KuppingerCole Report

LEADERSHIP COMPASS

By Alexei Balaganski

August 13, 2021

API Management and Security - Cequence Security Excerpt

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

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

Content

Excerpt from Market Compass API Management and Security

Exclusive Rights for Cequence Security

1 Introduction / Executive Summary

From what used to be a purely technical concept created to make developers' lives easier, Application Programming Interfaces (APIs) have evolved into one of the foundations of modern digital business. Today, APIs can be found everywhere - at homes and in mobile devices, in corporate networks and in the cloud, even in industrial environments, to say nothing about the Internet of Things.

As companies are struggling to maintain their business agility, to react to the ever-changing market demands and technology landscapes, the need to deliver a new application or service to customers as quickly as possible often trumps all other considerations. Rapidly growing demand for exposing and consuming APIs, which enables organizations to create new business models and connect with partners and customers, has tipped the industry towards adopting lightweight RESTful APIs, which are commonly used today.

The rapid adoption of REST APIs also coincided with the exponential growth of cloud computing and mobile device proliferation, where they were the perfect medium to enable integrations between these heterogeneous systems and facilitate data exchange on a massive scale. In a world where digital information is one of the "crown jewels" of many modern businesses (and even the primary source of revenue for some), APIs are now powering the logistics of delivering digital products to partners and customers. Almost every software product or cloud service now comes with a set of APIs for management, integration, monitoring, or a multitude of other purposes.

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

Perhaps the most notable trend is the rapid expansion of the scope of both modern API management and API security solutions. Nowadays, API gateways for publishing REST API endpoints can certainly already be considered "legacy products". New API technologies, like GraphQL or gRPC, have grown from research projects into widely adopted solutions for specific use cases, where they provide much better flexibility or

performance than REST APIs. Modern loosely coupled cloud-native application architectures demand API management solutions that can handle complicated traffic patterns and deal with ephemeral container-based infrastructures.

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

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

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

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

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

1.1 Highlights

- Both API management and API security market segments continue to evolve and grow, driven by a massive increase in API adoption, as well as by an ongoing pressure of security and compliance risks APIs are exposed to.
- The tempo of the API evolution continues to increase, with multiple new standards, protocols and

architectures emerging, expanding the scope for API management solutions beyond just the traditional REST APIs.

- Fueled by widely publicized large-scale data breaches and new compliance regulations in various industries, the overall awareness of API security risks and challenges continues to rise.
- With standard API management capabilities quickly becoming a commodity, vendors specializing in these solutions are focusing on increasing their functional coverage to address new business requirements, involve new stakeholders, and improve productivity for developers.
- Some vendors no longer consider API management a standalone market, offering these functions as a part of larger enterprise integration platforms.
- API discovery and security monitoring solutions continue to be the most popular class of products offered on the API security market, but solutions addressing other phases of the API lifecycle are growing in popularity.
- The market consolidation trend continues, with larger established vendors acquiring small innovative startups, integrating their technologies into more comprehensive, unified security platforms.
- The notion of data-centric security that incorporates API security as one of the major layers in an integrated, layered architecture is emerging, with several vendors already offering such integrated platforms.
- The overall leaders in the API management and security market are (in alphabetical order): 42Crunch, Axway, Broadcom, Curity, Forum Systems, Google Apigee, Imperva, Red Hat, Sensedia, and WSO2.

1.2 Market Segment

We have long recognized the API Economy as one of the most important current IT trends. Rapidly growing demand for exposing and consuming APIs, which enables organizations to create new business models and connect with partners and customers, has tipped the industry towards adopting lightweight RESTful APIs, which are commonly used today, along with the growing variety of alternative protocols and standards.

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

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

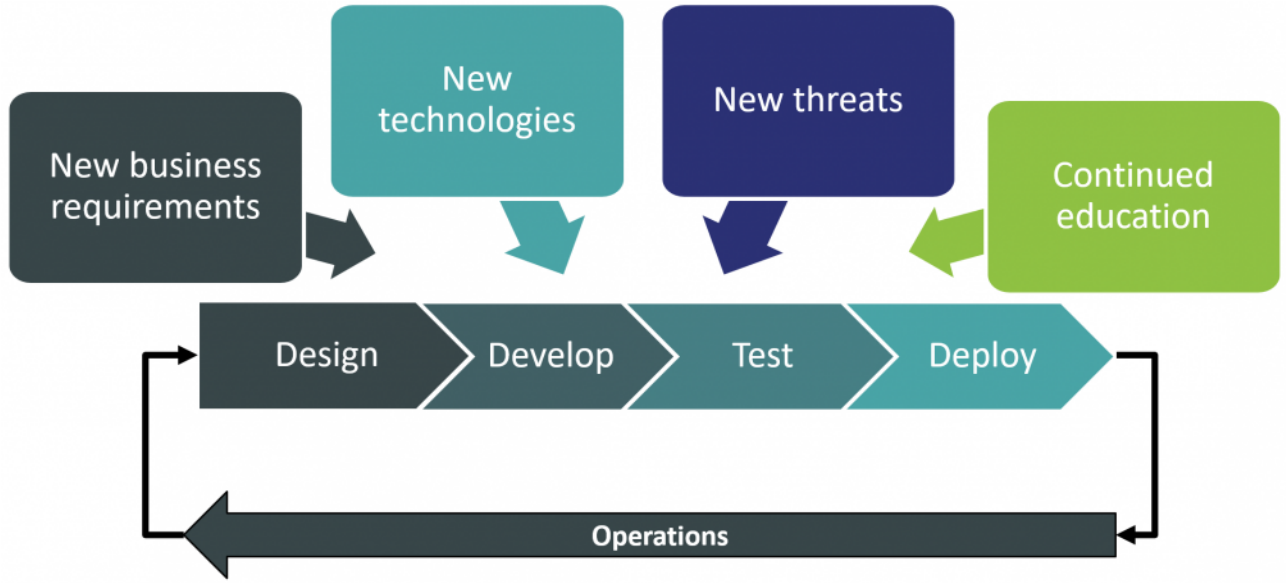


Figure 1: API Lifecycle

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

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

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

On the other hand, the growing awareness of the general public about API security challenges has dramatically increased the demand for specialized tools for securing existing APIs. This has led to the

emergence of numerous security-focused startups, offering their innovative solutions, usually within a single area of the API security discipline.

Unfortunately, as the diagram below illustrates, the field of API security is very broad and complicated, and very few (if any) vendors are currently capable of delivering a comprehensive security solution that could cover all required functional areas. Although the market consolidation continues, with larger vendors acquiring these startups and incorporating their technologies into existing products, expecting to find a "one-stop shop" for API security is still a bit premature.

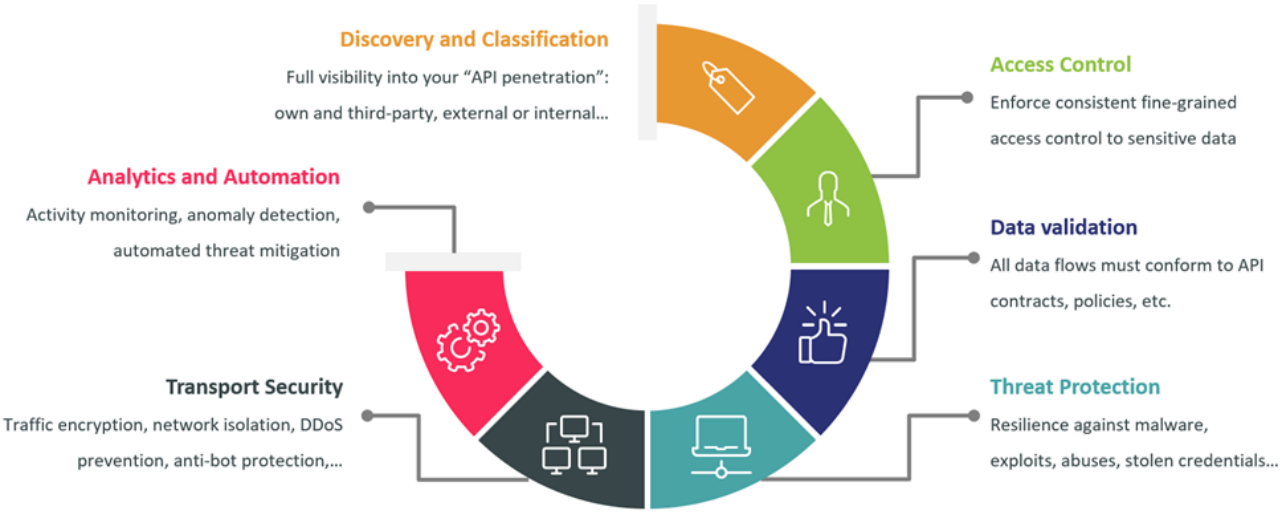


Figure 2: The Scope of API Security

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

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

1.3 Delivery Models

Since most of the solutions covered in our rating are designed to provide management and protection for APIs regardless of where they are deployed - on-premises, in any cloud, or within containerized or

serverless environments - the very notion of the delivery model becomes complicated.

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

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

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

1.4 Required Capabilities

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

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

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

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

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

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

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

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

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

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

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

A strong focus is put on integration into existing security infrastructures to provide consolidated monitoring, analytics, governance, or compliance across multiple types of information stores and applications.

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

Some additional functional capabilities for this Leadership Compass include:

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

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

- overall functionality and usability
- internal service security
- size of the company
- number of customers and end-user consumers
- number of developers
- partner ecosystem
- licensing models

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

2 Leadership

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

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

- Product
- Innovation
- Market

2.1 Overall Leadership

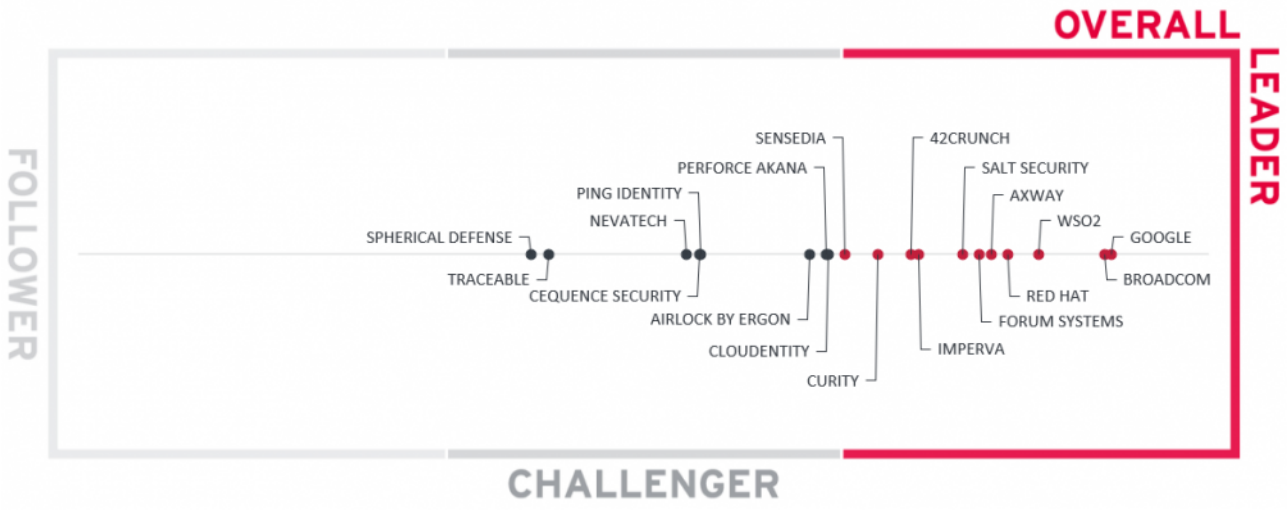


Figure 3: The Overall Leadership rating for the API Management and Security market segment

The Overall Leadership rating provides a consolidated view of all-around functionality, market presence, and

financial security. However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we strongly recommend looking at all the leadership categories as well as the sections on each vendor and their offering to get a comprehensive understanding of the players in this market and what use cases they support best.

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

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

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

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

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

There are no Followers in the overall leadership rating.

Overall Leaders (in alphabetical order):

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

- Salt Security
- Sensedia
- WSO2

2.2 Product Leadership

The first of the three specific Leadership ratings is about **Product** leadership. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services. In the Product Leadership rating, we look specifically for the functional strength of the vendors' solutions, regardless of their current ability to grab a substantial market share. This is why we have a mix of large and small vendors among the leaders.

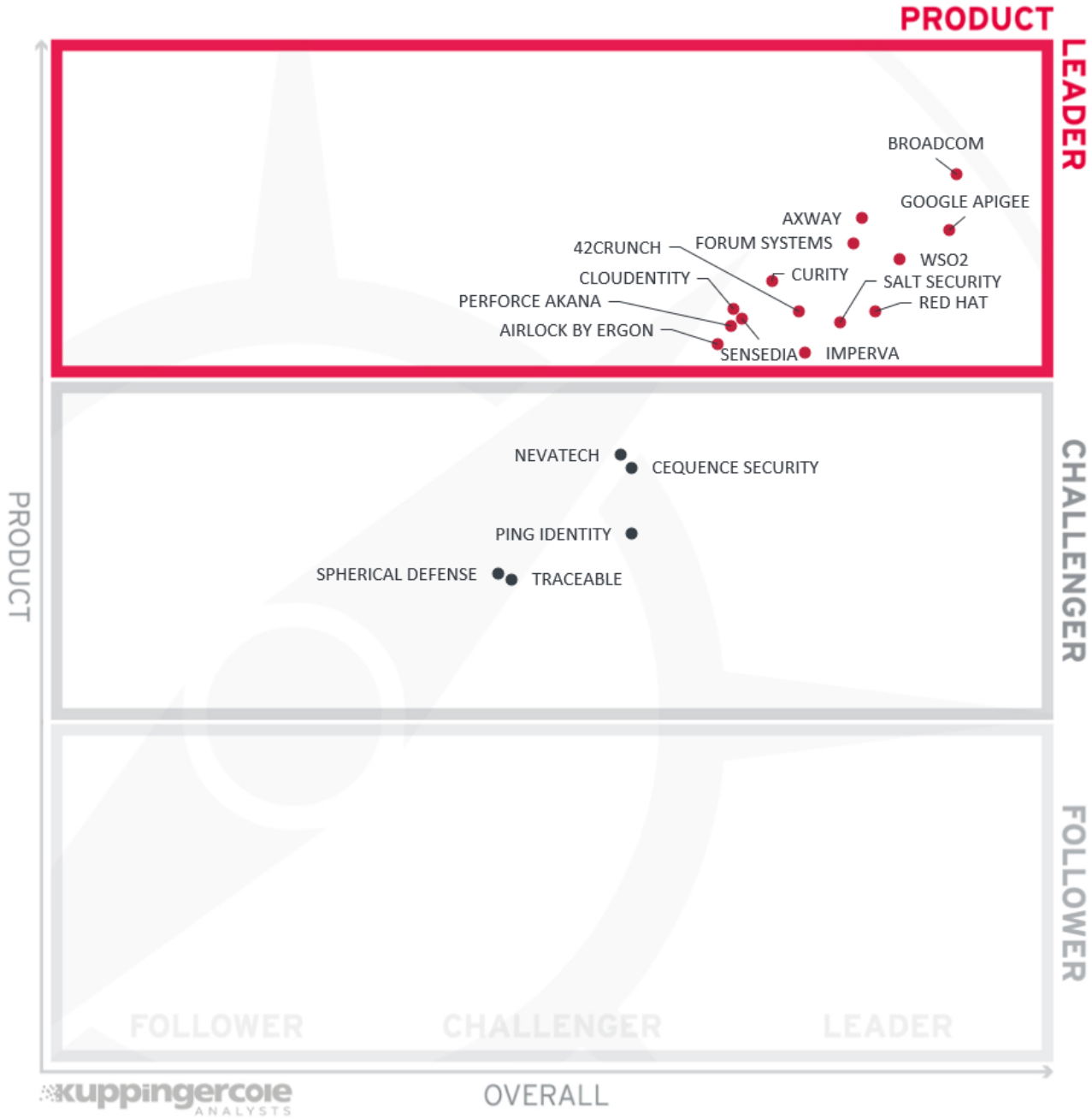


Figure 4: Product Leaders in the API Management and Security segment

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

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

Product Leaders (in alphabetical order):

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

2.3 Innovation Leadership

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

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

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

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

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

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

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

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

Innovation Leaders (in alphabetical order):

- 42crunch
- Airlock by Ergon
- Axway

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

2.4 Market Leadership

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

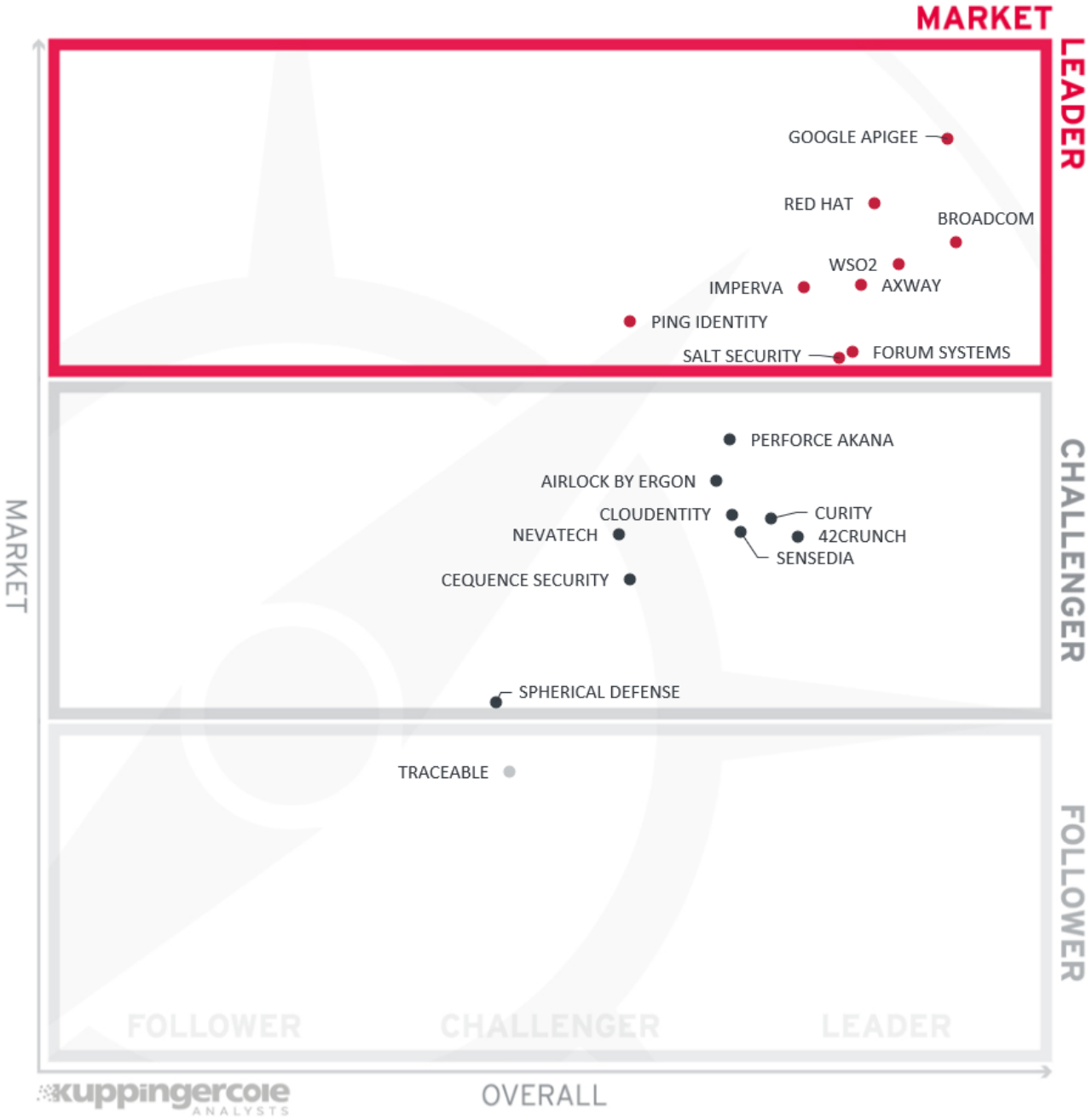


Figure 6: Market Leaders in the API Management and Security segment

Please note that this rating does not reflect the overall market presence of large vendors but is only limited to the market shares of their respective API management and security products.

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

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

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

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

Market Leaders (in alphabetical order):

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

3 Correlated View

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

3.1 The Market/Product Matrix

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

Figure 7: The Market / Product Matrix

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

Among the Market Champions, we can find the usual suspects - large, well-established vendors like Axway, Broadcom, Google, Imperva, Red Hat, and WSO2, followed by Forum Systems and Salt Security.

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

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

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

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

3.2 The Product/Innovation Matrix

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

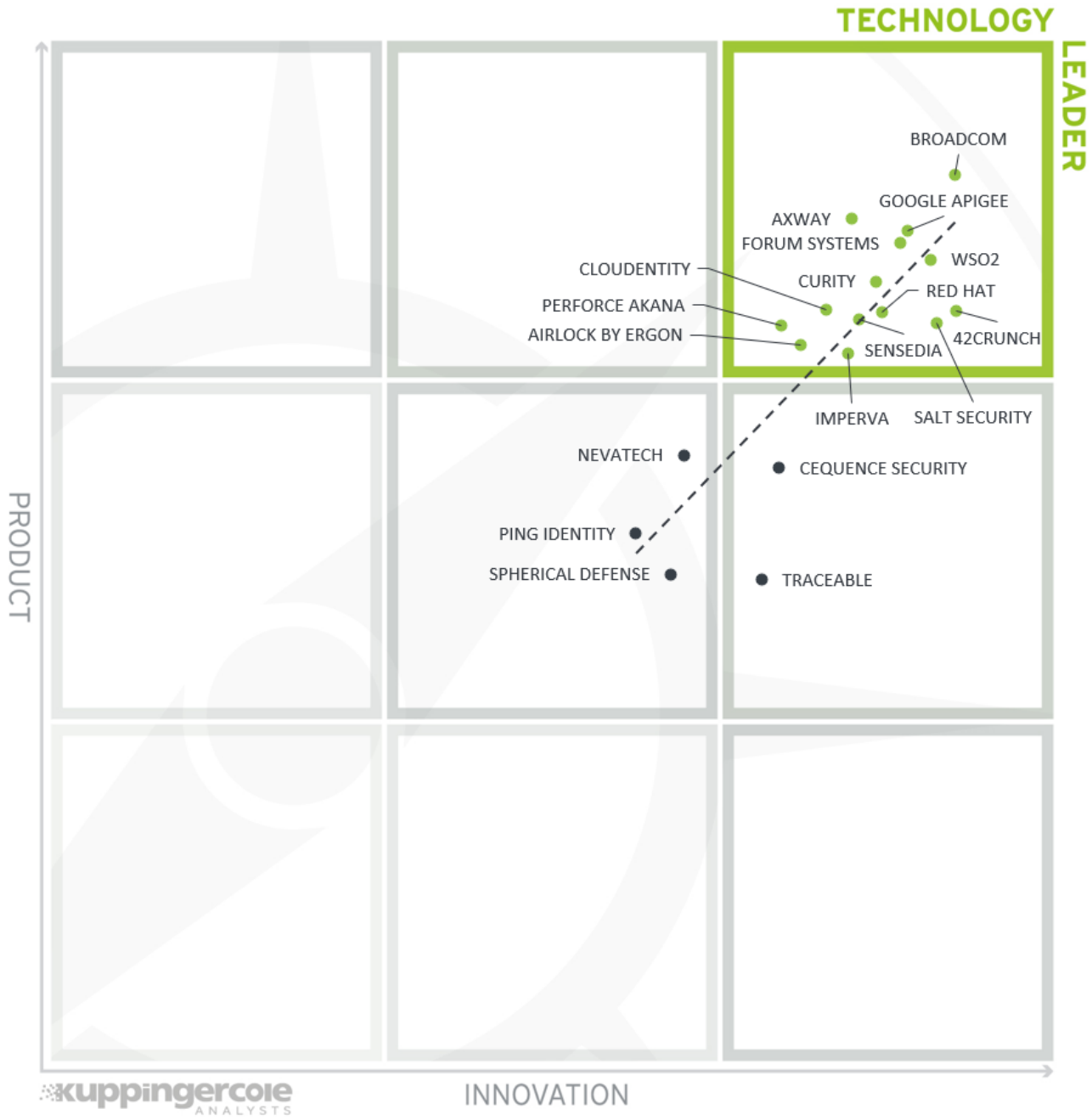


Figure 8: The Product / Innovation Matrix

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

Again, among the Technology Leaders, we have a healthy mix of both large established players and innovative solutions from smaller vendors. Traceable and Cequence Security can be found in the right middle box, indicating their position in the early stage of the startup lifecycle, when even a highly innovative

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

3.3 The Innovation/Market Matrix

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

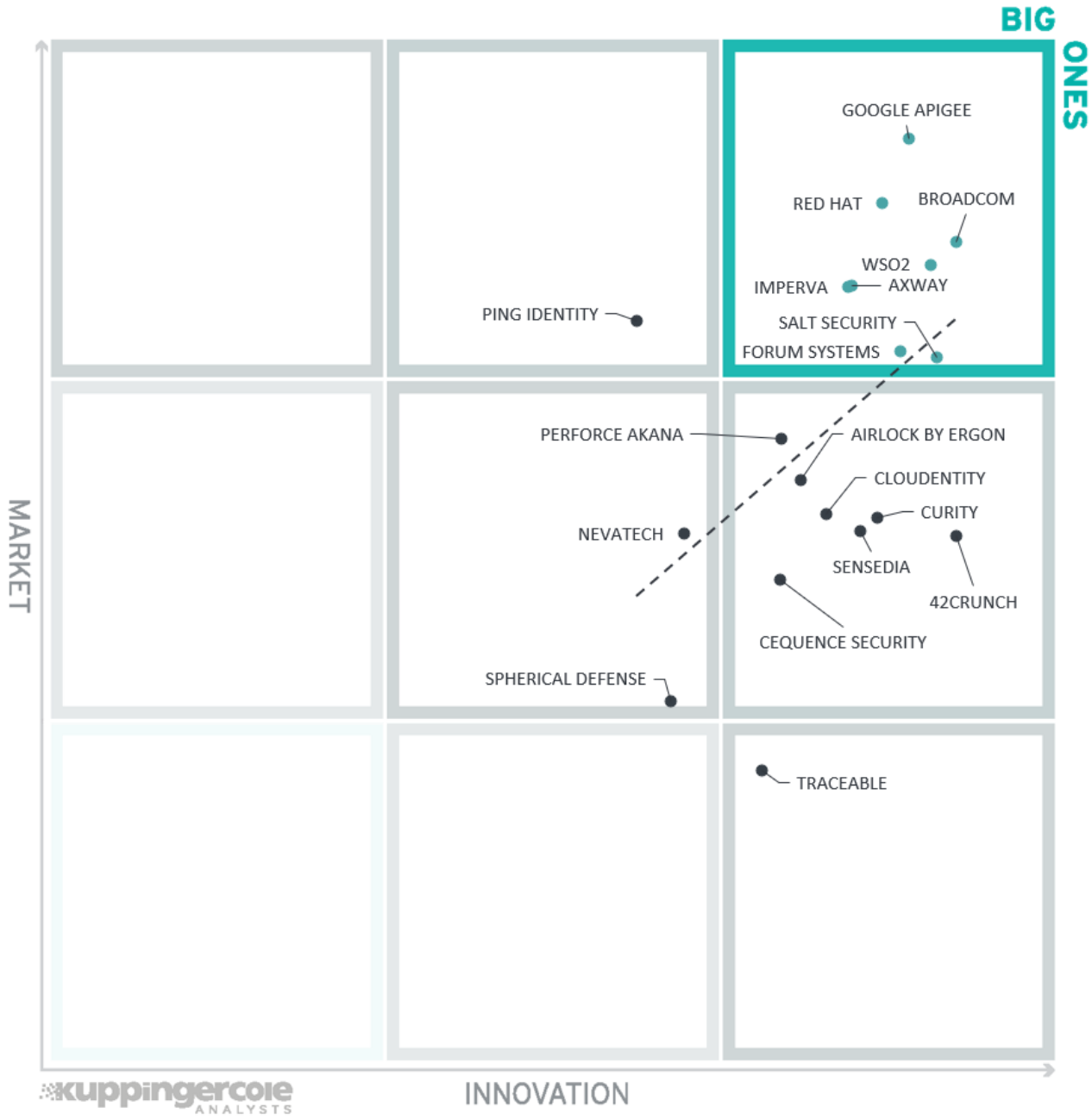


Figure 9: The Innovation/Market Matrix

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

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

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

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

4 Products and Vendors at a Glance

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

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

Based on our evaluation, a comparative overview of the ratings of all the products covered in this document is shown in Table 1.

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

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
42Crunch	strong positive	weak	neutral	positive
Airlock by Ergon	positive	neutral	positive	positive
Axway	positive	positive	strong positive	positive
Broadcom Inc.	strong positive	strong positive	strong positive	strong positive
Cequence Security	positive	neutral	neutral	neutral
Cloudentity	positive	neutral	neutral	positive
Curity	positive	positive	positive	positive
Forum Systems	positive	positive	strong positive	positive
Google Apigee	positive	strong positive	strong positive	strong positive
Imperva (was acquired by Thoma Bravo)	positive	positive	strong positive	strong positive
Nevatech	neutral	neutral	neutral	neutral
Perforce Akana	neutral	positive	positive	positive
Ping Identity	neutral	positive	strong positive	positive
Red Hat	positive	positive	strong positive	strong positive
Salt Security	strong positive	positive	positive	positive
Sensedia	positive	positive	positive	neutral
Spherical Defense	positive	neutral	neutral	neutral
Traceable	positive	weak	weak	weak
WSO2	strong positive	strong positive	positive	strong positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

Spider graphs

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

- **API Lifecycle Management** - here we evaluate the core capabilities of an API management platform, which cover all major stages of an API lifecycle: from architecting an API strategy to developing, deploying, and refining your APIs to daily management and operations, including API monetization.
- **Deployment and Integration** - with the rapid proliferation of API use cases and deployment scenarios, API management platforms must support a wide range of deployment options, from traditional on-premises appliances and static gateways to modern dynamic microservice-based architectures, serverless applications, and IoT, being able to play well together with popular third-party products.
- **Developer Portal and Tools** - exposing APIs for consumption, providing documentation and collaboration functions, onboarding, and managing developers and their apps are among the functions we are looking for here, DevOps and DevSecOps integrations included.
- **Identity and Access Control** - supporting multiple identity types, standards, protocols, and tokens and providing flexible dynamic access control that is capable of making runtime context-based decisions. This does not only apply to the APIs themselves, but management interfaces and developer tools as well.
- **API Vulnerability Management** - discovering existing APIs and analyzing their conformance to API contracts, security best practices, and corporate policies is the only truly proactive approach towards API security. Intelligent prioritization of discovered vulnerabilities by business risk assessment improves both developer productivity and overall security posture.
- **Analytics and Security Intelligence** - continuous visibility and monitoring of all API transactions and administrative activities allow for quick detection of not just external attacks, but infrastructure changes, misconfigurations, insider threats, and other suspicious activities.

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

The spider graphs provide comparative information by showing the areas where vendor services are stronger or weaker. Some vendor services may have gaps in certain areas, while being strong in other areas. These kinds of solutions might still be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic implementations of API Management and Security technologies.

5.1 Cequence Security

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

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

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

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

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

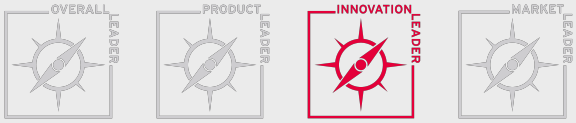
Strengths

- Integrated application security platform powered by purpose-built AI-driven analytics engine.
- A broad set of technology integrations enable the discovery and protection of both external and internal APIs.
- Automated API inventory simplifies management, creation of policies.
- Inline deployment enables instant blocking of detected threats.
- Real-time API risk assessment with sensitive data leakage discovery and configurable, extensible risk modeling.

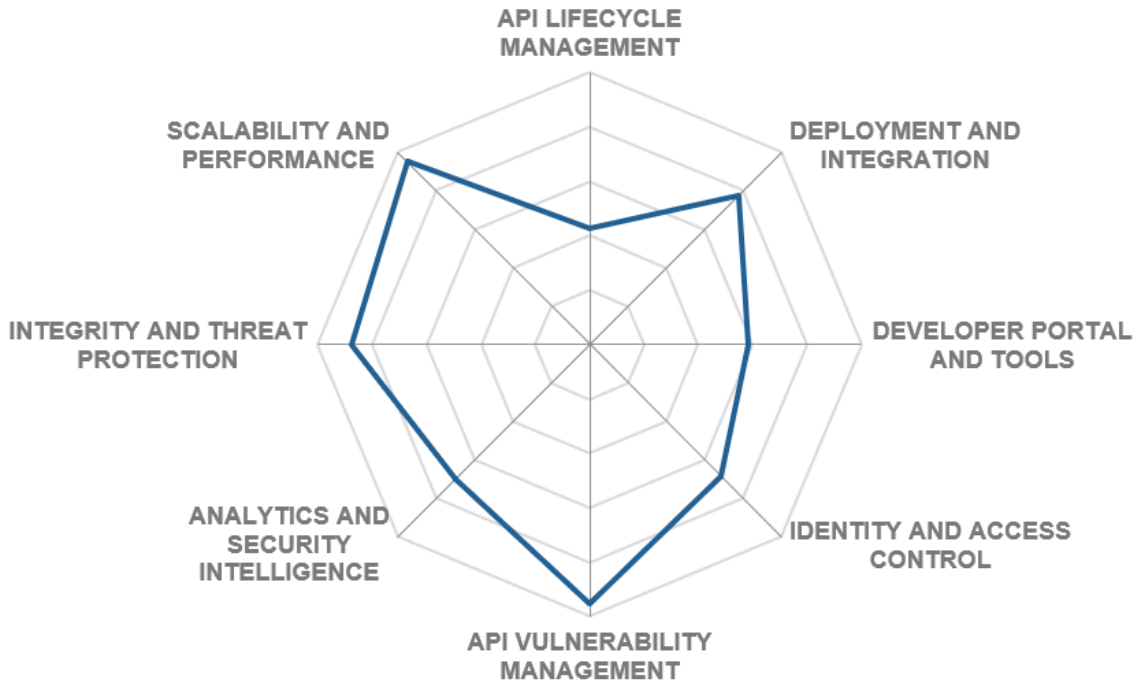
Challenges

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

Leader in



CEQUENCE SECURITY



6 Related Research

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

Methodology

About KuppingerCole's Leadership Compass

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

It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

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

Types of Leadership

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

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

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- **Security**
- **Functionality**
- **Integration**
- **Interoperability**
- **Usability**

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

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

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

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

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

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

We focus on security, functionality, integration, interoperability, and usability for the following key reasons:

- Increased People Participation—Human participation in systems at any level is the highest area of cost and potential breakdown for any IT endeavor.

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

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

Vendor rating

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

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

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

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

Financial strength – even while KuppingerCole doesn't consider size to be a value by itself, financial strength is an important factor for customers when making decisions. In general, publicly available financial information is an important factor therein. Companies which are venture-financed are in general more likely to become an acquisition target, with massive risks for the execution of the vendor's roadmap.

Ecosystem – this dimension looks at the ecosystem of the vendor. It focuses mainly on the partner base of a vendor and the approach the vendor takes to act as a "good citizen" in heterogeneous IT environments.

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

Rating scale for products and vendors

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

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

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. E.g. for security, this can indicate some gaps in fine-grain control of administrative entitlements. E.g. for market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral
Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. E.g. for functionality, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For company ratings, it can indicate, e.g., a regional-only presence.

Weak
Below-average capabilities in the product ratings or significant challenges in the company ratings, such as very small partner ecosystem.

Critical
Major weaknesses in various areas. This rating most commonly applies to company ratings for market position or financial strength, indicating that vendors are very small and have a very low number of customers.

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

Copyright

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

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

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