KuppingerCole Report

LEADERSHIP COMPASS

By Alexei Balaganski

August 13, 2021

API Management and Security

This Leadership Compass provides an overview of the market for API management and security 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.

By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 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 homes and in mobile devices, in corporate networks and in the cloud, even in industrial environments, to say nothing about the Internet of Things.

As companies are struggling to maintain their business agility, to react to the ever-changing market demands and technology landscapes, the need to deliver a new application or service to customers as quickly as possible often trumps all other considerations. 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 RESTful APIs, which are commonly used today.

The rapid adoption of REST APIs also coincided with the exponential growth of cloud computing and mobile device proliferation, where they were the perfect medium to enable integrations between these heterogeneous systems and facilitate data exchange on a massive scale. In a world where digital information is one of the "crown jewels" of many modern businesses (and even the primary source of revenue for some), 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.

When the previous edition of our Leadership Compass was published in 2019, our research indicated the growing awareness of the critical role of security in API management solutions, representing a massive change since our first edition back in 2015. Fast forward 18 months and we can clearly see that the tempo of the API market evolution is only increasing.

Perhaps the most notable trend is the rapid expansion of the scope of both modern API management and API security solutions. Nowadays, API gateways for publishing REST API endpoints can certainly already be considered "legacy products". New API technologies, like GraphQL or gRPC, have grown from research projects into widely adopted solutions for specific use cases, where they provide much better flexibility or performance than REST APIs. Modern loosely coupled cloud-native application architectures demand API management solutions that can handle complicated traffic patterns and deal with ephemeral container-based infrastructures.

These trends not only reshape the basic capabilities of modern API management platforms (for example, enforcing API quotas with rate limiting simply does not work for GraphQL APIs, where requests to the same endpoint can vary in size and complexity), they redefine the scope of API security solutions as well. In a sense, we can already observe the same developments within API security that we've seen on a larger scale for cybersecurity as a whole: with too many different types of infrastructure that need protecting, the

overall complexity of security solutions grows exponentially.

Some vendors are already promoting alternative approaches towards API security, which are more data-centric and proactive in nature than traditional infrastructure monitoring and security analytics. This might sound controversial, but one potential scenario for the future development of the API security market is that it will evolve into multiple specialized types of security capabilities which will be integrated with other existing areas of cybersecurity -- for example, into XDR security analytics platforms or integrated data protection or application security solutions.

Because of these ongoing developments, some of the ratings presented in this Leadership Compass might deviate somewhat from the previous edition. This by no means indicates that some of the solutions covered in our rating have suddenly become less functionally capable -- it is the market that has evolved, and some of the existing capabilities simply no longer align with the modern requirements. We will, of course, continue to follow the latest developments in the field of API security in our future publications as well.

In the meantime, our general recommendation for customers remains the same: both API management and API security should not be considered as standalone, isolated components of your IT infrastructures. On the contrary, choosing the right product should be a part of a comprehensive strategy that covers such aspects as application development and operations, data protection, and regulatory compliance.

Only by combining proactive application security measures for developers with continuous activity monitoring and deep API-specific threat analysis for operations teams and smart, risk-based, and actionable automation for security analysts one can ensure consistent management, governance, and security of corporate APIs and thus the continuity of business processes depending on them.

1.1 Highlights

- Both API management and API security market segments continue to evolve and grow, driven by a massive increase in API adoption, as well as by an ongoing pressure of security and compliance risks APIs are exposed to.
- The tempo of the API evolution continues to increase, with multiple new standards, protocols and architectures emerging, expanding the scope for API management solutions beyond just the traditional REST APIs.
- 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.
- With standard API management capabilities quickly becoming a commodity, vendors specializing in these solutions are focusing on increasing their functional coverage to address new business requirements, involve new stakeholders, and improve productivity for developers.

- Some vendors no longer consider API management a standalone market, offering these functions as a part of larger enterprise integration platforms.
- 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 market consolidation trend continues, with larger established vendors acquiring small innovative startups, integrating their technologies into more comprehensive, unified security platforms.
- The notion of data-centric security that incorporates API security as one of the major layers in an integrated, layered architecture is emerging, with several vendors already offering such integrated platforms.
- The overall leaders in the API management and security market are (in alphabetical order): 42Crunch, Axway, Broadcom, Curity, Forum Systems, Google Apigee, Imperva, Red Hat, Sensedia, and WSO2.

1.2 Market Segment

We have long recognized the API Economy as one of the most important current 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 RESTful APIs, which are commonly used today, along with the growing variety of alternative protocols and standards.

Unfortunately, many organizations tend to underestimate the potential security challenges of opening up their APIs without a security strategy and infrastructure in place. Such popular emerging technologies as the Internet of Things or Software Defined Computing Infrastructure (SDCI), which rely significantly on API ecosystems, are also bringing new security challenges with them. New distributed application architectures like those based on microservices are introducing their own share of technical and business problems as well.

Creating a well-planned strategy and reliable infrastructure to expose their business functionality to be consumed by partners, customers, and developers is a significant challenge that has to be addressed not just at the gateway level, but along the whole information chain from backend systems to endpoint applications.

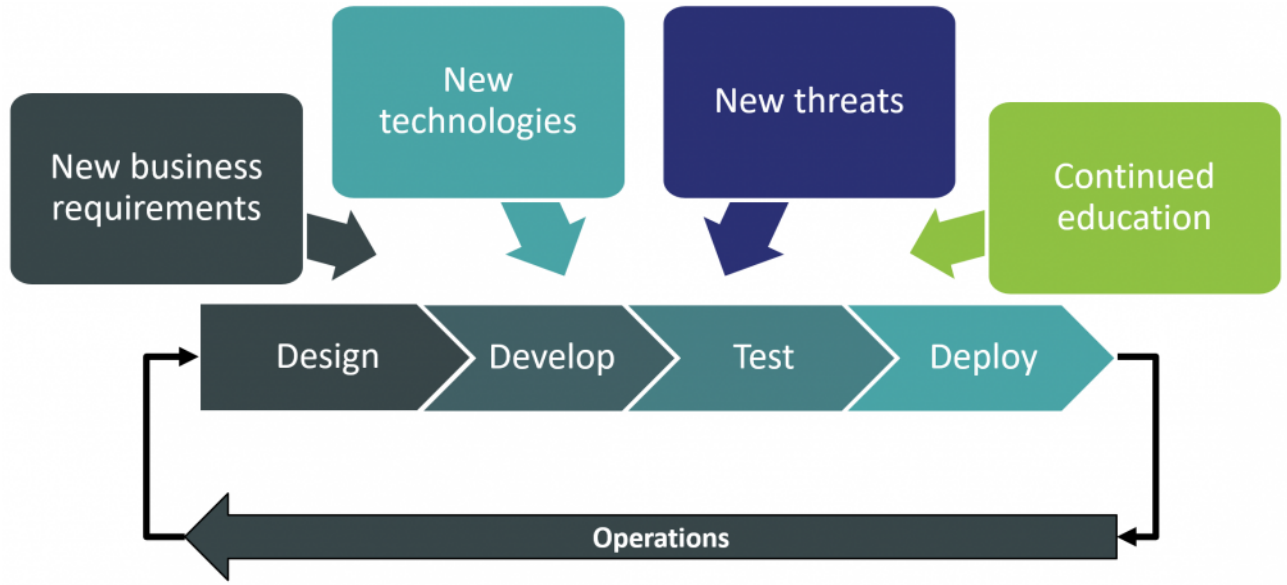


Figure 1: API Lifecycle

It is therefore obvious that point solutions addressing specific links in this chain are not viable in the long term, and KuppingerCole's analysis is primarily looking at integrated API management platforms, but with a strong focus on security features either embedded directly into these solutions or provided by specialized third-party tools closely integrated with them.

When the previous edition of the Leadership Compass on API security was published, the industry was still in a rather early emerging stage, with most large vendors focusing primarily on operational capabilities, with very rudimentary threat protection functions built into API management platforms and dedicated API security solutions almost non-existent. In just a few years, the market has changed dramatically.

On one hand, the core API management capabilities are quickly becoming almost a commodity, with, for example, every cloud service provider offering at least some basic API gateway functionality built into their cloud platforms utilizing their native identity management, monitoring, and analytics capabilities. Enterprise-focused API management vendors are therefore looking into expanding the coverage of their solutions to address new business, security, or compliance challenges. Some, more future-minded vendors are even no longer considering API management a separate discipline within IT and offer their existing tools as a part of larger enterprise integration platforms.

On the other hand, the growing awareness of the general public about API security challenges has dramatically increased the demand for specialized tools for securing existing APIs. This has led to the emergence of numerous security-focused startups, offering their innovative solutions, usually within a single area of the API security discipline.

Unfortunately, as the diagram below illustrates, the field of API security is very broad and complicated, and very few (if any) vendors are currently capable of delivering a comprehensive security solution that could cover all required functional areas. Although the market consolidation continues, with larger vendors

acquiring these startups and incorporating their technologies into existing products, expecting to find a "one-stop shop" for API security is still a bit premature.

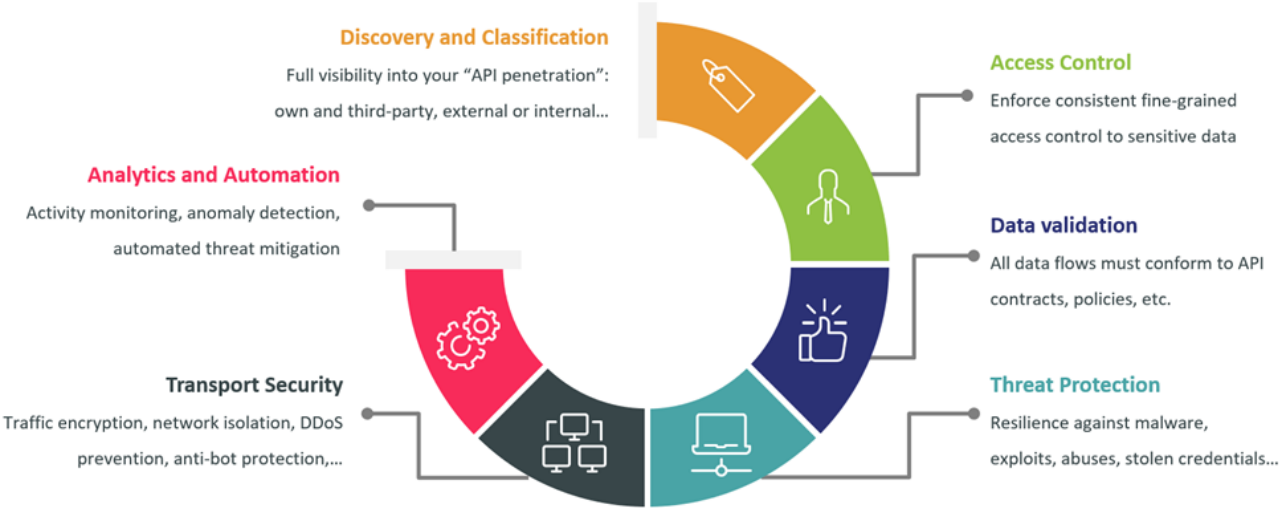


Figure 2: The Scope of API Security

Although the current state of API management and security market is radically different from the situation just a few years ago, and the overall developments are extremely positive, indicating growing demand for more universal and convenient tools and increasing quality of available solutions, it has yet to reach anything resembling the stage of maturity.

Thus, it's even more important for companies developing their API strategies to be aware of the current developments and to look for solutions that implement the required capabilities and integrate well with other existing tools and processes.

1.3 Delivery Models

Since most of the solutions covered in our rating are designed to provide management and protection for APIs regardless of where they are deployed -- on-premises, in any cloud, or within containerized or serverless environments -- the very notion of the delivery model becomes complicated.

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 additional capabilities are now being offered as Software-as-a-Service 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.

1.4 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 -- 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 Productization and Monetization - converting existing APIs into revenue streams requires the functionality to package multiple APIs into convenient business-oriented products, making them available for tiered consumption according to various monetization plans. Additionally, monetization requires comprehensive reporting capabilities and billing management.

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 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.

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.

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.

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.

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

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.
- supporting heterogeneous distributed environments including cloud, containers, microservices, and serverless platforms.

The following are our standard criteria against which we evaluate products and services:

- overall functionality and usability
- internal service security

- size of the company
- number of customers and end-user consumers
- number of developers
- partner ecosystem
- licensing models

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

2 Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Compass. The Compass provides a comparison based on standardized criteria and can help to identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of the pilot phase, based on the specific criteria of the customer.

Based on our rating, we created the various ratings. The Overall rating provides a combined view of the ratings for

- Product
- Innovation
- Market

2.1 Overall Leadership

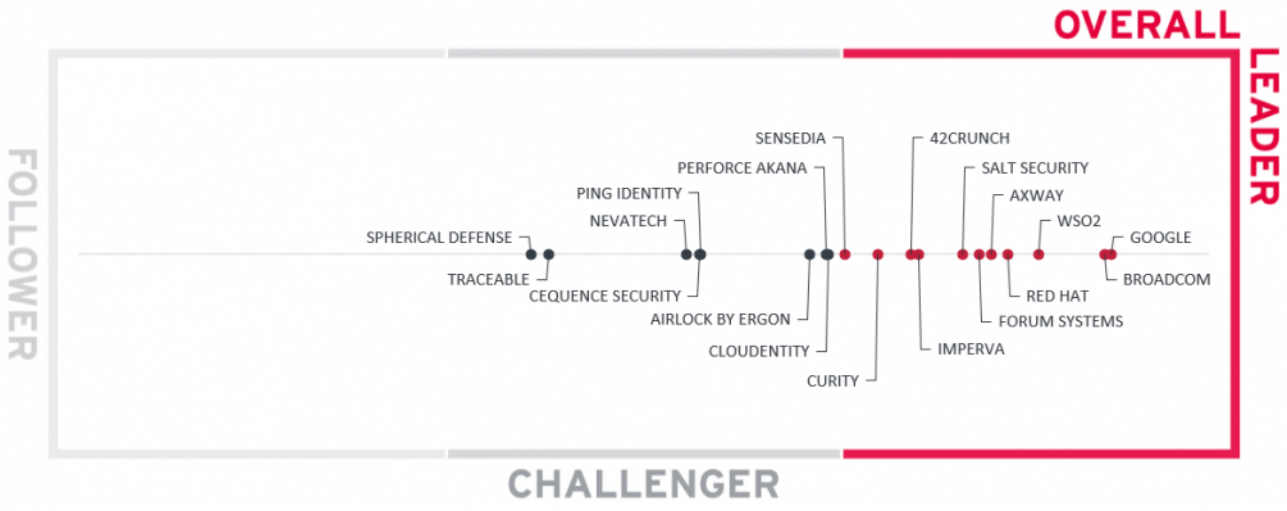


Figure 3: The Overall Leadership rating for the API Management and Security market segment

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 strongly recommend looking at all the leadership categories as well as the sections on each vendor and their offering to get a comprehensive understanding of the players in this market and what use cases they support best.

This year's list of Overall Leaders mirrors to a large extent the situation in the previous edition of this Leadership Compass: most companies in this category are veteran players in the API management and security market, offering comprehensive enterprise-level highly integrated platforms for the most demanding customers.

Axway, Broadcom, Google, Red Hat, and WSO2 are all large established vendors with a global presence, strong partner networks, and large customer bases. This year, they are joined by Imperva, another veteran application security vendor. Thanks to their strong investment in API security, Imperva has substantially improved its ratings and became an Overall Leader as well.

Forum Systems is still being recognized for its continued "security first" approach in its product design, as well as ongoing innovations in areas like DevOps and API analytics.

42Crunch, Curity, and Salt Security, relatively small and focusing on narrower functionality segments, have joined the leaders as well, due to their improved financial stability, steady innovation, and continued investment into new functionality. Sensedia, a Brazilian company offering a comprehensive fully integrated API management stack, continues to improve their presence outside their native Latin American market.

Airlock by Ergon, Cloudentity, and Perforce Akana are found among the Challengers so close to the leaders that they have strong chances to cross the border in the next edition of this Leadership Compass. The rest of the vendors are found somewhat behind. Lacking the combination of an exceptionally strong market and product leadership, they still deliver mature solutions excelling in certain functional areas.

There are no Followers in the overall leadership rating.

Overall Leaders (in alphabetical order):

- 42Crunch
- Axway
- Broadcom
- Curity
- Forum Systems
- Google Apigee
- Imperva
- Red Hat

- Salt Security
- Sensedia
- WSO2

2.2 Product Leadership

The first of the three specific Leadership ratings is about **Product** leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services. 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. This is why we have a mix of large and small vendors among the leaders.

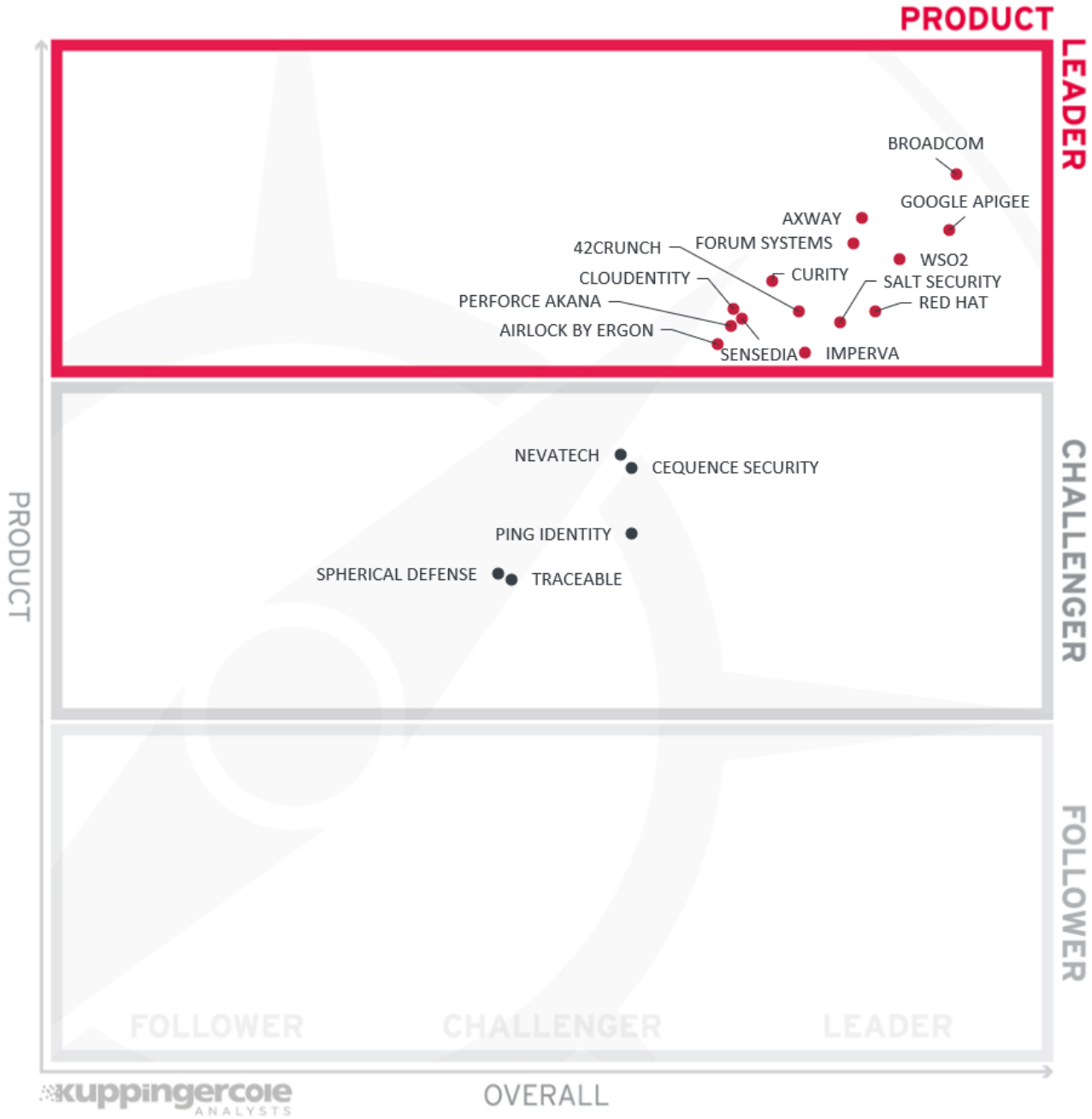


Figure 4: Product Leaders in the API Management and Security segment

Most large vendors mentioned earlier are present in the Leaders segment, including Apigee, Axway, Broadcom, Imperva, Perforce, Red Hat, and WSO2. However, company size is not the only thing that matters. Forum Systems and Sensedia, as already mentioned earlier, are notable for their comprehensive capabilities. Smaller startup companies like 42crunch and Salt Security are nevertheless able to deliver innovative API security features. Cloudentity and Curity, focusing only on identity and authorization for APIs, manage to deliver robust access control and security solutions for modern microservice-based application architectures.

The rest of the vendors are populating the Challengers segment of our product rating. This does not diminish their achievements in specific areas of the API market but rather highlights their focus on a relatively narrow segment of the capabilities we're analyzing. With the scope of API security quickly expanding, vendors must act especially fast to keep up with the changes and offer comprehensive, broad coverage for new API-related security challenges. Most of the companies that landed in the Challenger segment this year have a strong opportunity to become leaders in the next Leadership Compass edition.

Product Leaders (in alphabetical order):

- 42crunch
- Airlock by Ergon
- Axway
- Broadcom
- Cloudentity
- Curity
- Forum Systems
- Google Apigee
- Imperva
- Perforce Akana
- Red Hat
- Salt Security
- Sensedia
- WSO2

2.3 Innovation Leadership

Next, we examine **Innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements.

Innovation is not limited to delivering a constant flow of new releases. Rather, innovative companies take a

customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

Our Innovation Leadership shows an impressive mix of both large and small vendors. This clearly indicates, on one hand, the huge potential for ongoing innovation on various areas of API management and security, and on the other hand shows 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.

Large global vendors like Axway, Broadcom, Google, Imperva, Perforce, or Red Hat have enough resources at their disposal to continuously expand and improve their API management platforms and deliver consistent innovation over years. Somewhat smaller companies like Forum Systems, Sensedia, and WSO2 with their comprehensive API platforms manage to achieve the Leader status in our rating as well.

Yet even small companies like 42crunch, Cequence Security, Cloudentity, Curity, Ergon, Salt Security, or Traceable have been rated high on innovation because of their disruptive product developments in their respective focus areas of API security.

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.

Figure 5: Innovation Leaders in the API Management and Security segment

Innovation Leaders (in alphabetical order):

- 42crunch
- Airlock by Ergon
- Axway

- Broadcom
- Cequence Security
- Cloudentity
- Curity
- Forum Systems
- Google Apigee
- Red Hat
- Perforce Akana
- Salt Security
- Sensedia
- Traceable
- WSO2

2.4 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 financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

Figure 6: Market Leaders in the API Management and Security segment

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.

Completely unsurprisingly, we find all large veteran players among the Market Leaders, including both API management and API security vendors. This year, Forum Systems and Imperva have joined the segment as well, indicating their stronger market positions.

Most other smaller companies populate the Challengers segment, reflecting their ongoing journeys towards

a larger market presence. The only larger vendor here is Perforce, which has not yet established itself as a household name in the API management market. A notable change since our previous edition, 42crunch has managed to gain enough paying customers to upgrade from the Followers to the Challengers in our market rating.

The only company among the Followers is Traceable, reflecting its relatively short presence in the market since the launch.

Market Leaders (in alphabetical order):

- Axway
- Broadcom
- Forum Systems
- Google Apigee
- Imperva
- Ping Identity
- Red Hat
- Salt Security
- WSO2

3 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.

3.1 The Market/Product Matrix

The first of these correlated views contrasts Product Leadership and Market Leadership.

Figure 7: 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 Axway, Broadcom, Google, Imperva, Red Hat, and WSO2, followed by Forum Systems and Salt Security.

The vendors in the right middle box are those whose capable products are yet to win them a strong market

presence: here we find 42crunch, Cloudentity, Curity, Ergon, Perforce and Sensedia. The top middle box contains the vendors that, to an extent, owe their market presence to other products beyond the API segment. In this case, we can find Ping Identity here, a well-established identity and access management vendor.

Most other vendors can be found in the middle box, indicating average results both in product and market leadership -- they clearly have the potential for future improvement.

The only smaller vendor that is yet to gain enough paying customers is Traceable, a young startup company -- it can be found in the bottom center box.

3.2 The Product/Innovation Matrix

This view shows how Product Leadership and Innovation Leadership are correlated. It is not surprising that there is a pretty good correlation between the two views with a few exceptions. The distribution and correlation are tightly constrained to the line, with a significant number of established vendors plus some smaller vendors. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

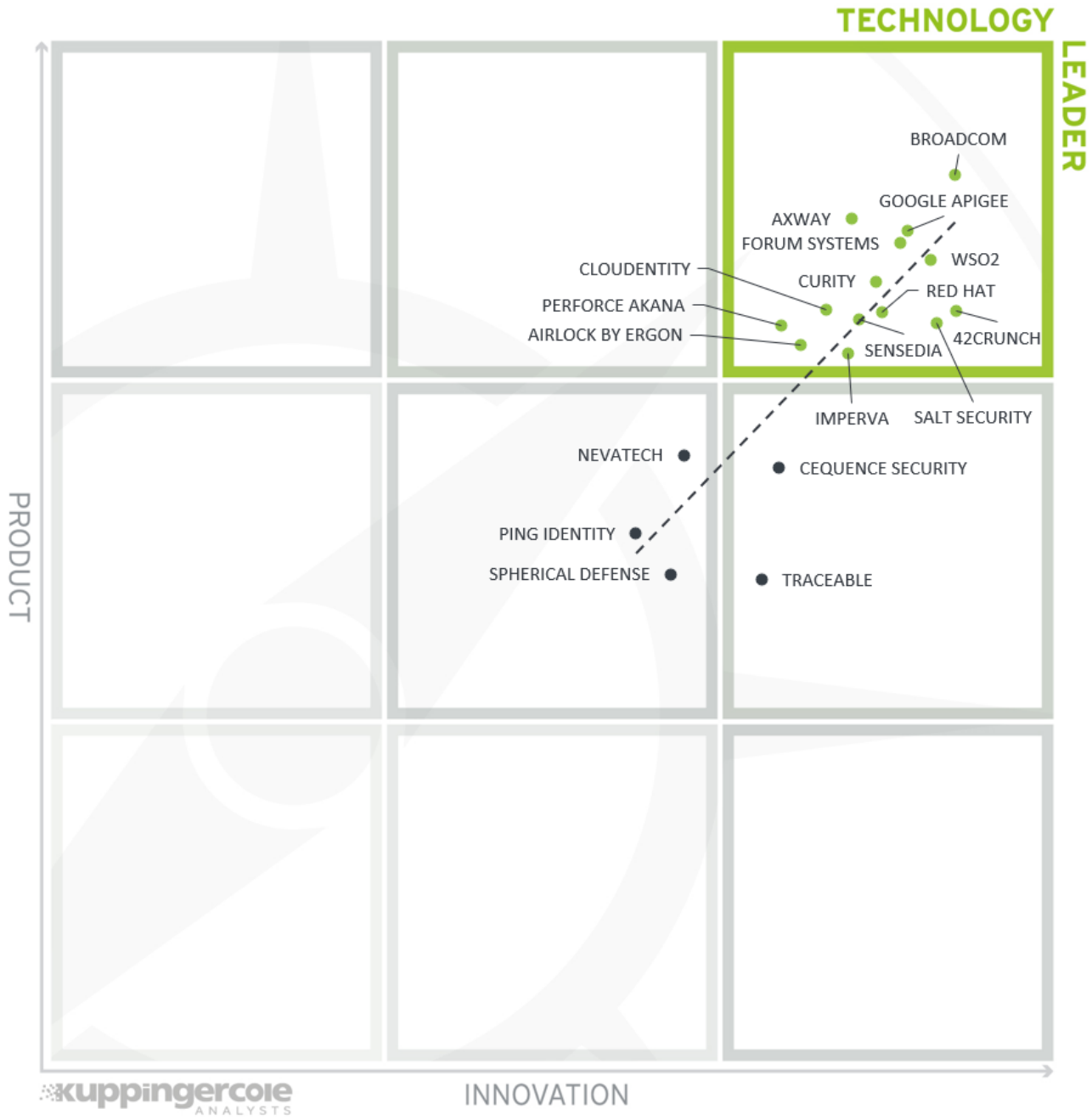


Figure 8: The Product / Innovation Matrix

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 management and security 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. Traceable and Cequence Security can be found in the right middle box, indicating their position in the early stage of the startup lifecycle, when even a highly innovative

technology has not been fully implemented in a mature product yet. Nevatech, Ping Identity, and Spherical Defense can be found in the middle box, showing their potential for increased R&D.

3.3 The Innovation/Market Matrix

The third matrix shows how Innovation Leadership and Market Leadership are related. 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, highly innovative vendors have a good chance of improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

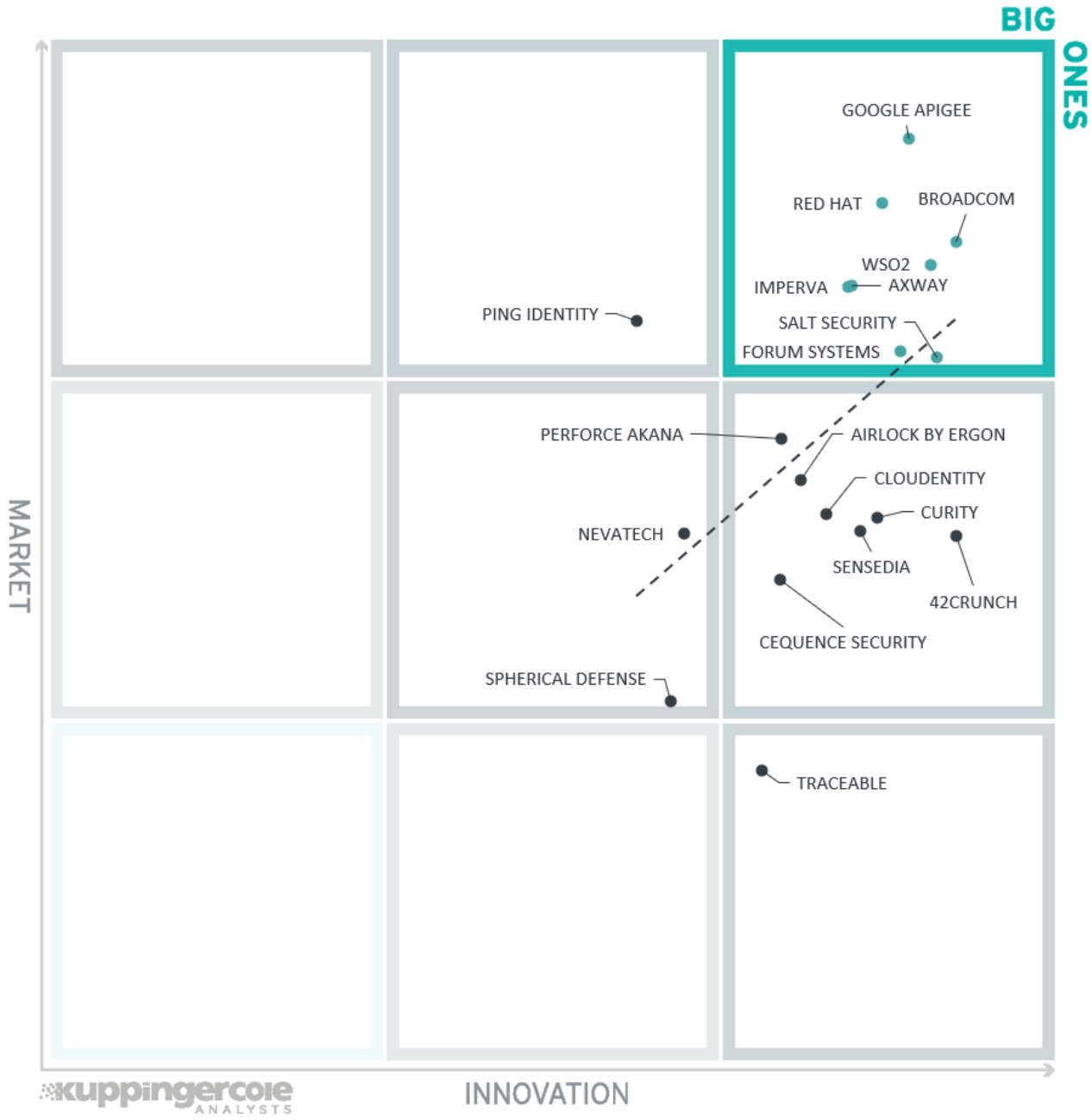


Figure 9: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

Yet again, we observe the largest market players in the top right segment, joined this time by Forum Systems and Salt Security, innovative API security vendors that have already established substantial market presence. Most of the vendors are scattered across the right middle segment of the matrix, indicating their strong potential for improving their market position in the future.

The only companies found in the middle box are Nevatech with its relatively narrow but nevertheless successful focus on the Windows ecosystem and Spherical Defense, which is still working to improve their market visibility.

Traceable is the only vendor to be found in the bottom right corner -- as a young startup, they are yet to establish their customer base.

4 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 Management and Security. 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.

Product	Security	Functionality	Interoperability	Usability	Deployment
42Crunch	positive	positive	strong positive	strong positive	strong positive
Airlock by Ergon	strong positive	positive	positive	strong positive	strong 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	positive	positive	positive
Cloudentity	strong positive	positive	strong positive	strong positive	strong positive
Curity	strong positive	positive	strong positive	strong positive	positive
Forum Systems	strong positive	strong positive	strong positive	positive	strong positive
Google Apigee	strong positive	strong positive	strong positive	strong positive	strong positive
Imperva	strong positive	positive	positive	strong positive	positive
Nevatech	positive	positive	positive	positive	neutral
Perforce Akana	strong positive	positive	positive	strong positive	strong positive
Ping Identity	positive	positive	positive	neutral	neutral
Red Hat	positive	strong positive	strong positive	positive	positive
Salt Security	strong positive	strong positive	strong positive	positive	strong positive
Sensedia	positive	strong positive	positive	strong positive	positive
Spherical Defense	positive	positive	positive	positive	positive
Traceable	neutral	positive	neutral	positive	strong positive
WSO2	strong positive	strong positive	strong positive	strong positive	positive
Legend		critical	weak	neutral	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	weak	neutral	positive
Airlock by Ergon	positive	neutral	positive	positive
Axway	positive	positive	strong positive	positive
Broadcom Inc.	strong positive	strong positive	strong positive	strong positive
Cequence Security	positive	neutral	neutral	neutral
Cloudentity	positive	neutral	neutral	positive
Curity	positive	positive	positive	positive
Forum Systems	positive	positive	strong positive	positive
Google Apigee	positive	strong positive	strong positive	strong positive
Imperva (was acquired by Thoma Bravo)	positive	positive	strong positive	strong positive
Nevatech	neutral	neutral	neutral	neutral
Perforce Akana	neutral	positive	positive	positive
Ping Identity	neutral	positive	strong positive	positive
Red Hat	positive	positive	strong positive	strong positive
Salt Security	strong positive	positive	positive	positive
Sensedia	positive	positive	positive	neutral
Spherical Defense	positive	neutral	neutral	neutral
Traceable	positive	weak	weak	weak
WSO2	strong positive	strong positive	positive	strong positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 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. For the LC API Management and Security, we look at the following categories:

- **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.

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services 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 features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations of API Management and Security technologies.

5.1 42Crunch

42Crunch is a privately held API security startup company with offices in Dublin, Ireland, Montpellier, France, and Irvine, CA. 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 other stakeholders. 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 200,000 users.

Perhaps the most notable change since our last review is the substantial investment the company was able to secure in 2021, allowing it to increase its development team, as well as focus on growing market visibility, winning an impressive number of new enterprise customers.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

42crunch

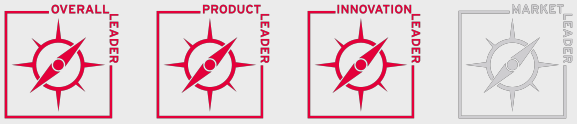
Strengths

- 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, including VS Code, IntelliJ, and Eclipse.

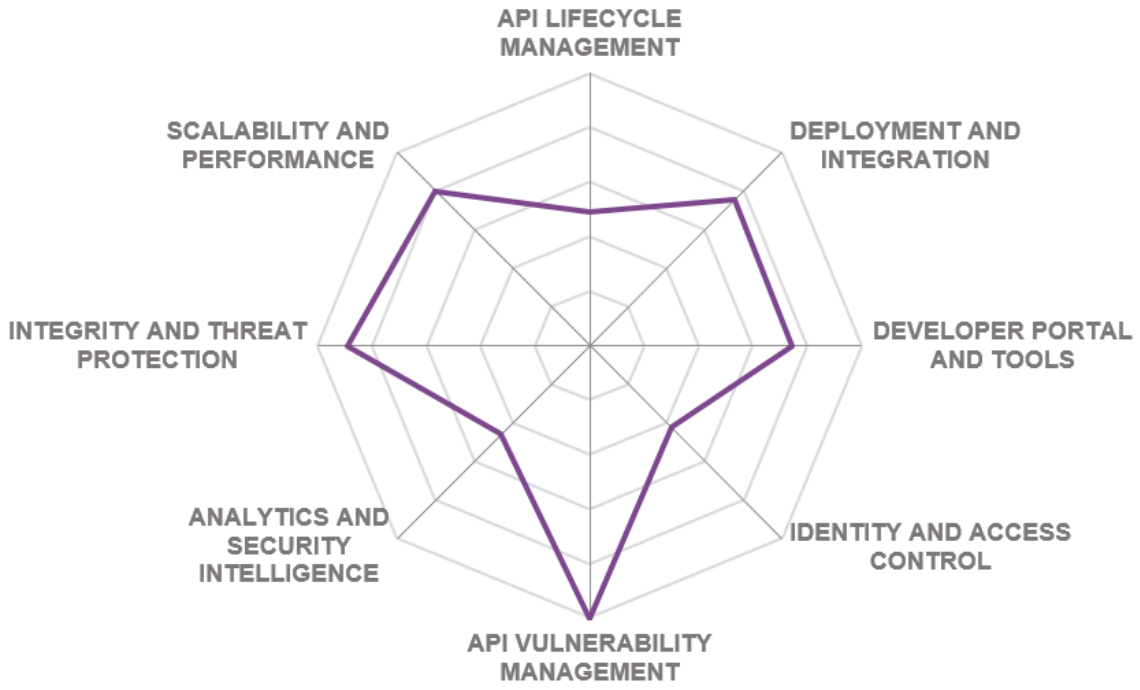
Challenges

- Small but growing enterprise customer base.
- Focus on proactive security only.
- Security analytics only with third-party tool integrations.

Leader in



42CRUNCH


API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.2 Airlock by Ergon

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. Their partner ecosystem is again focused in DACH but remains small in the other areas. Two primary technologies the company has been known for are Web Access Management and Identity Federation (Airlock IAM) and Web Application Firewall (Airlock WAF); together they form the foundation of Ergon's integrated offering.

A notable recent addition to the platform is support for modern containerized and microservice architectures with a lightweight and DSL configurable Airlock Microgateway. The platform supports hybrid policy management by separating shared and local policies to ease the collaboration between developers and security administrators.

Known until recently simply as Airlock Suite, the company's flagship product has been relaunched under the new Airlock Secure Access Hub brand. This new integrated platform 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 API does implement basic API management functions such as monitoring, statistics, or key management, they are fairly simple, and the company positions the product rather 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.

Unfortunately, Ergon is still fairly unknown outside its home market. However, the company's lean and well-integrated product can be recommended for evaluation by any company looking for an all-in-one solution for enforcing sensitive data protection across multiple channels, beyond just APIs.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

AIRLOCK®
SECURE ACCESS HUB

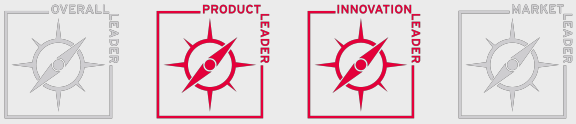
Strengths

- 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.
- Dynamic Value Endorsement for data validation without API contracts.
- Bug bounty program to validate and improve the products' security.

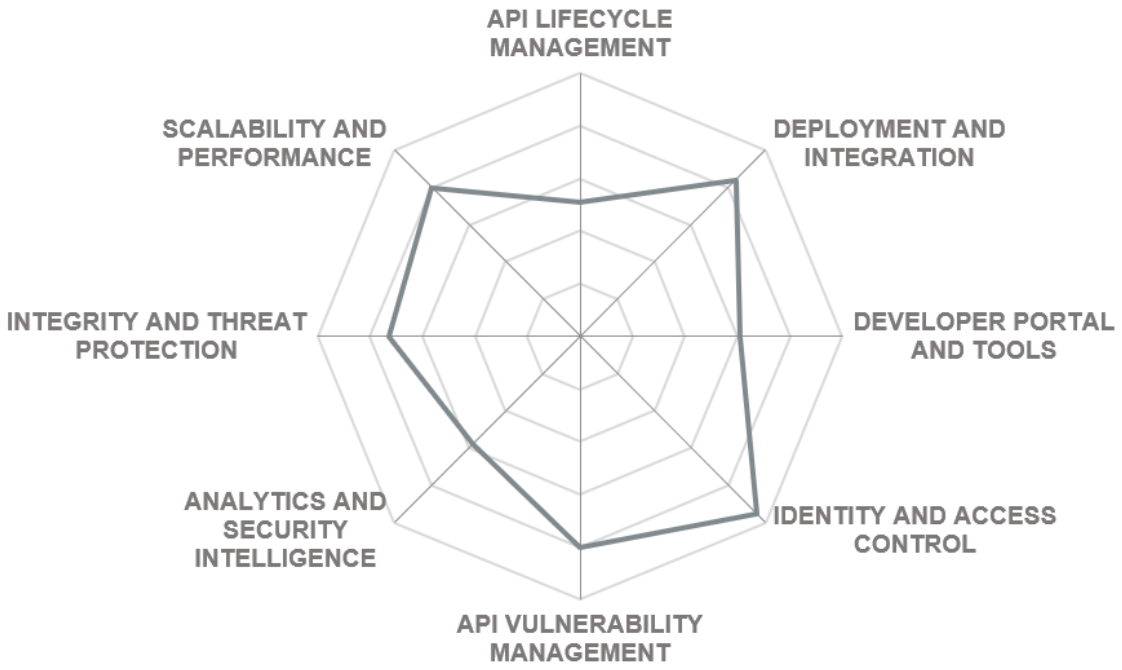
Challenges

- API monitoring and management capabilities are limited.
- No public-facing developer portal is available yet.
- Small partner ecosystem & limited global reach.

Leader in



AIRLOCK BY ERGON



5.3 Axway

Axway, founded in 2001, is a global software company headquartered in Phoenix, 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 Catalog and API Portal to enable collaborative API provider and API consumer experiences; Integration Builder and API Builder -- graphical low-code API tools for SaaS integration and microservice-based 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.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

axway

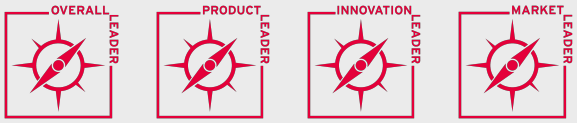
Strengths

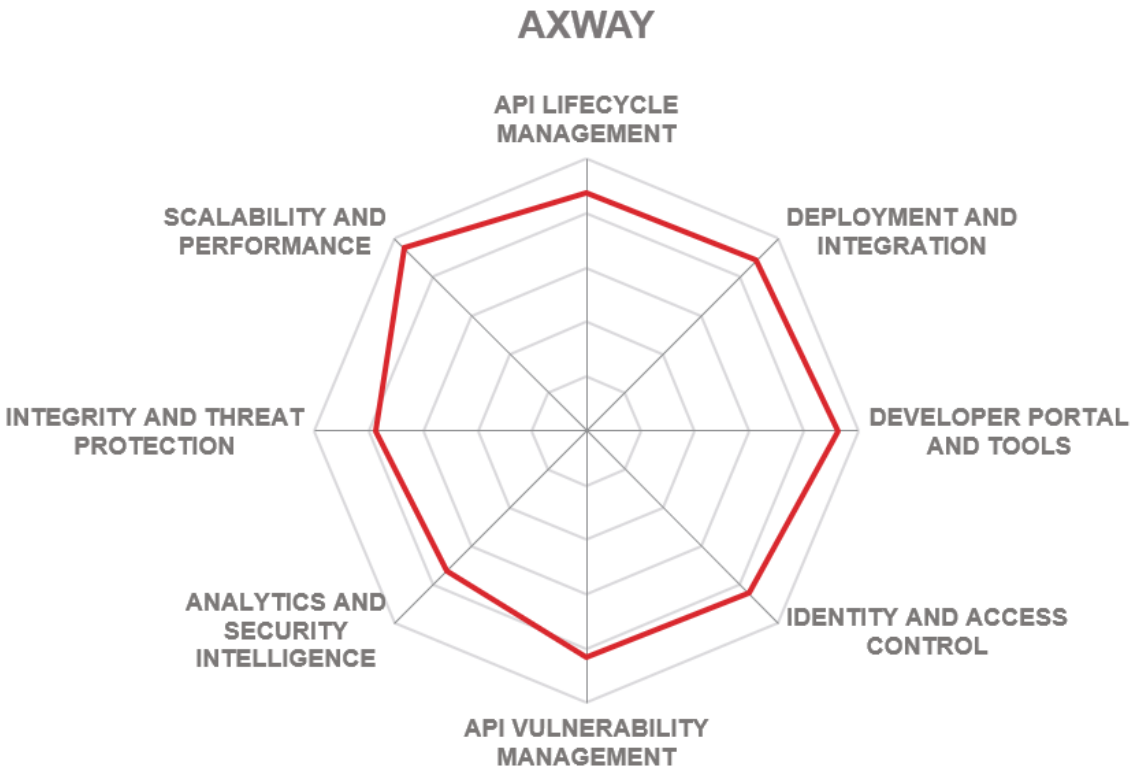
- Multiple gateway types (Axway and third-party), including support for microservices and cloud deployments - with a centralized management plane.
- Broad range of patterns and API types, including REST, SOAP, GraphQL, and AsyncAPI.
- Automated discovery of all API types across heterogeneous environments.
- Low-code integration tools for creating and orchestrating APIs.

Challenges

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

Leader in




AXWAY
API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.4 Broadcom Inc.

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 now 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-prem, multi-cloud, containerized, and mobile environments. Broadcom's API Academy offers the only industry-agnostic, free API certification program with multiple courses and exams.

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	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

BROADCOM®

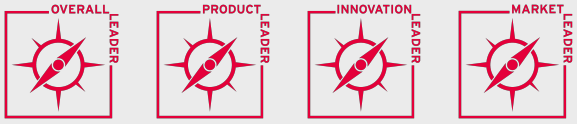
Strengths

- 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.
- Industry-agnostic API certification program

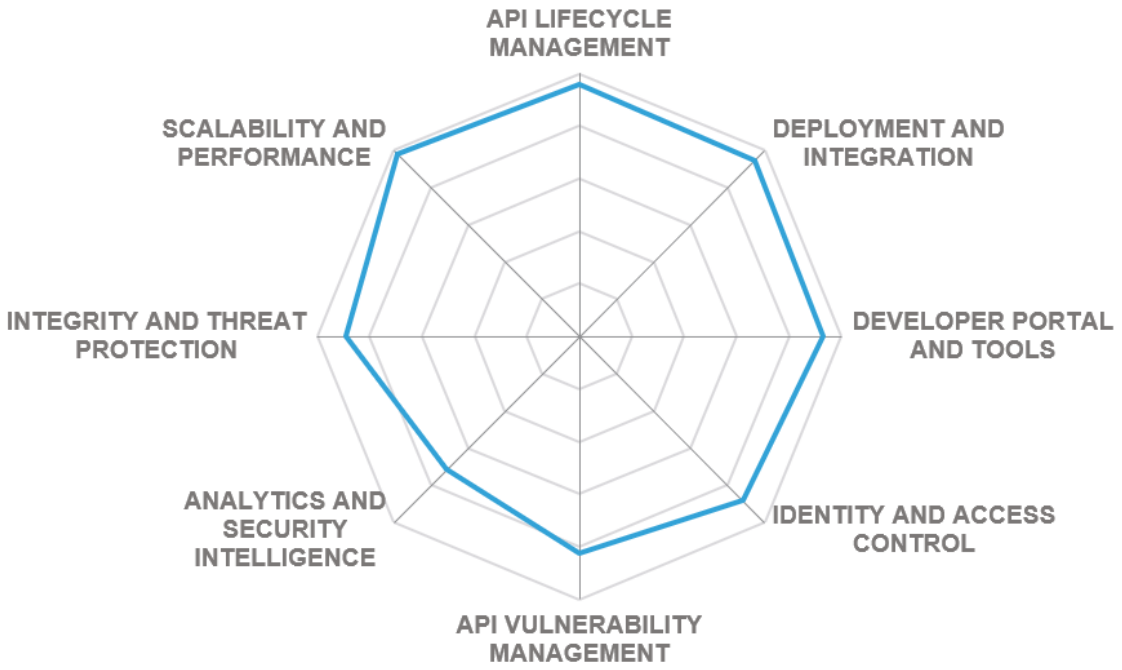
Challenges

- Targeted primarily towards large enterprise customers, might be too complex for smaller companies.
- Advanced API monitoring and analytics relies on additional Broadcom products.
- Lack of a single consistent UI across all parts of the platform.

Leader in



BROADCOM


API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.5 Cequence Security

Cequence Security is a cybersecurity company headquartered in Sunnyvale, California. Founded in 2015 by a group of security industry veterans previously from Palo Alto Networks and Symantec, 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, and risk assessment.

API Sentinel is the company's specialized API security product, a cloud-native, easily deployable solution for performing real-time API discovery and usage analysis, detection of OpenAPI specification non-conformance, and risk assessment according to multiple metrics and policies, helping users to identify and mitigate API-related security risks before they turn into data breaches. Together with the company's other solutions like Bot Defense and App Firewall, Cequence Security can offer its customers a comprehensive, well-integrated platform for addressing API risks at multiple stages of their lifecycles.

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 of each application or API, 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 built upon this foundation and implements discovery, monitoring, and real-time risk assessment for APIs in a wide variety of environments. As opposed to many competing solutions that typically focus either on edge deployment scenarios or on distributed, microservice-oriented architectures (deployed alongside business microservices and monitoring internal API traffic), API Sentinel, thanks to its flexible container-based architecture and breadth of technology integrations (API gateways, proxies, ingress controllers, load balancers, etc.) can mix and match both approaches. Ease of deployment and rich reporting functions ensure that even smaller companies without teams of experts trained in the field of API security can start with the platform without a lengthy setup and learning process.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●●○

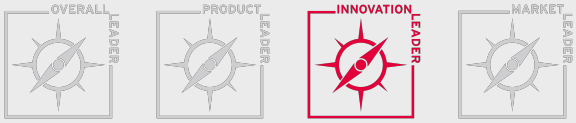
Strengths

- Integrated application security platform powered by purpose-built AI-driven analytics engine.
- A broad set of technology integrations enable the discovery and protection of both external and internal APIs.
- Automated API inventory simplifies management, 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.

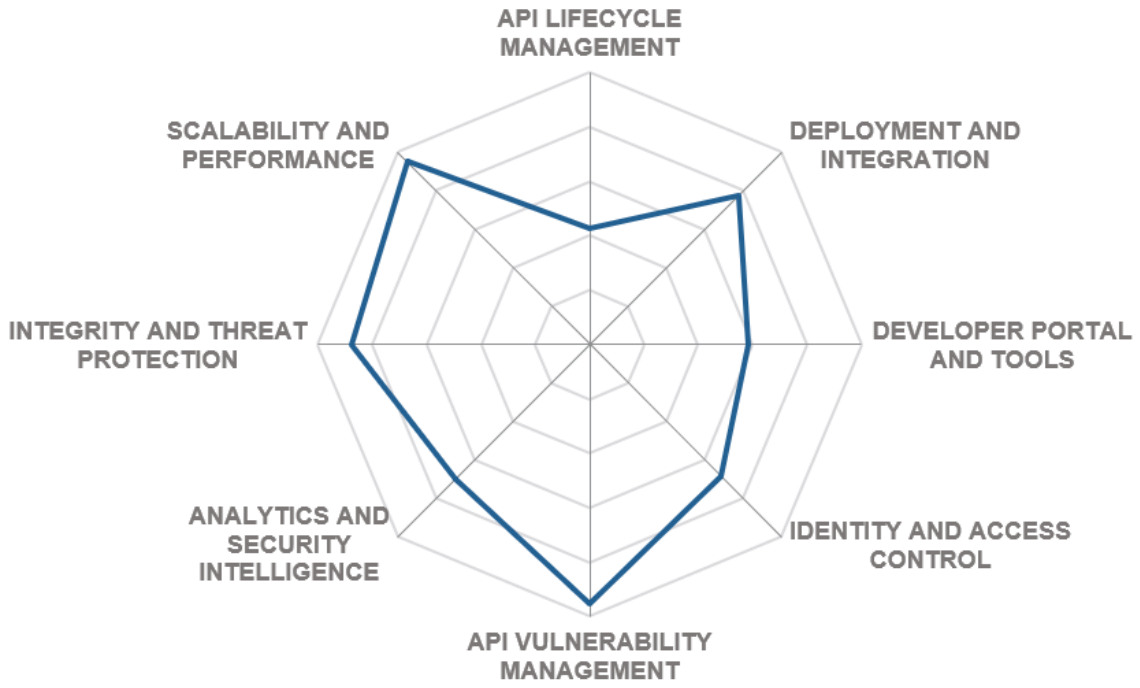
Challenges

- Individual modules of the Application Security Platform are not yet integrated into a single management console.
- The number of out-of-the-box content inspection patterns is still quite low.
- Customer base currently limited to North America, expanding to Europe

Leader in



CEQUENCE SECURITY



5.6 Cloudentity

Cloudentity is a privately held identity, authorization and governance company headquartered in Seattle, WA. Cloudentity was formed in 2016, focusing on securely connecting API driven applications to data using authorization, consent and governance within their Authorization Control Plane (ACP).

ACP provides automated fine-grained authorization and consent capabilities for any application architecture. Cloudentity's ACP discovers and protects APIs, providing rich data governance and lineage across public/private clouds, API Gateways, service meshes, and traditional architectures.

Cloudentity's platform provides a broad range of identity and API security services designed specifically for hybrid and micro-service architectures. 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 and governance; seamlessly integrating identity providers and externalizing identity and authorization for APIs.

The company uses the term "Microperimeter" to refer to the concept of deploying API discovery and authorization policy decision points as close to the API endpoints and workloads that need to be secured. In 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.

Although Cloudentity's authorization platform is technically not an API management or security solution in a traditional sense, 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. For more traditional security capabilities, the platform supports ML-based API discovery, session tampering parameter validation, protection against DDoS and token replay attacks, integrations with popular third-party API gateways, and auditing and logging via an analytics platform.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●●

CLOUDENTITY™

CUSTOMER IDENTITY AT CLOUD SPEED

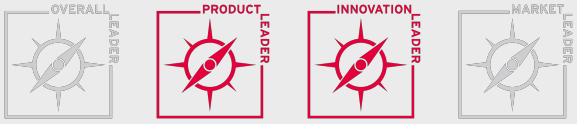
Strengths

- 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.

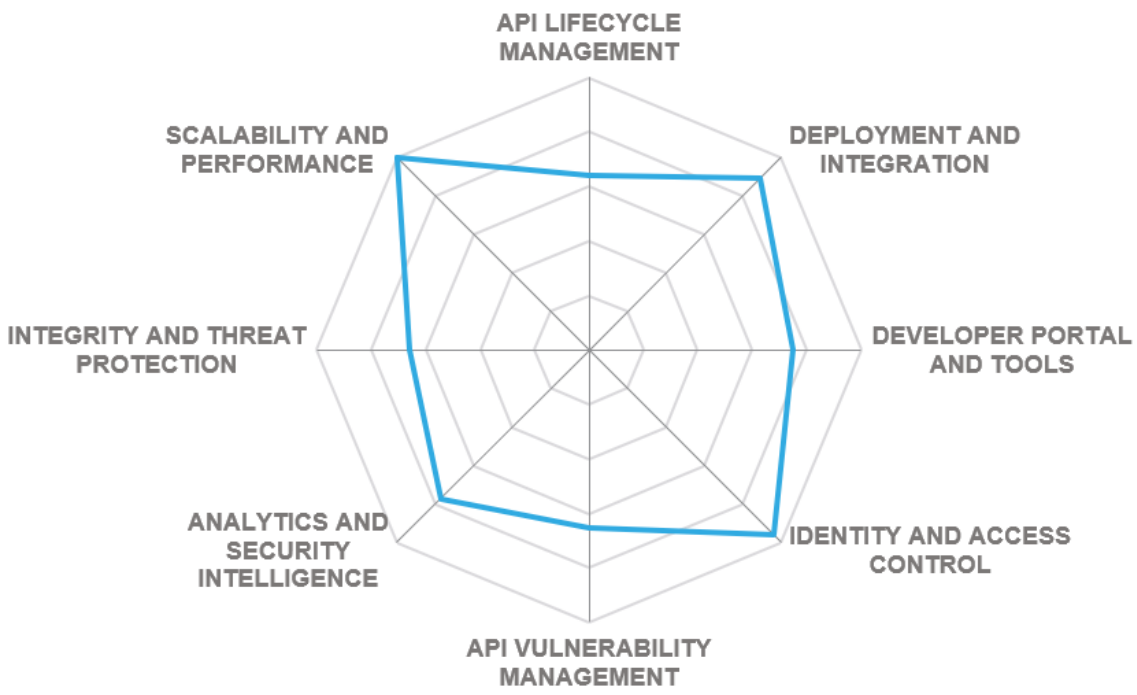
Challenges

- Not an API security solution in the traditional sense, focusing only on identity and authorization.
- Distributed architecture, less suitable for “legacy” APIs.
- Medium size customer base without the international reach of large companies

Leader in



CLOUDENTITY



5.7 Curity

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 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 OAuth2, 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, multi-factor authentication methods, Single Sign-On, and process workflows.

The foundation 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.

The flagship new feature recently implemented by Curity is their Hypermedia Authentication API, which allows creating native clients that use OAuth and OpenID Connect flows without relying on browser support. 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.

Curity Identity Server is not an API management or security solution. However, 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 proxy that implements simple and scalable data and privacy protection for publicly exposed API endpoints.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

CURITY

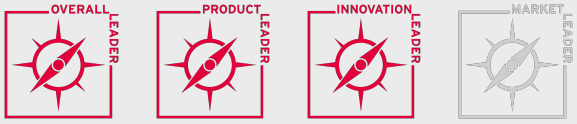
Strengths

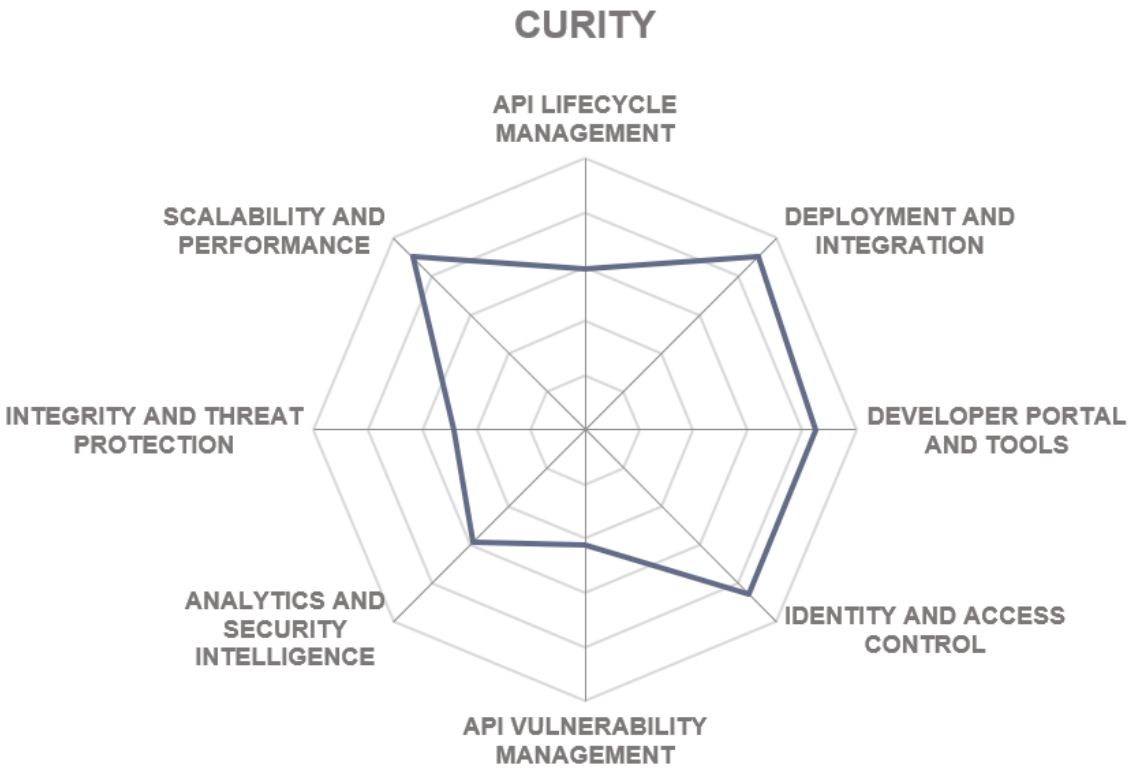
- Comprehensive support for OAuth and OIDC open standards.
- Combines flexible authentication with token-based API security controls.
- Hypermedia Authentication API for native clients.
- Comprehensive Open Banking compliance.
- Reference “phantom token” architecture for privacy protection.

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 EMEA

Leader in




CURITY
API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.8 Forum Systems

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.

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

In addition, the company's developer portal solution has been substantially reworked and improved for 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.

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	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●●

FORUMSYSTEMS
THE LEADER IN API SECURITY MANAGEMENT

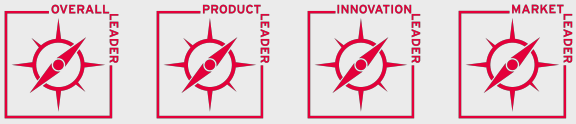
Strengths

- "Security by design" architecture for maximum reliability; FIPS 140-2 and NIAP NDPP-certified.
- Comprehensive API threat protection capabilities.
- Supports a broad range of identity and access control standards, tokens, and credentials.
- Significantly expanded choice of deployment and integration scenarios.

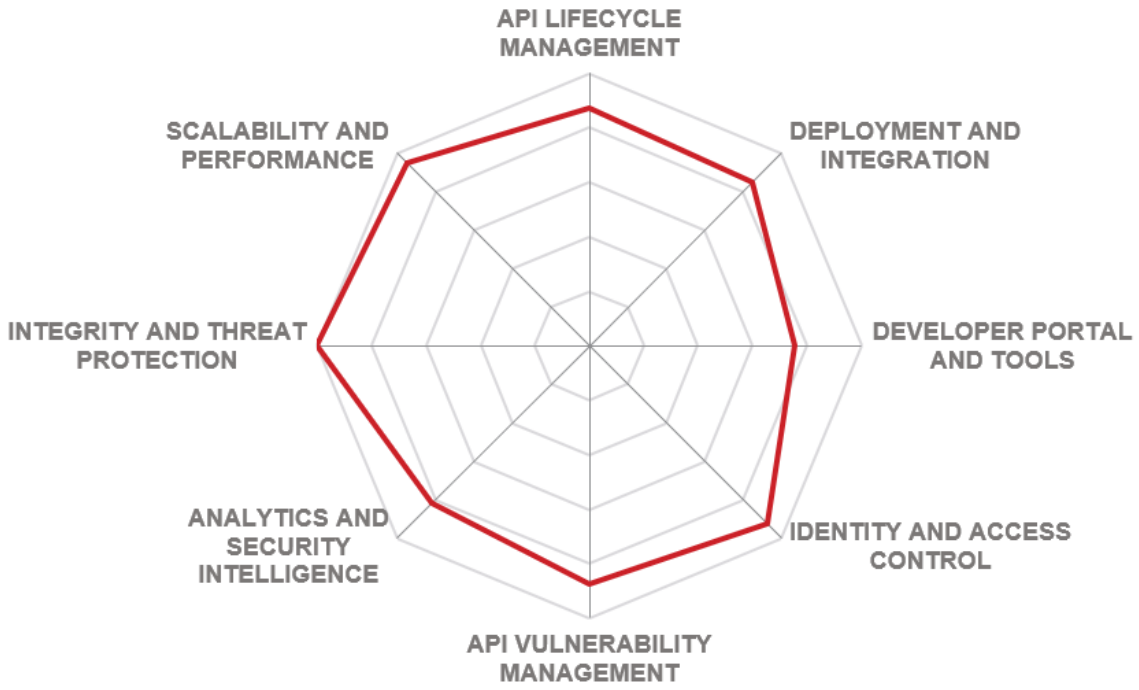
Challenges

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

Leader in



FORUM SYSTEMS



5.9 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 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.

In early 2021, Google has introduced Apigee X, a 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.

Security	● ● ● ● ●
Functionality	● ● ● ● ●
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●
Deployment	● ● ● ● ●

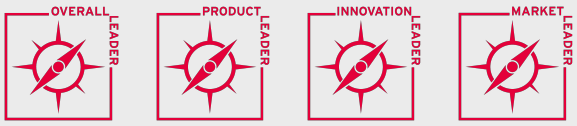
Strengths

- Comprehensive API management platform covering all aspects of API lifecycle.
- Three types of API gateways and Istio service mesh integrations.
- Sophisticated yet user-friendly policy management.
- Extended monitoring and analytics with Apigee Sense.
- Deep integration with other Google Cloud services, including web attack and DDoS protection.

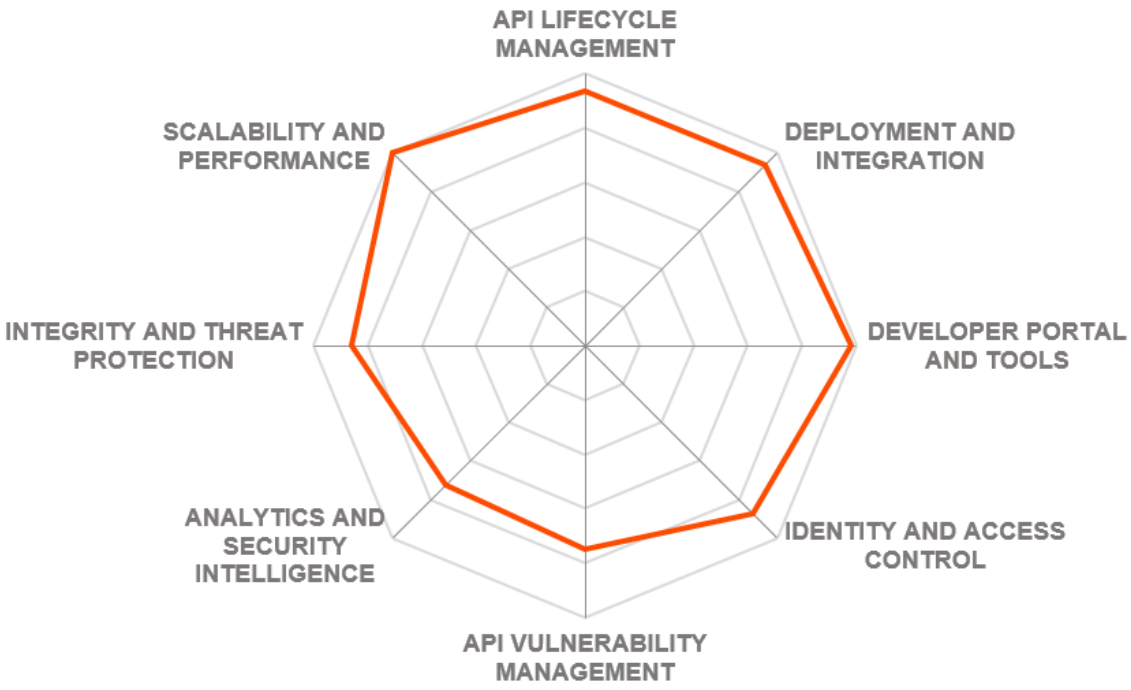
Challenges

- Security analytics lacks detailed views, no focus on forensic investigations.
- No third-party security tool integrations.
- Advanced security functions only achieved with custom extensions.

Leader in



GOOGLE APIGEE



5.10 Imperva (was acquired by Thoma Bravo)

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 and providing a substantial boost in R&D.

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 Application Security suite that provides services like CDN, 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 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 May 2021, Imperva has completed the acquisition of CloudVector, an API security-focused startup company, founded in 2018 in Los Altos, California, bringing in the technology for discovering, monitoring, and securing all corporate APIs regardless of their deployment environment. CloudVector's "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.

Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○

imperva

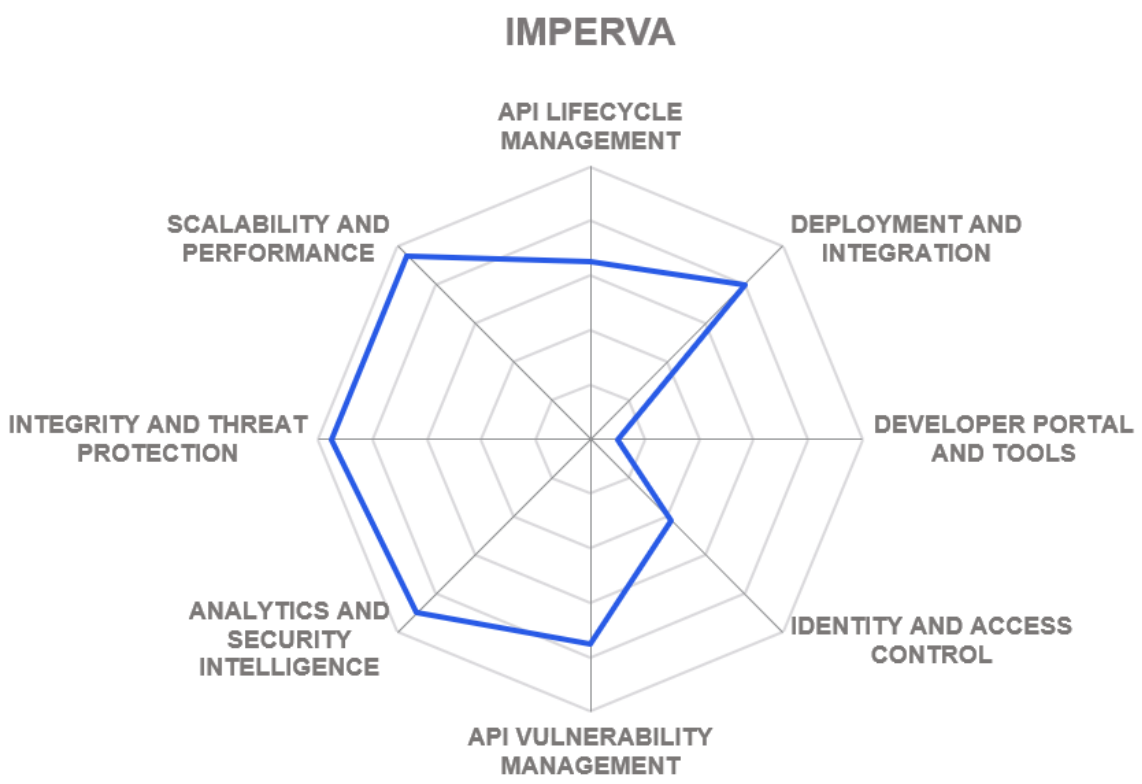
Strengths

- 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.
- Comprehensive API attack analytics and threat reputation intelligence.
- Strong platform hardening and security capabilities.

Challenges

- Support for microservice-based applications is still work in progress.
- Advanced API detection and response are not yet fully integrated into the platform.
- Does not provide tools for API developers.

Leader in


IMPERVA
API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.11 Nevatech

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 somewhat 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-prem, 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 May 2021, Nevatech has released the Sentinet 6.3. The new version introduces several major new features, such as virtualization profiles that allow quick, one-click virtualization of physical API services, storing of shared identities in the Sentinet Repository, improved management of OAuth credentials among others.

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.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●○
Deployment	●●●○○

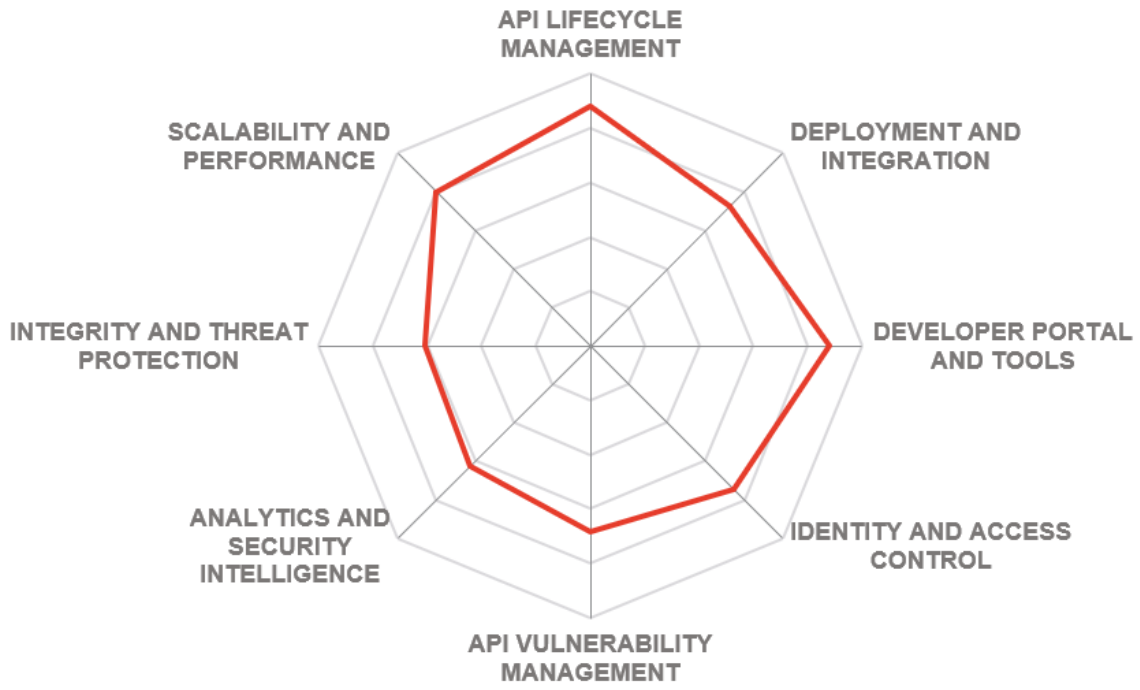
Strengths

- 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.

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.

NEVATECH


API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.12 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.

Although Akana API platform might not yet support 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	●●●●●
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●●

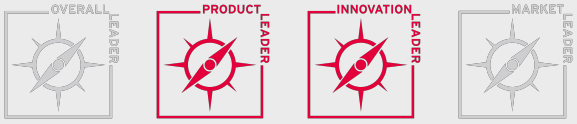
Strengths

- Fully integrated API management platform covering all aspects of 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.

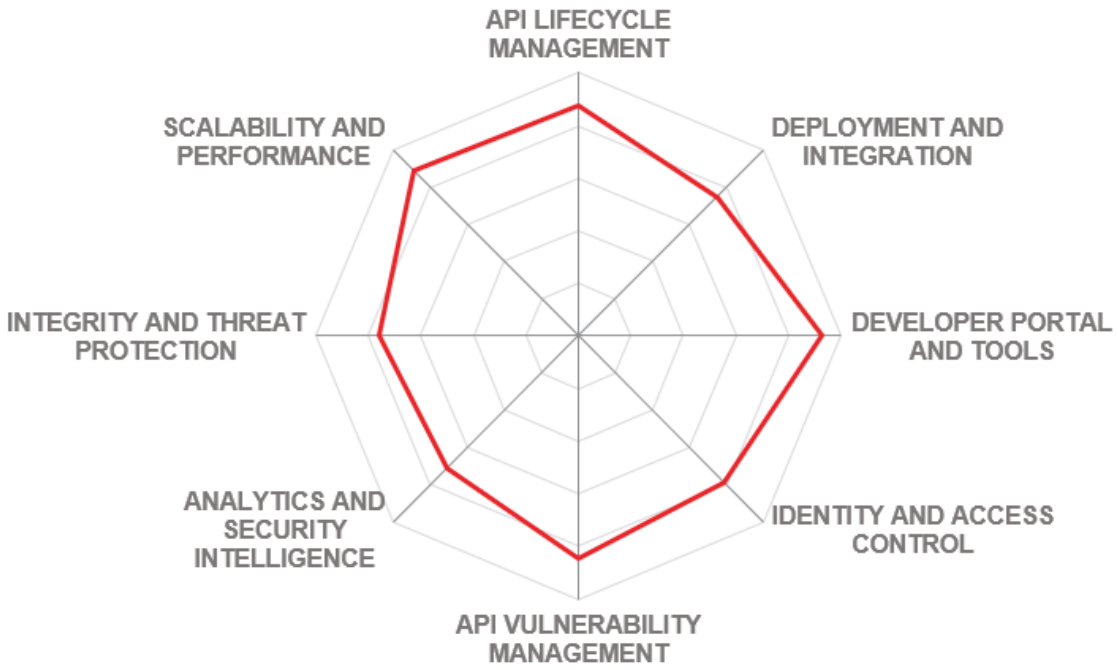
Challenges

- Community recognition not yet as strong as leading competitors.
- No support for modern standards like GraphQL or gRPC yet (roadmap item).
- Business analytics only available via a separately licensed product.

Leader in



PERFORCE AKANA



5.13 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 offers products like PingAccess, one of the leading access management solutions implementing identity-centric access controls for apps and APIs, with a comprehensive policy engine and risk-aware authorization, or PingAuthorize that provides centralized, fine-grained authorization policies for various data sources, including those accessed via APIs.

PingAuthorize is a general-purpose dynamic authorization solution that enables organizations to develop and enforce fine-grained security and compliance policies across multiple applications and data sources. By integrating with existing third-party API gateways, access management and governance policies can be seamlessly extended to APIs as well. This enables protection and automated blocking of various attack types and prevention of data breaches by filtering and redacting sensitive data.

In 2018, Ping Identity acquired Elastic Beam, a pioneering API security intelligence company that focused on deep visibility into API traffic, automatic API discovery, and AI-powered API attack detection and blocking. Now, this technology is offered as PingIntelligence for APIs.

PingIntelligence for APIs 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. Somewhat unusually, PingIntelligence also incorporates a deception technology to lure attackers to honeypots and enable instant, deterministic identification of hacking attempts.

Even though Ping identity's solution still lacks some important security capabilities (for example, API lifecycle management functions), its quick deployment, ease of use and comprehensive automation features still make it a notable contender for many potential customers, especially organizations lacking strong own API security expertise.

Security	●●●●○
Functionality	●●●●○
Interoperability	●●●●○
Usability	●●●○○
Deployment	●●●○○

Ping Identity

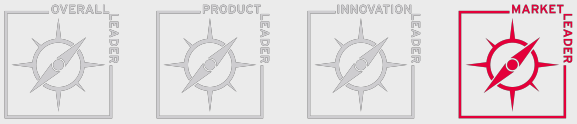
Strengths

- Dynamic fine-grained API access management from a leading vendor
- Proactive policy-driven enforcement of API security and data access beyond APIs
- AI-powered automated API monitoring and threat detection
- Unified visibility across heterogeneous API environments
- Strong partner ecosystem

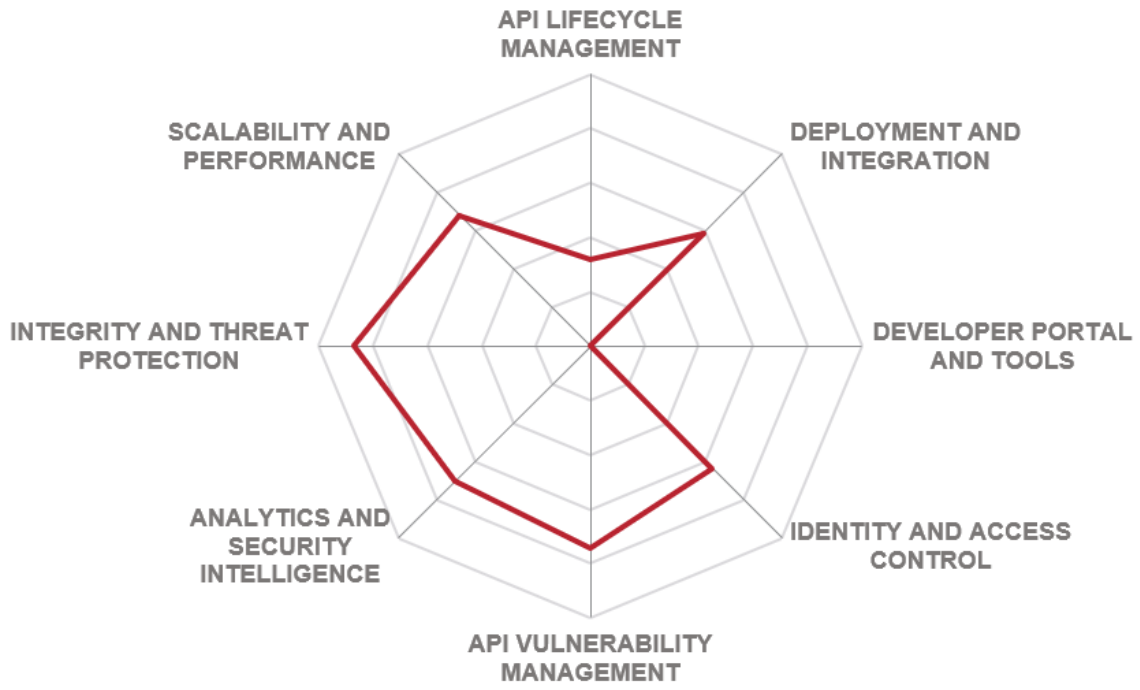
Challenges

- Comprises two standalone products, not fully integrated yet
- Limited support for API lifecycle management
- No support for API specification validation (thus no focus on DevSecOps)

Leader in



PING IDENTITY



5.14 Red Hat

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 Integration platform 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 Red Hat 3scale API Management, an open-source cloud-based API management platform, as well as the Red Hat AMQ messaging platform and Red Hat Fuse, distributed, cloud-native integration solution.

Originally offered as three independent products, now all three are fully unified within a single user interface and are offered as a single integration platform augmented by various managed services. Different deployment scenarios are available, ranging from a self-managed Red Hat Integration platform to Red Hat OpenShift® API Management, available as a managed service, to a SaaS-based offering retaining the original Red Hat 3scale API Management branding.

Regardless of the selected deployment option, Red Hat Integration provides full coverage not just for the full API lifecycle (from initial design to retirement), 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.

Security	●●●●○
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

Red Hat

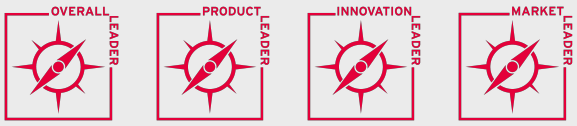
Strengths

- Unified platform for developing and integrating cloud-native apps.
- Designed for high performance, scalability, and hybrid deployments.
- Comprehensive support for microservices and serverless architectures.
- Flexible deployment options, from self-managed to SaaS
- Open-source codebase.

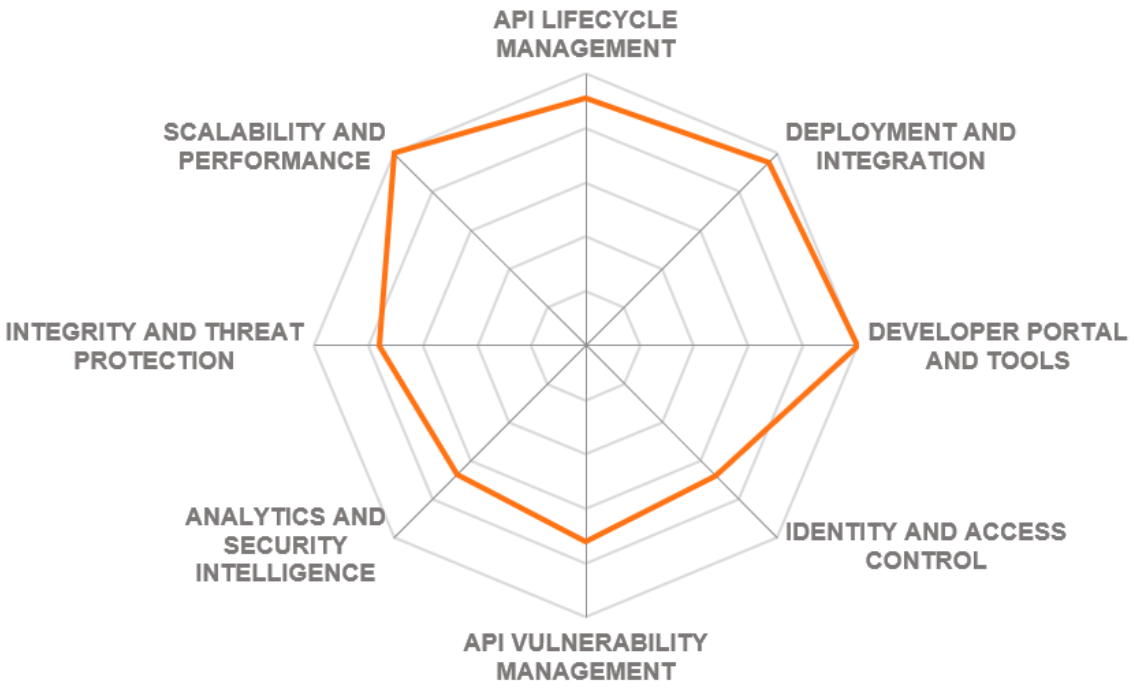
Challenges

- 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



RED HAT


API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.15 Salt Security

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-prem 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.

A notable recent development at Salt Security is the launch of Salt Labs, a forum for publishing API security research conducted by the company's own research team. The new unit focuses on raising public awareness of API risks and threats, providing recommendations for organizations to improve their security posture, and publicizing API security best practices.

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.

Security	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●●

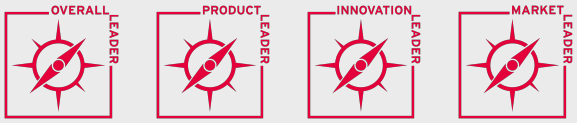
Strengths

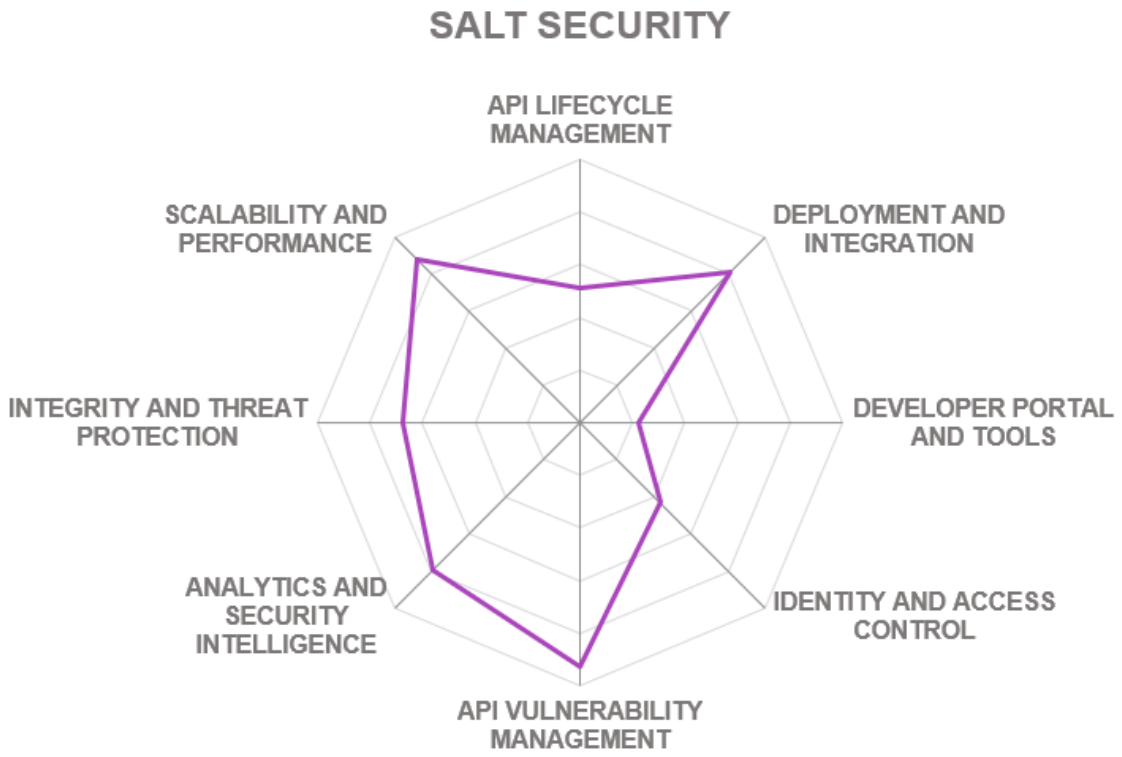
- Strong focus on runtime protection and security across the full API lifecycle
- Automatic and continuous discovery of new, outdated, and unknown APIs along with sensitive data exposure.
- Real-time detection of known and unknown API vulnerabilities and attacks.
- Based on unsupervised machine learning – no signatures, configuration, or training.

Challenges

- Privately held startup still building its team
- Partner network primarily in North America, still expanding to other regions
- Strongly focused on out-of-band monitoring, limited inline blocking options.

Leader in




SALT SECURITY
API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.16 Sensedia

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.

Perhaps the only drawback of the Sensedia API platform is that it's almost unknown outside of 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	●●●●○
Functionality	●●●●●
Interoperability	●●●●○
Usability	●●●●●
Deployment	●●●●○

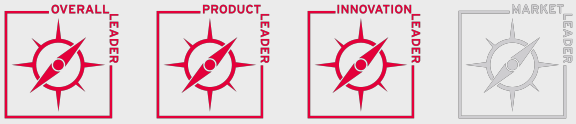
Strengths

- 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.

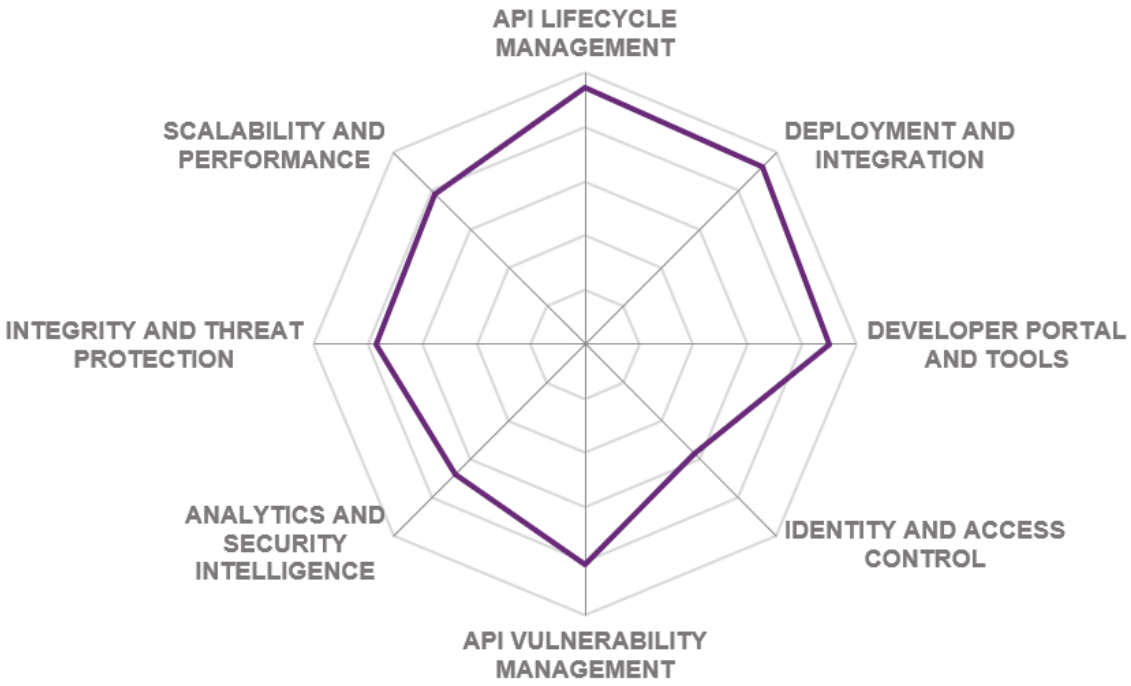
Challenges

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

Leader in



SENSEDIA


API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.17 Spherical Defense

Spherical Defense 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.

Spherical Defense's first product based on this technology is an API security solution that can protect not just traditional API endpoints exposed to the internet, but internal networks and even modern service meshes that power containerized applications as well. It utilizes unsupervised deep learning to analyze API traffic payloads flowing to a gateway to first create a normal profile and then to identify anomalies and threats.

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. After initial deployment, it will automatically progress between training stages and can be fully operational within just a few hours. In addition to network traffic, the engine can ingest other types of structured data flows, including logs. Integrations with popular API gateways are supported, as well as connectors to SIEM solutions like Splunk.

Spherical Defense 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.

Spherical provides remediation by means of a reverse proxy and integrations with API Gateways. The solution is able to block threats in real-time with low latency.

Security	● ● ● ● ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

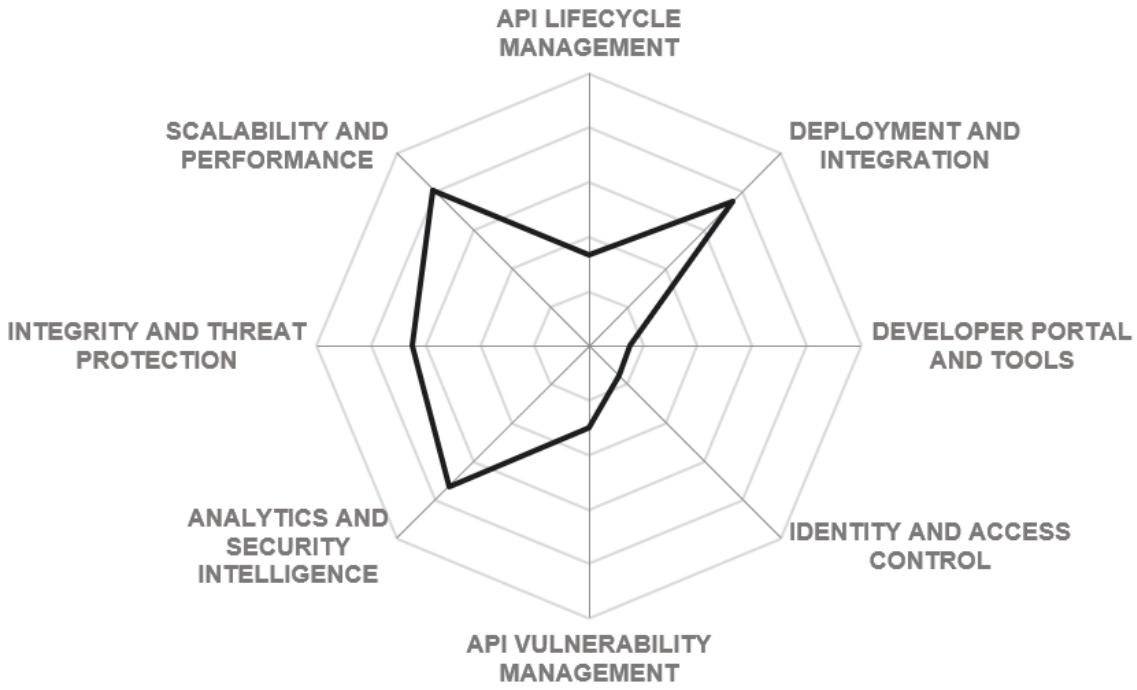
Strengths

- Fully autonomous, unsupervised deep learning technology.
- Supports multiple data ingestion mechanisms including traffic flows, infrastructure, and application logs.
- Deployed in minutes, fully operational in a few hours.
- Identifies and classifies multiple API-related threats.
- Innovative 3-D graphical interface.

Challenges

- Yet to establish a market presence.
- Built-in threat blocking is still limited, advanced functionality achieved via third-party integrations.
- No means to manage distributed deployments.

SPHERICAL DEFENSE



5.18 Traceable

Traceable is an application 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 the distributed tracing technology 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 is fed into a centralized security data lake, which can be utilized for forensic analytics, threat hunting, or compliance audits and reports. 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. 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.

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	● ● ● ○ ○
Functionality	● ● ● ● ○
Interoperability	● ● ● ○ ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ●

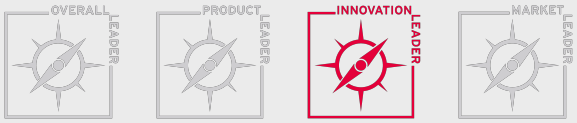
Strengths

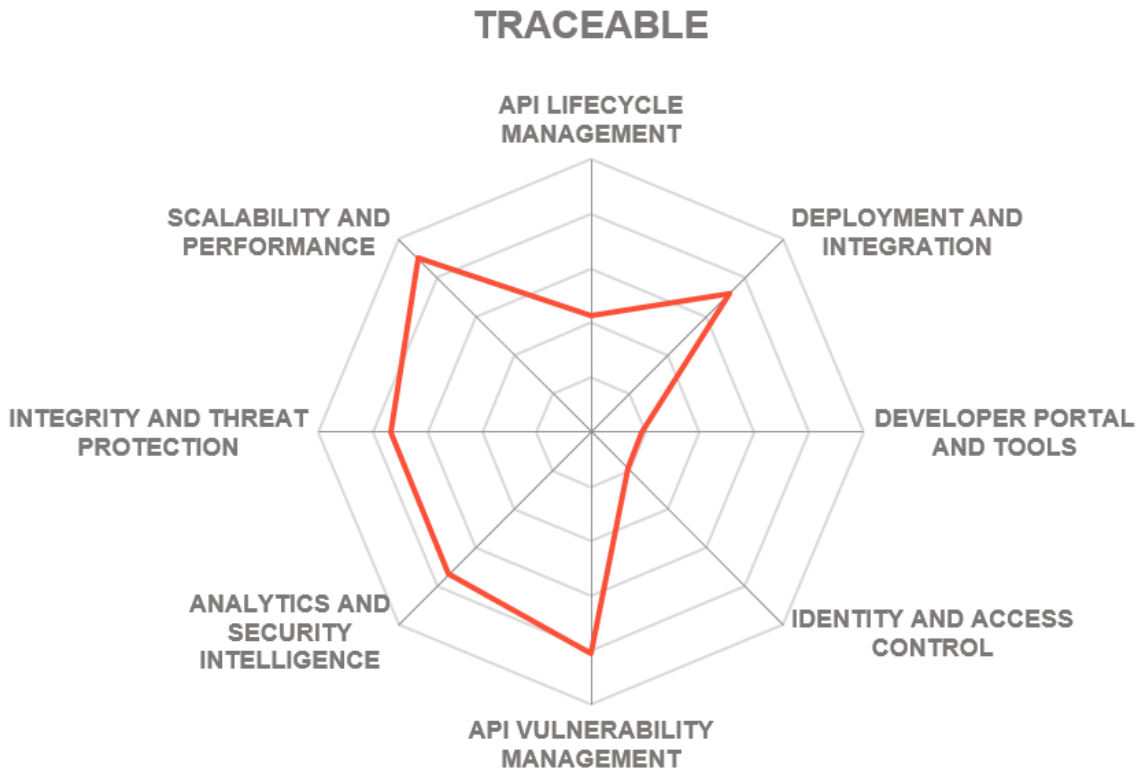
- Innovative distributed tracing technology to monitor and correlate data across environments.
- Unsupervised AI detection engine for identifying and classifying various attacks and suspicious activities.
- Rich forensic analytics, threat hunting, and compliance reporting capabilities.
- Built-in remediation actions for blocking API attacks.

Challenges

- Yet to establish a substantial market presence.
- API schema validation is not yet supported.
- DevOps integrations are still on the roadmap.

Leader in




TRACEABLE
API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

5.19 WSO2

WSO2 is a global application development company based in the US, UK, and Sri Lanka. 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.

WSO2 API Management solution is based on a set of open-source products developed by WSO2. The 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 latest release of WSO2 API Manager combines its API management capabilities with the 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 recent 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.

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	●●●●●
Functionality	●●●●●
Interoperability	●●●●●
Usability	●●●●●
Deployment	●●●●○

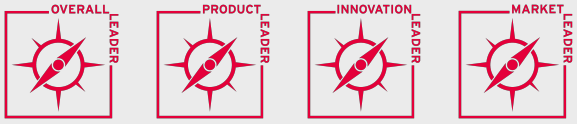
Strengths

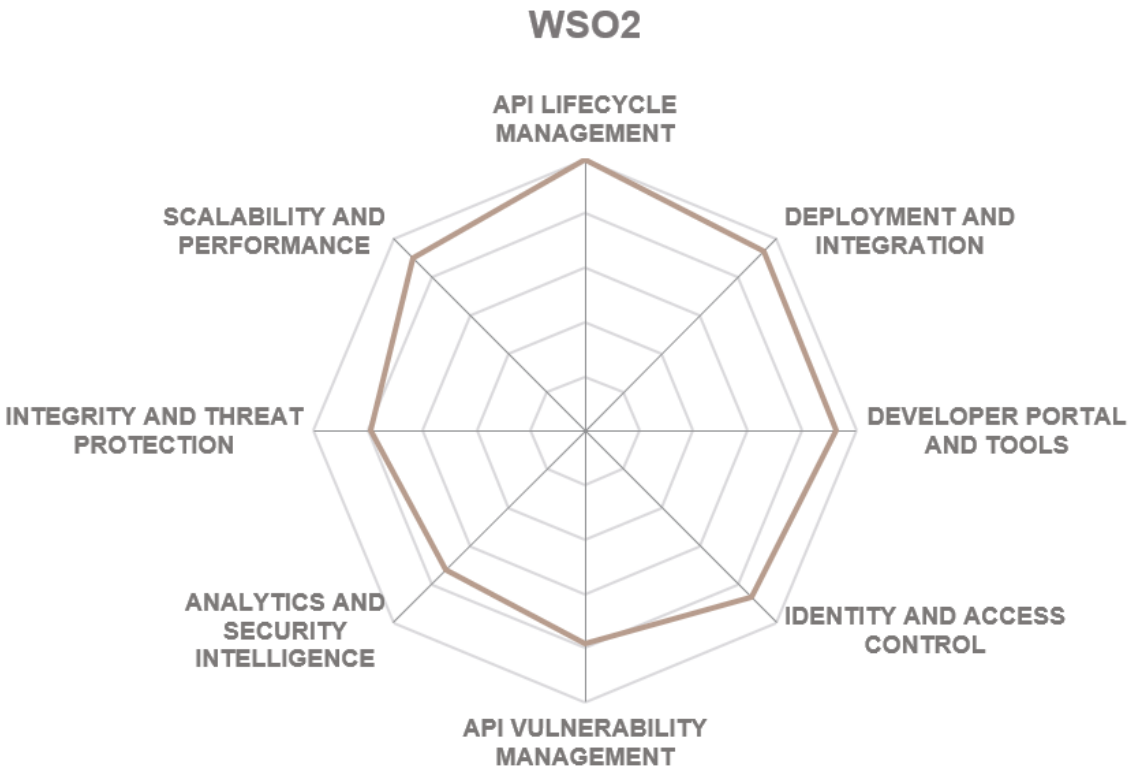
- Built on an integrated open-source platform for business-centric solutions.
- Now incorporates additional enterprise integration capabilities.
- Cloud-native support to expose microservices as managed APIs.
- AI-powered abnormal activity detection.
- Low-code cloud-native development platform with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

Challenges

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

Leader in




WSO2
API LIFECYCLE MANAGEMENT
DEPLOYMENT AND INTEGRATION
DEVELOPER PORTAL AND TOOLS
IDENTITY AND ACCESS CONTROL
API VULNERABILITY MANAGEMENT
ANALYTICS AND SECURITY INTELLIGENCE
INTEGRITY AND THREAT PROTECTION
SCALABILITY AND PERFORMANCE

6 Vendors to Watch

6.1 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.

6.2 Data Theorem

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.

Why worth watching: focusing primarily on modern application backends developed and deployed in public clouds, Data Theorem's API Discover provides continuous monitoring of customer's cloud environments to automatically discover, analyze and monitor any APIs, especially those leveraging serverless application frameworks. API Inspect service complements it by detecting potential security and privacy vulnerabilities in APIs by validating their encryption and authentication controls.

6.3 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.

6.4 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.

6.5 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.

6.6 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.

6.7 Wallarm

Wallarm is an application security startup company based in San Francisco, CA. Founded in 2014, Wallarm develops an AI-powered application security platform that combines the functionality of web application firewalls and dynamic application security testing.

Why worth watching: Wallarm's platform allows for the proactive identification of vulnerabilities in applications and APIs and the detection and blocking of zero-day attacks that target those vulnerabilities. The company's solution is developed on top of NGINX, a popular high-performance web server, and is primarily targeted towards customers with high-load web applications, APIs, or microservice-based projects in e-commerce, fintech, and Software-as-a-Service industries.

6.8 AWS

As a major cloud service provider whose cloud infrastructure is utilized by thousands of customers 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.

6.9 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.

6.10 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.

6.11 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.

7 Related Research

Leadership Compass: API Management and Security - 70311
Buyer's Compass: API Management and Security - 80215
Leadership Compass: Dynamic Authorization Management - 70966
Leadership Compass: Access Management and Federation - 70790
Leadership Compass: Identity API Platforms - 79012
Advisory Note: The Role of APIs for Business - 70946
Advisory Note: Connected Enterprise Step-by-step - 70999
Whitepaper: The Dark Side of the API Economy - 80019
Leadership Brief: Top Cyber Threats - 72574
Leadership Brief: Securing PSD2 APIs - 72596
Executive View: Cequence Security API Sentinel - 80538
Executive View: Apigee Edge API Management Platform - 80307
Executive View: PingAccess - 80323
Executive View: Ping Identity Data Governance - 70295
Executive View: Curity Identity Server - 80159
Executive View: Forum Sentry API Security Gateway - 70930
Executive View: Ergon Airlock Suite - 72509
Executive View: Axway API Management for Dynamic Authorization Management (DAM) - 71184
Executive View: Amazon API Gateway - 71451
Executive View: WSO2 Identity Server - 80060
Product Report: 3Scale API Management - 70626
Product Report: Layer 7 Technologies - 70627

Methodology

About KuppingerCole's Leadership Compass

KuppingerCole Leadership Compass is a tool which provides an overview of a particular IT market segment and identifies the leaders in that market segment. It is the compass which assists you in identifying the vendors and products/services in a market segment 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

As part of our evaluation of products in this Leadership Compass, we look at four leadership types:

- **Product Leaders**: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what 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 in 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. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

For every leadership type, we distinguish between three levels of products:

- **Leaders**: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in particular 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 products which lag behind 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 the 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 a given 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, as well as other sources.

Product rating

KuppingerCole as an analyst company regularly conducts evaluations of 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 of 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**
- **Integration**
- **Interoperability**
- **Usability**

Security – security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole Analysts IT Model. Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are

understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality – this is measured in relation to three factors. One is what the vendor promises to deliver. The second is the status of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the status of the industry and KuppingerCole expectations usually are virtually the same. In emerging markets, they might differ significantly, with no single vendor meeting the expectations of KuppingerCole, thus leading to relatively low ratings for all products in that market segment. Not providing what customers can expect on average from vendors in a market segment usually leads to a degradation of the rating, unless the product provides other features or uses another approach which appears to provide customer benefits.

Integration – integration is measured by the degree in which the vendor has integrated the individual technologies or products in their portfolio. Thus, when we use the term integration, we are referring to the extent to which products interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of names and passwords for every person involved, it is not well integrated. And if products use different databases or different administration tools with inconsistent user interfaces, they are not well integrated. On the other hand, if a single name and password can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability – interoperability also can have many meanings. We use the term “interoperability” to refer to the ability of a product to work with other vendors’ products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status so as to ensure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs.

Usability – accessibility refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes just good documentation can create adequate accessibility. However, we have strong expectations overall regarding well-integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

We focus on security, functionality, integration, 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 potential breakdown for any IT endeavor.

- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increases costs, but inevitably leads to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product security, functionality, integration, interoperability, and usability which the vendor has provided are of the highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

Vendor rating

For vendors, additional ratings are used as part of the vendor evaluation. The specific areas we rate for vendors are:

- **Innovativeness**
- **Market position**
- **Financial strength**
- **Ecosystem**

Innovativeness – this is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the market segment(s) the vendor is in. 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. An important element of this dimension of the KuppingerCole ratings is the support of standardization initiatives if applicable. 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 overall markets in which a vendor is active, e.g. 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 become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. 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 – beyond the Leadership rating in the various categories – a separate rating with five different levels. These levels are

Strong positive
Outstanding support for the feature area, e.g. product functionality, or outstanding position of the company, e.g. for financial stability.

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. 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. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., 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.
- **Denial of participation:** Vendors might decide on not participating in our evaluation and refuse to become part of the Leadership Compass document. KuppingerCole tends to include their products anyway as long as sufficient information for evaluation is available, thus providing a comprehensive overview of leaders in the particular 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 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 target is providing 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 of vendors not covered and their offerings in chapter Vendors and Market Segments to watch. In that chapter, we also look at some other interesting offerings around the market and in related market segments.

Content of Figures

Copyright

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 make 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.