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 in the most efficient way. 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
December 2019

Leadership Compass
API Management and Security
By KuppingerCole Analysts AG

Content

Related Research

Leadership Compass: API Security Management – 70958

Leadership Compass: Dynamic Authorization Management – 70966

Leadership Compass: Access Management and Federation – 70790

Advisory Note: The Open API Economy – 70352

Advisory Note: API Economy Ecosystem – 70625

Advisory Note: Connected Enterprise Step-by-step – 70999

Whitepaper: The Dark Side of the API Economy – 80019

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 – 80060Executive View: Curity Identity Server – 80159

Product Report: 3Scale API Management – 70626

Product Report: Layer 7 Technologies – 70627

1 Introduction

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.

APIs allow developers to create applications faster by enabling support for modern architectures like microservices. They ensure that applications from different vendors can exchange data seamlessly, orchestrate massive cloud infrastructures and global networks of smart devices. They enable business communications with suppliers, service providers, and customers. APIs can also unlock numerous new business models for companies to offer their core services in innovative ways, to reach new customer bases or to streamline sales and services across multiple channels.

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.

As it often happens in such scenarios, security quickly becomes an afterthought at best or, even worse, it is seen as a nuisance and an obstacle on the road to success. The success of an API is measured by its adoption and security mechanisms are seen as friction that limits this adoption. There are also several common misconceptions around the very notion of API security, notably the idea that existing security products like web application firewalls are perfectly capable of addressing API-related risks.

When the previous edition of our Leadership Compass was published, our research clearly indicated that the market for API management solutions was undergoing rapid growth, marked by a wave of acquisitions. This tendency has continued in the recent years as well. However, the more important trend is the growing awareness of the critical role of security in API management solutions. KuppingerCole thus continues placing a strong emphasis on API security but expands the coverage of this Leadership Compass to incorporate every step of the API lifecycle. 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 Market Segment

We have long recognized 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.

Unfortunately, many organizations tend to underestimate 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. 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.

Figure 1: API Lifecycle

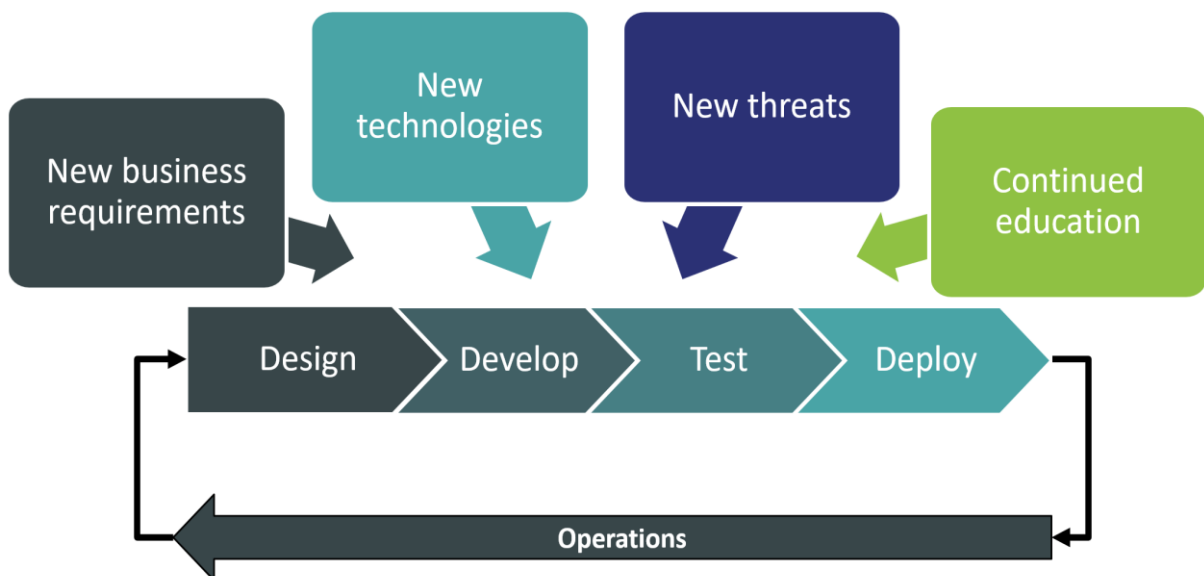When the previous edition of the Leadership Compass on API security was published, the industry was still in a rather early emerging stage, with most large vendors focusing primarily on operational capabilities, with very rudimentary threat protection functions built into API management platforms and 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 a 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 is already showing signs of undergoing consolidation, 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.
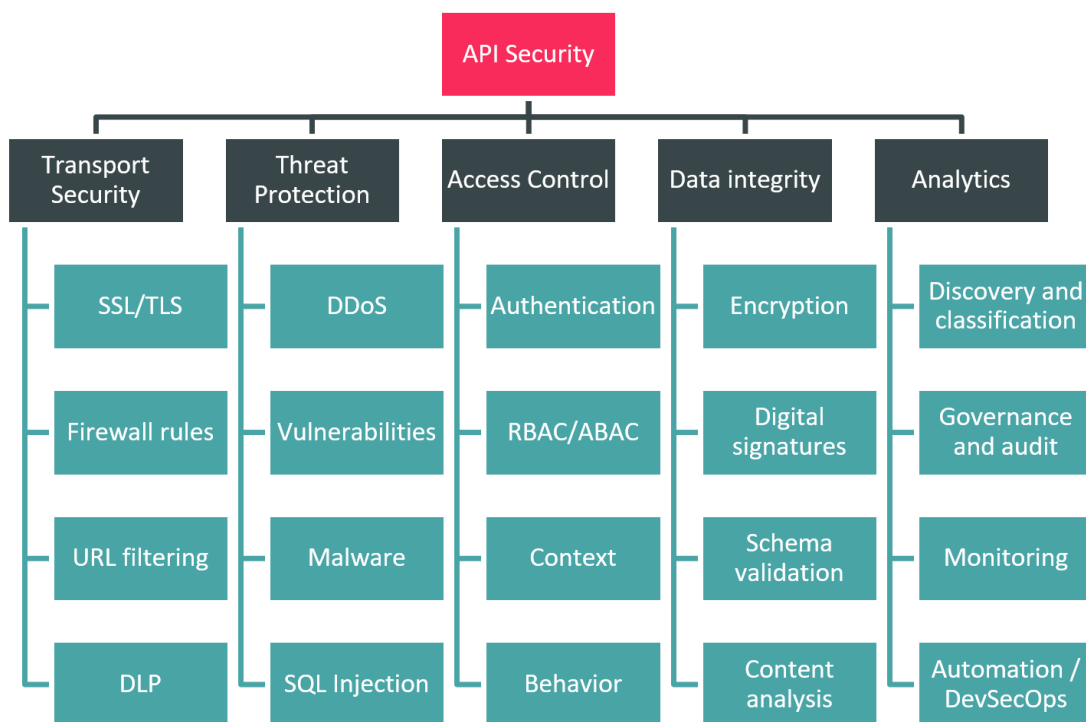
Figure 2: The Scope of API Security

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 is 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.

1.2 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 to 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.

1.3 Required Capabilities

When evaluating the products, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers

- number of developers
- partner ecosystem
- licensing models

- platform support

We also considered the following key functional areas of API management and security solutions:

- **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 3rd 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 to 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 allows 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.

2 Leadership

Selecting a vendor of a product or service must not be only based on the comparison provided by a KuppingerCole Leadership Compass. The Leadership 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 Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

2.1   Overall Leadership

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

The Overall Leadership rating is a combined view of the three leadership categories: Product Leadership, Innovation Leadership, and Market Leadership. This consolidated view provides an overall impression of our rating of the vendor's offerings in the particular market segment. Notably, some vendors that benefit from a strong market presence may slightly drop in other areas such as innovation, while others show their strength, in the Product Leadership and Innovation Leadership, while having a relatively low market share or lacking a global presence. Therefore, we strongly recommend looking at all leadership categories, the individual analysis of the vendors, and their products to get a comprehensive understanding of the players in this market.

In this year's Overall Leadership rating we can see that all rating leaders are veteran players in the API management market, capable of offering comprehensive enterprise-level highly integrated platforms for the most demanding customers. In fact, Apigee, Axway, Broadcom (formerly CA), and Red Hat 3scale are all large established vendors with massive global presence, well-developed partner networks and broad customer bases – all this ensures that their products' capabilities are further backed by financial stability and continued support of existing customers.

Forum Systems and Sensedia are the only companies that managed to get into the Leaders segment without so prominent market presence.

Forum Systems, which had the distinction of being the product Leader in our previous, more security-focused Leadership Compass, is still being recognized for its continued "security first" approach in their product design, as well as ongoing innovations in areas like DevOps and API analytics.

Sensedia is a Brazilian company, which, despite offering a comprehensive fully integrated API management stack, isn't particularly strong outside their native Latin American market yet.

The rest of the vendors are populating the Challengers segment. Lacking the combination of an exceptionally strong market and product leadership, they are hanging somewhat behind the leaders, but still deliver mature solutions excelling in certain functional areas. There are no Followers in this rating.

Again, we stress that the leadership in our rating does not automatically mean that the vendors are the best fit for a specific customer requirement. A thorough evaluation of these requirements and a mapping to the product features by the company's products will be necessary.

Overall Leaders are (in alphabetical order):

- Apigee (Google Cloud)
- Axway
- Broadcom (formerly CA Technologies)
- Forum Systems
- Red Hat 3scale
- 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.
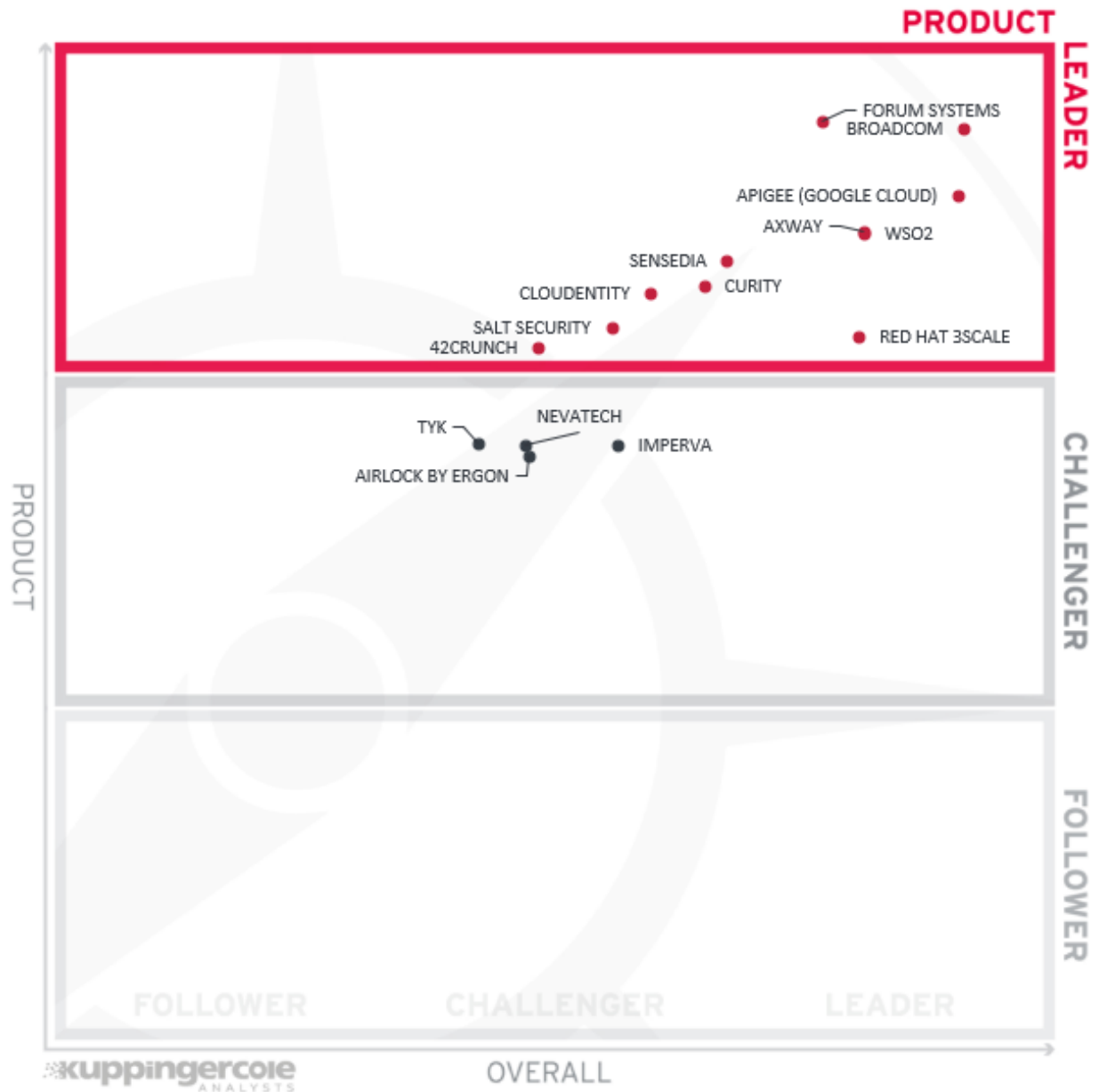

Figure 4: Product Leaders in the API Management and Security segment

In the Product Leadership rating, we look specifically for 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.

Most large vendors mentioned earlier are present in the Leaders segment, including Apigee, Axway, Broadcom, Red Hat and WSO2. However, we also have several smaller companies that were able to reach the leader status. Forum Systems and Sensedia, as already mentioned earlier, are notable for their comprehensive API management and security capabilities. Cloudentity, while focusing only on identity and authorization for APIs, manages to deliver a robust monitoring, access control and security solution

for modern microservice-based application architectures. Salt Security offers a completely passive AI-powered API security analytics solution that does not require any configuration or tuning. Finally, 42crunch, despite the company's young age, is uniquely focusing on proactive API security, offering a platform for API vulnerability management and runtime protection.

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. For companies like Imperva, this also reflects their very recent forays into API security; we expect their solution to mature and improve quickly in the near future.

Product Leaders are (in alphabetical order):

- 42Crunch
- Apigee (Google Cloud)
- Axway
- Broadcom (formerly CA Technologies)
- Cloudentity
- Curity
- Forum Systems
- Red Hat 3scale
- Salt Security
- Sensedia
- WSO2

2.3 Innovation Leadership

Another angle we take when evaluating products/services concerns innovation. Innovation is, from our perspective, a key capability in IT market segments. Innovation is what customers require for keeping up with the constant evolution and emerging customer requirements they are facing.

Innovation is not limited to delivering a constant flow of new releases, but focuses on a customer-oriented upgrade approach, ensuring compatibility with earlier versions especially at the API level and on supporting leading-edge new features which deliver emerging customer requirements.
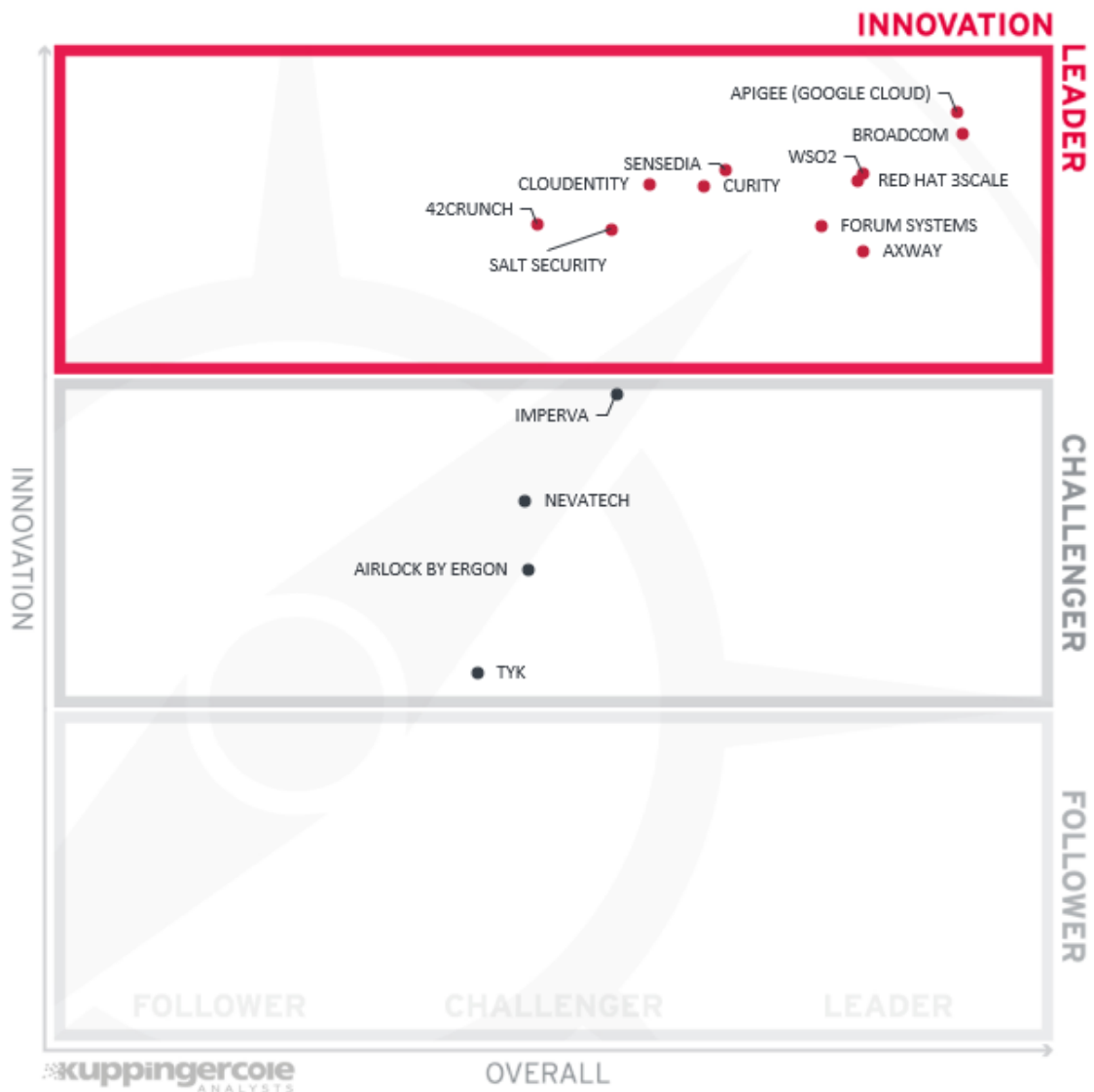
Figure 5: Innovation Leaders in the API Management and Security segment

As opposed to the product and market leadership ratings, 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 Broadcom, Google, Red Hat or Axway 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 Sensedia and WSO2 with their comprehensive API platforms manage to achieve the Leader status in our rating as well (Forum Systems, despite having a strong yet somewhat narrow focus on security in the past has recently dramatically expanded its API management product portfolio). Yet even quite small companies like 42crunch, Cloudentity, Curity or Salt Security have been rated high on innovation because of their disruptive product developments in their respective focus areas of API security.

Imperva, despite a strong overall maturity and market share is currently placed among the Challengers – their API security product has only recently been launched and needs some time to implement all planned capabilities.

The rest of the vendors are also positioned in the Challengers segment, reflecting perhaps the overall maturity of their products that comes with the unfortunate downside of somewhat slower pace of innovation.

Innovation Leaders are (in alphabetical order):

- 42Crunch
- Apigee (Google Cloud)
- Broadcom (formerly CA Technologies)
- Axway
- Cloudentity
- Curity

- Forum Systems
- Red Hat 3scale
- Salt Security
- Sensedia
- WSO2

2.4   Market Leadership

Here we look at Market Leadership qualities based on certain market criteria including but not limited to the number of customers, the partner ecosystem, the global reach, and the nature of the response to factors affecting the market outlook. Market Leadership, from our point of view, requires global reach as well as consistent sales and service support with the successful execution of marketing strategy.
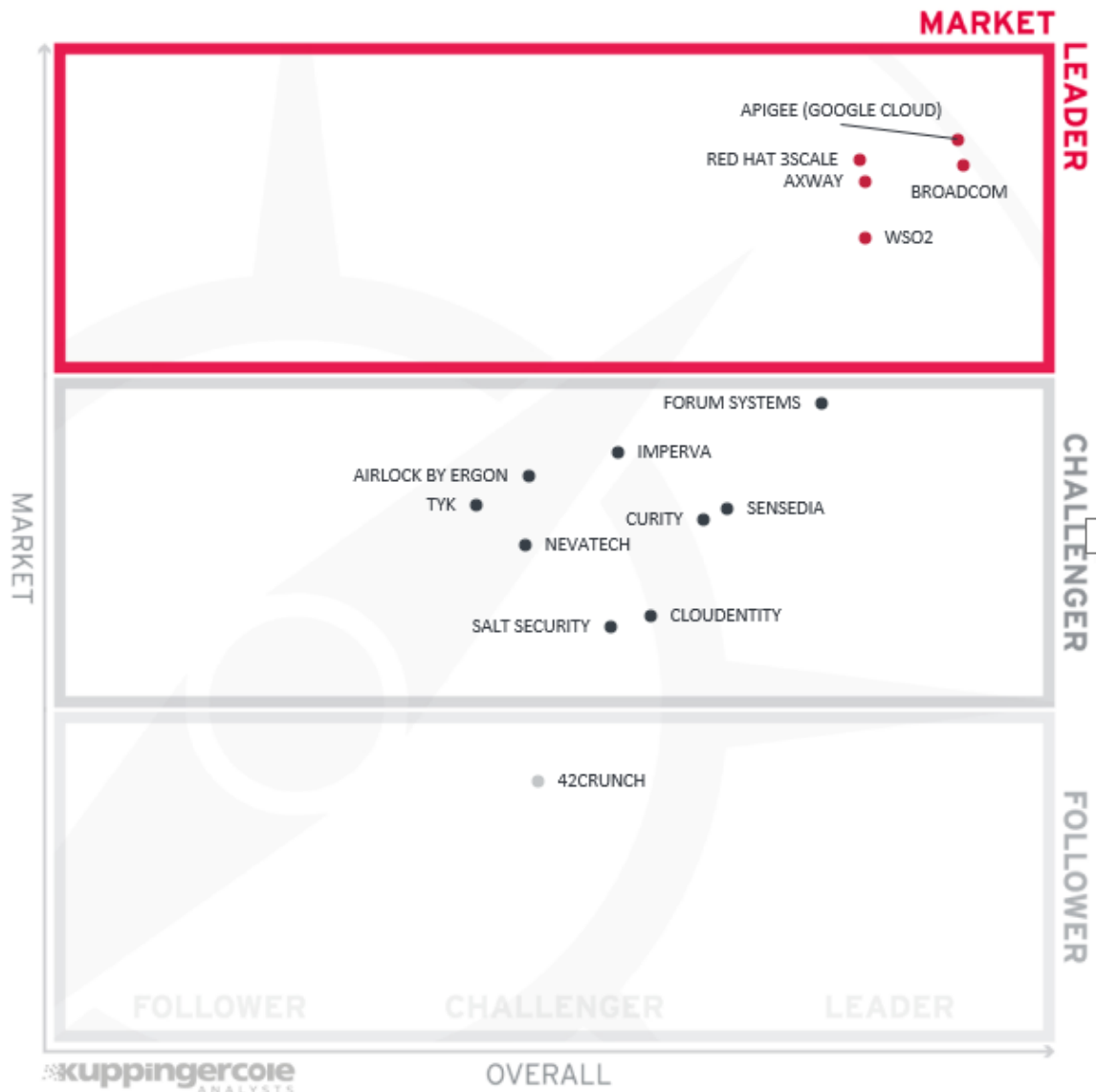
Figure 6: Market Leaders in the API Management and Security segment

Please note that this rating does not reflect the overall market presence of large vendors, but only limited to the market shares of their respective API management and security products. This is why we can find such large veteran players with global market presence as Axway, Broadcom, Google, Red Hat and WSO2 among the leaders, yet Imperva is still located among the Challengers.

In the Challenger segment, they are joined by almost all other participants of our rating. The only company that has slipped to the Follower segment is 42crunch, which is yet to gain a substantial number of paying customers.

Market Leaders are (in alphabetical order):

- Apigee (Google Cloud)
- Axway
- Broadcom (formerly CA Technologies)

- Red Hat 3scale
- WSO2

While the Leadership charts identify leading vendors in certain categories, many customers are looking not only for, say, 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 deliver additional 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 looks at Product Leadership and Market Leadership.

Figure 7: The Market / Product Matrix

In this comparison, it becomes clear which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership analysis. Vendors above the line are sort of "overperforming" in the market. It comes as no surprise that these are mainly the very large vendors, while vendors below the line are often innovative but focused on specific regions.

Among the Market Champions we can find the usual suspects – large, well-established vendors like Axway, Broadcom, Google and WSO2, closely followed by Red Hat.

The vendors in the right middle box are those whose capable products are yet to win them a strong market presence: here we find Forum Systems, Sensedia and Cloudentity.

In the bottom right box, we can observe 42crunch: its product is so new that it needs more time to establish any notable market position.

The rest of the vendors can be found in the middle segment, indicating their relatively narrow functional focus, which corresponds to limited potential for future growth or, in case of Imperva which only recently entered the API security market, the same maturity problem as the much smaller 42crunch is currently facing.

3.2 The Product/Innovation Matrix

The second view shows how Product Leadership and Innovation Leadership are correlated. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.
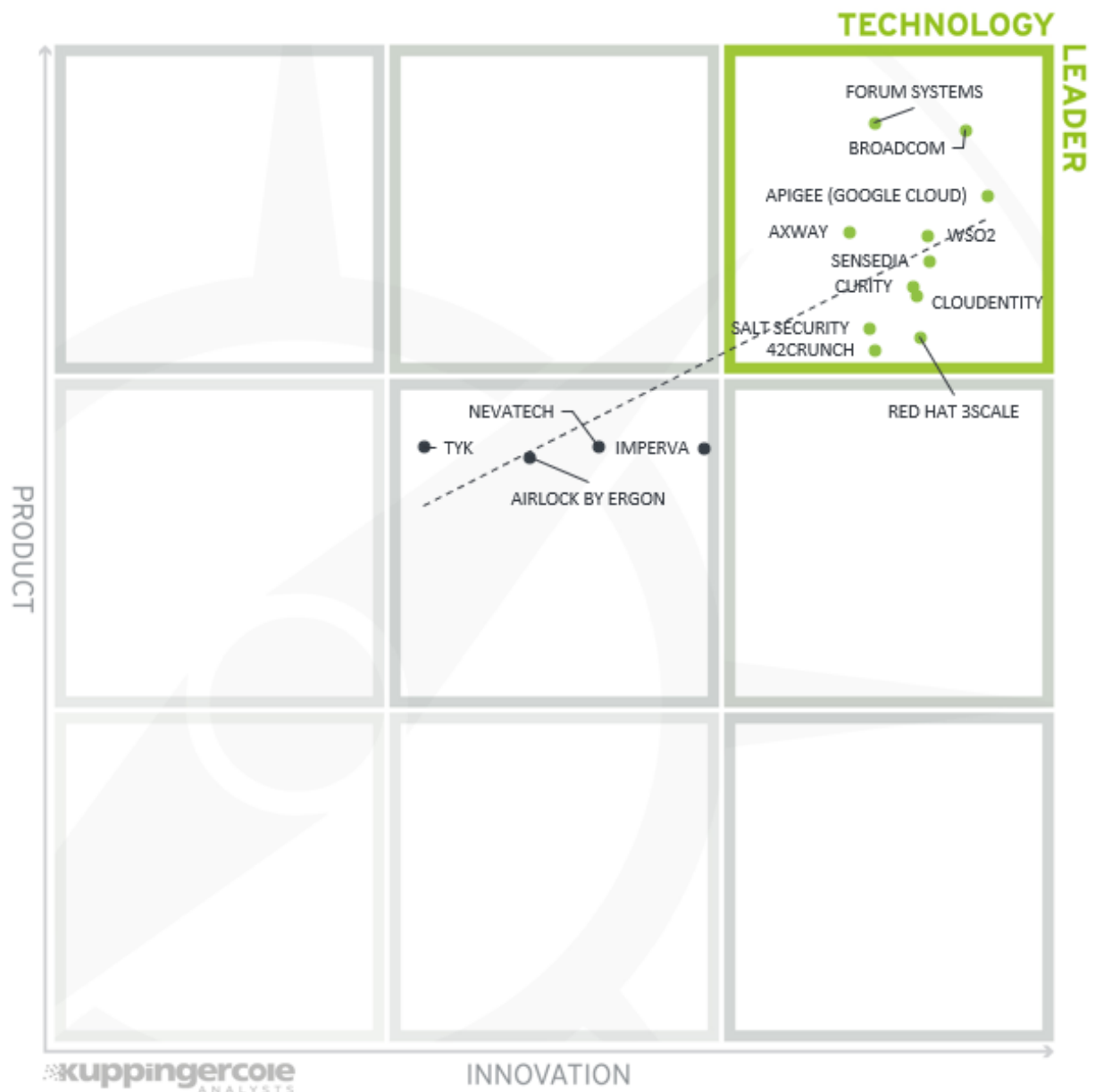
Figure 8: The Product / Innovation Matrix

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. Also worth noting is the lack of "followers" in this matrix.

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 to their future position in the market, depending on how they improve their Innovation Leadership position. On the other hand, vendors that are highly innovative have a good chance of improving their market position but often face risks of failure, especially in the case of vendors with a confused marketing strategy.
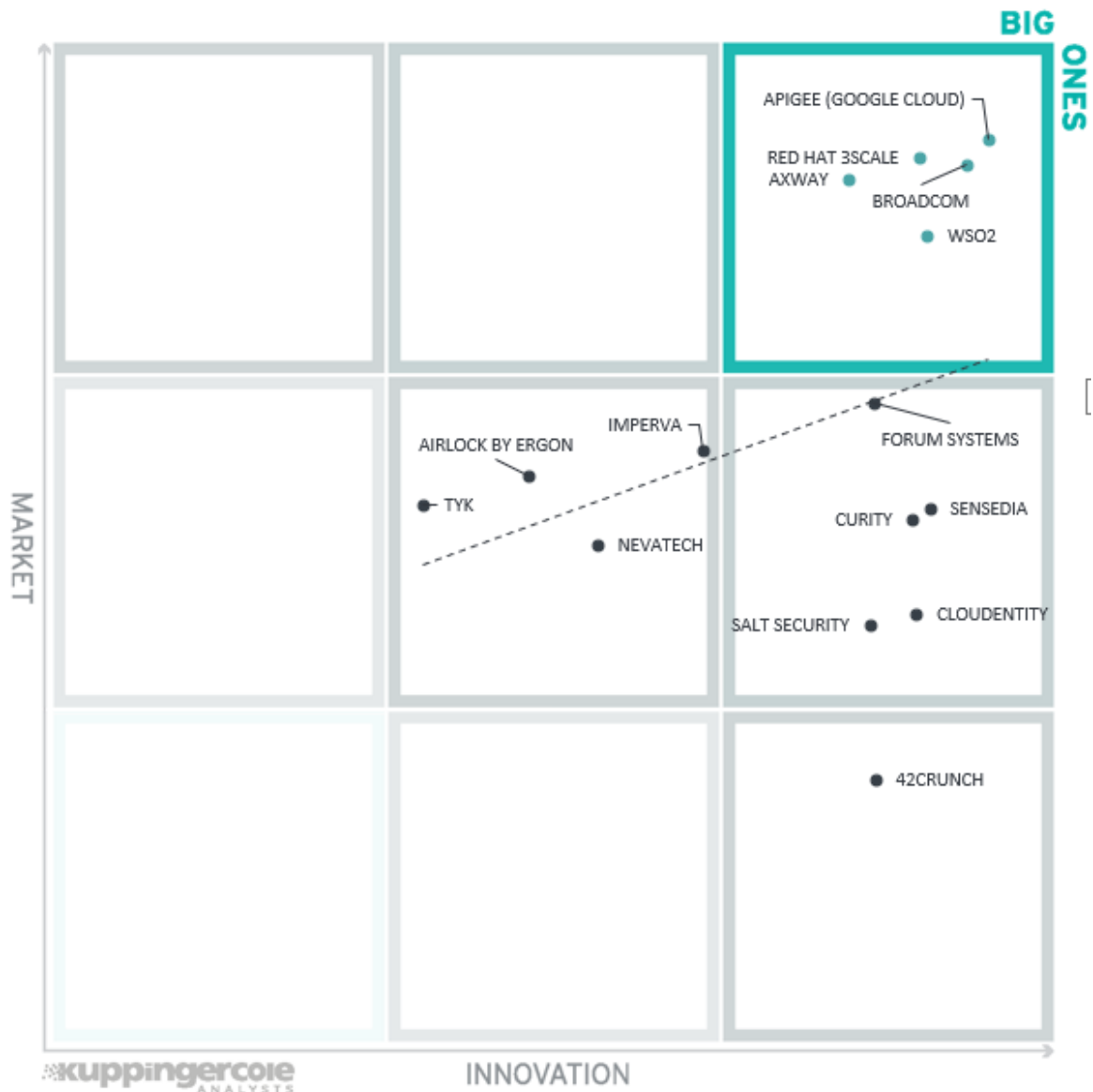
Figure 9: The Innovation/Market Matrix

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

Yet again, we observe the largest market players in the top right segment, with the rest of the vendors scattered across the right half of the matrix, indicating their strong potential for improving their market position in the future.

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 Database and Big Data 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 the table below.

Vendor	Security	Functionality	Integration	Interoperability	Usability
42CRUNCH	positive	positive	strong positive	positive	strong positive
AIRLOCK BY ERGON	strong positive	neutral	strong positive	neutral	positive
APIGEE (GOOGLE CLOUD)	strong positive	strong positive	strong positive	strong positive	positive
AXWAY	positive	strong positive	strong positive	strong positive	strong positive
CLOUDENTITY	strong positive	positive	positive	positive	strong positive
CURITY	positive	positive	strong positive	strong positive	strong positive
FORUM SYSTEMS	strong positive	strong positive	strong positive	strong positive	strong positive
IMPERVA	strong positive	positive	positive	positive	positive
BROADCOM	strong positive	strong positive	positive	positive	strong positive
NEVATECH	positive	positive	positive	positive	positive
RED HAT	positive	strong positive	strong positive	positive	positive
SALT SECURITY	strong positive	positive	strong positive	positive	positive
SENSEDIA	positive	strong positive	strong positive	positive	strong positive
TYK	positive	positive	positive	positive	positive
WSO2	strong positive	strong positive	strong positive	strong positive	positive

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

In addition, we also provide four additional ratings for the vendor. These go 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	Innovation	Market Position	Financial Strength	Ecosystem
42CRUNCH	strong positive	weak	weak	neutral
AIRLOCK BY ERGON	positive	positive	positive	neutral
APIGEE (GOOGLE CLOUD)	strong positive	strong positive	strong positive	strong positive
AXWAY	positive	strong positive	strong positive	strong positive
CLOUDENTITY	strong positive	neutral	neutral	neutral
CURITY	strong positive	positive	positive	neutral
FORUM SYSTEMS	positive	positive	positive	positive
IMPERVA	positive	neutral	strong positive	positive
BROADCOM	strong positive	strong positive	strong positive	positive
NEVATECH	positive	neutral	neutral	neutral
RED HAT 3SCALE	strong positive	positive	strong positive	strong positive
SALT SECURITY	strong positive	neutral	weak	neutral
SENSEDIA	positive	positive	positive	neutral
TYK	neutral	positive	neutral	positive
WSO2	strong positive	strong positive	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

In the area of innovation, we were looking for the service to provide a range of advanced features in our analysis. These advanced features include but are not limited to implementing practical applications of new innovative technologies like machine learning and behavior analytics or introducing new functionality in response to market demand. Where we could not find such features, we rate it as "Critical".

In the area of market position, we are looking at the visibility of the vendor in the market. This is indicated by factors including the presence of the vendor in more than one continent and the number of organizations using the services. Where the service is only being used by a small number of customers located in one geographical area, we award a "Critical" rating.

In the area of financial strength, a "Weak" or "Critical" rating is given where there is a lack of information about financial strength. This doesn't imply that the vendor is in a weak or a critical financial situation. This is not intended to be an in-depth financial analysis of the vendor, and it is also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding ecosystem applies to vendors which do not have or have a very limited ecosystem with respect to numbers of partners and their regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that the success and growth of companies in a market segment rely on strong partnerships.

This section contains a quick rating for every product we've included in this report. For some of the products, there are additional KuppingerCole Reports available, providing more detailed information.

In the following analysis, we have provided our ratings for the products and vendors in a series of tables. These ratings represent the aspects described previously in this document. Here is an explanation of the ratings that we have used:

- **Strong Positive:** this rating indicates that, according to our analysis, the product or vendor significantly exceeds the average for the market and our expectations for that aspect.

- **Positive:** this rating indicates that, according to our analysis, the product or vendor exceeds the average for the market and our expectations for that aspect.

- **Neutral:** this rating indicates that, according to our analysis, the product or vendor is average for the market and our expectations for that aspect.

- **Weak:** this rating indicates that, according to our analysis, the product or vendor is less than the average for the market and our expectations in that aspect.

- **Critical:** this is a special rating with a meaning that is explained where it is used. For example, it may mean that there is a lack of information. Where this rating is given, it is important that a customer considering this product look for more information about the aspect.

It is important to note that these ratings are not absolute. They are relative to the market and our expectations. Therefore, a product with a strong positive rating could still be lacking in functionality that a customer may need if the market in general is weak in that area. Equally, in a strong market, a product with a weak rating may provide all the functionality a particular customer would need.

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.

| Strengths	Challenges
● Proactive approach towards API security by design	● Small but growing customer base
● API contract analysis to proactively identify and remediate vulnerabilities and violations	● Focus on proactive security only; threat detection and security analytics only with 3rd party tool integrations
● Scalable API micro-firewall architecture for policy enforcement and threat protection	
● Comprehensive developer guidance and best practices with the API Security Encyclopedia	
● VS Code extension to provide instant feedback to developers	

Table 3: 42Crunch major strengths and challenges

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.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 4: 42Crunch rating
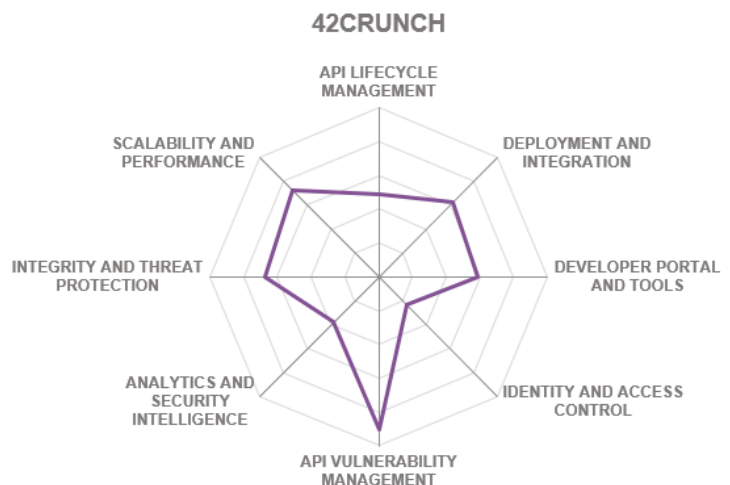
Centralized policy management and full process automation ensures that security becomes an integral part of the API lifecycle and can be applied automatically and at scale – across hybrid clouds or within microservice-based applications. In addition, 42Crunch invests considerable efforts into raising awareness about API security challenges among developers and other stakeholders. The company maintains an online API Security Encyclopedia, which offers the recent news, guidance and best practices to developers and security specialists.

5.2   Airlock by Ergon

Ergon is a Swiss-based company established in 1984 with customers primarily in DACH 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.

Strengths	Challenges
● Fully integrated platform for securing access management across web apps and APIs	● API monitoring and management capabilities are limited
● Built-in fraud prevention, application and mobile security functions	● Developer portal still quite rudimentary, lacks basic functions
● Dynamic Value Endorsement for data validation without API contracts	● Small partner ecosystem & limited global reach
● Good strong and adaptive authentication capabilities	

Table 5: Airlock major strengths and challenges

Known until recently simply as Airlock Suite, the company's flagship product has been recently 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 substantial range of security features.

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 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.

AIRLOCK BY ERGON

Security	strong positive
Functionality	neutral
Integration	strong positive
Interoperability	neutral
Usability	positive

Table 6: Airlock rating
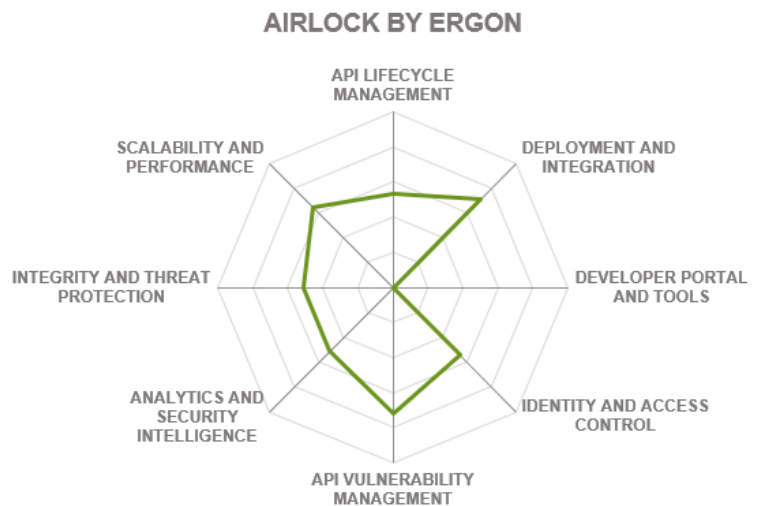
Unfortunately, Ergon is still fairly unknown outside its home market. However, the company's lean and well-integrated product can be recommended for evaluation by any company looking for all-in-one solution for enforcing sensitive data protection across multiple channels, beyond just APIs.

5.3 Apigee (Google Cloud)

Apigee is a product offered by Google Cloud, headquartered in Mountain View, CA. Apigee provides API management and predictive analytics solutions. Apigee was founded in 2004, the company entered 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's flagship product is Apigee Edge – a cloud-based platform 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; and Developer Services for building a community around APIs. 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.

| Strengths	Challenges
● Comprehensive API management platform covering all aspects of API lifecycle	● Security analytics lacks detailed views, no focus on forensic investigations
● Three types of API gateways and Istio service mesh integrations	● No official 3rd party security tool integrations; advanced functionality only achieved with custom extensions
● 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	

Table 7: Apigee major strengths and challenges

Apigee platform includes every possible capability one expects from such a platform to support end-to-end API management at every stage of 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.

By integrating with the Istio service mesh, Apigee seamlessly expands coverage to microservice-based applications as well.

APIGEE (GOOGLE CLOUD)

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 8: Apigee rating
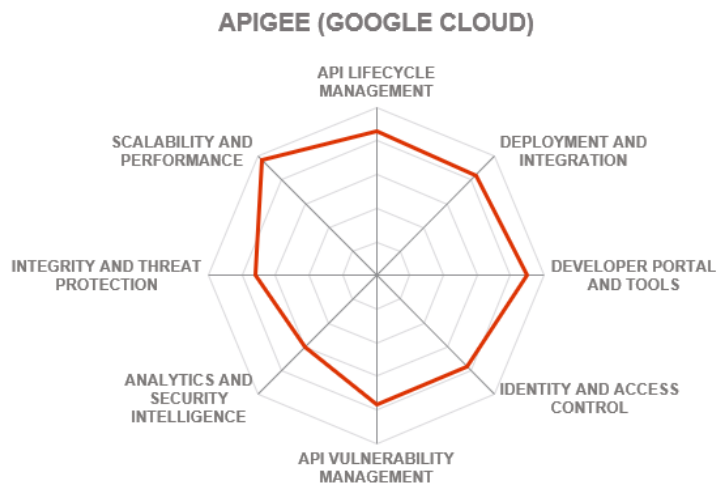
One of the notable recent developments is the announcement of the Apigee hybrid API management earlier this year. All capabilities which were previously delivered from the Google Cloud, can now be deployed in a hybrid configuration, where customers manage the runtime plane in a private cloud or a containerized environment, but continue to use the management plane provided by Apigee.

5.4 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. Since our previous Leadership Compass, the company has significantly restructured its portfolio, currently focusing on Axway AMPLIFY™ – a hybrid integration platform that unifies on-premises and cloud-based integration and governance capabilities to facilitate faster innovation and improved business efficiency.

| Strengths	Challenges
● Integral part of Axway AMPLIFY integration platform	● Built-in API firewall is quite limited, based on Apache ModSecurity
● Multiple gateway types, including support for microservices and cloud deployments - with a common control plane for management	● Advanced security analytics only available with 3rd party tool integrations
● Broad range of connectors and adapters for data sources, middleware, cloud services	● Quality of customer service and support seems to be a common complaint
● Graphical API Builder for creating and orchestrating microservice APIs	

Table 9: Axway major strengths and challenges

API Lifecycle Management is one of the key components of the company's integration platform. AMPLIFY API Management comprises the following products: API Manager for managing governance of APIs; API Gateway for enforcing security and governance policies on a broad range of API protocols; API Portal for onboarding API developers; API Builder – graphical low-code API integration tool that produces microservice-based API backends and data connectors; Embedded Analytics – configurable dashboards for API health and usage, as well as consumer engagement monitoring.

The latest release added major new features like the Multi-gateway Control plane for managing Axway and 3rd party gateways or AMPLIFY Streams for enabling event-driven streaming APIs.

Security	positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 10: Axway rating
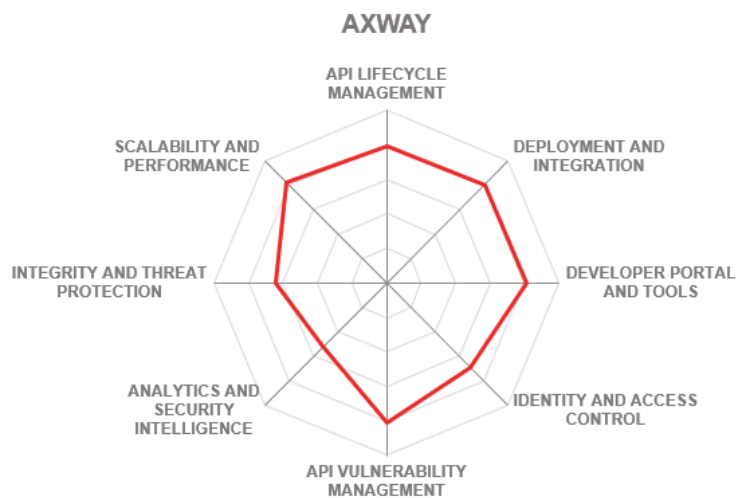
Axway's AMPLIFY Platform offers a robust set of capabilities for nearly every stage of API lifecycle. However, as a part of the company's overall hybrid integration platform, with solutions like AMPLIFY Unified Catalog and AMPLIFY Integration Builder, it can support even the largest enterprise customers with long-term integration strategies going beyond just APIs.

5.5 Cloudentity

Cloudentity is a privately held identity and access management company headquartered in Seattle, WA. Although the company has been in traditional IAM business since 1996, it was in 2016, when Cloudendity came up with CIAM.NEXT – an identity and authorization platform for APIs, microservices and other cloud workloads, designed for hybrid architectures. Combining API security tools with advanced authorization capabilities, Cloudentity can enforce the same secure access policies across any workload or platform.

| Strengths	Challenges
● Unified identity management across users, devices and applications	● Not an API security solution in traditional sense, focusing only on identity and authorization
● Microperimeter security approach towards service-level access policy enforcement	● Designed for microservices, less suitable for "legacy" APIs
● Broad range of modern and legacy workloads supported - on-premises and in the cloud	● Small but growing North American customer base and support ecosystem
● SPIFFE standard support for unique identities	

Table 11: Cloudentity major strengths and challenges

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 self-service, risk-based authentication, authorization, privacy/consent management and session mobility for the full lifecycle management of user, device and application identities.

The company uses the term "Microperimeter security" to refer to the concept of deploying security services as close to the things which need to be secured. In this approach, traditional network-level security controls like firewalls or API gateways are replaced with 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 enforce access and permission-based policies uniformly across them.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 12: Cloudentity rating
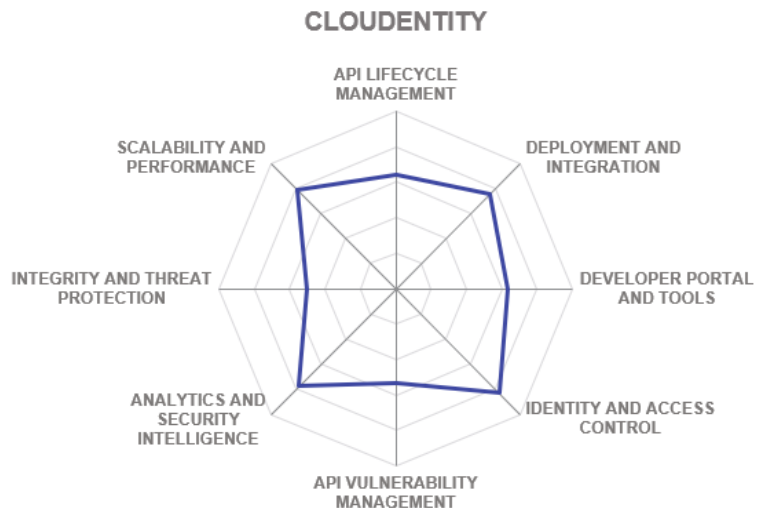
Although Cloudentity's authorization platform is technically not an API management or security solution in a traditional sense, its unorthodox approach towards uniform service-level access policy enforcement can significantly reduce the overall complexity of both legacy and modern applications that rely heavily on APIs to exchange sensitive data across hybrid IT environments. For more traditional security capabilities, the platform supports API ML-based API discovery, parameter validation, protection against DDoS and token replay attacks, integrations with popular 3rd party API gateways, and, last but not least, auditing and logging via an analytics platform.

5.6   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.

| Strengths	Challenges
● Comprehensive support for OAuth and OIDC open standards	● Young but growing company
● Combines flexible authentication with token-based API security controls	● Not an API security solution in traditional sense, focusing only on identity and access management
● Reference "phantom token" architecture for privacy protection	● No support for FIDO standards yet
● Modular API-driven architecture	

Table 13: Curity major strengths and challenges

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 Curity platform together with an existing API gateway provides a solution to enforce access control centrally on any API, not just standard-aware ones.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 14: Curity rating
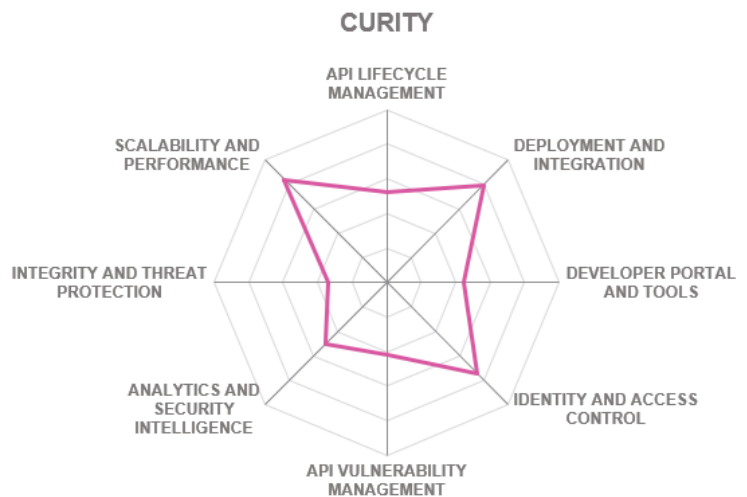
Curity Identity Server is not an API management or security solution. However, identity and flexible fine-grained access management are one of the cornerstones of securing APIs that expose sensitive information. The company provides a reference architecture that combines its identity server with an existing API proxy that implement a simple and scalable data and privacy protection for publicly exposed API endpoints. Notable for its comprehensive support for all major standards and extensible architecture, Curity helps developers centralize identity management and reduce complexity of their business APIs.

5.7   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".

| Strengths	Challenges
● "Security by design" architecture for maximum reliability; FIPS 140-2 and NIAP NDPP-certified	● Analytics platform is still largely a research project
● Comprehensive API threat protection capabilities	● Inconsistent and disconnected UIs between different products
● Supports a broad range of identity and access control standards, tokens, and credentials	
● Significantly expanded choice of deployment and integration scenarios	

Table 15: Forum Systems major strengths and challenges

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 strong focus on API security, the company has significantly updated and expanded its product portfolio in the last couple of years. 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. For these software-based form factors, provisioning and installation can be automated using workflow policies instead of writing code, further improving DevOps automation capabilities.

In addition, a number of new products have been introduced, including ForumPortal – an API developer portal, ForumAPITest for API Testing and ForumAPISim for API Simulation. The company has also recently unveiled the ForumAI platform for API operational analytics.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	strong positive

Table 16: Forum Systems rating
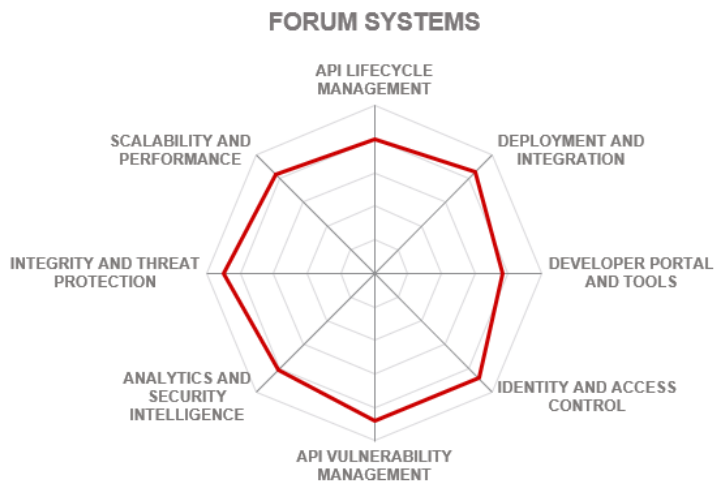
Perhaps the most interesting recent development, however, is the introduction of SaaS-based API security capabilities. Forum Systems works with the AWS partner network to make their existing security and IAM capabilities available as services. Implementing native support for AWSv4 signatures, Forum Sentry makes the full stack of AWS services accessible via the Sentry technology to ease the adoption of AWS services and eliminate coding required to do so. Forum Sentry is thus available as a highly secure hardened alternative to AWS's (as well as Azure's) own API gateway, making enterprise-grade API security accessible to any cloud customer.

5.8   Imperva

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.

| Strengths	Challenges
● Unified security platform for web application and API security	● Analytics limited to correlated data, forensic capabilities are expected in future releases
● Fully SaaS-based with preconfigured security policies	● No way to enroll APIs with no OpenAPI specifications available
● Positive security model based on OpenAPI specification	● Microservice-based applications covered by a separate AppSec solution (Imperva RASP)
● Vendor-agnostic, supports all major API gateways	
● Strong platform hardening and security capabilities	

Table 17: Imperva major strengths and challenges

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 to 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.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 18: Imperva rating
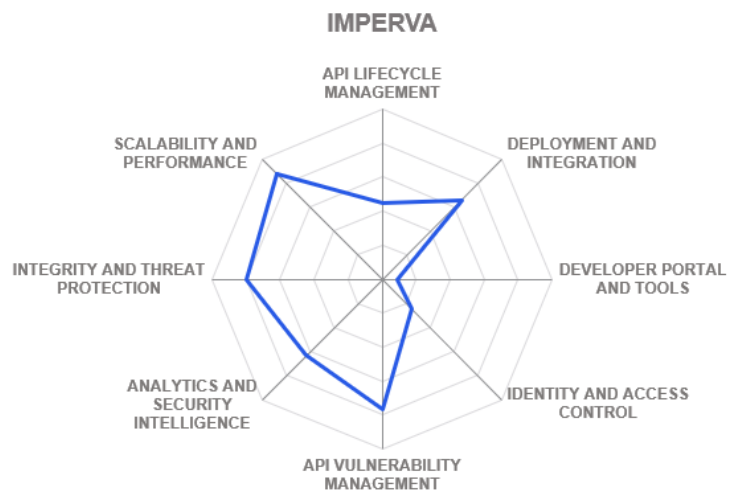
While not offering a full range of API security controls, Imperva API Security can nevertheless be recommended as the first layer of defense against common threats for web applications and gateways, especially for customers with limited security skills.

5.9   Layer7, Broadcom (formerly, CA Technologies)

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's been providing both on-prem and cloud-based API management solutions to hundreds of enterprise customers, and in 2013, it was acquired by CA Technologies to incorporate its product into their own portfolio of API design, management and security tools. In late 2018, CA was itself acquired by Broadcom, an American manufacturer of semiconductor and infrastructure software products. Since 2018, 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.

| Strengths	Challenges
● Full range of management tools for API lifecycle management and microservices	● Targeted primarily towards large enterprise customers, might be too complex for smaller companies
● Part of a larger integrated portfolio of identity, risk management and security products	● Lack of a single consistent UI across all products
● Unified deployment model for all supported environments	
● Advanced security capabilities through Intelligent automation	

Table 19: Broadcom major strengths and challenges

Within Broadcom, Layer7 brand now represents the new unified approach towards integration and security for the whole digital infrastructure of a large modern enterprise, with 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 portfolio that includes products like the API Gateway, Developer Portal, Live API Creator (a visual low-code tool for quick API design) as well as Threat Analytics and ESD Integrations are now offered as a single product: Full Lifecycle API Management. Broadcom's software intelligence platform automation.ai brings in additional security capabilities based on intelligent automation, such as enforcement of least privilege access and identification of rogue users or device across all corporate resources.

Security	strong positive
Functionality	strong positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 20: Broadcom rating
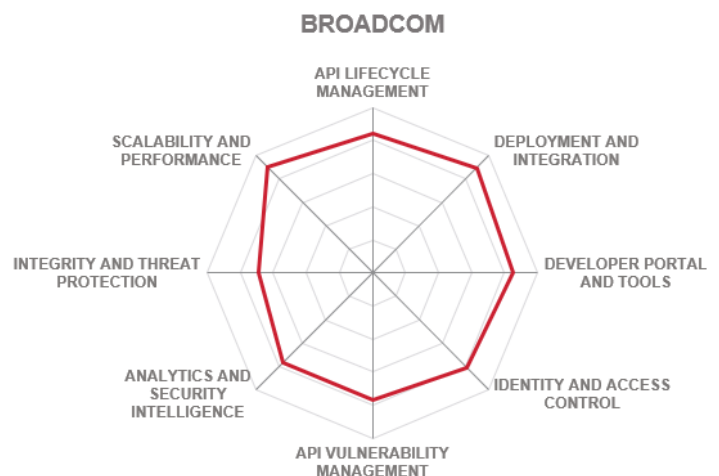
Layer7 API Management portfolio provides a complete solution for practically all API management scenarios imaginable, with a strong focus on enterprise-scale business-driven integration projects, thus making it particularly suitable for large enterprise customers with long-term API strategies.

5.10   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, by implementing their Sentinet platform completely on Microsoft .Net technology and thus specifically targeting customers running Microsoft environments.

Strengths	Challenges
● Implemented entirely in .Net, optimized for Windows environments	● Limited application outside of the Windows ecosystem
● API management and Governance through the built-in repository	● API threat controls are quite rudimentary, implemented as custom extensions
● Simple, but highly flexible distributed architecture	
● High level of extensibility via standard .Net interfaces	

Table 21: Nevatech major strengths and challenges

Nevatech Sentinet is a flexible, lightweight and scalable API Management and API Governance platform that supports major API standards like SOAP and REST, 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 which 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 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.

The latest 6.0 release finally adds a full-featured Developer Portal based on a customizable content management system.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 22: Nevatech rating
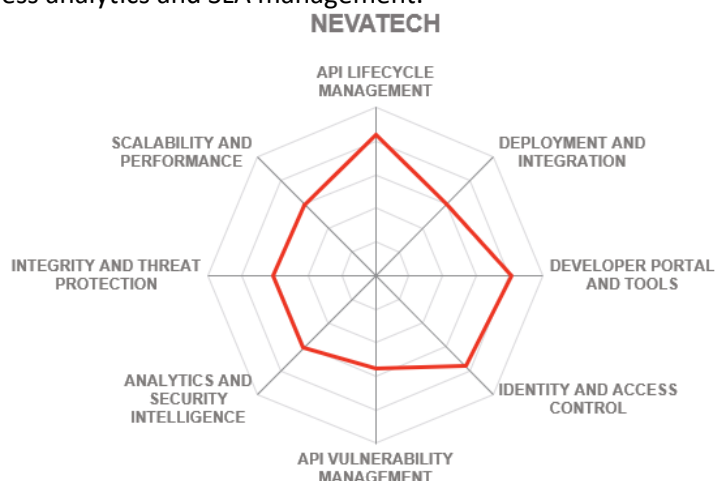
Nevatech's solution can primarily be recommended to companies heavily invested into Microsoft technologies, both on-premises and in Azure Cloud. For such scenarios, the platform offers quick deployment, native support for all relevant standards and protocols and multiple options for adding custom functionality via extensions.

5.11   Red Hat 3scale

3scale is an internet technology company based in San Francisco, California, USA. Founded in 2007, it brought its first API management product to the market in 2009. 3scale cloud-based API Management platform is designed with ease and flexibility in mind and provides all necessary means to open, distribute, and monetize APIs.

In June 2016, the company has been acquired by Red Hat, which subsequently open-sourced the entire 3scale codebase. Currently, 3scale is a part of Red Hat Integration product, which also includes the AMQ messaging platform and Fuse, distributed, cloud-native integration solution. Since July 2019, Red Hat itself is a subsidiary of IBM.

| Strengths	Challenges
● Cloud-native platform designed for high performance, scalability and hybrid deployments	● No longer offered as a standalone solution
● Part of a broader Red Hat's platform for agile Integration	● API threat protection functions provided by third party partners
● Comprehensive support for microservices and serverless architectures	
● Codeless API design studio	
● Open Source codebase	

Table 23: Red Hat major strengths and challenges

3scale API Management provides a managed cloud-based platform for management, analytics, monetization, and developer support functions, which is completely decoupled from the API delivery layer, which is implemented via integrations with technology partners like cloud infrastructure providers or content delivery networks. This approach ensures superior scalability and performance, as well as unmatched developer flexibility, especially for modern distributed and hybrid application architectures.

Security	positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 24: Red Hat rating

RED HAT 3SCALE

After the acquisition, 3scale API Management is no longer marketed as a standalone product, but rather promoted as an integral component of Red Hat Integration suite, which in turn constitutes a part of Red Hat Middleware portfolio. Lacking any native security analytics, Red Hat partners with third party vendors like Ping Identity and Imperva to incorporate them into customer deployments. This makes 3scale more suitable for enterprise customers with large and complex heterogeneous API infrastructures.
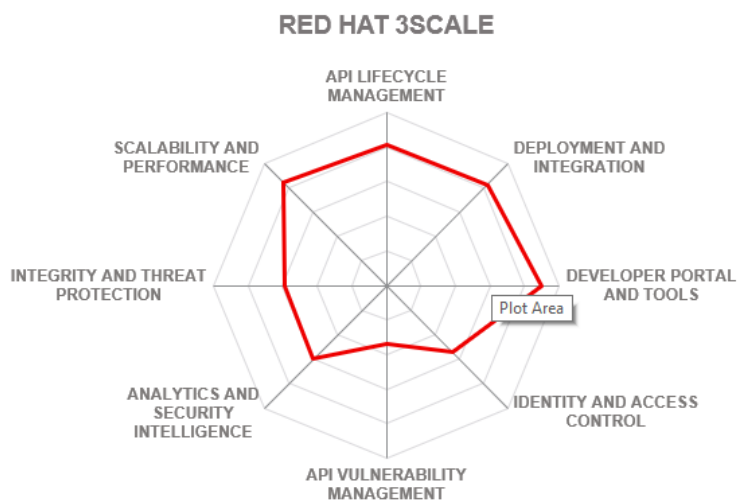
5.12   Salt Security

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 unified API threat protection platform that protects SaaS, web, mobile, microservices and IoT applications from API threat vectors. Harnessing the power of AI, big data and behavioral analytics, the platform does not require any configuration and can be deployed in minutes.

Strengths	Challenges
● Fully passive monitoring, no changes in infrastructure required	● Built-in mitigation capabilities limited to remediation insights
● Continuous discovery of new APIs and their vulnerabilities	● API protection available only with 3rd party tool integrations
● Real-time detection of known and unknown API vulnerabilities and attacks	● Integrations a based on custom webhooks, not standard APIs
● Based on unsupervised machine learning – no configuration or training	

Table 25: Salt Security major strengths and challenges

Salt Security is an API discovery and security monitoring solution that can cover all types of APIs, whether own or third-party, internal or external, official or "shadow". Unlike legacy solutions like WAF, Salt Security uses a signature-free, adaptive learning approach and requires no supervision or configuration to identify and prevent API attacks. 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 monitoring agents on API gateways, proxies, application servers or in containers.

Upon discovery, the platform identifies API functionality (e.g., granular API structure or whether PII is being processed) and analyzes it for known vulnerabilities. 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 or integrating with existing enforcement infrastructure for blocking.

Security	strong positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 26: Salt Security rating

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 any native mitigation controls, it can be integrated into existing enforcement points like WAFs or API gateways for threat blocking.
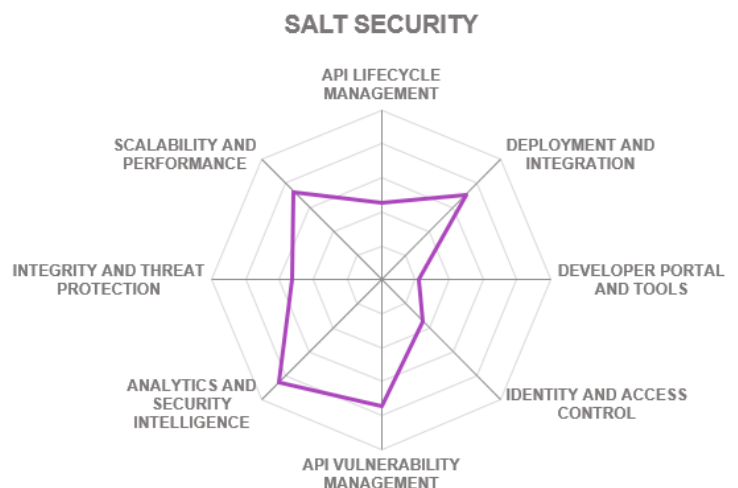
5.13 Sensedia

Sensedia is an API management company headquartered in Campinas, Brazil. Founded in 2007 as a SOA vendor, it has launched its API management platform in 2012 and quickly became a market leader in Brazil. Since 2018, the company is slowly expanding into international markets as well. Sensedia provides a full-featured API management platform that incorporates tools for every stage of 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.

| Strengths	Challenges
● Full-featured API management platform with tools for all phases of API lifecycle	● Very little market presence outside of Brazil
● Flexible deployment options with support for hybrid architectures	● Advanced threat protection is only supported through 3rd party partnerships
● API Studio for exposing legacy backends	
● Comprehensive API threat detection controls	
● Broad range of consulting services	

Table 27: Sensedia major strengths and challenges

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 Top 10 OWASP threats with a broad range of built-in security functions. A potential downside of this approach is a notable lack of prepackaged 3rd party integrations.

Security	positive
Functionality	strong positive
Integration	strong positive
Interoperability	positive
Usability	strong positive

Table 28: Sensedia rating
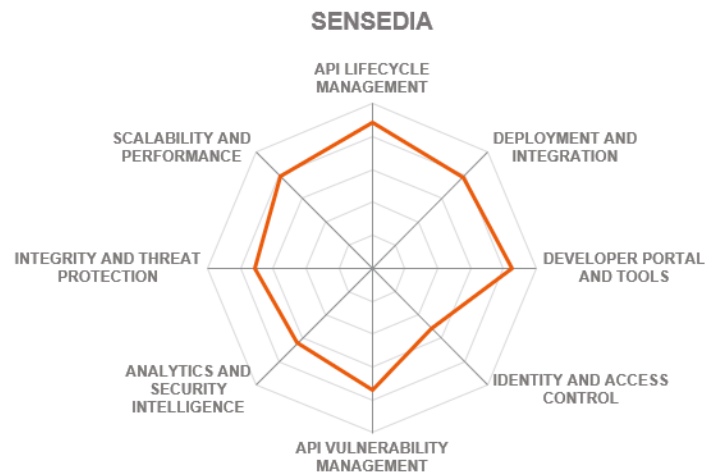
Perhaps the only drawback of Sensedia API platform is that it's almost unknown outside of its home market in Brazil. Sensedia aims to change it though as the company is expanding to the European market, just recently opening a UK office, as well as establishing partnerships with global system integrators.

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.

5.14 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, Tyk platform is designed for multi-DC and multi-cloud deployments, high performance and full backwards compatibility.

| Strengths	Challenges
● Designed for scalability, optimized for containers and microservices	● Built-in API security functions quite rudimentary; advanced protection requires 3rd party tool integration
● Centralized management for distributed and multi-cloud architectures	● SaaS option currently only available in the US
● Large number of integrations with DevOps tools, everything is API-driven	
● Open Source codebase, large community	

Table 29: Tyk major strengths and challenges

Tyk Enterprise is a modern, lightweight API management platform built around Tyk, the popular open source API Gateway project. 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.

In addition to the gateway, 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. Self-service capabilities help make life easier for both own and 3rd party developers.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 30: Tyk rating
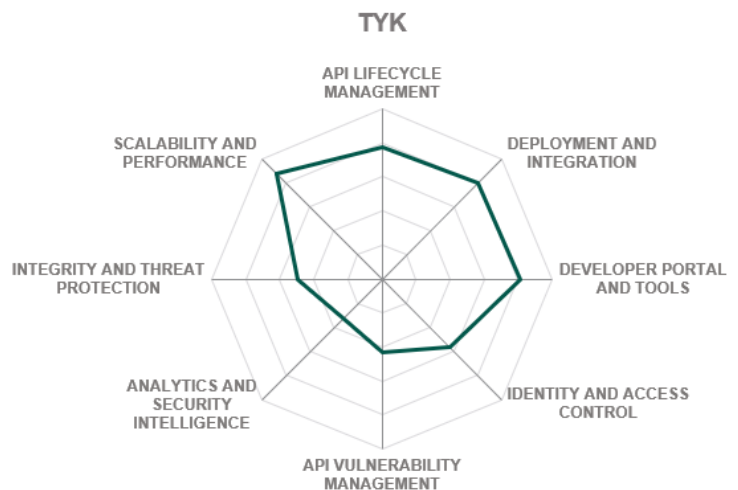
Although not as feature-rich and comprehensive as its enterprise-grade counterparts, Tyk can be an ideal choice for modern agile companies or developer teams that expect their tools start small and then grow along with their projects. With all functionality available for free non-commercial use, Tyk is also a perfect solution for educational or non-commercial API projects.

Yet, Tyk has also proven popular with large enterprises and government agencies around the world as well, which indicates its ability to scale for any project size.

5.15 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.

| Strengths	Challenges
● Built on an integrated open source platform for business-centric solutions	● Advanced authentication and access control require integration with other WSO2 products
● Flexible deployment options including containerized environments	● Threat prevention functions are limited
● Cloud-native support to expose microservices as managed APIs	● UI isn't particularly user-friendly
● Can be extended and adapted to most complex customer requirements	
● AI-powered abnormal activity detection	

Table 31: WSO2 major strengths and challenges

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 flexibility and open source nature of the platform enables different customizations to address most complex deployment scenarios.

Security	strong positive
Functionality	strong positive
Integration	strong positive
Interoperability	strong positive
Usability	positive

Table 32: WSO2 rating
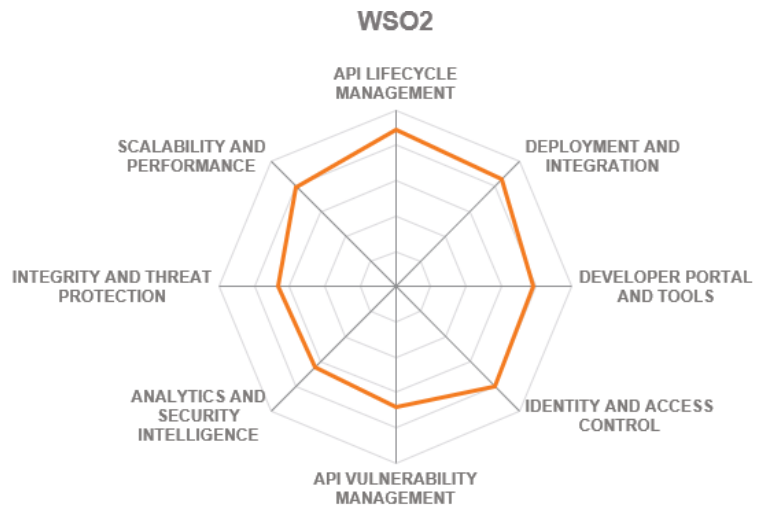
Although WSO2's API solution is quite functional out-of-the-box, it's the platform's flexibility that makes it ideal for projects where API management is a part of a bigger infrastructure and customizability is an important requirement. And, of course, WSO2's solution based on Open Source provides the lowest total cost of implementation.

6 Vendors to watch

In addition to the vendors evaluated in detail in this Leadership Compass, there are several companies that for various reasons were unable to participate in the rating but are nevertheless worth mentioning.

Some of the vendors below are focusing primarily on other market segments yet show a notable overlap with the topic of our rating. Others have just entered the market as startups with new, yet interesting products worth checking out. Finally, we'll mention the API management services which are offered by major cloud service providers as a part of their native PaaS portfolios.

6.1   Akana by Perforce

Akana, known until 2015 as SOA Software, is 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 their scope towards API management and security and cloud integration. In 2016, Akana was acquired by Rogue Wave Software, and in January 2019, both companies became a part of Perforce, one of the leading providers of software lifecycle, version control, and code analysis tools.

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.

6.2   CloudVector

CloudVector, until recently known as ArecaBay, is an API security-focused startup company, founded in 2018 in Los Altos, CA. Claiming to be the first API Detection & Response solution provider, the company offers a platform for discovering, monitoring and securing all corporate APIs regardless of their technology or deployment environment.

The company's API-DR approach focuses on 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.

6.3   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.

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.

6.4   Kong Inc.

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.

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

6.5   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. 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.

6.6   Ping Identity

Ping Identity is a privately held 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 fine-grained access controls for apps and APIs, with a comprehensive policy engine and risk-aware authorization, or PingDataGovernance that provides centralized, fine-grained access control to various data sources, including those accessed via APIs.

After a recent acquisition of Elastic Beam, a pioneering API security intelligence company, Ping now offers PingIntelligence for APIs, which provides deep visibility into API traffic, discovers APIs automatically, provides AI-powered API attack detection and blocking, and uses deception controls to identify intrusions in real time.

6.7   Spherical Defence

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

Spherical Defence's first product based on this technology is an "AI Web Application Firewall" -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. The product can be deployed entirely on-premises or in a private cloud and is able to utilize GPU acceleration for high performance.

6.8   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. 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.

6.9 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 to proactively identify vulnerabilities in applications and APIs and to detect and block zero-day attacks that target those vulnerabilities.

The company's solution is developed on top of NGINX, a popular high-performance web server and load balancer and is primarily targeted towards customers with high-loaded web application, API and microservice-based projects in e-commerce, fintech, and Software-as-a-Service industries.

6.10 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 their own native API management services. In addition, the company's own services expose their own APIs or provide means to develop custom APIs quickly.

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.

6.11 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.

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.

6.12 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. Just like AWS, 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.

With the introduction of 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.

6.13 Oracle Cloud

Oracle Cloud incorporates its own complete API lifecycle management platform as well. 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.

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 particular 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.

7.1 Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in a 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 of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.

- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the market segment. They provide several of the most innovative and upcoming features we hope to see in the market segment.

- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in all areas.

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

- Leaders: This identifies the Leaders as defined above. Leaders are products which are exceptionally strong in 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 that market segment. Input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and a questionnaire sent out before creating the KuppingerCole Leadership Compass, as well as other sources.

7.2   Product rating

KuppingerCole as an analyst company regularly does 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 IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). 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 vendors deal 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.

---

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

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. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

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 the lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and weak infrastructure.

---

[2] https://www.kuppingercole.com/report/cb_apieconomy16122011

7.3 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.

7.4 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 the market position or financial strength, indicating that vendors are very small and have a very low number of customers.

7.5 Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider graph for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For the field of Database and Big Data Security, we look at the following eight areas:

API Lifecycle Management	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	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 3rd 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 to 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 allows for quick detection of not just

	external attacks, but infrastructure changes, misconfigurations, insider threats and other suspicious activities.
Integrity and Threat Protection	Securing APIs and services from hacker attacks and other threats requires a multilayered approach to address both transport-level attacks and exploits specific to messaging protocols and data formats.
Scalability and Performance	Maintaining continuous availability of the enterprise services even under high load or a denial-of-service attack is the most crucial requirement for an API infrastructure. A modern API management solution should also address the challenges of lightweight distributed architectures.

These spider graphs add an extra level of information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas while being strong in other areas. These might be a good fit if only specific features are required. Given the breadth and complexity of the full scope of database security, only very few largest vendors have enough resources to offer solutions that cover all of the areas; thus, we do not recommend overlooking smaller, more specialized products – often they may provide substantially better return of investment.

7.6 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 of 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 a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

Despite our effort to cover most aspects of API management and security in this Leadership Compass, we are not planning to review the following products:

- Solutions that only cover a single area of API management, like developer portals or API monetization

- Solutions that focus on a specific industry only, like securing banking APIs

- Products or services that exist solely to extend the functionality of other API management solutions and provide no standalone value

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 the chapter *Vendors to watch*. In that chapter, we also look at some other interesting offerings around the Database and Big Data Security market and in related market segments.

8 Copyright

The Future of Information Security – Today

KuppingerCole supports 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 Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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