose, the solution combines a multitude of traditional hackers' techniques like fuzzing with symbolic execution and machine learning to perform the testing, but it goes beyond that in several ways. First, it also relies on automation to generate and run thousands of tests, providing much broader coverage than traditional tools.


On the other hand, similar to modern analytics solutions in other areas of cybersecurity, Mayhem relies on ML to filter out the false positives, irrelevant findings, and other noise to reduce the number of results to a usable and immediately actionable minimum. It will also continue to self-learn from earlier findings and improve future tests. Each finding is enriched with additional information like CWE, OWASP, etc., aggregated by a multitude of criteria according to customer's needs, deduplicated, and ranked by risk scores.

This ensures that, compared to other testing solutions, developers only receive a handful of findings instead of thousands of useless alerts, and yet, these findings are limited to real, exploitable risks. Each defect can be automatically tracked in a ticketing system, with the ticket status updated on the fly as soon as the problem is resolved.

With such a dramatic contrast to traditional vulnerability scanners, a major concern can be identified: how can the vendor prove that a small number of findings still provides sufficient coverage as opposed to a much longer list generated by a competing product? This is indeed a major area for Mayhem's future development – the ability to explain, match, and compare findings with 3rd party tools.

The company places a strong emphasis on automated integrations with CI/CD pipelines, complex infrastructure, and external tools. Unfortunately, currently this is somewhat done at the expense of the platform UI – in the future releases, we expect to see more sophisticated reporting tools, including the possibility to directly produce compliance reports.

Security	positive
Functionality	positive
Deployment	positive
Interoperability	positive
Usability	positive



ForAllSecure

Table 14: ForAllSecure's rating

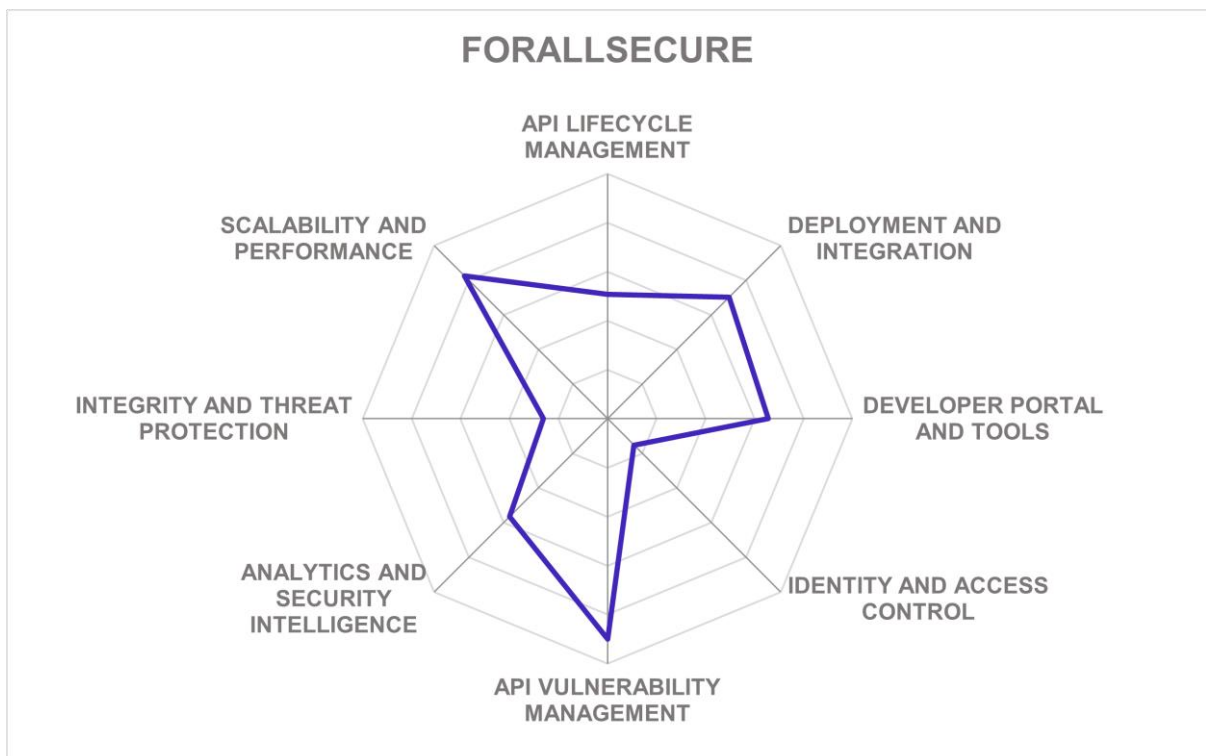
Strengths

- Innovative approach to code and API security testing that focuses only on proven, exploitable risks.
- Flexible containerized architecture suitable for large-scale, hybrid, or even air-gapped deployments for highly regulated enterprises.
- High degree of intelligent automation at every stage of the DevOps pipeline.
- Hundreds of integrations, languages, and frameworks natively supported.
- Findings come with risk scores, exploitability analysis, actionable guidelines for fixing.

Challenges

- The solution only focuses on security testing; no other functionality is included.
- It can be difficult to explain to customers how a low number of findings still provides sufficient coverage.
- Limited reporting and compliance capabilities.

Leader in



Forum Systems – Forum Sentry

Forum Systems is a privately held independent engineering company based in Needham, MA. Founded in 2001, the company provides gateway-based solutions for API and cloud security. Since the very beginning, the company offers mission-critical large-scale solutions with a heavy emphasis on “security by design”.

Forum Sentry API Security Gateway is the only product on the market where security forms an integral foundation of the architecture and was not added later as an afterthought. The solution is unique in its approach towards security by not allowing any third-party extensions or libraries, which ensures resilience against known and not yet discovered vulnerabilities. While still maintaining a strong focus on API security, the company has significantly updated and expanded its product portfolio.

The flagship gateway is available in multiple form factors – from traditional hard appliances to virtualized images that can be deployed on-premises or in any cloud, as well as containers for deployment into Kubernetes clusters. Native images for Azure and AWS cloud deployments are provided, to say nothing about the next-generation hardware platform for physical deployments, delivering 10x faster throughput and integrated HSM modules.

With over 100 new features since our last review, Forum Systems continues to expand the functionality of the gateway to address the changing technological landscape and customer demands. Notably, it continued to expand the range of available form factors, now supporting generic and hardened containerized deployments, a fully encapsulated virtualized rendition of hardware for major public clouds, and additional regions for government customers.

The company’s developer portal solution offers better developer experience and seamless integration with Forum Sentry gateway policies. The policies themselves have been constantly expanded as well, adding support for numerous new protocols and technologies and industry-specific requirements. With support for global variables, it is now possible to build reusable policy artifacts and modernize existing policies more efficiently.

The company’s technology has also been adapted for implementing Zero Trust architectures using Forum Sentry Cyber Secure PEP (Policy Enforcement Points) to enforce secure access policies to sensitive resources. Using a hardened, secure-by-design architecture to implement policy enforcement addresses a critical yet often overlooked challenge of PEPs being the most critical and least protected components of Zero Trust architectures.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	positive



Table 15: Forum Systems’ rating

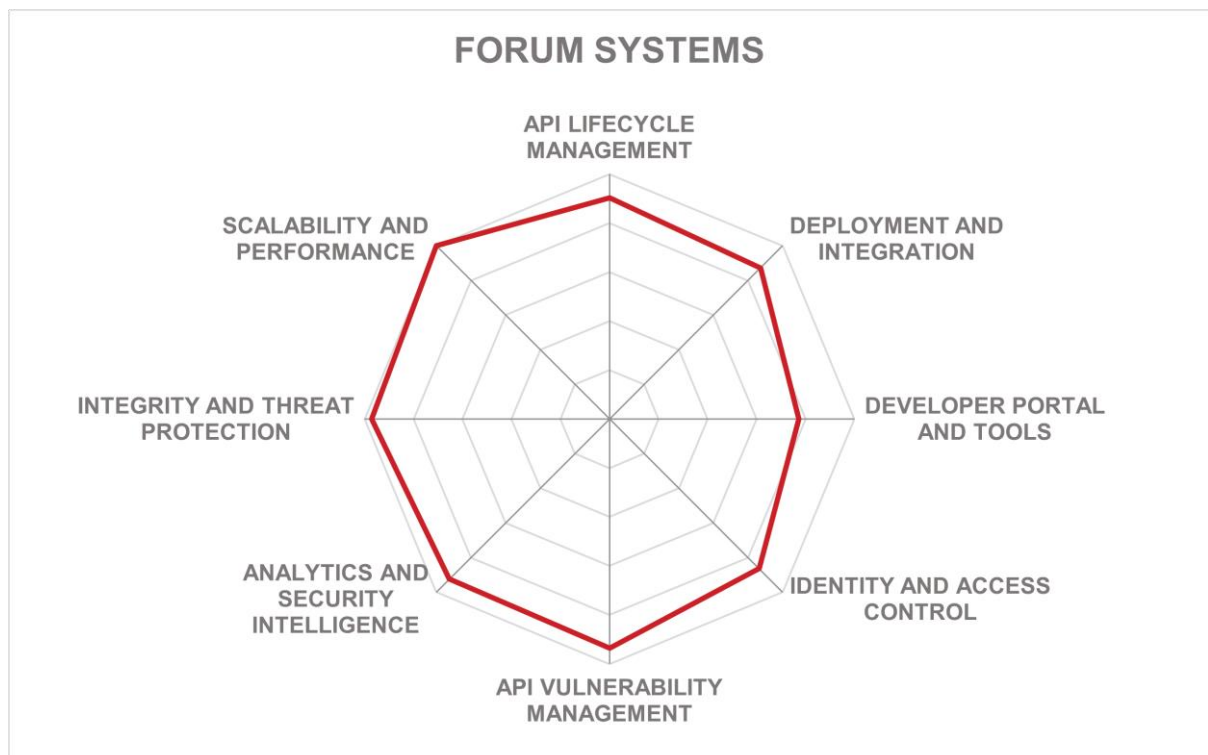
Strengths

- “Security by design” architecture for maximum reliability; FIPS 140-2 and NIAP NDPP-certified.
- Broad range of deployment factors from hardened hardware appliances to fully encapsulated virtual images to containers for microservice architectures.
- Sophisticated and constantly expanded API transformation capabilities.
- Comprehensive API threat protection functionality.
- Supports a broad range of identity and access control standards, tokens, and credentials.
- Significantly expanded choice of deployment and integration scenarios supporting highly regulated and government customers.

Challenges

- No support for modern API protocols like GraphQL or gRPC.
- Behavior analytics is only possible with third-party integrations.
- Inconsistent UIs between different products.

Leader in



Google – Apigee

Apigee is a product offered by Google Cloud, headquartered in Mountain View, CA. Apigee provides a full lifecycle API management solution including advanced security, monetization, and predictive analytics. Apigee was founded in 2004, the company entered the API management market in 2010, and was acquired by Google in 2016. In 2015, Apigee became one of the founding members of the OpenAPI initiative.

Apigee offers public cloud, hybrid, and private cloud deployment options for designing, managing, and analyzing APIs. It comprises a set of API Services for managing, securing, and extending APIs with additional backend functionality; Analytics Services for collecting, analyzing, and reporting on various technical, operational, and billing statistics; Developer Services for building a community around APIs; and Monetization Services for driving new revenue with API products. After the company was acquired by Google, it now offers its services as a part of Google Cloud Platform but continues to provide an on-premises offering as well.

Apigee platform includes every possible capability one expects from such a platform to support end-to-end API management at every stage of the API lifecycle. From API design to publication, productization, and monetization to monitoring and security live endpoints – everything is managed from a single web-based console. Through its adapters for Envoy and Istio service mesh, Apigee seamlessly expands coverage to microservice-based applications as well.

Apigee X is the next generation of the platform tightly integrated with Google's cloud services to deliver enhanced scalability and performance and improved automation powered by machine learning. Most notably, however, Apigee X integrates GCP capabilities like Cloud Armor web application firewall for improved API security and Cloud IAM for more sophisticated authentication and access management for APIs. With this release, Apigee can finally be considered an integral part of the Google Cloud Platform.

With the latest developments in the field of generative AI, Google is adding support for its Duet AI conversational assistant technology across all its products, including Apigee. Now customers can create API specifications by describing them in natural language. Additionally, the Apigee API hub now provides autogenerated recommendations for creating API proxies and integrations, or even create extensions to be deployed to Vertex AI or ChatGPT. API security capabilities are now powered by AI as well, providing automated posture assessment, protection against malicious attacks, as well as recommendations on hardening existing infrastructure against abuse.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



Table 16: Google's rating

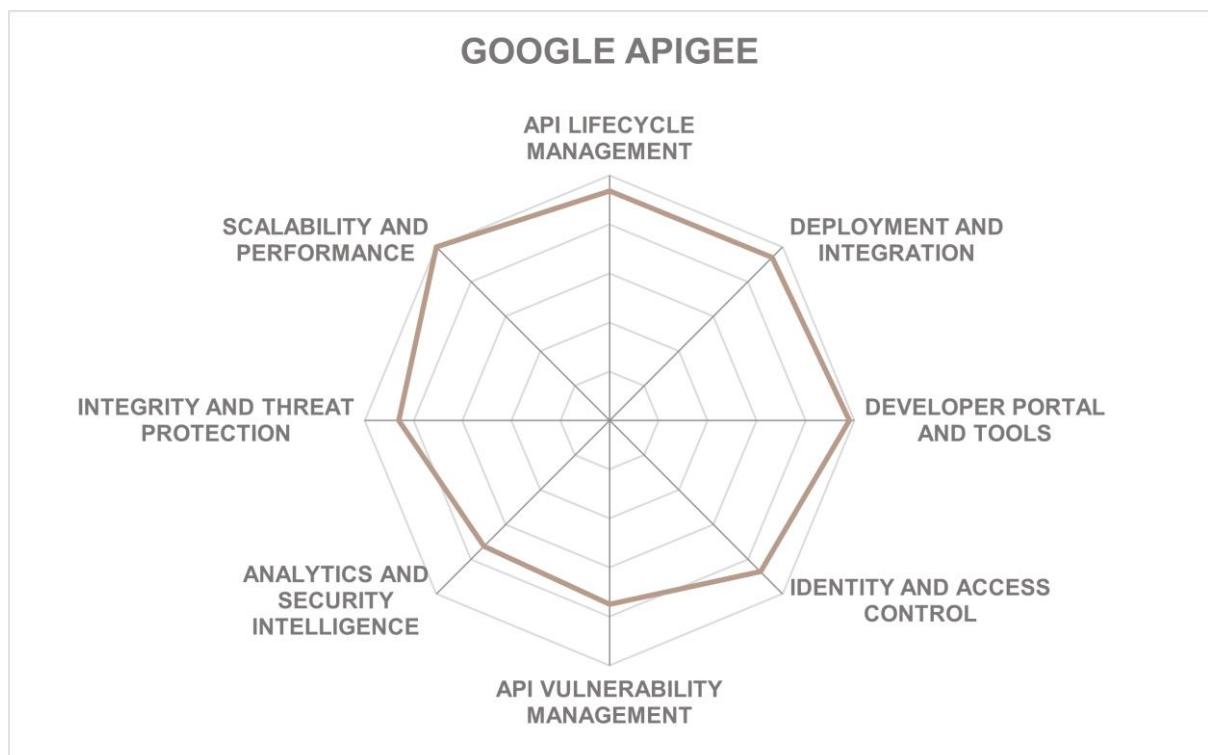
Strengths

- Comprehensive API management platform covering all aspects of the API lifecycle.
- Support for multiple major API standards: REST, gRPC, SOAP, and GraphQL.
- Extended monitoring and analytics with Apigee Sense.
- Deep integration with other Google Cloud services, including web attack and DDoS protection.
- Strong generative AI-based productivity-enhancing capabilities.

Challenges

- Hybrid deployments require additional software, limited to supported Kubernetes platforms.
- Security analytics lacks detailed views, with no focus on forensic investigations.
- No third-party security tool integrations.

Leader in



Gravitee – API Management Platform

Gravitee is a next-generation API management vendor headquartered in Boulder, CO. Originally founded in 2016, the company has a distributed team primarily across France and the United Kingdom. Gravitee was founded as an open-source company and remains a strong contributor to this day, with the vision of developing a new kind of API management platform that unifies synchronous and asynchronous APIs.

Such an approach reflects the current trend that sees the very notion of API expanding from just the REST style to include event-based communications like Kafka or MQTT. The need for unification and standardization across all kinds of APIs for consistent visibility, management, and security is also increasing, especially among enterprise customers with complex hybrid IT landscapes.

Gravitee offers support for both traditional API technologies like SOAP, REST, or GraphQL and event-driven protocols like Websockets, webhooks, or data streaming in a single platform across the entire API lifecycle. The Gravitee platform is available as an open-source Community Edition and commercial Enterprise edition, both comprising the following products:

- Gravitee Cockpit as the multi-tenant central management console,
- Gravitee API Management for managing and securing APIs,
- Gravitee Access Management for secure authentication and authorization needs,
- Gravitee API Designer as a visual self-service API design environment,
- Gravitee Alert Engine to enable multichannel notifications for various events.

The platform supports multiple deployment models from completely on-premises to hybrid to fully managed SaaS (the latter is only available as a commercial option though). There is native support for Kubernetes deployments with the Gravitee Operator and Ingress Controller.

From the security perspective, the platform supports strong authentication, identity federation, and a comprehensive permissions model for fine-grained access management. Basic protection capabilities like traffic shaping are supported but unfortunately, there are no official integrations with third-party security solutions yet.

For API designers and developers, Gravitee offers full lifecycle management with a unified developer portal that supports both OpenAPI and AsyncAPI specifications, full support for API versioning, staging, etc. A powerful visual designer is offered for no-code API specification design – it is currently limited to REST APIs, however (a unified designer is currently in the works).

Security	strong positive
Functionality	strong positive
Deployment	positive
Interoperability	positive
Usability	positive

gravitee.io

Table 17: Gravitee's rating

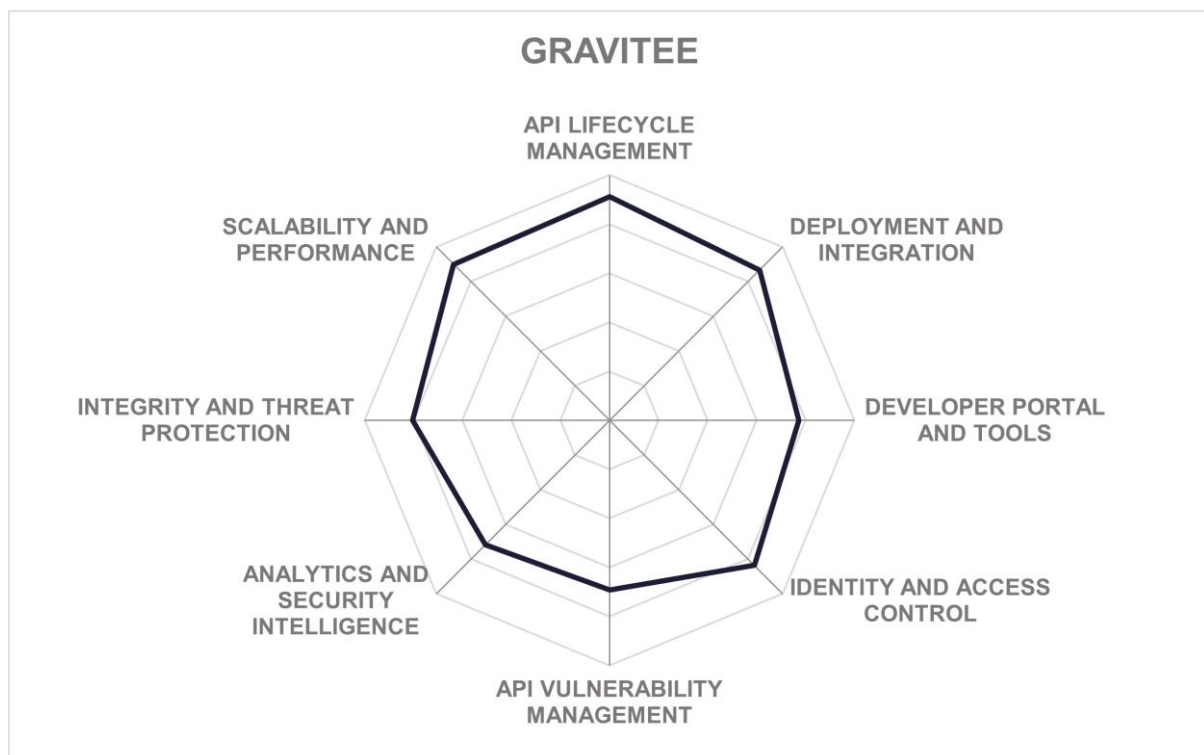
Strengths

- Unified support for synchronous and asynchronous API technologies in a single platform.
- Can expose the same backend as both sync and async APIs.
- Native support for Kubernetes architectures.
- Strong authentication and access management capabilities.
- Visual editors for API design, flow mediation, security settings.
- Open-source codebase.

Challenges

- The full range of capabilities is only available in the commercial Enterprise Edition.
- API Designer functionality is currently limited to OpenAPI specifications.
- Market presence is still limited to Europe, starting to expand to the US.

Leader in



Imperva – Application Security Platform

Imperva is an American cybersecurity solution company headquartered in Redwood Shores, California. Back in 2002, the company's first product was a web application firewall, but over the years, Imperva's portfolio has expanded to include several product lines for data security, cloud security, breach prevention, and infrastructure protection as well. In 2019, Imperva was acquired by private equity firm Thoma Bravo, making it a privately held company. In July 2023, the French multinational cybersecurity vendor Thales has announced the intent to acquire 100% of Imperva.

As a veteran Web Application Firewall vendor, Imperva had a strong presence in the application security market for years, so it's only logical for them to finally expand their portfolio to support API protection as a part of the company's like integrated CDN, fraud protection, account take over, advanced bot protection, load balancing and DDoS protection for any HTTP-based traffic with unified security policies and analytics.

It extends Imperva's proven web application security capabilities with an API-specific "positive security" model based on OpenAPI standard: by analyzing API contracts, the platform can automatically create and enforce protection policies and detect API attacks. Alternatively, it can integrate with existing API management solutions to import API definitions automatically.

Delivered as a SaaS service, the platform does not require any software deployment and supports integrations with many popular API gateways. Unified monitoring and analytics give users full visibility into their application security posture across different environments.

In 2021, Imperva has completed the acquisition of CloudVector, an API security-focused startup company, bringing in the technology for discovering, monitoring, and securing all corporate APIs regardless of their deployment environment. The API detection and response solution is now incorporated into Imperva's overall API security suite, providing full API visibility and "shadow API" prevention, generating up-to-date specifications for each API and detecting deviations from those specs and other anomalies in real time.

In 2023, Imperva has expanded the coverage of the solution by adding support for modern GraphQL and gRPC standards as well as continuing to deliver on its strategic "API Security Anywhere" promise. This notion refers to both the ability to deploy the solution in a variety of cloud and hybrid environments, as well as partnerships with all major API gateway vendors to provide standalone API security across them.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	positive
Usability	positive



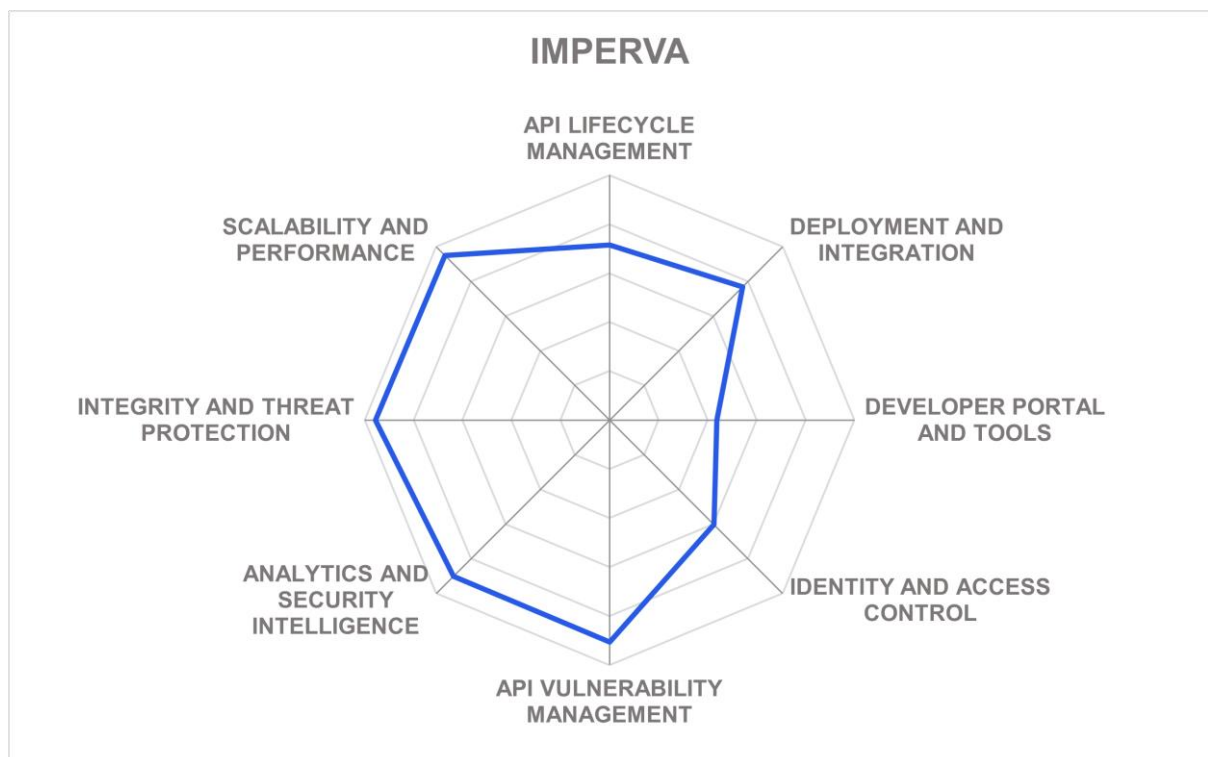
Table 18: Imperva's rating

Strengths

- Unified security platform for web application and API security.
- Fully SaaS-based with preconfigured security policies.
- Positive security model based on OpenAPI specification as well as on auto-learning.
- Support for GraphQL and gRPC standards.
- Comprehensive API attack analytics and threat reputation intelligence.
- Strong platform hardening and security capabilities.

Challenges

- Full support for microservice-based architectures is still a work in progress.
- Advanced API detection and response are not yet fully integrated into the platform.
- Available tools for API developers are improving but still limited.



Nevatech – Sentinet

Nevatech is a privately owned software company based in Atlanta, GA. Founded in 2011, the company provides SOA and API management infrastructure and tools for on-premises, cloud, and hybrid deployments. Nevatech is unique among its competitors, implementing their Sentinet platform completely on Microsoft .NET technology, and thus particularly beneficial for customers running Microsoft environments.

Nevatech Sentinet is a flexible, lightweight, and scalable API Management and API Governance platform that supports major API standards like REST and SOAP, as well as microservices or mobile APIs regardless of their deployment scenario. However, as it's completely built on the Windows platform, it's uniquely optimized for deployments that involve Microsoft technologies. Sentinet's architecture is equally suitable for on-premises, cloud, or hybrid deployments, as well as for custom scenarios like, for example, native Microsoft Biztalk Server or Azure platform integration.

The platform offers convenient tools for designing, developing, and testing APIs and provides a central repository for APIs, their metadata, and documentation. On the operations side, it ensures high availability, secure access management, auditing, and business analytics and SLA management.

In early 2023, Nevatech has released Sentinet 6.3, the latest version of the platform, which introduced numerous new features and improvements, such as a new flexible caching architecture, secure management of certificates and client credentials, virtualization profiles for quick deployment of new services, and the ability to create custom code to create complex payload transformations.

Nevatech's solution can primarily be recommended to companies heavily invested in Microsoft technologies, both on-premises and in Azure Cloud. For such scenarios, the platform offers quick deployment, native support for all relevant standards and protocols, and multiple options for adding custom functionality via extensions.

Although the company only addresses a somewhat limited number of potential customers, it is recognized for the high quality of its support service and strong commitment to usability and productivity improvements in its solution.

Security	positive
Functionality	positive
Deployment	positive
Interoperability	neutral
Usability	positive



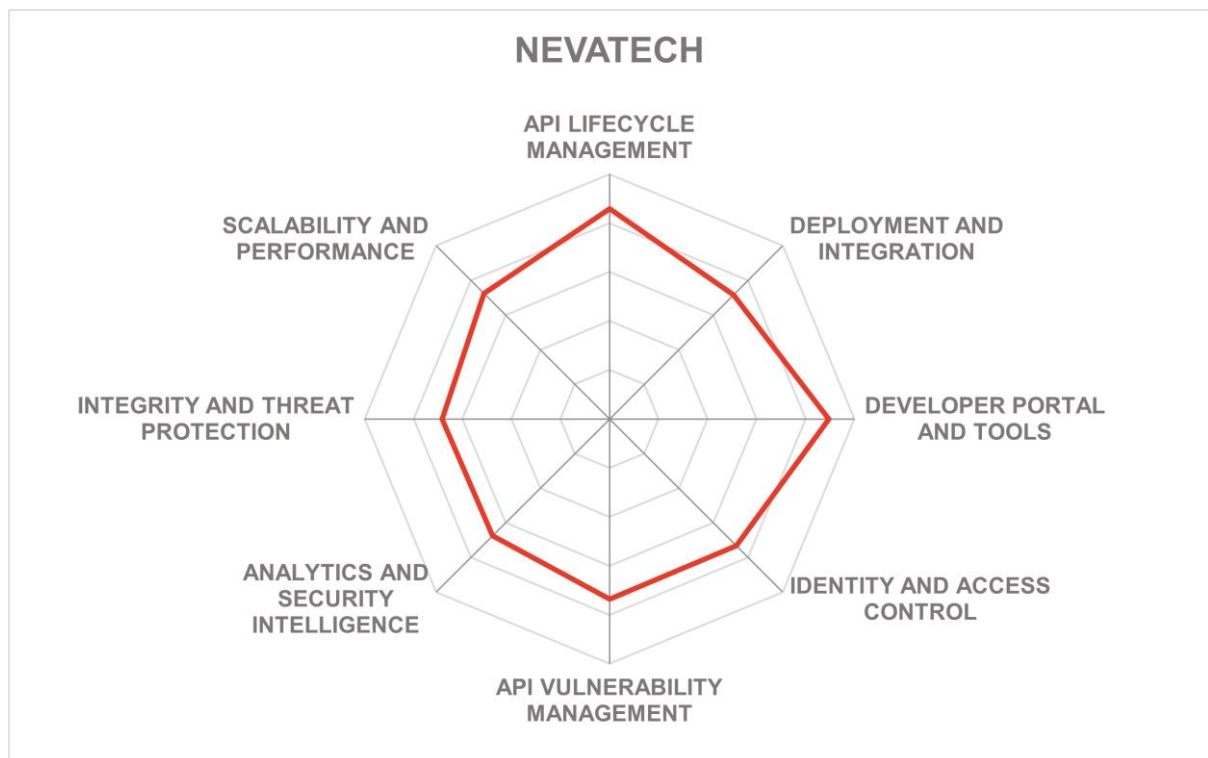
Table 19: Nevatech's rating

Strengths

- Integrated platform for all phases of the API lifecycle.
- Implemented entirely in .NET, optimized for Windows environments.
- API management and Governance through the built-in repository.
- Simple, but highly flexible distributed architecture.
- High level of extensibility via standard .NET interfaces.
- Strong focus on usability and customer satisfaction.

Challenges

- Targeted primarily towards the Windows ecosystem.
- API threat controls are quite rudimentary, implemented as custom extensions.
- No tools for compliance audit and reporting beyond basic audit changes.



Noname Security – API Security Platform

Noname Security is a privately held company with the HQ in Silicon Valley and additional offices in Tel Aviv, Israel and Amsterdam, Netherlands. Established in 2020 with a strategic vision of a complete, proactive API security platform, the company has already managed to attract many high-profile enterprise customers as well as to raise impressive funding from venture capital. Just a year after emerging from stealth, Noname Security had reached a \$1 billion valuation, becoming the first API security Unicorn.

Noname offers a broad range of deployment options, from a fully managed SaaS option to completely on-premises and hybrid scenarios. For customers in regulated industries or geographies, the entire solution can be confined to an isolated customer-controlled environment, fulfilling not just data residency regulations, but also much more stringent corporate (or government) requirements.

From the architectural standpoint, the Noname API Security Platform currently comprises three modules accessible from a single user interface. Together, these three functional areas combine into a unified API security platform that offers comprehensive capabilities for every stage of the API lifecycle, from early development to run-time operations.

API Posture Management helps discover and classify every API, detect security and compliance issues with them, and protect sensitive data. The platform uses passive traffic and log analysis techniques to identify any managed and unmanaged API available across on-premises and cloud environments. An impressive selection of API standards is supported, including REST, GraphQL, SOAP, XML-RPC, JSON-RPC, and gRPC.

API Runtime Protection is focused on detecting and blocking API attacks, data leaks, and suspicious activities in real time. It utilizes the unsupervised ML-based behavior algorithms to analyze API traffic, service logs, configuration files, and its own inventory findings to establish behavior baselines for each monitored API endpoint. Deviations from normal behavior are aligned with known vulnerabilities like OWASP API Top 10 and other types of issues like data leaks and corruption, configuration drifts, authorization issues, abuse, etc.

Active Testing, Noname's API security testing product, extends security coverage further to the left by helping identify vulnerabilities in API code before it is even deployed into production. The platform currently offers over 160 tests that simulate different types of malicious traffic, including but not limited to every vulnerability covered by the OWASP API Top 10.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	positive



Table 20: Noname Security's rating

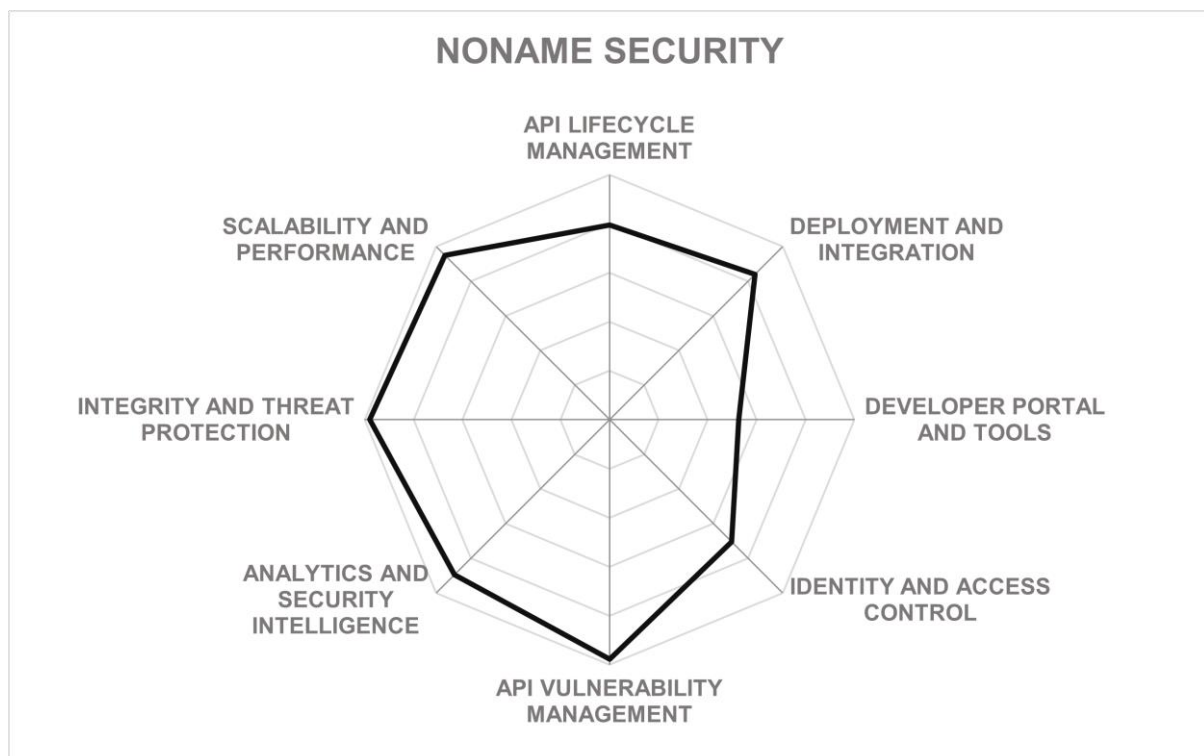
Strengths

- Integrated API security platform that covers all major phases of the API lifecycle.
- Support for all notable API standards in on-premises and cloud environments.
- Flexible deployment options, including fully on-premises scenarios for highly regulated customers.
- Large technology ecosystem with numerous third-party integrations for DevOps and security teams.
- Intelligent, business-relevant API testing with a large library of out-of-the-box tests and flexible automation capabilities.

Challenges

- API Testing integrations are limited to CI/CD pipelines, not offered for development environments.
- Inline blocking capabilities are fairly basic; advanced automated remediation functionality is planned for early 2024.
- Cannot actively validate OpenAPI specifications with API gateways to enforce adherence to specific schemas yet.

Leader in



Perforce – Akana

Perforce is one of the leading providers of software lifecycle management tools, headquartered in Minneapolis, Minnesota. Established in 1995, the company is primarily known for its version control system, but through a series of acquisitions in the later years, it has established a massive portfolio of application development, developer collaboration, agile planning, and other products for creating and running software.

In 2019, Perforce acquired Akana, known until 2015 as SOA Software, a veteran player in the API management market. Founded in 2001 and based in Los Angeles, CA, it initially focused on web services and SOA before gradually expanding its scope towards API management and security and cloud integration. The Akana Enterprise API Platform continues to be a key part of Perforce's product portfolio, providing an end-to-end API management solution for managing and securing each stage of the API lifecycle.

Akana API Platform is a fully integrated API management, transformation, and security platform that can address a multitude of enterprise use cases from API design and development to business application integration to the modernization of legacy services, while transparently supporting hybrid and multi-cloud environments.

Akana offers complete API lifecycle management, integrating with API design tools, development environments, and CI/CD pipelines, offering DevOps automation and governance. In addition, the platform provides multiple built-in security policies to enforce secure access, protect from external threats, and ensure compliance with regulations like PSD2 or PCI-DSS.

Since our previous review, a major addition to the platform has been support for the GraphQL standard. With the acquisition of the continuous testing platform BlazeMeter, this solution now expands Akana's API testing capabilities as well, improving security, governance, and oversight capabilities.

Although Akana API platform might not yet support all the latest cutting-edge API technologies, its strong overall focus on delivering fully integrated end-to-end API development, management, and security capabilities across multi-cloud and hybrid environments and, of course, an impressive portfolio of other DevOps products, are not to be overlooked. Customers that need a single platform for solving a variety of business challenges (from modern application development to mainframe modernization) might look no further.

Security	strong positive
Functionality	positive
Deployment	positive
Interoperability	positive
Usability	strong positive



Table 21: Perforce's rating

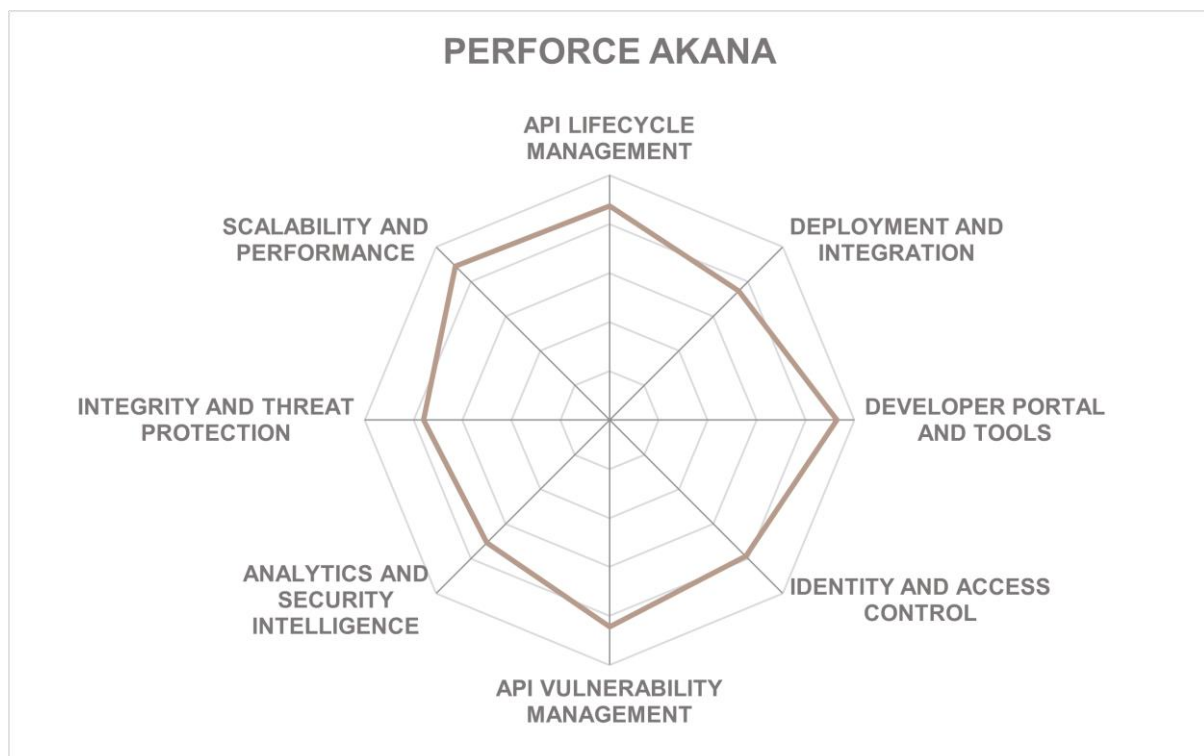
Strengths

- Fully integrated API management platform covering all aspects of the API lifecycle.
- Comprehensive access management, threat detection, and protection capabilities.
- Smart Portal with unified access for API developers and consumers.
- Includes an API modernization platform for mainframes.
- Built-in API analytics seamlessly integrates with multiple platforms.

Challenges

- Community recognition is not yet as strong as leading competitors.
- Support for modern API standards is limited to GraphQL only.
- Business analytics is only available via a separately licensed product.

Leader in



Red Hat – 3scale API Management

Red Hat is a multinational software company that develops enterprise open-source solutions, including cloud, infrastructure, application development, and integration technologies. Founded in 1993, the company is known for its enterprise Linux operating system, as well as for hybrid cloud management, virtualization, Kubernetes, and other solutions. In 2019, Red Hat was acquired by IBM and now operates as an independent subsidiary.

One of the company's primary areas of expertise is enabling cloud-native development solutions, and the Red Hat Application Foundations is one of the key parts of this portfolio. It provides a broad set of technologies to connect applications and data across modern distributed, hybrid environments. It includes 3scale, an API management platform, as well as the AMQ messaging platform and Red Hat build of Apache Camel, a distributed, cloud-native integration solution.

Originally offered as three distinct products, these technologies are now aligned to fully harness the capabilities of the Kubernetes Operator pattern and offered together as part of Application Foundations along with cloud native application frameworks. Acting in combination, these capabilities accelerate customer adoption of cloud native and hybrid application and service integration patterns quickly and consistently.

Regardless of the selected deployment option, Red Hat Application Foundations provides full coverage not just for the full API lifecycle (from initial design to retirement) with 3scale API Management, but incorporates comprehensive service orchestration, data transformation, real-time message streaming, and other methods of application connectivity – all within the same cloud-native technology platform with a rich set of developer tools, DevOps pipelines, and additional services to address the requirements of just about every kind of enterprise customer.

One of the key differences of 3scale is its hybrid-cloud architecture. This is achieved by a logical separation of concerns into two main elements: the API management policy execution (e.g., at an API gateway) with the API management policy configuration (API manager), which communicate asynchronously. This ensures resilience against connection failures and improves overall performance.

The upstream open-source projects maintained by Red Hat and community contributors form the basis of the 3scale platform which Red Hat packages and supports for enterprise customer use across their cloud and on-premises environments.

Security	positive
Functionality	strong positive
Deployment	positive
Interoperability	strong positive
Usability	positive



Table 22: Red Hat's rating

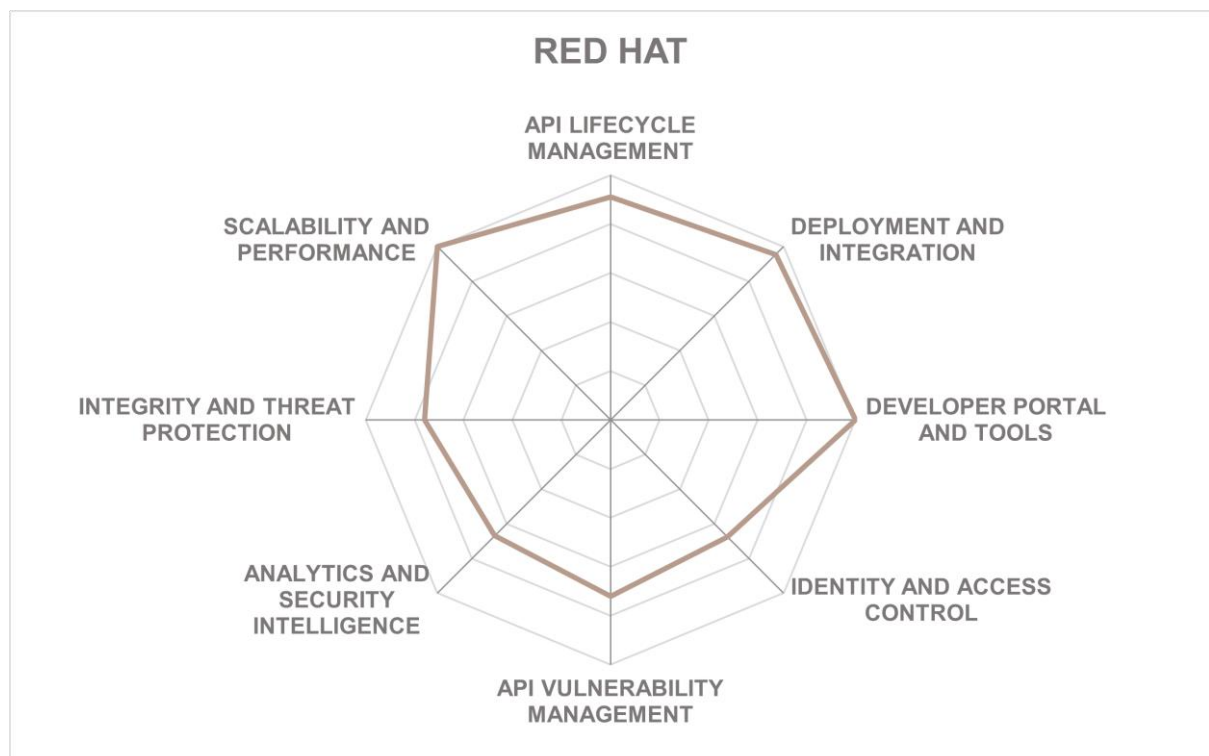
Strengths

- Comprehensive technologies for developing and integrating cloud-native apps.
- Optimized operator experience for manageability and scalability on OpenShift.
- Comprehensive support for microservices and serverless architectures.
- Flexible deployment options, supporting cloud & on-premises environments with a Kubernetes-based API management core, distributed gateways, and powerful customization.
- Designed for high performance, scalability, and hybrid deployments.
- Open-source codebase.

Challenges

- No longer offered as a standalone solution.
- No full feature parity between self-managed and SaaS offerings.
- API threat protection functions are provided by third-party partners.

Leader in



Salt Security – API Protection Platform

Salt Security is a privately held API security startup company based in Palo Alto, CA. Founded in 2016 by alumni of the Israeli Defense Force, the company offers a patented API threat protection platform that protects SaaS, web, mobile, microservices, and IoT applications from API threat vectors across build, deploy, and runtime phases. Harnessing the power of AI, big data, and behavioral analytics, the platform does not require any configuration and can be deployed in minutes.

Salt Security covers all types of APIs, whether own or third-party, internal or external, known or “shadow” and “zombie”. Salt Security has no impact on application performance or functionality and requires no changes to applications or infrastructure since it is deployed as a cloud service with an optional on-premises hybrid server. Salt collects API traffic across application environments from load balancers, API gateways, WAFs, Kubernetes clusters, cloud VPCs, and app servers - to dynamically provide a full inventory and protect APIs.

Upon discovery, the platform identifies API functionality (e.g., granular API structure and whether sensitive data such as PII is being processed) and analyzes it for known vulnerabilities and misconfigurations. It helps remediate these vulnerabilities by offering prioritized insights for security analysts and recommendations to developers. Combining this knowledge with real-time behavior monitoring, it will identify active API attacks, sending alerts to SIEM solutions, and integrating with existing enforcement infrastructure for blocking.

Salt Security combines real-time API behavior analytics with proactive vulnerability analysis to not just detect ongoing attacks on APIs, but to be able to rank them by risk impact and produce actionable recommendations for remediation. Although it does not provide own mitigation controls, it can be integrated with existing infrastructure like WAFs or API gateways for threat blocking. Salt can also be set up to forward insights to development teams using existing workflows and tools such as Jira and ServiceNow, making it easy to track vulnerabilities through to resolution.

Since our last review, the company has substantially increased its customer base and introduced the Salt Technical Ecosystem Partner program to partner with best-of-breed security vendors and make API security insights a part of existing workflows. The inaugural partners include companies focusing on dynamic and interactive application security testing to enable shifting left for API security.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	positive
Usability	strong positive



Table 23: Salt Security's rating

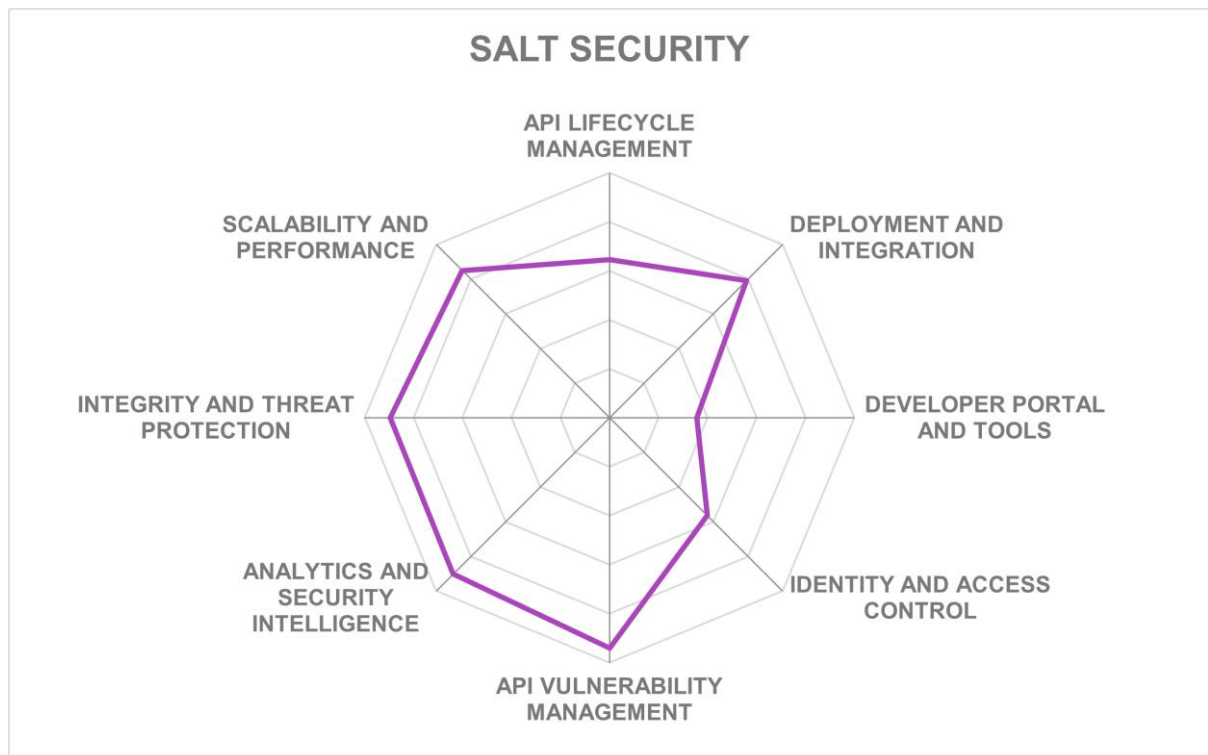
Strengths

- Strong focus on runtime protection and security across the full API lifecycle.
- Automatic and continuous discovery of new, outdated, and unknown APIs along with sensitive data exposure.
- Real-time detection of known and unknown API vulnerabilities and attacks.
- Based on supervised and unsupervised machine learning – no signatures, configuration, or training.
- Growing technical partner ecosystem for best-of-breed security coverage (like API testing)

Challenges

- Partner network primarily in North America and Europe, still expanding to other regions.
- Strongly focused on out-of-band monitoring, limited inline blocking options.

Leader in



Sensedia – API Platform

Sensedia is an API management company headquartered in Campinas, Brazil. Founded in 2007, the company provides a full-featured API management platform that incorporates tools for every stage of the API lifecycle from design to operations, analytics, and governance, incorporating robust security functions as well. Notably, the whole platform is entirely developed in-house without any acquisitions or technology partnerships.

Sensedia API management solution comprises several core modules, which can be licensed separately, but still form a tightly integrated platform: Developer Portal for publishing APIs and engaging developers; API Design and Studio Manager for creating and maintaining APIs, including monetization; API Gateway for applying API transformations and enforcing security and access policies; Analytics; and Lifecycle – the module for API governance.

Somewhat unusually for a platform of entirely own development, the solution implements impressive functional capabilities in nearly every aspect of API management and security: for example, it can address all OWASP API Security Top 10 threats with a broad range of built-in security functions. Sensedia is improving its range of prepackaged third-party integrations by integrating with vendors for FAPI/CIBA Compliance, logging integration, and new SSO and SAML mechanisms while rolling out new out-of-the-box SaaS connectors.

Currently, Sensedia is expanding beyond the traditional API management into a full-featured modern application platform by combining its API platform with other services such as Sensedia Events Hub and Sensedia Service Mesh, as well as offering a managed “API care” service that provides proactive monitoring of customers’ sensitive APIs.

The most recent addition to the Sensedia platform are its integration capabilities. With more than 40 out of the box connectors that enable service composition and orchestration, process automation, data transformation, and B2B ecosystem integration, the company can now offer a universal solution that combines API management and integration platform as a service functionality.

Perhaps the only drawback of the Sensedia API platform is that it’s almost unknown outside its home market in Brazil and the rest of Latin America. Sensedia is changing that as the company is increasing its reach in the European market, where they already operate as well as expanding into the United States and establishing partnerships with global system integrators. Any company looking for a full-featured yet well-integrated API management and security platform from a single hand can be encouraged to consider Sensedia for evaluation.

Security	positive
Functionality	strong positive
Deployment	strong positive
Interoperability	positive
Usability	strong positive



Table 24: Sensedia's rating

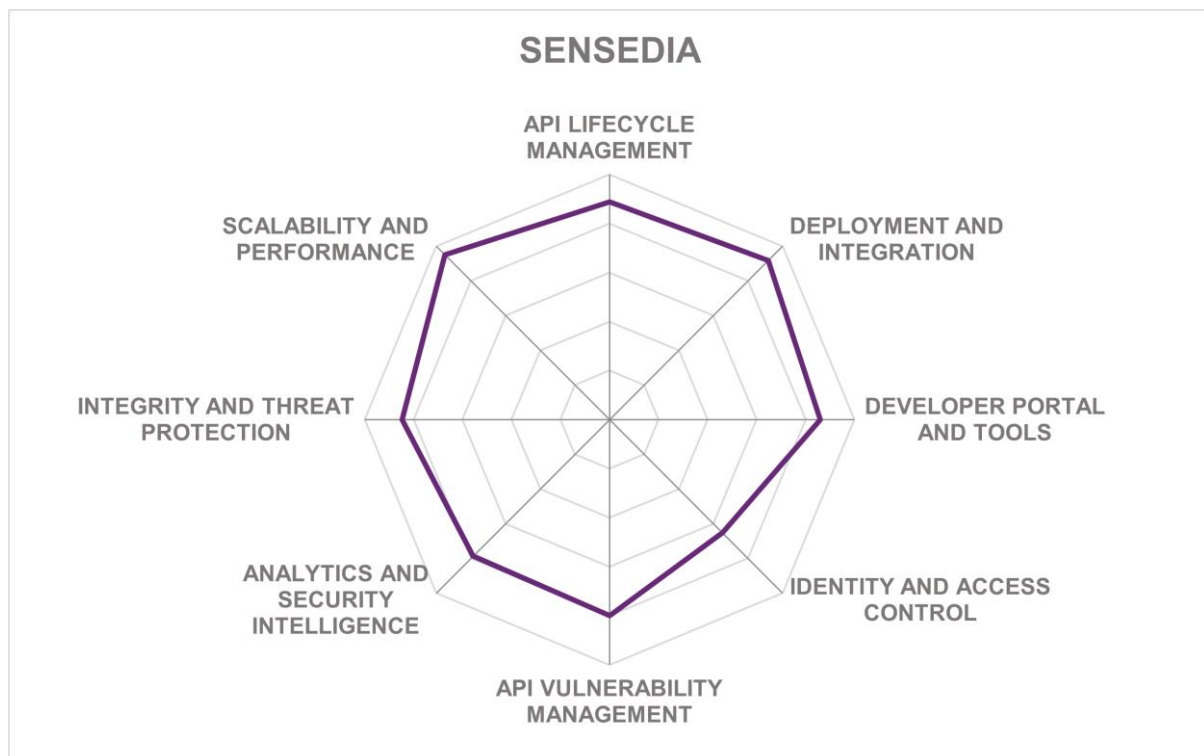
Strengths

- Full-featured API management platform with tools for all phases of API lifecycle.
- Part of a larger integration platform.
- Flexible deployment options with support for hybrid architectures.
- Comprehensive API threat detection controls.
- Broad range of consulting services.

Challenges

- Small but growing market presence outside Latin America.
- Limited anomaly detection, no behavior analytics.
- Advanced threat protection is only supported through third-party partnerships.

Leader in



Traceable – API Security Platform

Traceable is an API security startup based in San Francisco, California. Established in 2019 by veterans of the application performance monitoring market, the company develops an innovative distributed tracing technology for cloud-native applications, which helps monitor, investigate, and protect multiple cloud environments like microservices, service meshes, serverless functions, and APIs. Combining it with an unsupervised machine learning platform to correlate operational and security data across various components of modern cloud-native applications and APIs, Traceable can offer customers not just full visibility into code execution but also into data flows and user activities.

The AI behavior engine provides false positive reduction, identification and classification of suspicious activities, and detection of various known and unknown attacks. All collected and enriched data (not just malicious events) is fed into a centralized security data lake that can retain it substantially longer than competing solutions. This “360 API Context” capability ensures that a broad range of analytics and protection scenarios can be implemented on top of this data, including slow and low attack discovery, sensitive data exposure tracking, fraud and abuse prevention, application behavior analysis, incident analysis, and hunting for hidden indicators of compromise (IoCs).

Specifically for APIs, Traceable adds continuous API discovery and dynamic risk assessment, with risk and trust postures quantified separately for each endpoint and each user. Traceable also provides API Security Testing that can be run manually or in DevSecOps pipelines to identify API vulnerabilities and misconfigurations before they reach production. However, the main differentiator of the solution is that its focus extends beyond just APIs, providing a unified security context for application code, data, and user behaviors as well.

Among the recent additions to the platform, we can mention the API fraud module, specifically focusing on analyzing the business-level behavioral patterns of corporate APIs and not just identifying anomalies but aligning them with known business-level fraud scenarios. In addition, the company has introduced a Zero Trust API Access solution that aims to reduce the API attack surface by combining continuous adaptive authorization, dynamic access policies and intelligent rate limiting. The goal is to minimize implicit trust in API infrastructures, aligning nicely with the tenets of the Zero Trust security model.

Besides rich forensic capabilities that allow customers to investigate API vulnerabilities, malicious attacks, and suspicious user behaviors, Traceable’s platform can provide protection against OWASP API Top 10 attacks, implement incident response processes, and even block API attacks automatically at the IP or user level.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	positive
Usability	positive



Table 25: Traceable’s rating

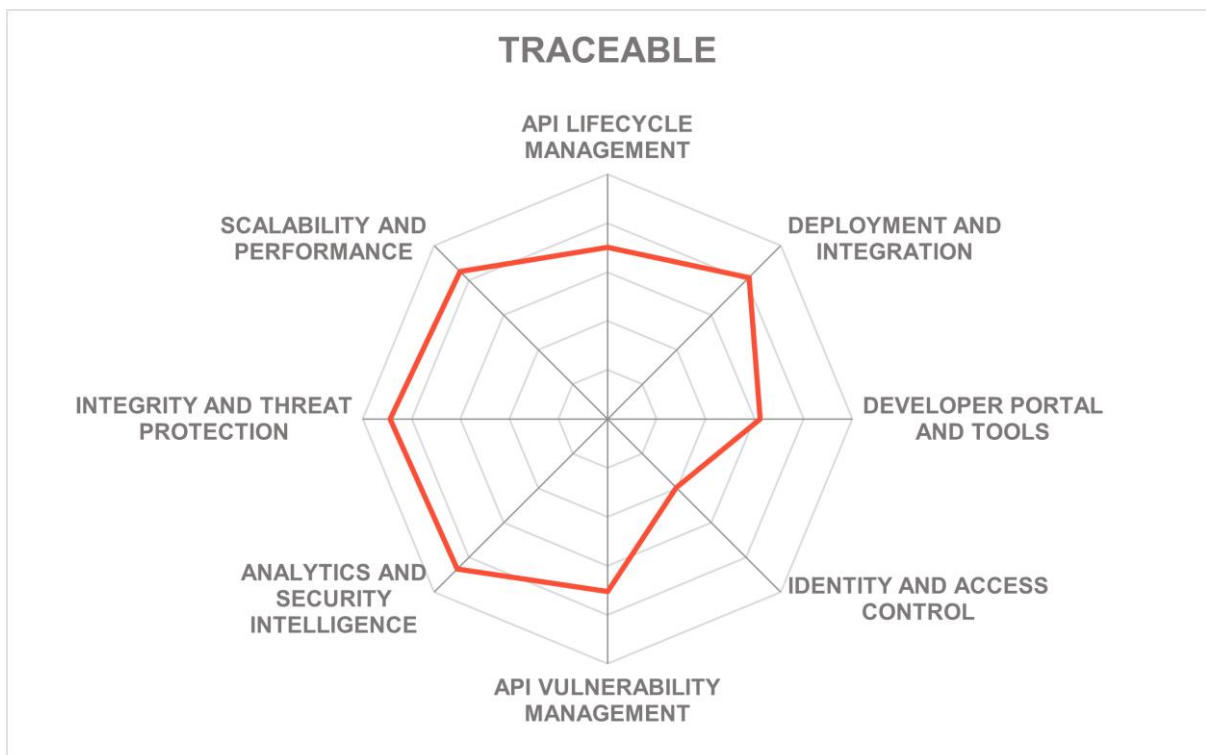
Strengths

- Innovative distributed tracing technology to monitor and correlate data across application components and environments.
- Unsupervised AI detection engine for identifying and classifying various attacks and suspicious activities.
- Rich forensic analytics, threat hunting, and compliance reporting capabilities.
- Built-in remediation actions for blocking API attacks.
- API security testing solution to close the secure API development lifecycle loop.

Challenges

- Built for enterprise customers, it's harder to sell to the small to medium markets who want more self-serve options.
- The partner ecosystem is still fairly small, needs to grow to keep up with competitive pressure.
- UX in complex use cases could benefit from improvement to decrease time to value for users.

Leader in



Wallarm – Advanced API Security

Wallarm is an application and API security vendor based in San Francisco, CA. Founded in 2016 with the vision for end-to-end API security, the company now delivers an integrated platform for API discovery and posture management, real-time API protection, as well as for API security testing. The solution unifies API security and next-generation WAF capabilities to protect the entire web application and API portfolio for a customer, even in complex multi-cloud environments.

The Wallarm platform combines two solutions: cloud-native web application and API protection (WAAP), which provides runtime threat prevention and protection capabilities for apps and APIs, and Advanced API Security, which focuses on API discovery, vulnerability management, sensitive data detection, and API testing for complete protection against advanced API-specific threats.

With a strong focus on protecting cloud-native environments, Wallarm offers an impressive range of deployment options, from traditional API gateways and load balancers to Kubernetes and containers, serverless functions, hybrid cloud environments, or even agentless SaaS scenarios. Wallarm Nodes enable deep inline inspection with near-zero latency but can also operate out of band on mirrored traffic.

Wallarm API Discovery provides runtime visibility into the entire API inventory to catalog, monitor, and protect any type of API. API Leak Management enables automatic discovery of leaked API keys and secrets and prevents their proliferation. API Abuse Prevention enables real-time protection against automated abuse – malicious bots, account takeover, or L7 denial-of-service attacks. Finally, API Security Testing automates security tests of APIs in development and integrates into existing CI/CD pipelines.

The platform provides protection against OWASP Top 10 web and API threats (it even has a dedicated dashboard for better visibility into those) but does not stop there – with distributed rate limiting, virtual patching, sensitive data discovery and rich forensic capabilities, it makes regulatory compliance much easier even for highly regulated customers.

Among the most recent capabilities, API abuse prevention is worth noting, making it essentially an API attack surface management solution. Orphan API discovery (finding endpoints that are present in a specification but are no longer actively used) is another new function that expands existing coverage of shadow APIs and helps solve both maintenance and security issues.

Security	positive
Functionality	positive
Deployment	strong positive
Interoperability	strong positive
Usability	positive



Table 26: Wallarm's rating

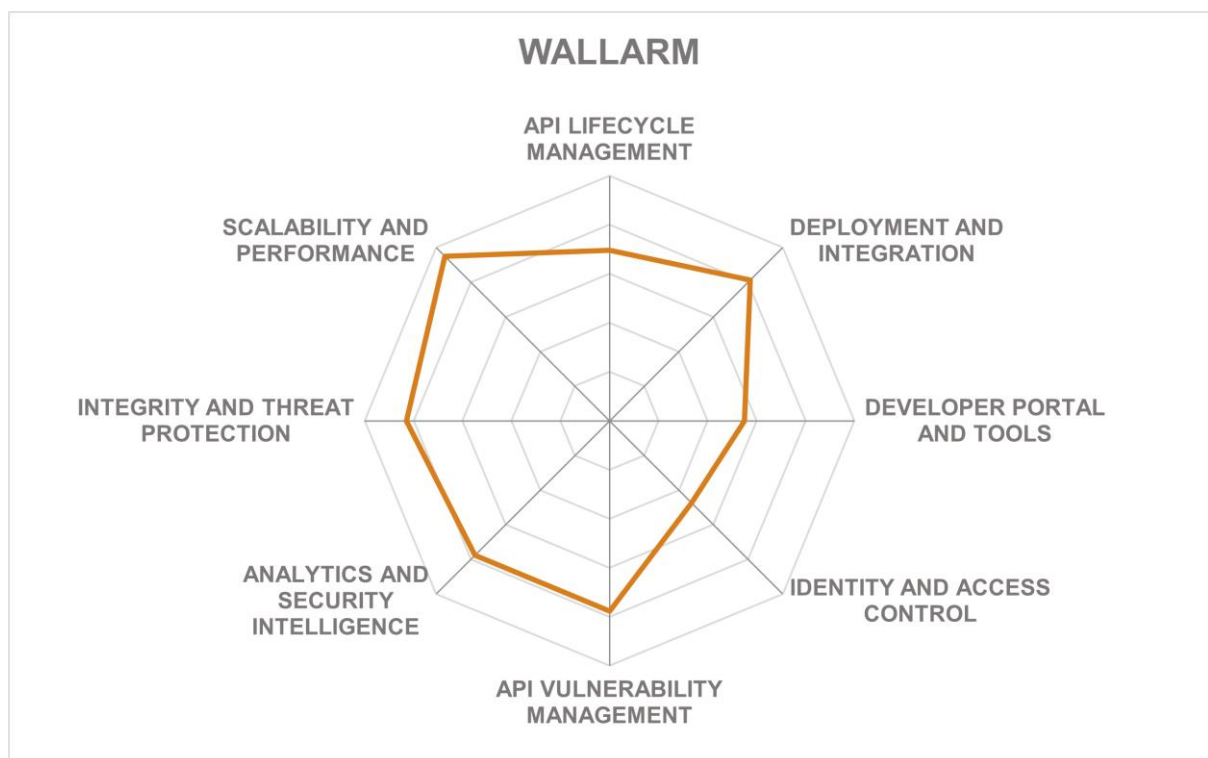
Strengths

- A consolidated platform combining web application and API security capabilities.
- Impressive range of supported deployment scenarios, both inline and out of band, microservices, and serverless functions.
- Support for all major API standards, including REST, SOAP, GraphQL, gRPC, and WebSocket.
- Numerous supported integrations with development, security, and collaboration tools.
- Comprehensive API testing capabilities that allow developers and security teams to collaborate efficiently.

Challenges

- Market presence is mostly limited to the US, expanding to Europe and Latin America.
- Does not offer any API lifecycle management functionality.
- Limited reporting capabilities.

Leader in



WSO2 – API Manager, API Platform for Kubernetes, Choreo

WSO2 is a global application development company based in the US, UK, and Sri Lanka with additional teams in EMEA, APAC and LATAM. Founded in 2005, the company offers a wide array of open-source software solutions that can enable digital innovation and digital transformation. These products can handle enterprise challenges in today's world in the areas of API management, integration, identity management, and smart analytics/stream processing.

The WSO2 API Management solution is based on a set of open-source products developed by WSO2. WSO2 API Manager inherits features from Enterprise Integrator, Identity Server, Event Processor, and API Micro-gateway.

With these capabilities, it offers a powerful platform that can cater to the modern business requirements in today's API Management arena, including cloud-native API Management, extended security for APIs, containerized API Management deployments, exposing microservices as well-managed APIs and scalable deployment patterns.

The recent release of WSO2 API Manager combines its API management capabilities with those of WSO2 Enterprise Integrator, thus integrating such additional capabilities as microservices integration, data streaming, enterprise integration connectors, and visual tools for managing and monitoring all kinds of application integration processes.

Another notable addition to the company's API portfolio is Choreo, an innovative low-code development platform, which allows quick, cloud-native development and deployment of modern apps, APIs, and integration scenarios with a strong focus on a visual design approach.

The most recent new product in this family is the WSO2 API Platform for Kubernetes, which extends K8s fundamental abstractions to the API world, can be deployed to any cluster, natively supports multi-environment and multi-tenant deployments with a single control plane, and is 100% open source. The company is working hard on integrating all these products into a single, completely unified API management, service development, and integration platform that spans on-premises, containerized and SaaS deployments.

Although WSO2's API solution is quite functional out-of-the-box, it's the platform's flexibility that makes it ideal for projects where API management is a part of a bigger infrastructure and customizability is an important requirement. The flexibility and open-source nature of the platform enable different customizations to address most complex deployment scenarios.

Security	strong positive
Functionality	strong positive
Deployment	strong positive
Interoperability	strong positive
Usability	strong positive



Table 27: WSO2's rating

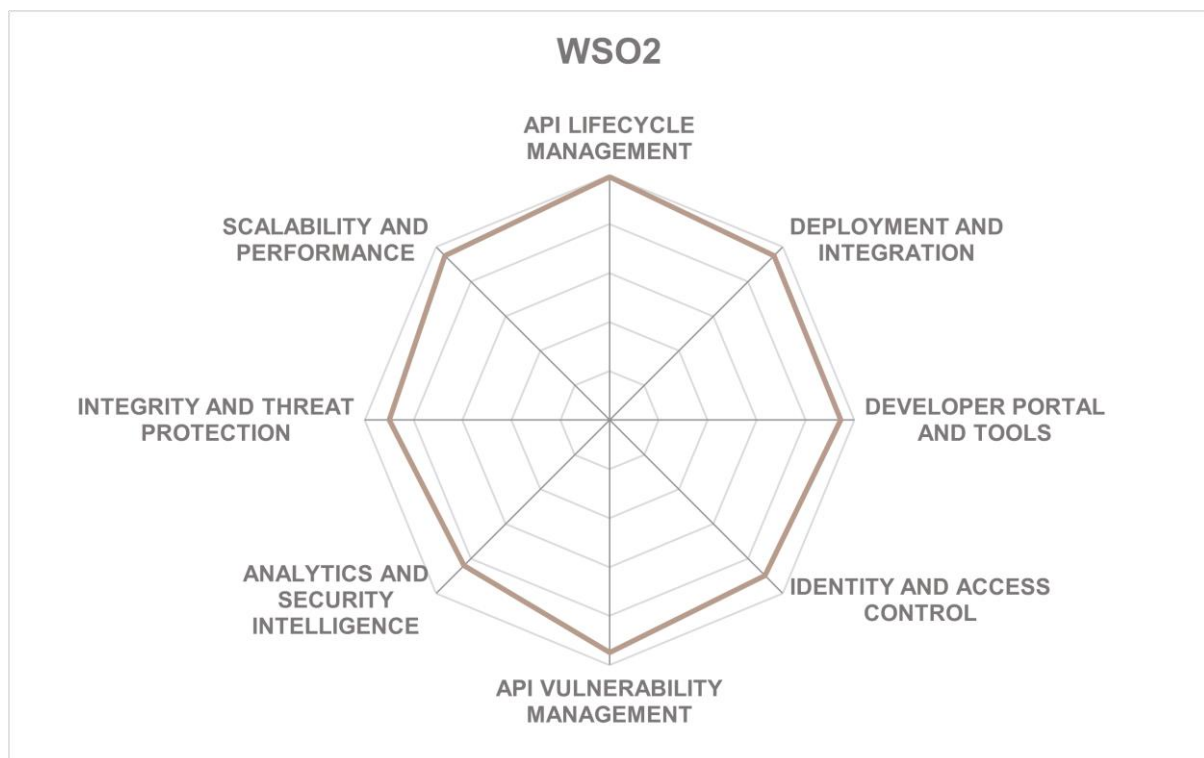
Strengths

- Built on an integrated open-source platform for business-centric solutions.
- Native support for complex multi-tenant Kubernetes deployments with a single management plane.
- Now incorporates additional enterprise integration capabilities.
- Cloud-native support to expose microservices as managed APIs.
- AI-powered abnormal activity detection.
- Low-code cloud-native development platform with API marketplace.

Challenges

- Advanced authentication and access control require integration with other WSO2 products.
- Threat prevention functions are limited.
- Report customization is only possible with external tools.

Leader in



Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

Check Point

Check Point Software Technologies is an international cybersecurity solution provider with dual headquarters in San Carlos, CA and Tel Aviv, Israel. Since its establishment in 1993, the company has grown from a specialized network security vendor into a provider of a broad portfolio of security. Currently, the company offers its entire cybersecurity portfolio as a consolidated Check Point Infinity security architecture comprising network, cloud, and user security solutions, as well as unified management and security operations.

Why worth watching: Check Point CloudGuard, the company's cloud and application security solution is offered as an integrated preemptive security platform that combines a cloud-native WAF with specialized API security capabilities, bot prevention, intrusion detection, and even file security. In addition to API behavior analysis, the platform includes "crowd behavior analysis" to improve risk scoring based on user activity.

Citrix

Citrix Systems is a multinational software company that provides solutions for digital workspace, application delivery and security, and cloud services. Founded in 1989, the company is primarily known as a leading provider of remote desktop and application services, but as a part of its application security business, Citrix offers Application and API security – a comprehensive, layered security solution that combines web application firewall, bot management, API gateway, and SSL termination capabilities.

Why worth watching: available across multiple form factors (from hardware appliances to cloud-native containerized and SaaS offerings), the platform provides consistent, centrally controlled API protection across multi-cloud and hybrid environments and is available as a fully managed solution.

Fastly

Fastly is an American edge cloud platform provider headquartered in San Francisco, CA. Established in 2011 as a content delivery network, the company has grown into a full-featured platform combining network services, compute capabilities, as well as security and observability functionality. In 2020, Fastly acquired Signal Sciences, a web application and API security vendor. Since 2022, it also owns Glitch, a popular online web application development platform.

Why worth watching: Fastly's security portfolio offers a broad range of capabilities including an intelligent next-generation web application firewall (WAF), API protection, DDoS mitigation, bot management, and managed security services. With its global edge cloud platform, Fastly can offer both scalability and flexibility for the most sophisticated deployments, as well as a high degree of automation for threat mitigation with its patented SmartParse technology.

Kong

Kong Inc. is a privately held company headquartered in San Francisco, CA. Founded in 2017 and backed by investors like Jeff Bezos of Amazon and Eric Schmidt of Google, the company is the developer of Kong Gateway, one of the most popular open-source API gateway projects, as well as Kong Enterprise, a service control platform for managing APIs and microservices across multi-cloud and hybrid environments.

Why worth watching: developed from the ground up to enable simple, scalable, and extensible support for modern microservices-based application architectures, Kong enjoys the support of a large open-source community. Kong Enterprise extends the OSS project with monitoring, automation, and security capabilities.

MuleSoft

MuleSoft is another veteran player in the API management market. Founded in 2006 in San Francisco, CA, MuleSoft has been focusing on providing a unified application integration platform to connect devices, applications, and data sources across on-premises and cloud environments.

Why worth watching: developing, publishing, and re-using APIs is the technological foundation for any integration platform, and the company provides a range of products and services for quick low-code development and testing of APIs, a comprehensive online marketplace for publishing and consuming APIs and other assets, as well as a data protection and security layer to stop threats and prevent data breaches.

Orca Security

Orca Security is a cloud security vendor based in Portland, OR. Established in 2019, the company is pioneering the agentless approach towards cloud security. The Orca platform combines security capabilities for cloud infrastructure, workloads, data, identities, and APIs in a single solution.

Why worth watching: Orca's patented SideScanning technology does not require agents and does not impact running workloads. For APIs, it provides a dynamic inventory of managed and unmanaged endpoints, actionable data on misconfigurations and vulnerabilities, and risk prioritization beyond just APIs.

Ping Identity

Ping Identity is a publicly traded software company headquartered in Denver, CO. Founded in 2002, the company has grown into one of the leading providers of identity federation and access management solutions. A leading provider of identity and access management solutions, the company has also expanded into API security by acquiring Elastic Beam, a pioneering security intelligence company.

Why worth watching: Ping API Intelligence is a real-time monitoring and threat detection solution for API traffic. By using automated API discovery and detection powered by AI models, the product can quickly centralize API monitoring, detect anomalies and suspicious activities, and block attacks automatically. Through integrations with other Ping products, it can offer comprehensive visibility and protection across on-premises and clouds.

Radware

Established in 1996, with corporate HQ in North America and its international headquarters in Tel Aviv, Israel, Radware specializes in application delivery and cybersecurity solutions. The company provides a broad range of application security solutions in a suite, including API Protection.

Why worth watching: Radware API Protection maps the API attack surface by leveraging an automated discovery algorithm and generating tailored security policies to detect and block API-focused attacks in real time. It also uses a combination of access controls, DLP, bot management, and DoS mitigation tools to protect against API security threats.

Spherical Defence

Spherical Defence is a British security startup company based in London. Founded in 2017, the company is developing an innovative application security monitoring technology that is capable of unsupervised analysis of any machine-to-machine communications and JSON payloads - from HTTP traffic to system logs – analyzing over 150 telemetry points and detecting any anomalies in system or user behavior.

Why worth watching: As opposed to many other ML-based security solutions, Spherical Defense's product is fully autonomous and unsupervised – it does not require any manual configuration or training. It does not just identify anomalies in API traffic but can classify them into multiple categories of attacks, including excessive data exposure, malicious injection, sensitive information transmission, and even adversarial attacks against ML models.

TIBCO Cloud Mashery

TIBCO Software is a leading provider of integration, analytics, and event processing solutions. Founded in 1997 as The Information Bus Company, TIBCO has grown over the years to offer a comprehensive Connected Intelligence Cloud platform to connect data sources and business applications across hybrid environments. In 2015, TIBCO has

acquired Mashery, a pioneer API management vendor, the company that supposedly invented the very concept of API Management.

Why worth watching: the cloud-native Mashery platform includes all the necessary tools to create APIs from existing data sources, to design, package, and market API products, to onboard and engage developer communities, and to enforce security policies on API gateways and embedded micro-gateways.

Tyk

Tyk Technologies Ltd is a privately held company with sales offices located in London, Singapore, and Atlanta. Since 2015, it has been the primary force behind the Tyk Open Source API gateway and Tyk Enterprise, an API Management platform designed for DevOps. Comprising their own codebase built from the ground up instead of wrapping existing products from other vendors, the Tyk platform is designed for multi-DC and multi-cloud deployments, high performance, and full backward compatibility.

Why worth watching: Designed and maintained by a dedicated developer team, the open-source API gateway provides the full range of functionality free of charge, with commercial licensing available only for the management dashboard built on top of it. Tyk Enterprise includes an API management dashboard to manage, maintain and secure APIs across multiple gateways along with built-in policy management, operational analytics, and reporting. Tyk's integrated developer portal provides functions for developer onboarding, API documentation, and usage analytics.

AWS

As a major cloud service provider whose cloud infrastructure is utilized by millions of active customers every month to develop and host their business services, applications, and APIs, AWS naturally offers its own native API management services. In addition, the company's services expose their own APIs or provide the means to develop custom APIs quickly.

Why worth watching: from low-level infrastructure services like Amazon EC2 or AWS Lambda to data-centric services like Amazon Kinesis or DynamoDB or any other third-party endpoint: Amazon API Gateway offers a fully managed solution for publishing, maintaining, and monitoring those APIs. By providing tight integration with existing AWS cloud infrastructure, security, and identity services, it enables exposing existing backend services or creating new ones quickly, without the need to manage resources or identities.

IBM Cloud

As an integral part of IBM Cloud, the company offers its own API Connect platform for managing and securing APIs across multiple clouds. API Connect is a full-featured API Management platform that provides tools for creating, publishing, and monetizing APIs.

Why worth watching: built around a single, highly secured IBM DataPower Gateway, the platform provides comprehensive management capabilities for each stage of the API lifecycle, as well as the most common security and data protection functions like transport layer encryption, secure authentication, and DoS protection.

Microsoft Azure

Microsoft's Azure cloud platform offers API management capabilities as well, with an API Gateway and Developer Portal being the key services that power this offering. Microsoft puts a strong focus on quick API development using such services as Azure Functions for creating serverless code, Logic Apps for visual workflow automation without writing code, or the fully managed web app platform called App Service.

Why worth watching: with the introduction of the API Management consumption tier, developers are now free to choose a modern development model with instant provisioning, automated scaling, and high availability over the traditional centralized gateway architecture.

Oracle Cloud

To support developers during the API design phase, Oracle's offering incorporates the API Flow platform from Apiary, offering visual tools and guidance for building API guidelines, collaborating on API contract design, rapid prototyping, testing, and debugging new APIs. In addition, Oracle API Management includes comprehensive access management, threat detection, and protection capabilities, as well as analytics and integration with other company's development, integration, and mobile services.

Why worth watching: Oracle Cloud provides a complete set of services to manage the lifecycle of APIs, from design and prototyping to deployment to monitoring and monetization across on-premises, Oracle Cloud, and third-party cloud environments.

Methodology

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

Customers must always define their specific requirements and analyze in greater detail what they need. This report doesn't provide any recommendations for picking a vendor for a specific customer scenario. This can be done only based on a more thorough and comprehensive analysis of customer requirements and a more detailed mapping of these requirements to product features, i.e., a complete assessment.

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities we expect from products in that market segment. They are mature.
- **Market Leaders:** Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- **Innovation Leaders:** Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.
- **Overall Leaders:** Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. They might have slight weaknesses in some areas, but they become Overall Leaders by being above average in all areas.

For every area, we distinguish between three levels of products:

- **Leaders:** This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in certain areas.
- **Challengers:** This level identifies products which are not yet Leaders but have specific strengths which might make them Leaders. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- **Followers:** This group contains vendors whose products lag in some areas, such as having a limited feature set or only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for specific use cases and customer requirements, but are of limited value in other situations.

Our rating is based on a broad range of input and long experience in that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, and other sources.

Product rating

KuppingerCole Analysts AG as an analyst company regularly evaluates products/services and vendors. The results are, among other types of publications and services, published in the KuppingerCole Leadership Compass Reports, KuppingerCole Executive Views, KuppingerCole Product Reports, and KuppingerCole Vendor Reports. KuppingerCole uses a standardized rating to provide a quick overview on our perception of the products or vendors. Providing a quick overview of the KuppingerCole rating of products requires an approach combining clarity, accuracy, and completeness of information at a glance.

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Deployment
- Interoperability
- Usability

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well, there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logical and intuitive, as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly, and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics:

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to add technical capabilities in a direction which aligns with the KuppingerCole understanding of the market segment(s). Innovation has no value by itself but needs to provide clear benefits to the customer. However, being innovative is an important factor for trust in vendors because innovative vendors are more likely to remain leading-edge. Vendors must support technical standardization initiatives. Driving innovation without standardization frequently leads to lock-in scenarios. Thus, active participation in standardization initiatives adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market or the relevant market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't lead to a very low overall rating. This factor considers the vendor's presence in major markets.

Financial strength - even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are, in general, more likely to either fold or become an acquisition target, which present risks to customers considering implementing their products.

Ecosystem is a measure of the support network vendors have in terms of resellers, system integrators, and knowledgeable consultants. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a “good citizen” in heterogeneous IT environments.

Again, please note that in KuppingerCole Leadership Compass documents, most of these ratings apply to the specific product and market segment covered in the analysis, not to the overall rating of the vendor.

Rating scale for products and vendors

For vendors and product feature areas, we use a separate rating with five different levels, beyond the Leadership rating in the various categories. These levels are:

Strong positive	Outstanding support for the subject area, such as product functionality, or outstanding position of the company for financial stability.
Positive	Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.
Neutral	Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.
Weak	Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.
Critical	Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

KuppingerCole tries to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, including vendors which are only active in regional markets such as Germany, Russia, or the US.

However, there might be vendors which don't appear in a Leadership Compass document due to various reasons:

- **Limited market visibility:** There might be vendors and products which are not on our radar yet, despite our continuous market research and work with advisory customers. This usually is a clear indicator of a lack in Market Leadership.
- **Declined to participate:** Vendors might decide to not participate in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway if sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the market segment.
- **Lack of information supply:** Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- **Borderline classification:** Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

The goal is to provide a comprehensive view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

We provide a quick overview about vendors not covered and their offerings in chapter Vendors to Watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Related Research

[Leadership Compass: API Management and Security](#)

[Buyer's Compass: API Management and Security](#)

[Market Compass: Dynamic Authorization Management](#)

[Leadership Compass: Access Management](#)

[Leadership Compass: Identity API Platforms](#)

[Advisory Note: The Role of APIs for Business](#)

[Whitepaper: The Dark Side of the API Economy](#)

[Whitepaper: Meeting PSD2 Challenges with Ergon Airlock Suite](#)

[Leadership Brief: Top Cyber Threats](#)

[Leadership Brief: Securing PSD2 APIs](#)

[Executive View: Cequence Security API Sentinel](#)

[Executive View: Apigee Edge API Management Platform](#)

[Executive View: Curity Identity Server](#)

[Executive View: Forum Sentry API Security Gateway](#)

[Executive View: WSO2 Identity Server](#)

[Executive View: Noname API Security Platform](#)

Copyright

©2023 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole does not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators, and software manufacturers in meeting both tactical and strategic challenges and making better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.