KuppingerCole Report

LEADERSHIP COMPASS

By Richard Hill

Identity API Platforms

Identity API Platforms expose APIs to capabilities ranging from IAM to Federation and more while supporting both the agile and DevOps paradigms that address the more complex IT environments seen today. This Leadership Compass will give you an overview and insights into the Identity API Platform market; providing you a compass to help you find the product that you need.

By **Richard Hill**
rh@kuppingercole.com
August 30, 2019

Content

Content of Figures

1 Introduction

Many different factors are driving Digital Transformation in the market today. One factor is the change in how businesses interact with their consumers requiring changes in the services they provided to their customers. Another factor is more on the technical side that addresses the implementation of new Digital Services that have become more complex due to the different environments and the many integration points to consider. This is driving the rapidly growing demand for exposing and consuming APIs. APIs are enabling organizations to create new business models, connect with partners and customers while providing a seamless experience by linking systems and services together.

These changes in which services expose and consume APIs are also enabling agile paradigms and DevOps by providing a well-defined set of APIs to security services instead of creating their own identity and security (and other) services in each and every application again and again. One of the most common use cases we currently see is around Digital Services for customers that are created against "identity backends. Although the concept and use of Application Programming Interfaces (APIs) have been around for quite some time, the availability of IAM and its associated APIs has grown into a new market segment KuppingerCole calls Identity API Platforms in this Leadership Compass. To get to the how or why this new Identity API Platforms market segment has developed; it may be helpful to look at how IAM has changed over time.

Traditionally, the IT environment has run within the walls of their perimeter. IAM solutions were more monolithic, centralized and identities were managed and stored on-premises. Local access control systems were used to ensure employees have access to just the resources they need through authentication & authorization, with the ability to audit user access.

And then we started to see federation hubs, or bridges that extended the reach of where identity and access controls reside. Federation allowed for the secure exchange user information that could be between divisions with organizations or between organizations in the same sector. Single sign-on (SSO) systems gave users the ability to authenticate once, not only across multiple IT systems but organizations too.

Cloud services gave organizations new options for IT, motivated by the business need to increase IT flexibility, and scalability, while reducing cost. Under the umbrella of IDaaS, there are many abilities. Not only traditional IAM but also capabilities ranging from SSO to full Identity Provisioning.

As organizations began reaching out to customers and gathering info about the consumers who are using their products & services, they found that they needed to provide a better digital experience. This improved user experience manifested through the use of consumer's mobile devices or social networks and providing an easier onboarding experience for consumers. But they also needed to be concerned about privacy compliance such as GDPR or PSD2.

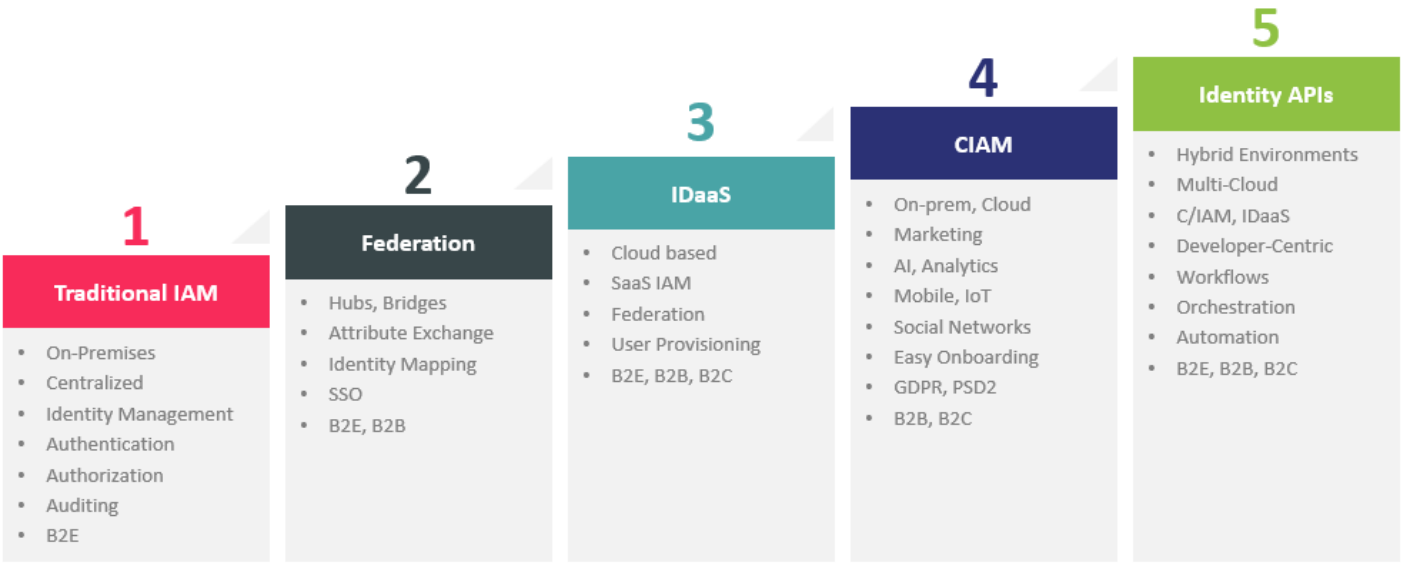


Figure 1: Evolution of IAM over time

Now we are beginning to see Identity APIs platforms becoming available. This market is driven by the need to meet emerging IT requirements such as hybrid environments that span across on-premises, the cloud, even multi-cloud environments supporting the different functional requirements of IAM, Federation, IDaaS & CIAM, as well as the ability to select these market segment capabilities a la carte as needed. By exposing key functionality via APIs, it allows for workflow and orchestration capabilities across environments as well as better DevOps support through automation. Another critical characteristic of Identity API Platforms is their focus on being developer-centric. In a nutshell, IAM is continuing to evolve to meet the growing list of IAM requirements.

1.1 Market Segment

The Identity API Platforms share many of the same capabilities seen in the IAM, CIAM, IDaaS, and Adaptive Authentication/Consumer Authentication market segments. In fact, many offerings in the market today are serving multiple segments. Although there are crossover capabilities between these segments, Identity API Platforms must support the basic functionality of identity and user management, authentication, authorization, and support for auditing. Other capabilities can be added to the Identity API Platforms based on the solutions target market use cases such as capabilities found in CIAM to support consumers like user consent management workflows, federation in IDaaS, or more intelligent authentication as seen with Adaptive Authentication as well as support for compliance and access governance offered by IGA solutions. Beyond these capabilities, evolving requirements such as IoT, workflows and orchestration, DevOps, and API security functionality are also taken into account.

Where Identity API Platforms diverge from the COTS solutions offered in the past, is defined by the use cases of Identity API Platforms. Identity API Platform use cases focus on vendors that allow its customers to build their identity backend for defined services through APIs whether on-premises, the cloud or in hybrid environments. Other Identity API Platform use cases are targeted at organizations that due to the complexity of internal processes and other operational reasons are looking to build their own C/IAM platform, automate or enhance existing IAM capabilities. Also, where traditional turn-key COTS are primarily UI driven, Identity API Platforms use cases require that the solution is developer ready and can provide anywhere in the range from COTS API Toolkits such as widgets and SDKs that facilitate rapid development to a pure API platform.

Since Identity API Platforms are developer-centric, useful online developer portals with proper API documentation and code examples, are all needed to build a good developer ecosystem.

This leadership compass focuses on those Identity API Platforms that provide a higher percentage of their IAM, CIAM, and IDaaS capabilities via API. All use cases (IAM, CIAM, IDaaS) should support APIs for core functionality at a minimum. Support for more advanced and modern technologies that support risk/context-based authentication and authorization, biometrics, mobile support, and graph-based APIs, to name a few are evaluated in the ratings as well.

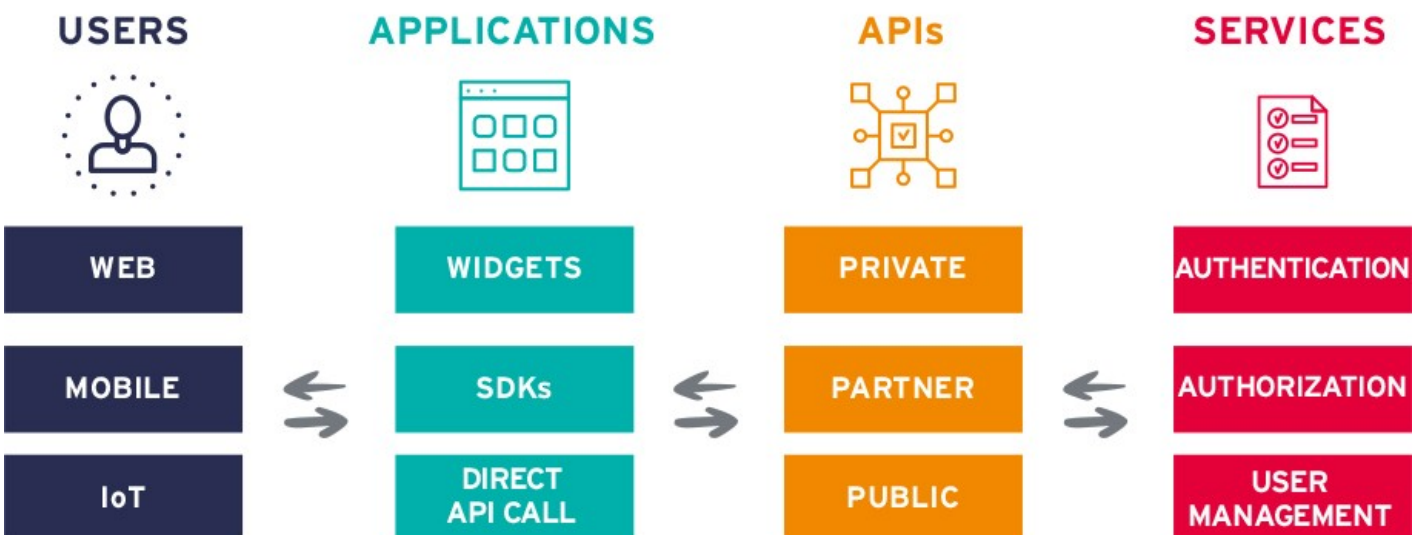


Figure 2: High level architectural overview of IAM API usage

Picking solutions always require a thorough analysis of customer requirements and a comparison with product features. Leadership does not always mean that a product is the best fit for a particular customer and their needs. However, this Leadership Compass will help to identify those vendors that customers should look at more closely.

1.2 Delivery models

Since most of the solutions covered in our rating are designed to offer comprehensive Identity API Platform capabilities regardless of the location of the IT environment, we considered all delivery models in this Leadership Compass, which includes on-premises, private cloud, public cloud, multi-cloud, and hybrid deployment environments.

Although all delivery models are looked at, it is worth considering the pros and cons of each delivery model against the use case for Identity API platforms. For instance, an ideal Identity API Platform that can serve smaller use cases while also integrating e.g., identities of a company across all the digital services should be delivered in such a way that allows setting up instances of the service immediately. Also, it is good to be aware that in most cases public cloud solutions are generally multi-tenant, while some cloud services are actually single-tenant. Other approaches use container-based deployments to provide consistent delivery of a vendor's solution, whether cloud-hosted or on-premises. Ultimately selecting the right Identity API platform delivery model will depend on the customer requirements and their use cases.

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 several specific features. These functional areas, which are reflected in the spider charts for each company in Chapter 5.1 include:

- **Identity & User Mgmt APIs**
  APIs that allow for the management of identities and user account management, including associated directory services and databases.
- **Authentication API**s
  Authentication method support via APIs within the range of username/password to biometrics and anything in between. Also, consideration of SSO and session management availability.
- **Authorization APIs**
  APIs that controls user or administrator permission/access rights to resources such as policy management, RBAC, or dynamic authorization.
- **Audit & Compliance APIs**
  APIs that support monitoring of a user's access to resources, or administrators changes to the system, as well as APIs that provide auditing and forensic capabilities to aid in industry compliance use cases and security incident analysis as examples.
- **Workflow & Orchestration APIs**
  APIs that allow for the automation of workflows such as access requests, user self-registration or user consent, or the orchestration of more than one workflow or activity.
- **API security**
  A solution's ability to secure APIs against hacker attacks and other threats using methods such as encryption, rate limiting, content filtering, and schema validation.
- **DevOps APIs**
  APIs that provide IT environment support options for both developers and the operations team with their tools, automation, and continuous integrations.
- **API Developer Support**
  The vendor's ability to support the developers using the solution's APIs through documentation, tutorials, and tools as well as Knowledge-base, Community support / platform for developer.

In our effort to cover most aspects of Identity API Platforms in this Leadership Compass, we are not covering the products or elements of product functionality that:

- Strictly require UI interaction to use, control or configure their Identity product services
- APIs used only internally by the vendor company or product
- APIs used for managing specific partners only and their accounts (e.g. billing)
- Have a limited set of APIs that fail to meet the minimum required IAM functionality

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 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 Identity API market segment

The Overall Leadership rating is a combined view of the three Leadership categories, i.e., 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 benefit, e.g. from a strong market presence will slightly drop in other areas such as innovation, while others show their strength, e.g. 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 gain a comprehensive understanding of the players in that market segment.

In the Overall Leadership rating chart, we see a maturing market that is slightly crowded and is represented by the thirteen vendors we chose to represent in our Leadership Compass rating.

In the market for Identity API Platforms, there are six companies in the Overall Leaders segment. These include ForgeRock, Ping Identity, WSO2 as more established players with strong offerings and customer base, complemented by a mix of established and younger companies, Okta, Auth0, and Akamai which have held its market share and make up the lower portion of the Leaders segment.

The remainder of the vendors falls into the Challenger segment making up more than half of the companies being evaluated, with only one distinct grouping near the top of this section. In the top group are more established vendors with good offerings and the potential of becoming overall leaders in the future. Pirean stands out towards the center of the Challenger segment with room to grow their offering. The remaining three vendors are grouped at the bottom of the Challenger segment, which includes Ubisecure, Optimal IDM, with ViewDS trailing in the overall rating.

None of the companies evaluated placed in the Followers section.

Leadership does not automatically mean that these 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):

- Akamai
- Auth0

- ForgeRock
- Okta
- Ping Identity
- 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.

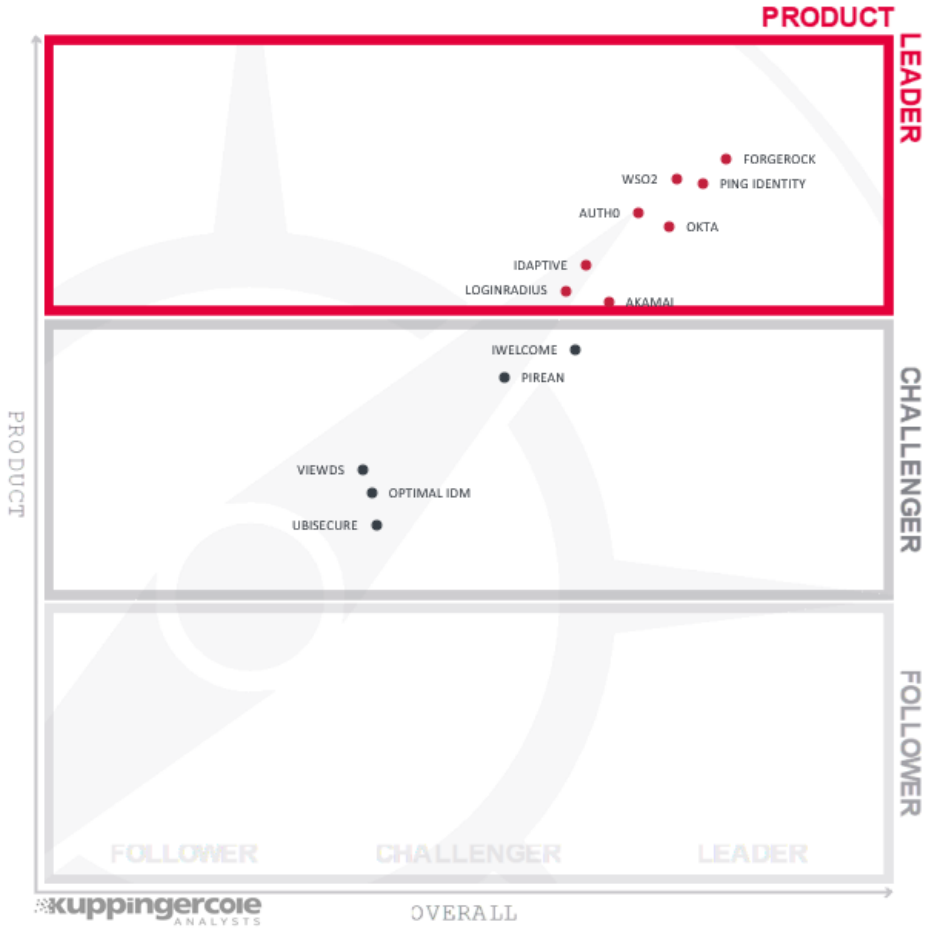


Figure 4: Product Leaders in the Identity API Platform market segment

Product Leadership is the view in which we focus on the functional strength and completeness of the Identity API Platform product. Since the Identity API Platform market is maturing, we find no followers, some challengers, and a greater number of vendors qualifying for the Leaders segment.

As vendors offer a wide variety of Identity API Platform capabilities and differ in how well they support these capabilities, it is important for organizations to perform a thorough analysis of their Identity API Platform requirements to align their priorities while evaluating an Identity API Platform solution.

In the Product Leadership, there are three distinct groupings. In the top group, ForgeRock is leading, followed by WSO2, and Ping Identity, all with both strong product and overall ratings. In a center grouping, both Auth0 and Okta also having product strengths that might fit well for the specific Identity API Platform requirements of customers. The third group appears in the lower section of this segment, which includes the vendors Idaptive, LoginRadius, and Akamai near the bottom border. All Product Leaders have their specific strengths, but with varying degrees of feature strengths. In the Challenger section, there are also some clear groupings. Two vendors, iWelcome and Pirean, appear near the upper border of the Challenger section and have good product features, but may lack some product features we expect to see to put them in a leadership position. In a second grouping towards the mid to lower section of the Challenger section, we see ViewDS, Optimal IdM, and Ubisecure with a stronger product than overall rating. All five products in the Challenger section are found to be good products, but didn't make it into the Leaders sections because of maturity or missing some of the features found amongst the leaders.

Product Leaders (in alphabetical order):

- Akamai
- Auth0
- ForgeRock
- Idaptive
- LoginRadius

- Okta
- Ping Identity
- 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.

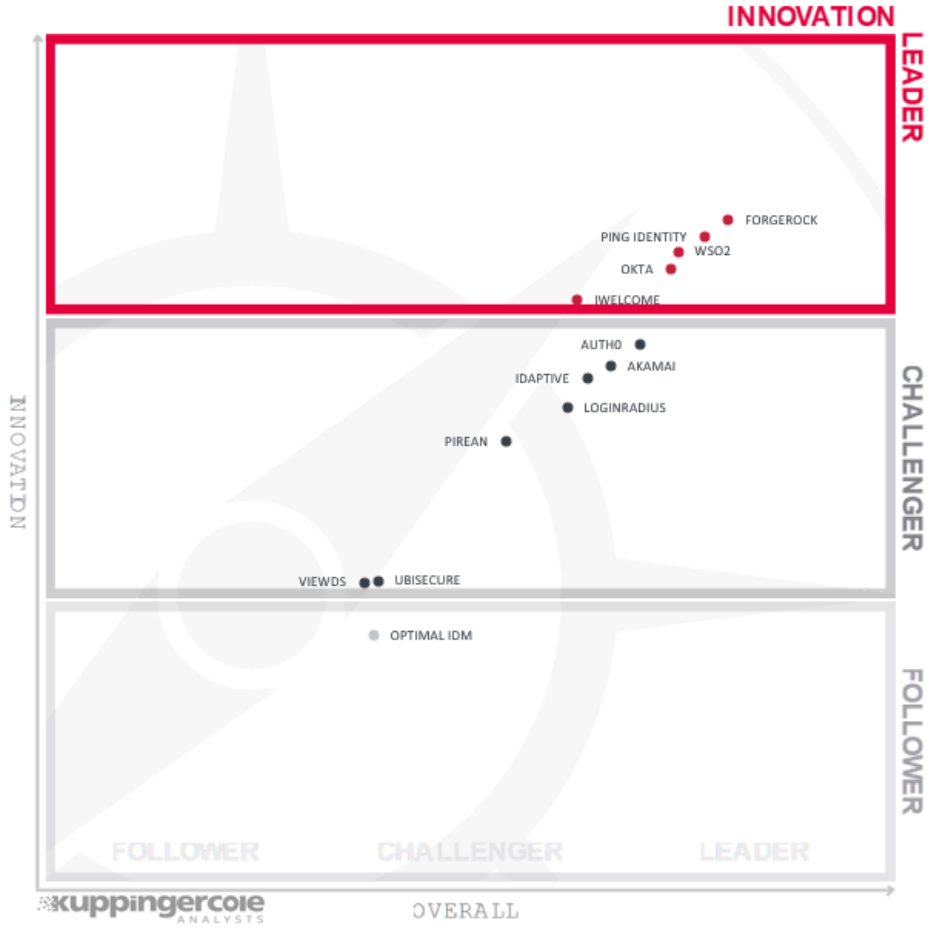


Figure 5: Innovation Leaders in the Identity API market segment

We have rated only a few vendors as Innovation Leaders in the Identity API Platform market, which has driven this market forward through the innovation of their products. The leaders are ForgeRock, Ping Identity, WSO2, Okta, and iWelcome.

The graphics need to be carefully read when looking at the Innovation capabilities, given that the x-axis indicates the Overall Leadership while the y-axis stands for Innovation. Therefore, while some vendors are closer to the upper right edge, others being a little more left score slightly higher regarding their innovativeness.

In the Challenger section of Innovation Leadership evaluation, we find the majority of vendors with Auth0, Akamai, Idaptive and LoginRadius grouped near the upper border with Pirean in the mid-section and with Ubisecure and ViewDS near the bottom border. Given the relative maturity of Identity API Platform solutions, the amount of innovation we see is somewhat limited. The vendors, however, still continue to differentiate by innovating in niche areas.

Only one vendor is included in the Follower section, which is Optimal IdM. Optimal IdM presents a good product but falls behind in innovative features when compared to the other vendors.

Innovation Leaders (in alphabetical order):

- ForgeRock
- iWelcome
- Ping Identity
- Okta
- 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 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 successful execution of marketing strategy.

Figure 6: Market Leaders in the Identity API Platform market segment

The Market Leadership evaluation, the top three are ForgeRock, Ping Identity, and Okta primarily for their more extensive global customer base, partner, and support network. The bottom section of market leadership is comprised of Akamai, Auth0 and WSO2.

In the Challenger section, we find most of the remaining vendors having good products but may be lacking in one or more areas of their customer base, partner, or support network compared to the market leaders.

The only vendor that appears in the Follower section is ViewDS, which is still a relatively small vendor and partner ecosystem.

Market Leaders (in alphabetical order):

- Akamai
- Auth0
- ForgeRock
- Okta
- Ping Identity
- WSO2

3 Correlated View

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.

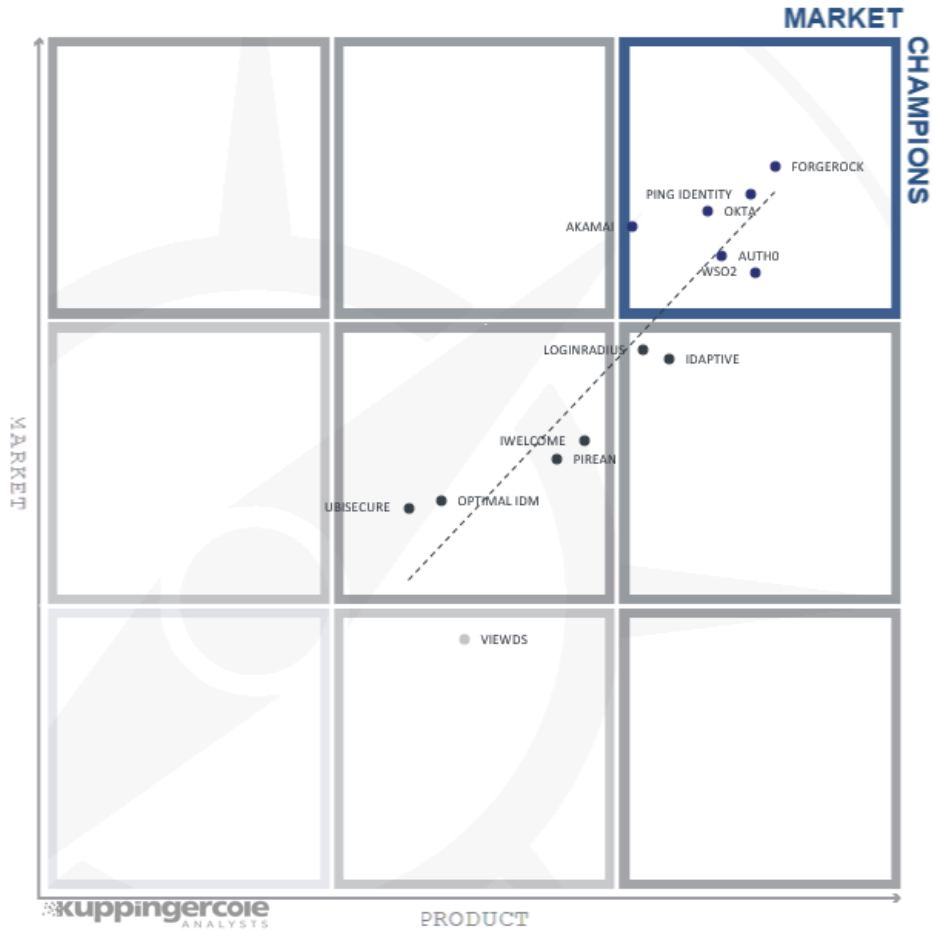


Figure 7: The Market/Product Matrix

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.

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.

In the upper right segment, we find the "Market Champions", which are leading in both the product and market ratings. This segment contains ForgeRock at the top followed by Ping Identity, and Okta. Others include Akamai, Auth0, and WSO2.

In the middle right-hand box, we see the vendors that deliver strong product capabilities for Identity APIs but are not yet considered Market Champions. All these vendors have a strong potential for improving their market position due to the stronger product capabilities that they are already delivering. These vendors are, from top to bottom, LoginRadius and Idaptive.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not Market Leaders as of yet. They also have average market success as compared to market champions. These vendors include iWelcome, Pirean, Optimal IdM, and Ubisecure.

Finally, in the lower middle section of the chart we fine ViewDS also with good but not leading-edge capabilities, and with a lower market presence.

3.2 The Product/Innovation Matrix

The second 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 few exceptions. This distribution and correlation are typical for most markets with a significant number of established vendors plus some smaller vendors.

Figure 8: The Product/Innovation Matrix.

Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

Here, we see a good correlation between the product and innovation rating, with most vendors placed close to the dotted line indicating a healthy mix of product and innovation leadership in the market.

Looking at the Technology Leaders segment, we find the leading vendors towards the left of center, scattered throughout the box. The top-notch vendors are ForgeRock, WSO2, Ping Identity, and Okta with vendors placing closer to the axis depicting a better balance of product features and innovation.

The top middle box indicates vendors that provide good product features while behind the Technology Leaders in innovation. Here we find (in alphabetical order), Akamai, Auth0, Idaptive, and LoginRadius.

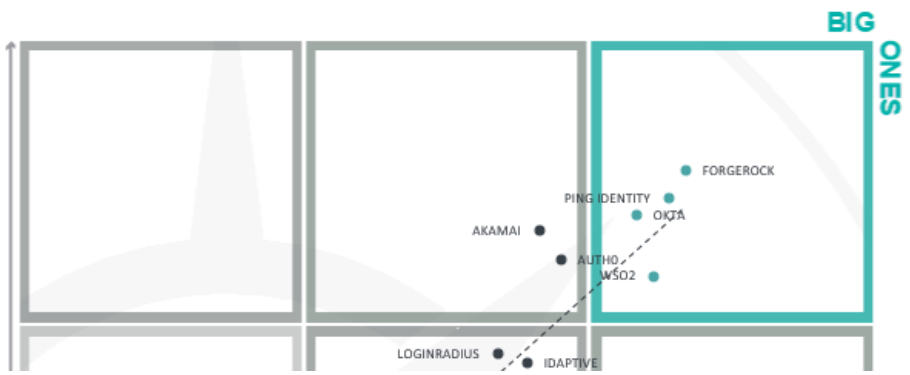
In the center of the chart, we see Pirean having more product features and more innovation than ViewDS and Ubisecure which appear further to the left of the center box.

iWelcome appears just inside the middle right box indicating more strength in innovation than the vendors in boxes to the left of it.

Optimal IdM shows up in the middle left box, pointing to less innovation while maintaining good product features.

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 on their market position but often face risks of failure, especially in the case of vendors with a confused marketing strategy.



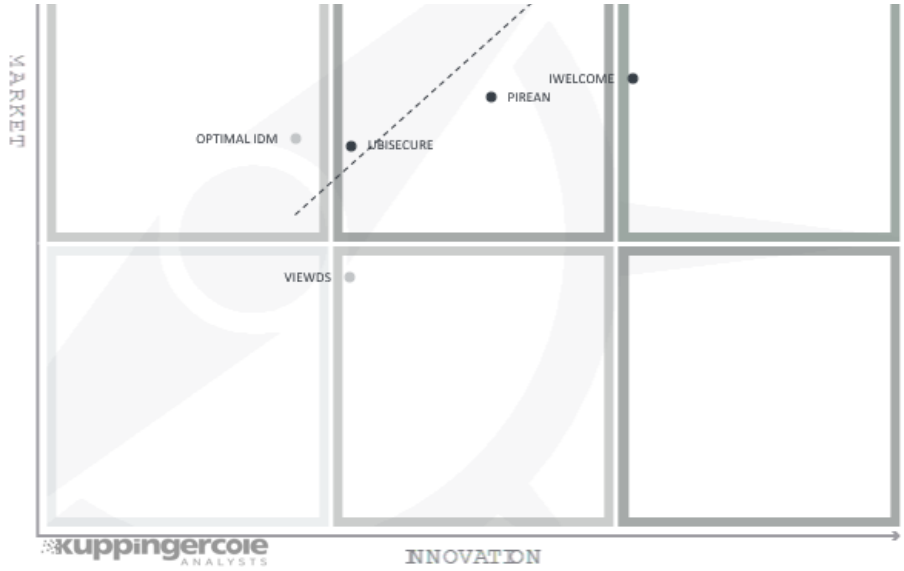


Figure 9: The Innovation/Market Matrix

Vendors 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.

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

In the upper right-hand corner box, we find the "Big Ones" in Identity API Platform market which are ForgeRock, Ping Identity, Okta and WSO2.

At the top and to the left of the Big Ones, in order of highest to lowest market, are Akamai, and Auth0.

The segment in the middle of the chart contains the vendors rated as Challengers both for Market and Innovation Leadership, with (in alphabetical order), Idaptive, LoginRadius, Pirean, and Ubisecure.

Again, we find iWelcome just inside the middle right box showing its strength in innovation.

Optimal IdM appears in the middle left box in this segment, with ViewDS appearing in the corner of the lower middle box indicating slightly more innovation, but having a lower market presence.

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 Identity Provisioning. 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.

4.1 Ratings at a glance

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	Integration	Interoperability	Usability
Akamai API Suite	strongly positive	positive	positive	positive	strongly positive
Auth0 API Suite	strongly positive	strongly positive	positive	positive	strongly positive
ForgeRock Identity Platform	strongly positive	strongly positive	strongly positive	strongly positive	strongly positive
Idaptive API Suite	strongly positive	positive	positive	positive	strongly positive
iWelcome CIAM	strongly positive	positive	positive	positive	positive
LoginRadius CIAM Platform	strongly positive	positive	positive	strongly positive	strongly positive
Okta API Access Management	strongly positive	strongly positive	positive	positive	strongly positive
Optimal IdM Suite	positive	neutral	neutral	neutral	neutral
Ping Identity Platform	strongly positive	strongly positive	strongly positive	positive	strongly positive
Pirean Access: One	positive	positive	positive	positive	positive
Ubisecure Identity Server	positive	neutral	neutral	neutral	neutral
ViewDS Suite	positive	neutral	positive	neutral	neutral
WSO2 Identity Server	strongly positive	strongly positive	positive	strongly positive	strongly positive

Legend: critical weak neutral positive strongly positive

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
Akamai	●	●	●	●
Auth0	●	●	●	●
ForgeRock	●	●	●	●
Idaptive	●	●	●	●
iWelcome	●	●	●	●
LoginRadius	●	●	●	●
Okta	●	●	●	●
Optimal IdM	●	●	●	●
Ping Identity	●	●	●	●
Pirean	●	●	●	●
Ubisecure	●	●	●	●
ViewDS	●	●	●	●
WSO2	●	●	●	●

Legend: ● critical ● weak ● neutral ● positive ● strongly positive

Table 2 requires some additional explanation regarding the "critical" rating.

In Innovativeness, this rating is applied if vendors provide none or very few of the more advanced features we have been looking for in that analysis, like support for multi-tenancy, shopping cart approaches for requesting access, and others.

These ratings are applied for Market Position in the case of vendors which have a very limited visibility outside of regional markets like France or Germany or even within these markets. Usually, the number of existing customers is also limited in these cases.

In Financial Strength, this rating applies in case of a lack of information about financial strength or for vendors with a very limited customer base but is also based on some other criteria. This doesn't imply that the vendor is in a critical financial situation; however, the potential for massive investments for quick growth appears to be limited. On the other hand, it's also possible that vendors with better ratings might fail and disappear from the market.

Finally, a critical rating regarding Ecosystem applies to vendors which have no or a very limited ecosystem with respect to numbers and regional presence. That might be company policy, to protect their own consulting and system integration business. However, our strong belief is that growth and successful market entry of companies into a market segment relies on strong partnerships.

5 Product/Service 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.

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 LC Identity API, we look at the following eight areas:

- **Identity & User Mgmt APIs**
  APIs that allow for the management of identities and user account management, including associated directory services and databases.
- **Authentication APIs**
  Authentication method support via APIs within the range of username/password to biometrics and anything in between. Also, consideration of SSO and session management availability.
- **Authorization APIs**
  APIs that controls user or administrator permission/access rights to resources such as policy management, RBAC, or dynamic authorization.
- **Audit & Compliance APIs**
  APIs that support monitoring of a user's access to resources, or administrators changes to the system, as well as APIs that provide auditing and forensic capabilities to aid in compliance and security incident analysis as examples.
- **Workflow & Orchestration APIs**
  APIs that allow for the automation of workflows such as access requests, user self-registration or user consent, or the orchestration of more than one workflow or activity.
- **API security**
  A solution's ability to secure APIs against hacker attacks and other threats using methods such as encryption, rate limiting, content filtering, and schema validation.
- **DevOps APIs**
  APIs that provide IT environment support options for both developers and the operations team with their tools, automation, and continuous integrations.
- **API Developer Support**
  The vendor's ability to support developers using the solution's APIs through documentation, tutorials, and tools as well as Knowledge-base, Community support / platform for developer.

The 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. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Identity API Platforms.

5.1 Akamai

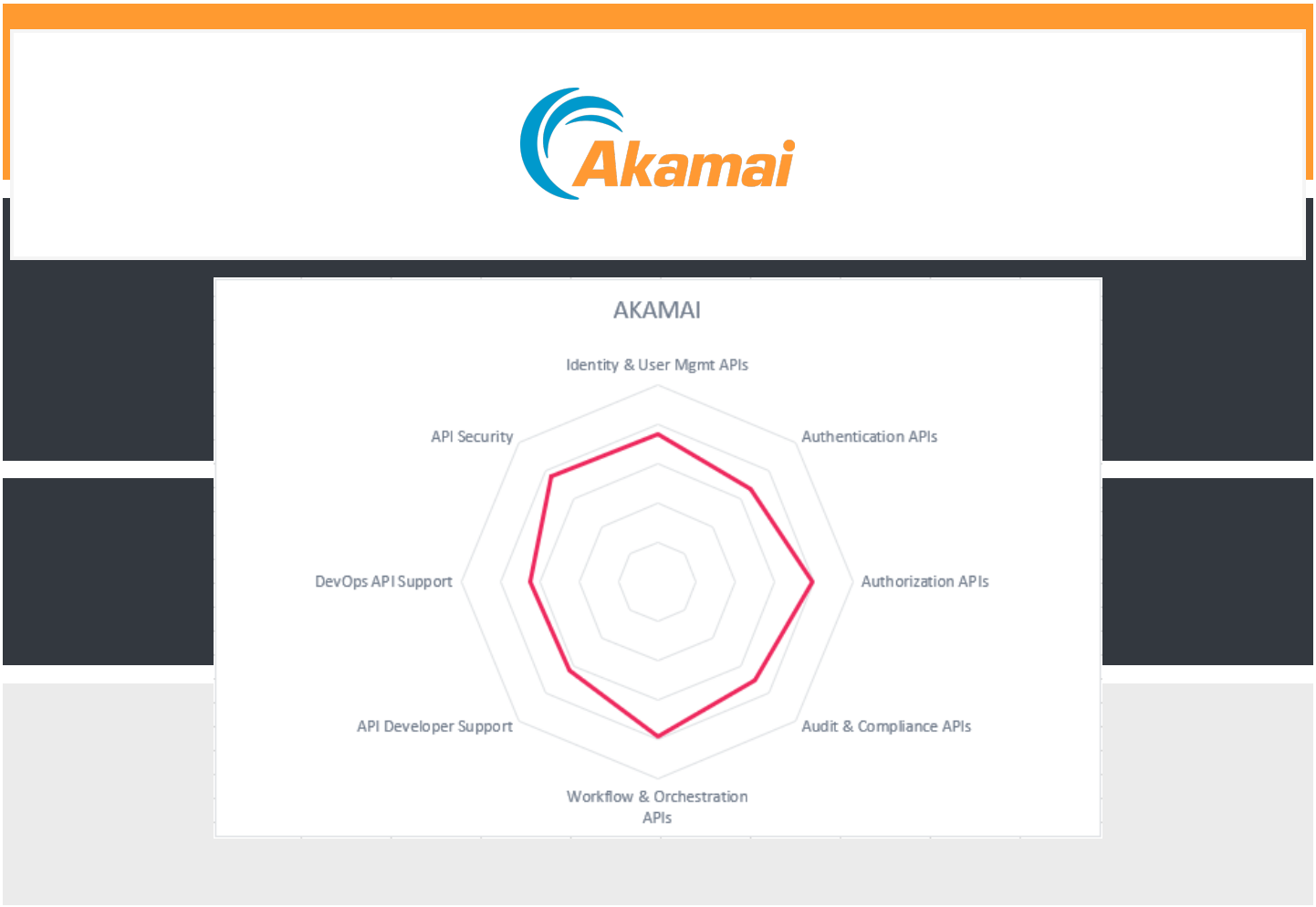
Akamai, recently acquired Janrain, which is private equity backed CIAM SaaS provider, based in Portland, Oregon. The company was launched in 2002 to provide user management and login capabilities for the social media market. Akamai Identity Cloud focuses on cloud-based CIAM and IDaaS APIs and gives full multi-tenancy for all components. Akamai only supports a public cloud product delivery model.

Akamai Identity and User Management capabilities provide identity federation APIs that support the most used standards such as SAML 2.0, OIDC, OAuth 2.0, JWT. Akamai Identity Cloud includes a directory designed to store multiple identity types with the ability to customize the data model. Integrations with other directory services such as Microsoft AD and Azure AD are also supported. Bulk provisioning and synchronization from LDAP or support for provisioning to/from other cloud services using cloud service APIs are provided, although SCIM bulk provisioning is not.

Akamai APIs are available for the most common authentication forms and standards, including mobile biometrics. Support for FIDO UAF and U2F is not given, although it's on their near-term roadmap. Federated authentication for social networks is well supported. APIs are available for RBAC and fine-grained access controls down to the data field level for both data and applications. RESTful APIs are also available to a risk analysis engine for risk-based access controls using the Akamai Advanced Policy Manager or integration with IBM's Trusteer.

Akamai only provides the REST API protocol and Webhooks although they do support both JSON and CSV, but not XML data formats. No API protocol conversions are supported. APIs for integration to other IAM, CIAM, or IDaaS platforms are available as well as integrations to CRM or other SaaS systems out-of-the-box. Akamai give online documentation for developers and widgets for registration, login, profile management, account recovery, change password and email verification, although only iOS and Android SDKs are given rather than the more popular programming languages. Akamai shows strength with workflow & orchestration APIs and API security.

Akamai has a strong presence in North America, good representation in EMEA and some presence in the APAC regions with many large enterprise clients around the world. Overall, Akamai provides good support to many areas of identity APIs and should be considered for companies looking a cloud-based CIAM solution.



5.2 Auth0

Auth0 is a rapidly growing company located in Bellevue WA (U.S.), London, Buenos Aires, Sydney and Tokyo, that operates a cloud-based identity platform for developers. Since being founded in 2013, they have been pioneering API-driven identity services. Auth0 can support a range of IAM use cases including CIAM, B2B, and B2E. The company's deployment models are cloud-based, including public, private and managed private cloud offering.

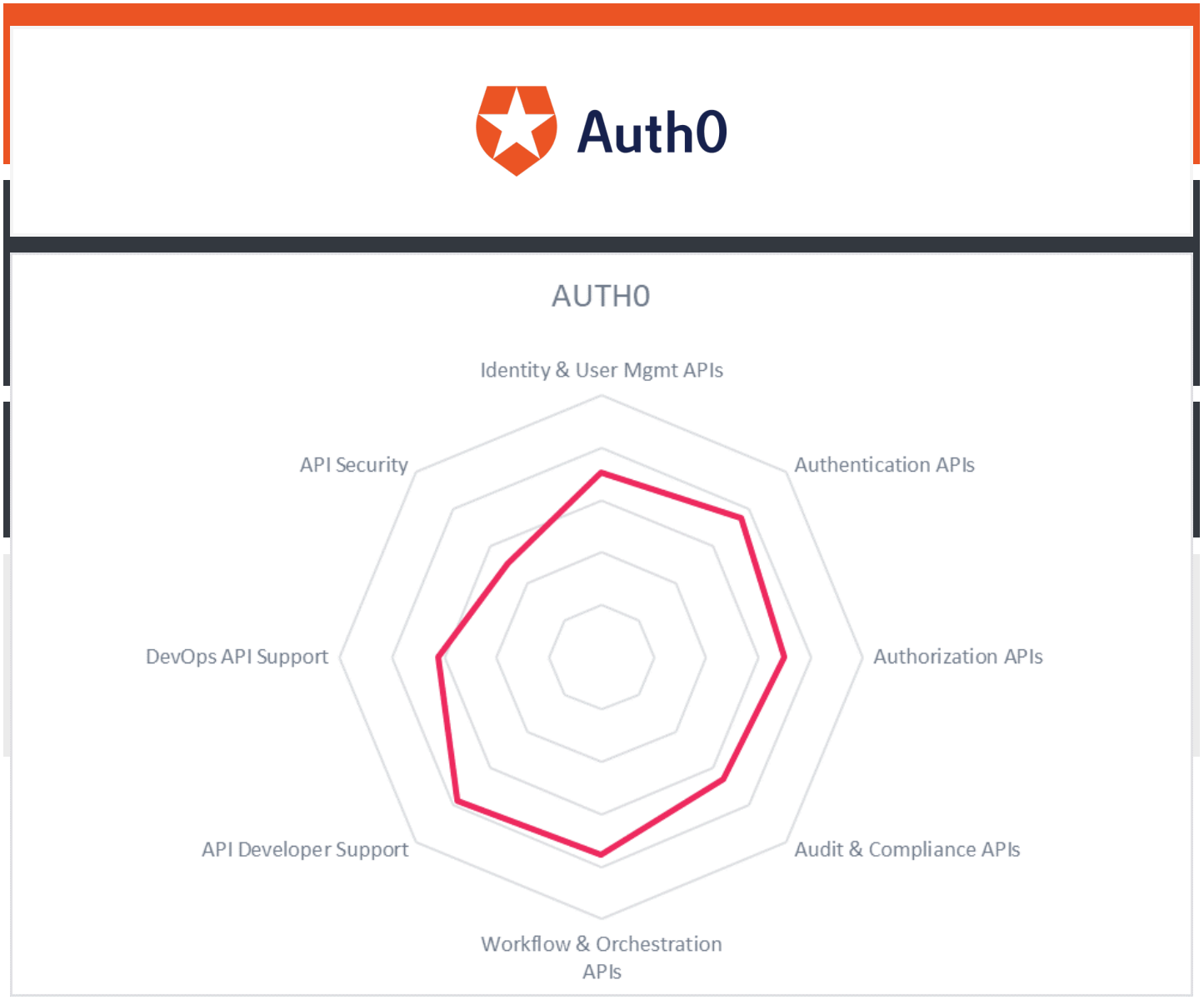
Auth0's APIs are primarily REST/JSON. Uniquely, Auth0 provides a RESTful interface to almost their entire management framework using their Management APIs, which gives customers the ability to manage aspects of their Auth0 account.

By default, Auth0 stores the users' credentials in a database, although customers can use their own user repository. Auth0 supports Microsoft Azure AD out-of-the-box as well as the ability to authenticate to MS AD, LDAP, and Integrated Windows Authentication (Kerberos). Auth0 can authenticate users with any identity provider using APIs. Identity Provider connections are provided out-of-the-box for identity federation, including Social, Enterprise, Database and Password-less connections. Auth0 supports OIDC, OAuth, SAML, and WS-Federation. Their federated identity connections provide their SSO capability that

allows users to authenticate. Only provisioning to/from other Cloud services using specific Cloud service APIs, such as Azure AD, is provided. Authentication APIs are well supported with the most popular forms and standards with some exceptions such as FIDO UAF & U2F. Auth0 also supports an extensive range of social network logins for federation authentication.

The Auth0 platform has a built-in tool to detect anomalies to prevent attacks as well as the ability to use rules to extend the built-in tool capabilities. Auth0 also provides brute force protection and breached password detection. One of Auth0's greatest strength is its developer tools, online support, and overall ecosystem.

The majority of Auth0 customers are focused in North America with an expanding presence in both the EMEA and APAC regions. A good worldwide network of system integrator partners is also available to customers. With Auth0's focus on good developer support and ecosystem to quickly build identity services, Auth0 shows as a leader in the Overall, Product, and Market Leadership categories.



5.3 ForgeRock

ForgeRock is a leader in the IAM space, providing a single integrated suite based on their Identity Platform, which consists of several software products. The components of that platform give broad support for Identity APIs. The ForgeRock Identity Platform focuses on IAM and CIAM use cases supporting on-premises, cloud, and hybrid delivery models.

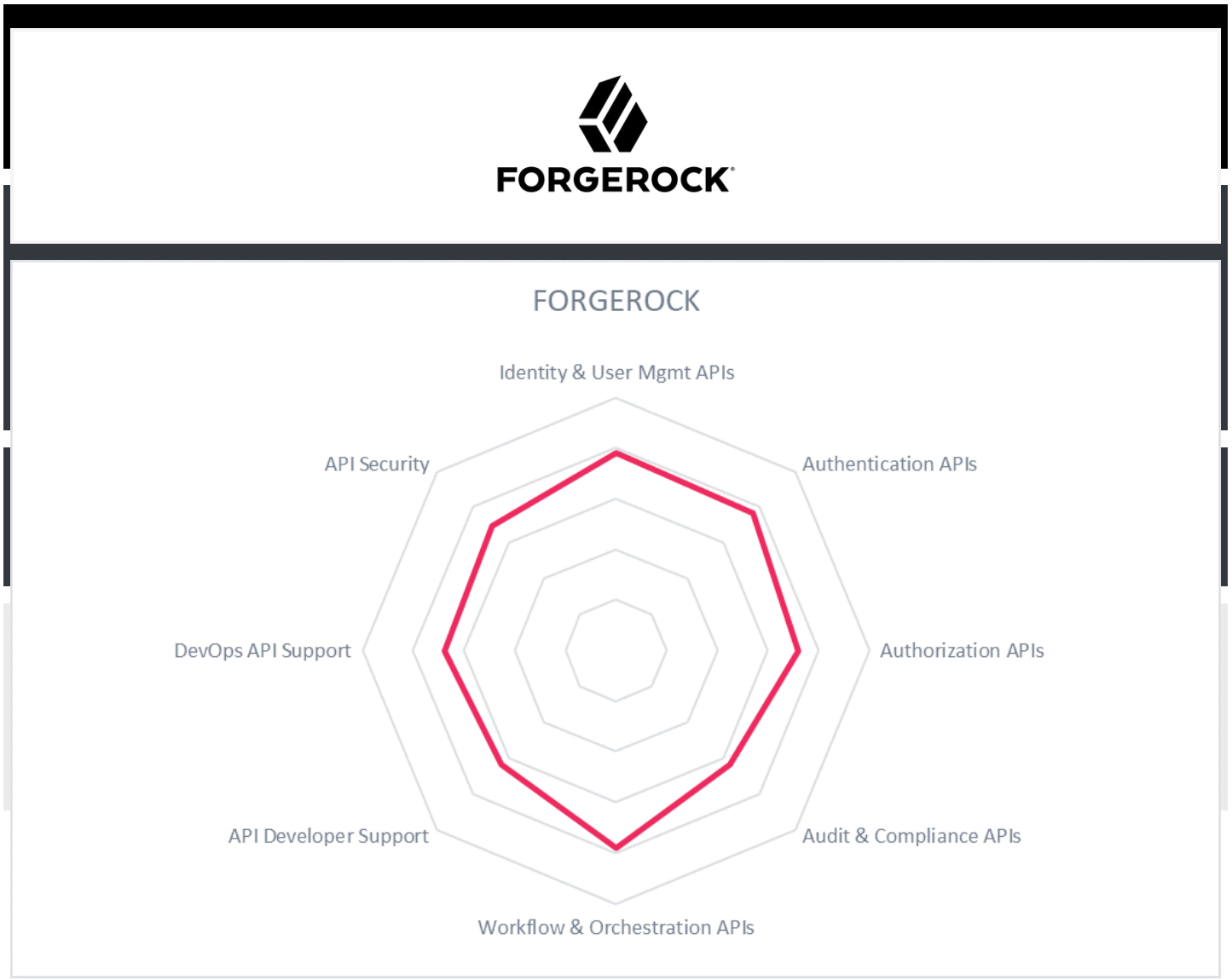
ForgeRock Identity Platform makes available the most popular API protocols and data formats. They give strong support for identity and user management APIs. REST APIs can be used to perform CRUD operations on user identities and provides good interoperability with directory service. ForgeRock identity federation APIs support all standards evaluated, including support for UMA. Bulk provisioning via LDAP, SCIM, or support for provisioning to/from other cloud services using cloud service APIs is fully supported.

The Identity Platform provides full authentication APIs evaluated in this report, including mobile and biometrics. Authorization APIs are provided for both RBAC and fine-grained access controls. Any attributes available on the user's profile are supported in policies for defining the fine-grain access control. A risk analysis engine is available via API but requires a 3rd party integration.

ForgeRock provides good support for workflows and orchestration APIs, which includes mobile identity management, Single Sign-Off, user consent, and family management, key activation, and support for application onboarding as some examples. Another area of ForgeRock's strength is IoT support APIs that can associate identities for smart, constrained and edge devices as well as support for the IETF's OAuth2 Device Flow Profile. The ForgeRock Identity Platform gives basic audit and compliance reporting APIs but can be enhanced through 3rd part integrations. ForgeRock provides developer documentation and code

gives basic audit and compliance reporting APIs but can be enhanced through 3rd part integrations. ForgeRock provides developer documentation and code examples, but lacks development widgets and only provides a Java SDK.

ForgeRock supports large companies split evenly between North America & EMEA and has a growing presence and partner ecosystem in the APAC region. ForgeRock provides a well-balanced solution for Identity APIs and continues to be venture-financed, allowing them to invest in product development heavily. This investment shows by their rapidly improving capabilities and is clearly indicated in the Innovation Leadership category. Overall, ForgeRock is amongst the leading-edge vendors in the IAM space and should be considered in product evaluations.



5.4 Idaptive

Founded in 2004 with headquarters in Santa Clara, California, Centrify spun out their IDaaS solution as a new company called Idaptive. Idaptive provides Identity APIs though their Idaptive Application Services and Idaptive Endpoint Services offerings. Their API product covers IAM, CIAM, and IDaaS use cases, but also supports APIs for Privileged Access Management, User Behavior Analytics, Endpoint Mobility Management (EMM) use cases as well. Idaptive's delivery model includes on-premises, cloud, and hybrid environments.

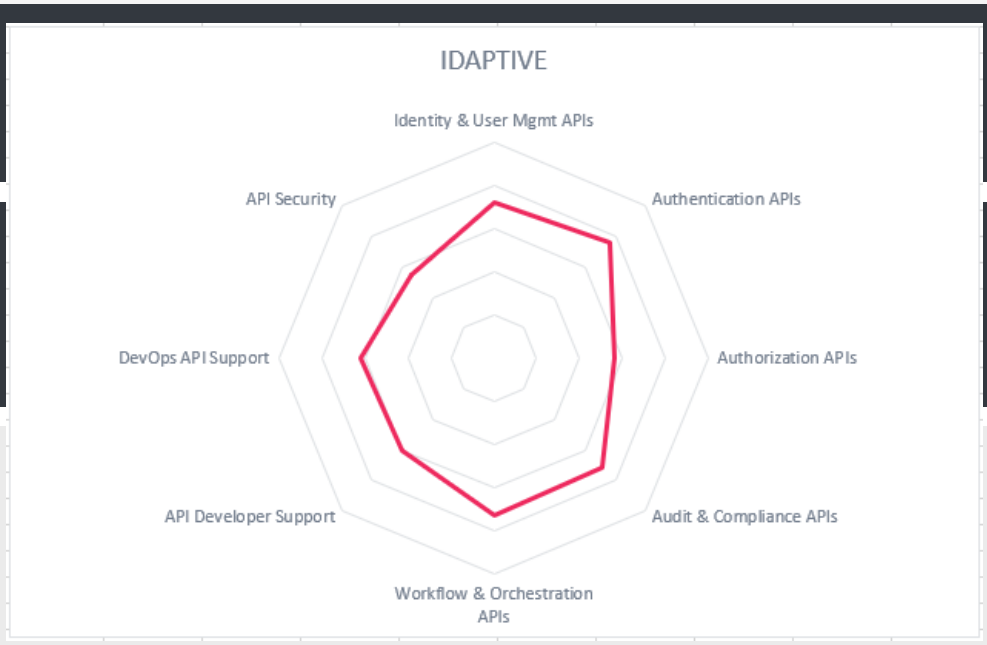
Idaptive only provides the REST API protocol, Webhooks, and WebSockets. API protocols such as RPC, OData, or SOAP are not supported. JSON is the only API supported data format. APIs are available to manage identities with their built-in user service, Idaptive Cloud Directory, that can be used to store users for customer applications. The Cloud User Management API allows calls to create, modify, and delete users, as well as retrieve information about current users within Cloud Directory. Integrations are available for both MS AD and Azure AD. Identity federation APIs support all standards evaluated, although UMA is not supported. Bulk provisioning APIs support LDAP and other cloud services as well as SCIM support.

APIs are available for the most common authentication forms, and standards, including support for mobile applications. API token authentication is not supported, and there is limited APIs for biometric authenticator form factors. Risk-based authentication is supported as well as step-up authentication, although weighting of risk factors within policies is not. The context-based authentication has a range of common context factors that are supported. Both RBAC and dynamic access controls are accessible via APIs. For dynamic fine-grained access controls, Idaptive can leverage user attributes stored in the directory, and runtime device attributes as well as attributes as part of a browser's UserAgent header field. APIs that allow CRUD functionality to access policies are not available.

Idaptive shows good API support for audit and compliance reporting, which includes support for major industry compliance frameworks. Both developer tools and API security are limited in support.

Idaptive has a strong market focus in the U.S. with some presence in the both the EMEA and APAC regions. Idaptive appears in the Product Leadership category as well as showing strength as a challenger as a Market Leader, making them a consideration for U.S. customers.

idaptive



5.5 iWelcome

iWelcome started in 2011, and is headquartered in the Netherlands. iWelcome IDaaS provides for both IDaaS and CIAM solutions with its strongest focus on CIAM & B2B use cases. Their delivery models are cloud-based supporting both public and private environments. iWelcome is offered as a micro-services-based SaaS and therefore run their service as multi-instance rather than multi-tenant, although all instances are segregated with a well-thought-out approach on scaling.

iWelcome only provides the REST API protocol, Webhooks, and WebSockets. API protocols such as RPC, OData, or SOAP are not supported, although data formats such as CSV, JSON, and XML are well supported. Also, iWelcome standardized on OpenAPI Specification (OAS) to allow for API discovery.

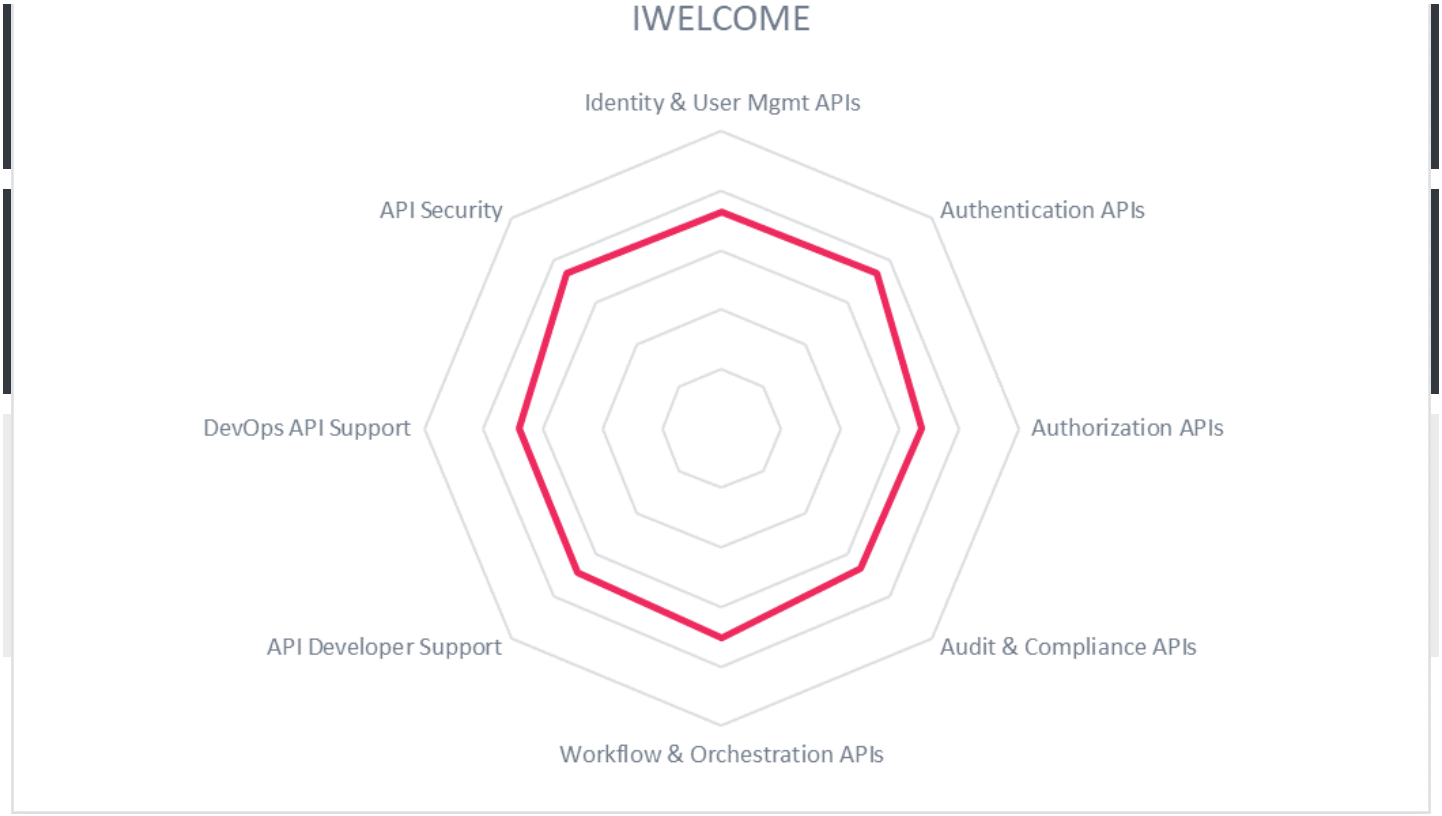
iWelcome's cloud-based identity platform includes an LDAP directory that's used for authentication purposes. A user-profile store is built on MongoDB with a wrapped API layer for customer queries. Only standards for the most modern identity federation APIs are supported, including SAML2, OIDC, OAuth2, JWT, Shibboleth, and UMA. iWelcome integrates with other Identity platforms, and their Consent Lifecycle Management can be integrated via APIs to support GDPR requirements to an existing platform. APIs are given for bulk provisioning from LDAP and support for SCIM. Provisioning to/from cloud services is also available using SCIM for input, REST and SOAP for output.

Most authentication forms and standards are available via API, including mobile biometrics. U2F has been implemented, although iWelcome does not deliver this capability out-of-the-box, but can be integrated when needed. Authorization APIs for risk-based access controls are not supported, but APIs for dynamic access controls are available as well as RBAC support for B2B and delegation scenarios.

Developer widgets are given as well as SDKs for the more popular programming languages. For API security, iWelcome uses their own API Gateway and uses NGNIX as its reverse proxy, which provides protection against the most common types of API attacks.

iWelcome customer base is almost entirely located in the EMEA region. As an EU-based company with their services run from EU-located datacenters and as such has strong support for GDPR. This is attractive for EU-based customers, which should have a look at iWelcome.

welcome



5.6 LoginRadius

Established in 2011, LoginRadius is a VC-backed CIAM vendor based in Vancouver, Canada. The LoginRadius cIAM Platform supports both CIAM and IDaaS use cases with cloud and hybrid delivery models. A solely on-premises delivery option is not available.

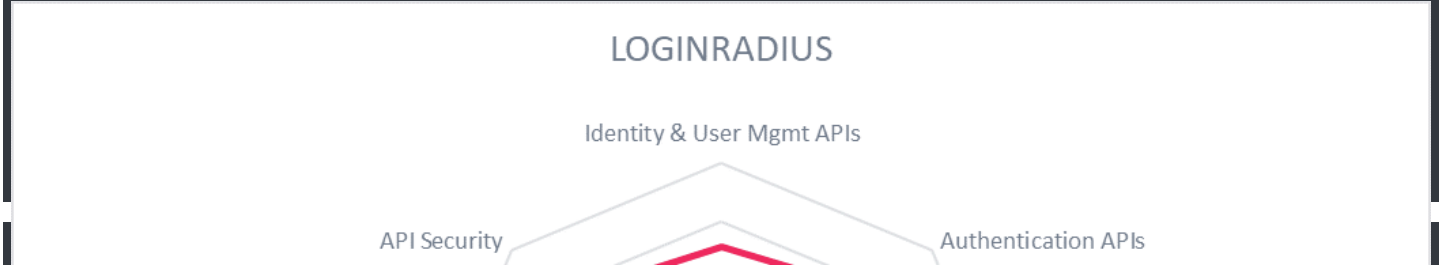
The LoginRadius cIAM Platform only supports the REST API protocol and RestHooks although they do support both JSON and CSV data formats, although support for XML is not given. LoginRadius provides centralization of SSO protocols such as SAML, Multipass, JWT, OIDC, OAuth, etc. The cIAM Platform has its own user directory that can be accessed via JS interfaces, SDK libraries or direct API implementation. Identity federation APIs are available for the most popular standards, although support for UMA is not given. Bulk provisioning APIs are available for LDAP and from other cloud service APIs.

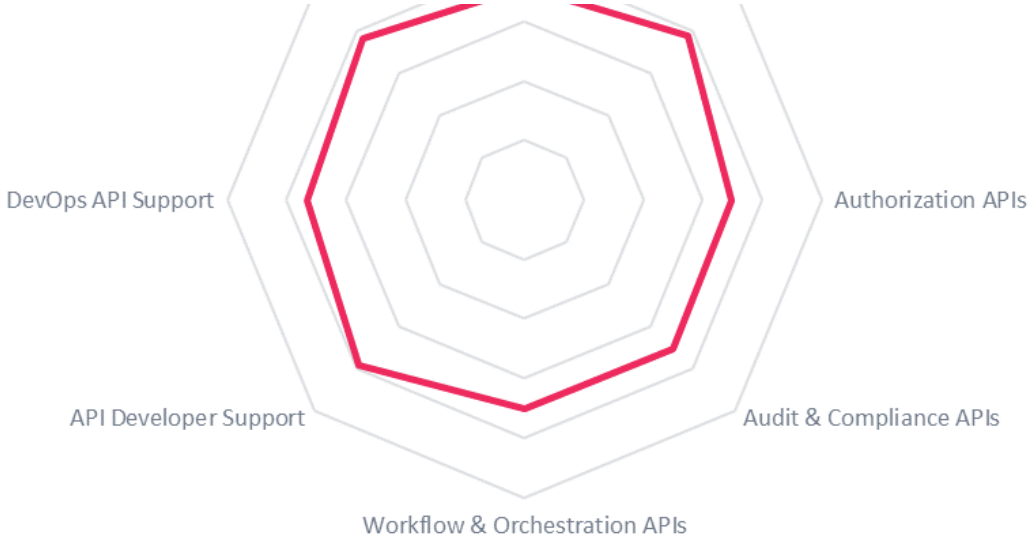
LoginRadius authentication APIs support the most common authentication forms and standards including support for mobile and biometrics, although support for FIDO UAF & U2F is not supported. Federated social authentication APIs extends to a large number of companies. Risk-based authentication using contextual factors (e.g. IP, Location, Event, Device factors) is given as well as support for step-up authentication. APIs are given to control user authorization through RBAC, fine-grained, and risk-based access controls using REST. Access policy CRUD functionality via API is not available.

The cIAM Platform supports auditing through log APIs as well as reports through a Rest API with JSON response or CSV export. Reports are also available for major industry compliance frameworks such as PCI DSS, SOX, and HIPAA. LoginRadius also has API support for IoT devices and supports the IETF's OAuth2 Device Flow Profile. API developer tools are provided by widgets and SDKs for the most popular programming languages. Good built-in security is provided for APIs against the most common attacks.

LoginRadius customers are primarily in North America and some presence in the EMEA region with multiple data centers within the EU for regulatory compliance. LoginRadius appears as a Challenger in the Overall, Innovation, and Market Leadership, but has a stronger standing in the Product Leadership category. In general, LoginRadius provides a well-rounded set of Identity API Platform capabilities.

loginradius





5.7 Okta

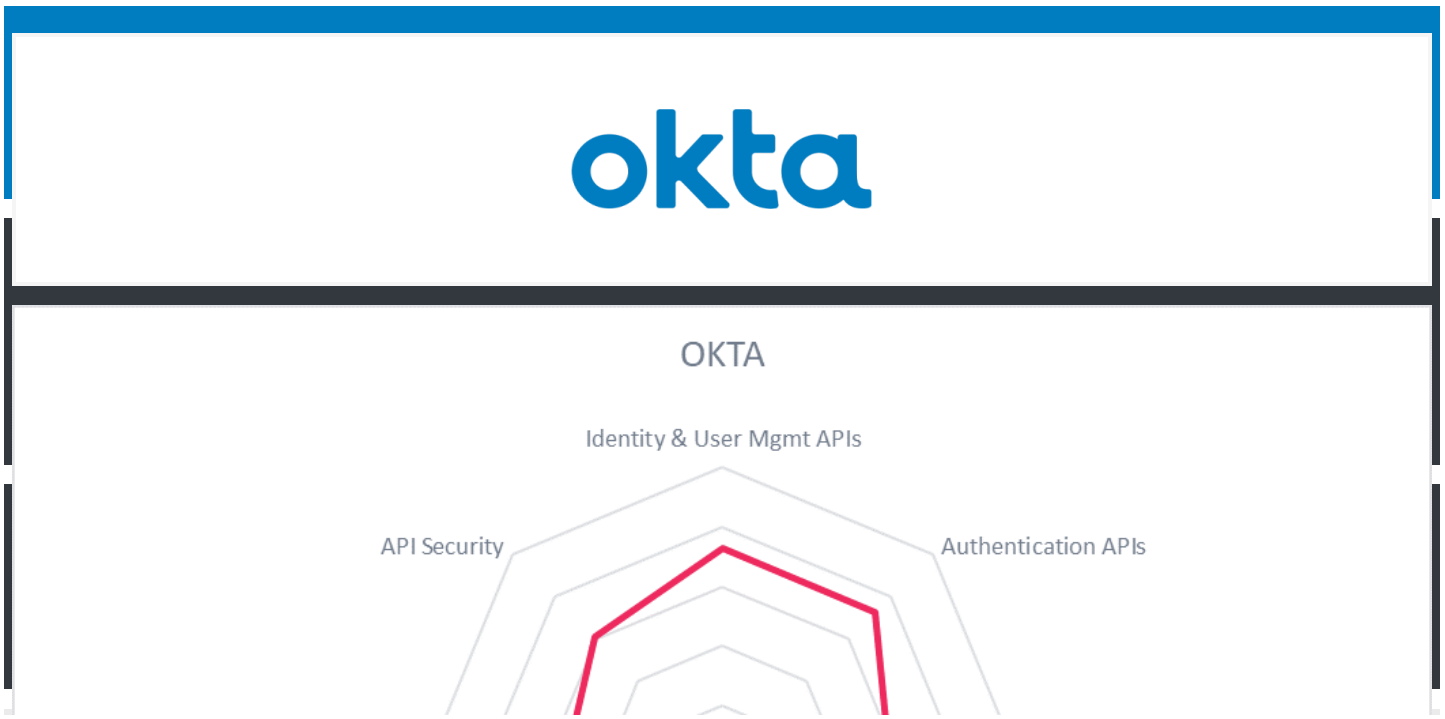
Okta, founded in 2009, is an independent leader in the IDaaS market. Their early focus was on delivering Single Sign-On to cloud services for enterprise users, however, over time they have added capabilities and making them available through an APIs. The Okta API Products and Okta API Access Management offering focus on IAM, CIAM, and IDaaS use cases with a public cloud product delivery model.

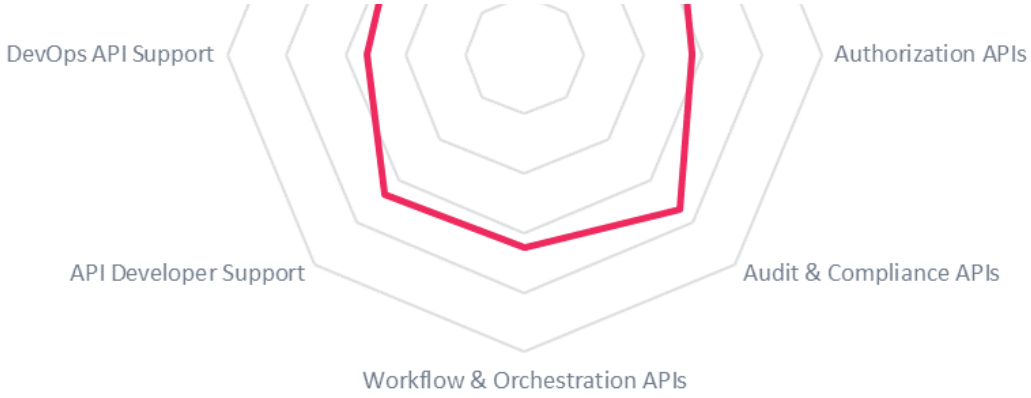
APIs are available to manage identities through CRUD functionality. Okta provides APIs to their Universal Directory as well the ability to integrate with Microsoft AD. In addition, Okta APIs supports the Hypertext Application Language (HAL). Okta identity federation APIs covers the majority of standards, including UMA. Also, there is API product support for integrations to other IAM, CIAM, or IDaaS platforms via SAML and Okta has an extensive Integration Network to a large number of applications.

Authentication APIs supports all major standards and forms of authentication, including biometrics. Authorization APIs are given for RBAC and fine-grained accesses control but requires a third-party integration to support risk-based access control. Okta provides audit and compliance through access to needed data via their APIs for report generation and is entirely GDPR compliant.

Okta provides good SDK support to developers for Java, .Net, Node.js, and Go. Other SDKs available include JavaScript, React, Vue, Angular, IOS Swift, Android Java, React Native, Xamarin. More than 80% of the Okta platform's functionality is available through widgets and provides a sign-in widget which includes out-of-the-box password reset, self-service registration, MFA enrollment, and MFA challenge. Okta has limited API security that includes rate limiting and DoS protection and relies on their security detection and response team to monitor and take action against threats and suspicious activity across its ecosystem.

Headquartered in San Francisco California and an office in San Jose, Okta customers are heavily centered in North America with a smaller portion located outside the U.S., and more recently opened an office in Munich, Germany with a focus on the EMEA region. Okta is a pure cloud offering, is fully multi-tenant and uses their own capacity management and automatic scaling systems, although relies on a third-party data centers (AWS). Okta is a leader in the Overall, Product, Innovation, and Market categories as well as showing good API support in the several areas including providing API developers tools for quick integration through their widgets and SDKs.





5.8 Optimal IdM

Established in 2005, Optimal IdM is a small company headquartered in Lutz, Florida, in the U.S, with other regional offices in the U.S. and Melbourne, Australia. Optimal IdM provides a fully integrated suite, which includes their OptimalCloud, Optimal Federation & Identity Services, and Virtual Identity Server. Their suite supports IAM, CIAM, and IDaaS use cases with an on-premises and public cloud delivery model.

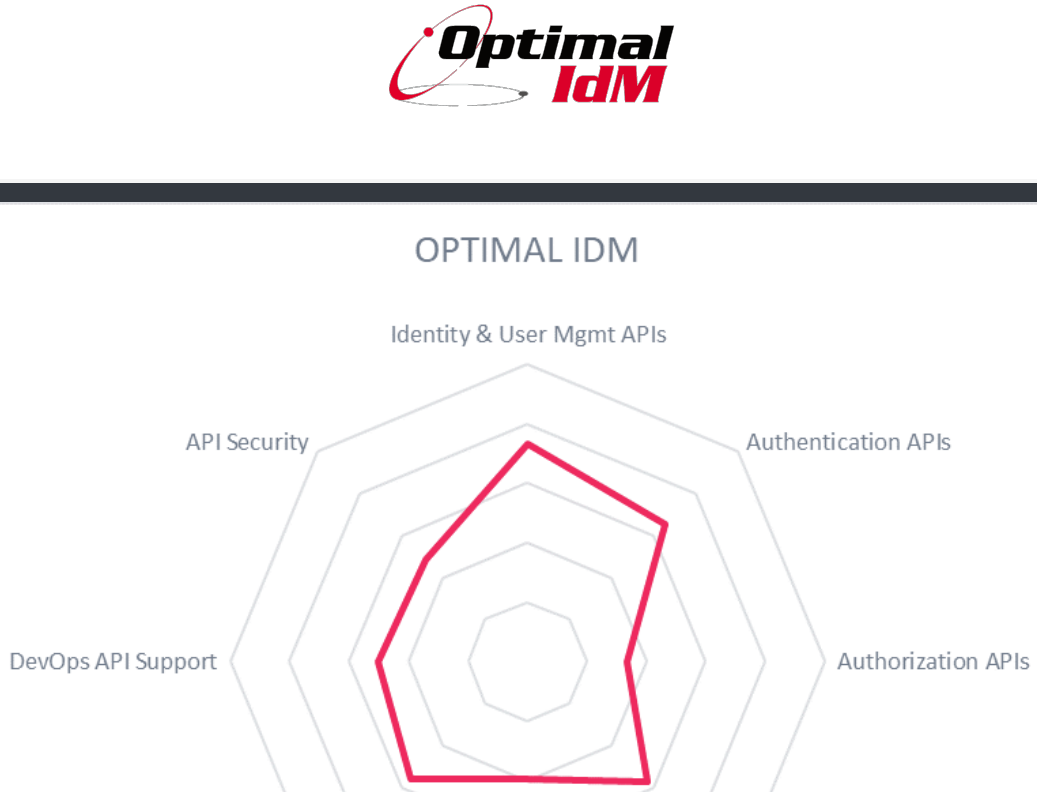
Optimal IdM offering primarily focuses on REST and SOAP API protocols, although their APIs support multiple data formats such as CSV, JSON, and XML. Optimal IdM supports API discovery, but protocol conversion, repackaging legacy, or custom protocols as standard-based APIs is not.

For identity and user management, Optimal IdM is unique in that all identities are managed by a SCIM API, which allows for user and group CRUD functionality. OptimalCloud, which stores users in AD-LDS, give directory support. APIs are also provided for integrations with MS AD and Azure AD. Bulk provisioning is supported out-of-the-box via SCIM from LDAP and to/from cloud services. APIs to support user self-registration are also available.

Optimal IdM gives good support for authentication APIs, which also includes FIDO U2F (FIDO UAF not available), API tokens, mobile, and biometric support. Federation authentication for the most popular social networks is also given. Risk and context-based authentication, as well as support for step-up authentication, is available, although currently, there is no support for SSO APIs. For authorization, Optimal IdM does not provide APIs for risk-based access control as well as missing APIs to perform CRUD functionality on access policies.

For workflow & orchestration APIs, only support for Single Sign-Off is given. Report support is available for major industry compliance frameworks. Optimal IdM provides limited support for developer tools. Only Java and .Net SDKs are given, and widget tools are not available. Some API security support is given for protection against common attack, but missing standard support features such as API rate limiting.

Optimal IdM customers are primarily focused in North America with a presence in the EMEA and APAC regions. Although Optimal IdM shows strength in the area of identity and user management APIs in this leadership compass, there are some gaps in other core Identity API Platform areas. Optimal IdM appears as a challenger in all leadership categories with the exception of the Innovation Leadership category, in which there is room for improvements.



5.9 Ping Identity

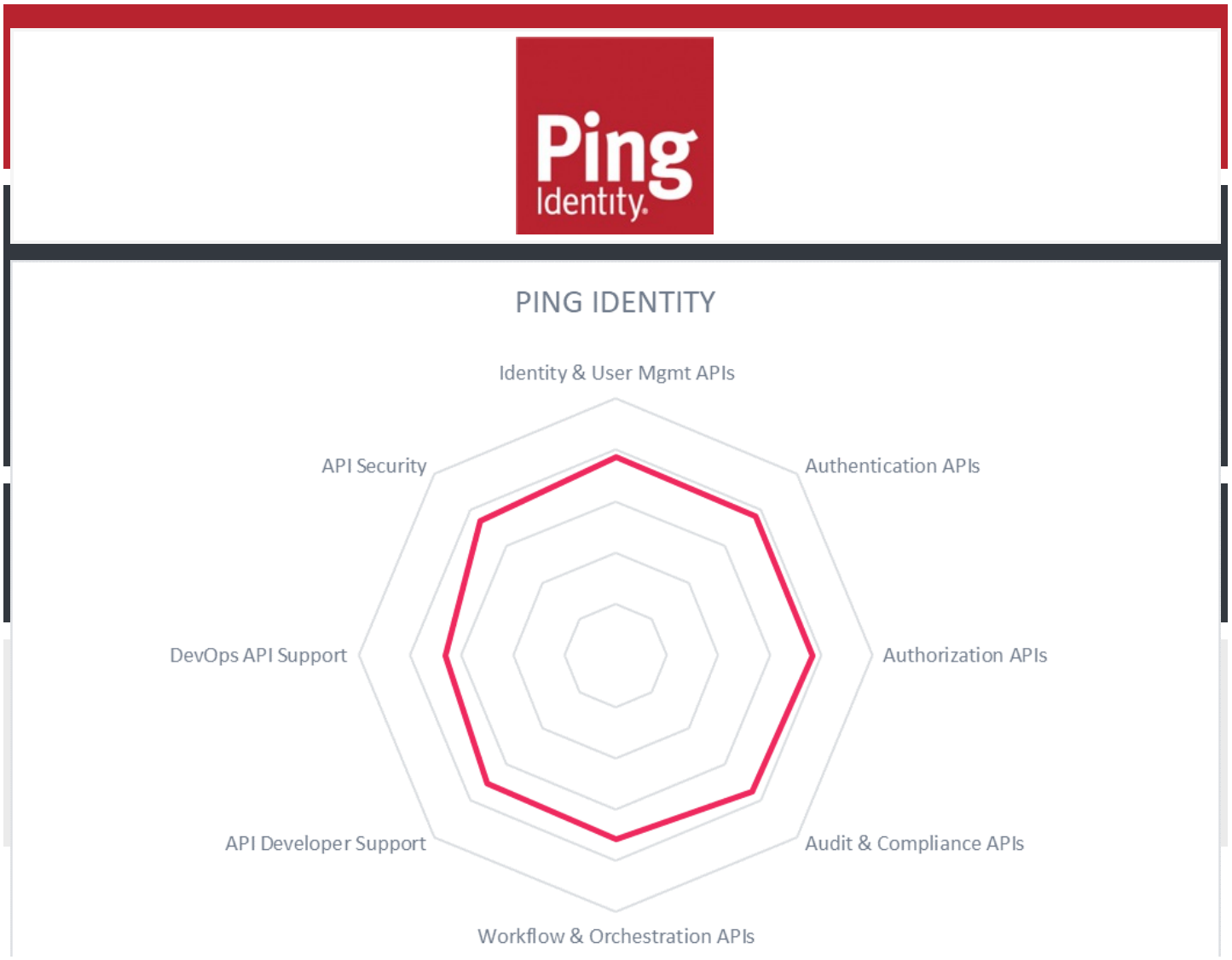
Ping Identity was founded in 2002 with a primary focus in the area of Identity Federation. Since then, Ping Identity has steadily grown to add features to fill out other areas of their Identity Platform, which is made up of a number of software products and cloud services. Their platform focuses on the IAM, CIAM, IDaaS as well as the API security markets. Their product delivery model covers on-premises, cloud, and hybrid environments.

The Ping Identity Platform provides APIs to manage identities which includes CRUD functionality, directory, and other data source access, as well as identity APIs for user management which provides for profile CRUD, password verification, password management, and account lifecycle. Support for most identity federation standards is available via APIs including Shibboleth for web-based Single Sign-on (SSO). Support for UMA is not given. Their APIs support the majority of popular authentication forms and standards. Authorization APIs are given for both RBAC and fine-grained access controls, as well as risk and contextual-based access controls.

APIs to orchestrate workflow are available and include capabilities for user consent and mobile application identity management, as well as workflows for API key activations and application onboarding. Ping provides good API development support through its developer portal with documentation, tools, and examples. They deliver development widgets for a number of administrative and user functions. SDKs are provided to developers for Java, .Net, Node.js, Python and C++.

Although Ping Identity Platform supports the REST API as well as OData and WebSocket protocols, it does lack support for some of the older protocols and standards such as RPC and SOAP. Ping offers a robust API security capability which includes real-time AI-based protection.

Ping Identity has a strong presence in North America and good representation in EMEA and APAC regions with a suitable partner ecosystem. They are established as a leader overall as well as leaders in the product, market, and innovation ratings. As such, the Ping Identity Platform should be included in any shortlist for Identity API Platform solutions to consider.



5.10 Pirean

Pirean is a UK-based software company founded in 2002 with offices in London and Sydney. More recently, Pirean was acquired by Exostar in 2018. The Pirean Access: One platform API focuses on IAM, CIAM, and IDaaS use cases. Delivery models can support on-premises, cloud, and hybrid environments. For the cloud delivery, multi-tenancy is supported within the Access: One framework. All deployments use container images, whether cloud hosted or on-premises.

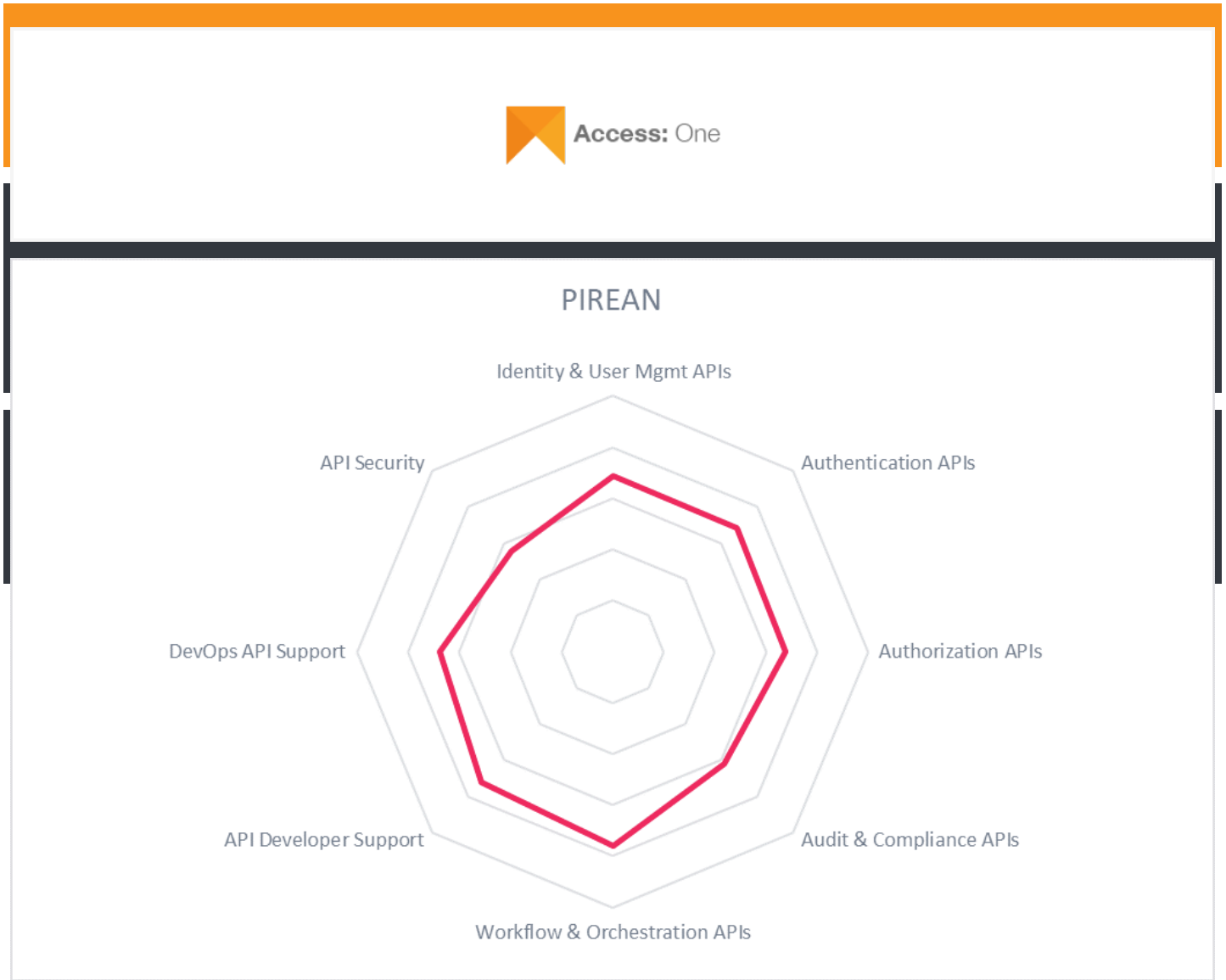
The Pirean Access: One platform APIs supports REST, Webhooks, and WebSockets as well as a Graph API. API data formats include both JSON and XML. API protocol conversion is not supported, but the Pirean web service interface is built on their workflow engine that can address different protocols to support API repackaging and translations.

For identity and user management, Access: One core APIs are available to perform CRUD operations on user identities. By default, the user directory is a cloud-based directory service implementation of an IBM Directory Server product that provides its scalability and resilience. Both integrations with MS AD and Azure AD are supported. APIs that allow for bulk provisioning and synchronization from LDAP or to/from cloud services is given, but SCIM support is not available. Supported identity federation APIs are SAML 2, OIDC, OAuth 2, JWT, and UMA. Integrations to other IAM, CIAM, IDaaS platforms to perform both the provider and consumer role for identities can be accomplished using SAML and OIDC SSO protocols.

Access: One provides all authentication forms and standards evaluated for APIs, including API tokens, biometrics, and mobile support. Federated social network login support is also given. APIs are available RBAC for authorizing users, but APIs for fine-grained or dynamic access is not provided, although authorization rules through their workflow engine can use any attributes in a user record.

Only nominal developer support is given though an Android & iOS (Objective-C & Java) SDKs, although a REST API reference documentation is available online. Pirean API security provides some built-in protection against common attacks but is limited in other areas. Workflow APIs are also available for mobile identity management and support for Single Sign-Off.

Pirean is a relatively small vendor with limited visibility outside of the UK but is expanding to the DACH and APAC regions. Pirean shows some strength in their product offerings and appears as a strong challenger in the Product Leader category.



5.11 Ubisecure

Ubisecure is a Finland based company established in 2002 with a customer base primarily in the Nordic region. Their Identity Server is delivered as a single integrated IAM with a fully integrated database and application server and focuses on IAM and CIAM use cases supporting on-premises, cloud, and hybrid delivery models.

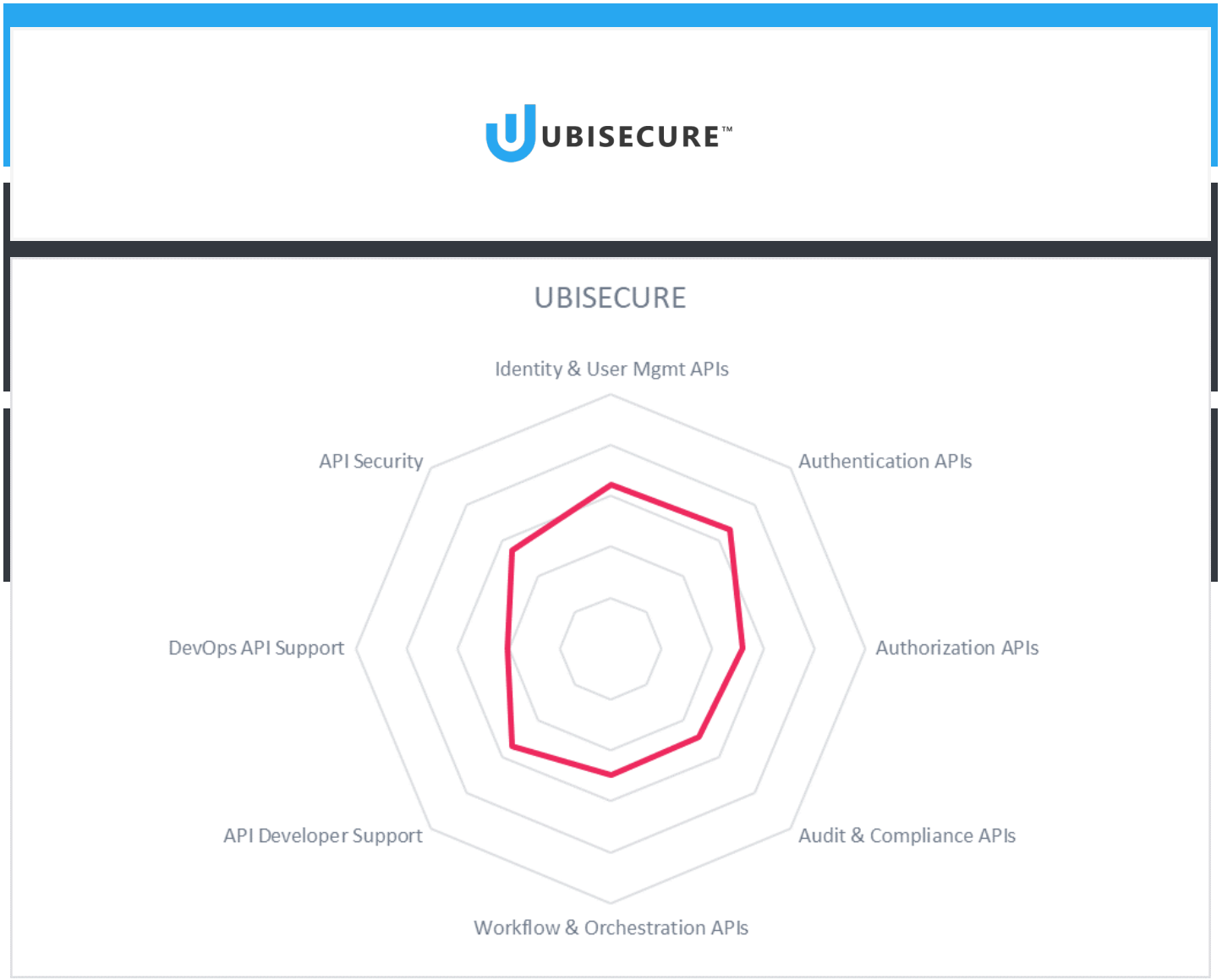
Ubisecure Identity and User Management capabilities provide identity federation APIs that support the most used standards like SAML 2.0, OIDC, OAuth 2.0, WS-Federation, JWT and less common ones such as TUPAS, Mobiilivarmenne/ETSI MSS 102 204, OIDC CIBA. Bulk provisioning via LDAP, SCIM, or support for provisioning to or from other cloud services using specific cloud service APIs are not provided.

Ubisecure APIs not only support the most common authentication standards, but they also support some not so common standards such as Certification Authentication Protocol (Cert AP) and the Swedish BankID (OIDC CIBA). Areas of authentication not covered by their Identity Server is support for mobile applications and biometrics. Also, application SSO integration APIs are provided as a base functionality for Ubisecure SSO.

Authorization APIs are provided for both RBAC and fine-grained access controls of users, although APIs for risk-based access controls are not supported. Audit and compliance APIs are not given as well as APIs to provide or integrate with fraud and cyber threat intelligence solutions. Workflow APIs are provided for identity management of mobile applications, family content management, and application onboarding.

Ubisecure Identity Server only supports the REST API protocol, although they do support both JSON and XML data formats. Their Identity Server API provides developer a UI login widget and development SDKs for Java and .Net. Ubisecure gives limited support for DevOps APIs and API security. APIs for integration to other IAM, CIAM, or IDaaS platforms are available as well as integrations to CRM or other SaaS out-of-the-box via federation API calls.

Ubisecure has a relatively small presence outside the Nordic region and a limited partner ecosystem. Although they provide some interesting features in some specific areas, and their Identity Server has a strong focus on security, they lack innovation in areas that offer more advanced API capabilities.



5.12 ViewDS

Founded in 2009, ViewDS is a privately held identity management company headquartered in Melbourne, Australia. ViewDS provides a suite of solutions that support both IAM and IDaaS use case with an on-premises, cloud, and hybrid deployment models. For cloud delivery, ViewDS API layer container is fully multi-tenant and is intended to run with a single instance per Docker host.

ViewDS supports both the REST and OData APIs as well as SOAP for SAML 2 IdP and SP endpoint support. Also, the APIs support both JSON and XML for SAML support for data import/export. Their solutions provide API discovery and protocol conversions between OData to LDAP, OIDC to LDAP authentication, and

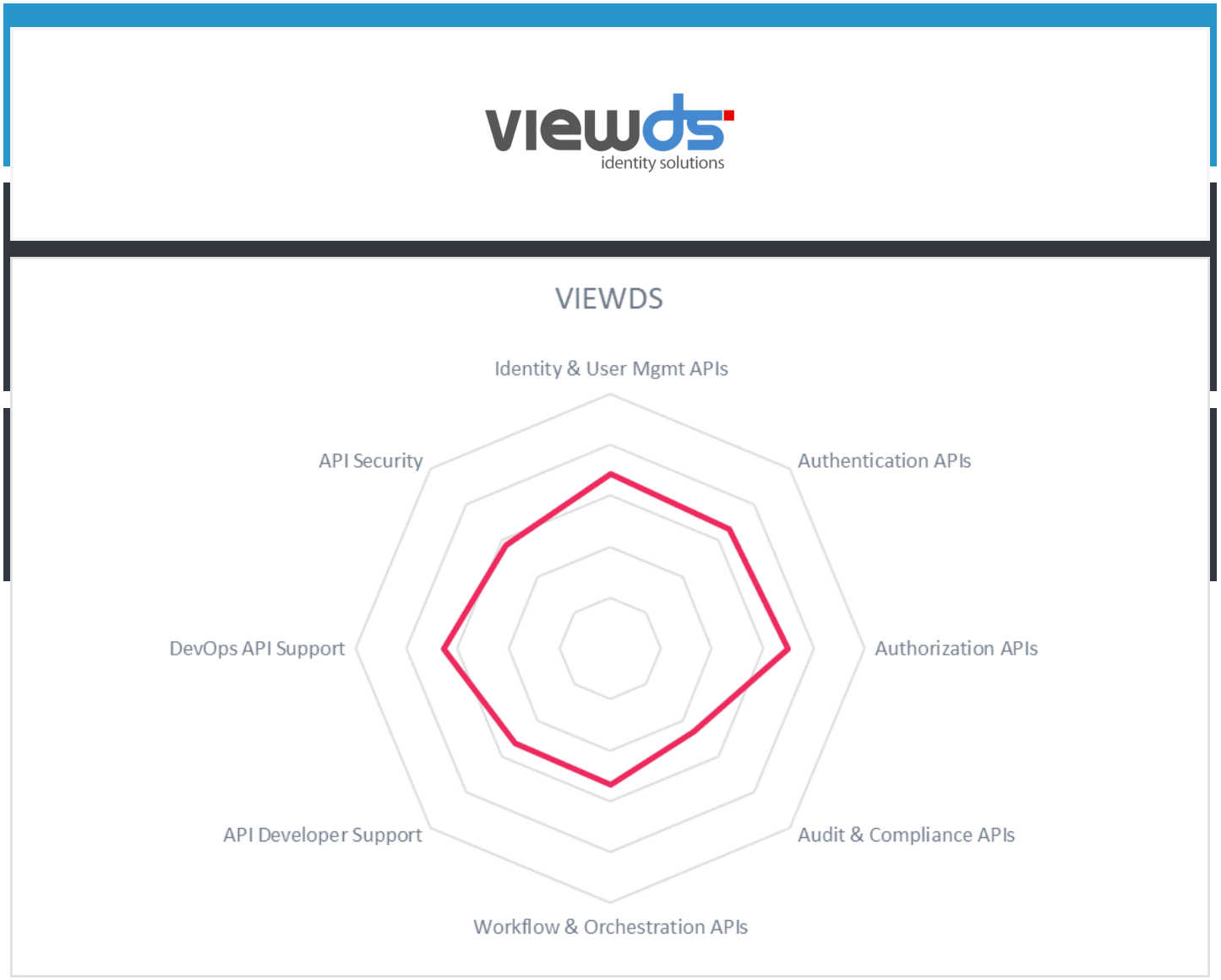
OIDC to SQL authentication.

ViewDS provides APIs to manage identities, including CRUD functionality. APIs are given to the ViewDS LDAP directory as well as a containerized directory server that can be run in a public or private cloud environment. Their graph-based OData API supports data access to identity data, and API support is also given for both MS AD and Azure AD integrations. APIs for identity federation supports SAML 2, OIDC, OAuth 2, and JWT. APIs for bulk provisioning and synchronization from LDAP and other cloud services are available, although support bulk provisioning from SCIM is not.

Authentication APIs are given for most authentication forms and standards including API tokens and support for mobile application, but APIs to biometrics is not given. Although risk-based and step-up authentication is not available, time and IP address attributes can be used for context-based authentication. Both OIDC and SAML are support for their SSO APIs. Authorization APIs are provided for both RBAC and fine-grained or dynamic access controls.

Limited APIs are available for audit and compliance reporting, although reporting development is on the ViewDS roadmap. Missing are developer API support tools such as widgets & SDKs.

ViewDS customers are primarily focused in the APAC region, with an additional presence in the U.K. and North America. The ViewDS API driven platform provides good flexible deployment capabilities across multiple environments and appears as a challenger in the Product and Innovation Leadership category, although there is room for improvement in the area of market presence.



5.13 WSO2

WSO2 Identity Server is based on open source and provides Identity and Access Management (IAM) capabilities as a single integrated IAM suite. WSO2 Identity Server APIs focus on IAM, CIAM, and IDaaS use cases with a primary focus on Identity Federation and SSO. WSO2 Identity Server supports on-premises, cloud, and hybrid delivery models.

Good Identity and user management API capabilities are provided, including support for most federation standards, including SCIM 2.0 and UMA when accompanied by a Protection API Access Token (PAT). Complete SSO setup and access to SSO metadata can be done via APIs. The majority of authentication standards are supported by their APIs including FIDO U2F, mobile authentication, and biometrics. Beyond RBAC, fine-grained access control is provided with XACML, including support for the XACML REST/JSON profile, by exposing their PDP functionality as an API.

Identity Server API documentation is provided online with its API descriptions and examples, while a more comprehensive developer portal for API support is given with WSO2 API Manager. WSO2 currently doesn't support development widgets to abstract the raw APIs and speed development. Also, only Java SDKs are provided to developers. Workflow & Orchestration APIs are given and include mobile app workflows for identity management and support for Single Sign-Off. Support for consent management, application onboarding, and API key activation workflows are also available via APIs.

on. Support for consent management, application onboarding, and API key activation workflows are also available via APIs.

Although WSO2 Identity Server APIs has good functional coverage in the IAM areas of identity, authentication, authorization, and auditing, it only supports REST/JSON and SOAP API protocols. WSO2 Enterprise Integrator (EI) is required for other protocol support or conversion.

WSO2 customers are focused in North America and the EMEA regions with some presence in the APAC region supporting small to large company sizes, with a good partner ecosystem. WSO2 Identity Server APIs shows strength in interoperability with a large number of other IAM, CIAM, and IDaaS platforms in these markets as well integrations with CRM and other SaaS systems. Overall, WSO2 has consistently made improvements in its Identity Server and has moved it in a positive direction.

6 Vendors to watch

Besides the vendors covered in detail in this Leadership Compass document, we observe some other vendors in the market that have credible Identity API Platform capabilities in the market. A few of these vendors have decided not to participate in this KuppingerCole Leadership compass for their own reasons, but since we find them interesting and worth a mention, we decided to include them here. These vendors may not fully fit into the market segment of Identity API Platforms or do not meet our eligibility criteria to be considered in this evaluation. We provide short abstracts for these vendors below.

6.1 Accenture Security – Memority

The French system integrator, Arismore, founded Memority. With the acquisition of Arismore by Accenture Security, Memority has become part of that larger group. That gives Memority access to a global network of resources and the potential of expanding its currently small market share significantly.

Memority is an IDaaS B2E solution constructed specifically for that purpose, and as such provides APIs to its services. Memority offers a good feature set for Identity Provisioning and Identity Federation, as well as baseline Access Governance features. For authentication, Memority provides Adaptive Authentication capabilities, where major features such as support for FIDO Alliance standards, risk-based authentication based on contextual factors, and flexible integration of 3rd party authentication are supported. Memority offerings support both on-premise and cloud services.

6.2 Amazon AWS – Cognito

Amazon Cognito offers authentication, authorization, and user management capabilities for both web and mobile applications. All services are exposed via APIs, meaning it could be categorized as more of a Do-It-Yourself C/IAM solution. Cognito supports OAuth, OIDC, and SAML for federation, allowing users to sign in using social media credentials. Cognito is built for controlling access to Amazon resources. Amazon's computing environment is PCI-DSS, SOC, ISO/EIC 27001, ISO/EIC 27017, ISO/EIC 27018, and ISO 9001 compliant. KuppingerCole will follow developments in Amazon Cognito.

6.3 Avoco Secure – Trust Platform

provides APIs with a focus on security, privacy, and usability. The API platform is a toolkit providing extended ecosystem functionality to deliver multiple components, including IDPs, hubs, brokers, verification, and, blockchain. The blockchain piece is blockchain-agnostic and privacy enhanced.

The Avoco Trust Platform wasn't derived from traditional IAM but instead was built to UK government security standards for high assurance verification of consumer identities. Avoco Secure partners offer customer profile stored in cloud or hybrid installations. Any of the components generated using the Avoco Trust Platform APIs are available either as a cloud-based service or can be directly integrated into customer's on-premise environments. Trust Platform accepts username/password, SMS OTP, and social logins from Facebook, Twitter, Microsoft, LinkedIn, and Google. It has many second factors available OOTB and also integrates to third-party credential management services that offer biometrics. Risk-based authentication is managed using dynamic rules. It accepts federated login via SAML, OIDC, and OAuth. Using REST APIs, the Avoco Identity platform can feed data to SIEM/RTSI systems and Splunk. Avoco Secure also provides privacy consent management functionality, although the Trust Platform does support UMA. Family management can be achieved via a delegated administration model.

The Avoco Trust Platform is an interesting offering considering its consent management and identity verification service provider integration. KuppingerCole will continue to monitor Avoco Secure and will include them in future publications.

6.4 Cloudentity

Cloudentity is headquartered in Seattle, Washington. In 2014, Cloudentity leveraged their IAM expertise from Syntegrity into a next-gen platform based on micro-services providing a fully-featured CIAM solution with a cloud-first approach. Cloudentity utilizes many of the latest container and orchestration technologies, such as Docker, Kubernetes, Istio, and Pivotal, to deliver their services. Their solution can run on-premise or in the cloud and offer a hosted service. Cloudentity licensing options is based on the number of micro-services used, rather than per-user bases.

Cloudentity CIAM capabilities are microservices and include identity and user management, authentication, authorization, and delegated administration, to name a few. Addition capabilities can be added a la carte such as IDP & SP federation, risk analysis, token exchange, MFA, and analytics services. All services of Cloudentity are accessible via their API layer using REST over HTTPS. In fact, every action available within their web UI is also available through their APIs.

Cloudentity's modern approach of containerized services that improve scalability and flexibility, and which can be deployed in the hybrid environments seen today, makes Cloudentity a promising vendor to watch.

6.5 EmpowerID

EmpowerID with its product also named EmpowerID was founded in 2005, and formerly known as The Dot Net Factory. EmpowerID supports medium to large companies primarily in the U.S. and northern Europe. EmpowerID supports on-premises with the service also offered as a Cloud solution by partners of EmpowerID.

EmpowerID delivers a comprehensive feature set for Identity and Access Management, Single Sign-On, and workflow development platform. Their entire range of EmpowerID capabilities is available via APIs. Support for new technologies and standards like OAuth, OpenID, RESTful APIs, or integrated STS (Secure Token Service) feature sets is broad. Provisioning to cloud services is supported out-of-the-box through calls to those systems proprietary REST APIs. Third party SIEM or Security Intelligence Platforms are also supported out-of-the-box if those platforms are capable of calling EmpowerID's REST API to consume their data.

EmpowerID has a relatively small partner ecosystem and runs on Microsoft platform only, which may be a challenge for some organizations, but overall, EmpowerID is a very interesting and innovative solution. It provides a well thought-out and flexible approach to its IAM and workflow APIs.

6.6 Ergon – Airlock IAM

Ergon is a privately held Swiss-based company established in 1984. With customers primarily in DACH and growing across EMEA and the APAC regions, it has a strong history of providing IAM solutions to customers in a variety of industries, including finance. Their partner ecosystem is again focused in DACH region and remains small in the other areas.

The Airlock Suite provides a good and comprehensive set of Authentication, Web Access Management, Identity Federation and Web Application Firewall capabilities. The suite is made up of the Airlock IAM, Airlock WAF, and Airlock Login, in which the Airlock WAF is tightly integrated with Airlock IAM. Each component of the Airlock suite provides REST API interfaces to access certain features of their product. With the Ergon Airlock WAF, API security functionality that directly addresses technical requirements of PSD2 is available. Further roadmap development includes REST APIs with workflows.

6.7 Gigya – CIAM Platform

Gigya, recently acquired by SAP, is a software vendor headquartered in Mountain View, California with additional offices worldwide (including London, Hamburg and Paris, Melbourne and Sydney, Singapore and the original starting point Tel Aviv). Founded in 2006, they focus on providing solutions in the area of Customer Identity and Access Management Solutions and is well-established amongst the leading products in the CIAM market.

Gigya CIAM Platform is offered as a fully multi-tenant SaaS solution, with the ability to store and govern consumer profiles. Gigya has broad support for social registration and logins and excels at identity and marketing analytics.

Gigya offers both SDKs and direct REST APIs to their core service. Their Web SDK provides access to Gigya's add-ons, which essentially wraps calls to their REST APIs. The Server-Side SDK is used to integrate the Gigya's platform for server-side application, but is not part of their core offering. Gigya also provides SDKs for both iOS and Android mobile device platforms, as well as the Cordova mobile development framework. Direct REST API calls can be made to Gigya service, which gives access to account, audit, profile management, social, and report functionality to name a few.

6.8 Google – Cloud IAM

Google's cloud IAM platform is intended to managing access and permissions for both users and services that wish to access an organization's resources on the Google Cloud platform. It consolidates control to allow access to these resources in one place for an organization by defining policies for identities (users & service accounts), roles and resources.

The Google Cloud IAM provides APIs for IAM policies including querying auditable services and lint validation of policies. Other APIs focus on organizations roles, permissions, project service accounts, roles and user or system managed keys. Credential APIs are also available to generate access or ID tokens and other APIs for digital signing.

6.9 IBM – Cloud IAM

IBM is a large fortune 500 company headquartered in Armonk, NY with a global presence in North America, EMEA, and APAC regions. IBM has customer deployments within many industry sectors, such as Financial and Business Services, Healthcare, Retail, Automotive, Technology, Public Sector, Distribution, Entertainment, Transportation, Utilities and Consumer Goods.

IBM Cloud IAM allows organizations to authenticate a user when accessing their platform services, as well as restricting access to their resources on the IBM Cloud platform. Their IAM Identity Services API allows organizations to perform identity operation through the management of API Keys and Service IDs or identities used by an application or service. APIs for token operations are also provided to generate IAM access tokens for a user or service ID.

6.10 Microsoft Azure – AD B2C

Microsoft Azure Active Directory B2C is their cloud identity management service focused on facilitating business to consumer applications. Built upon Microsoft Azure AD, the B2C offering is architected to scale and perform well with hundreds of millions of users and over one billion logins per day. Cloud services have been one of the primary drivers in Microsoft's business portfolio.

Microsoft Azure AD B2C provides RESTful APIs to facilitate authentications against an identity, as well as the use of their Graph API to perform CRUD operations on Azure AD data and objects such as users, groups and applications. Other RESTful APIs allow integration with systems such as SIEM/RTSI, CRM, and big data analytics. Given Microsoft's commitment to cloud services, we expect it to continue to mature over time.

6.11 OpenText Cocisint – Cloud Identity Platform

Founded in 1991, OpenText is a large publicly-traded Canadian software company headquartered in the Great Lakes region. With their acquisition of Covisint in mid-2017, OpenText gained a leading Cloud Identity Platform that supports B2B, B2C, IGA, as well as support for IoT.

The OpenText Covisint Identity Platform provides delegated administration, compliance and governance monitoring, Single Sign-On multi-factor authentication, and authorization services. APIs are available for authentication, attribute-based authorization, registration, and API-based file transfer or API-driven Reporting are available too.

6.12 OneLogin

OneLogin was founded in 2009 and is headquartered in the San Francisco Bay Area. They were one of the first vendors to enter the IDaaS market. OneLogin supports a large number of pre-configured cloud services that can be easily connected and provide services for access management, single sign-on, user provisioning, mobile identity, compliance, and both multi-factor and adaptive authentication.

The OneLogin Cloud Directory support APIs for user CRUD and other user services such as assigning roles, setting passwords and state. Multi-factor authentication APIs are also supported as well as OAuth and SAML. The ability to get roles and group information is given and support for user login as well as the ability to access event information.

6.13 OpenIAM – IAM Suite

OpenIAM has been in the IAM market since 2008. They moved from an open source model to a model which mandatorily involves a commercial component and open source. OpenIAM is a is a mid-sized company that faces the challenges of a limited partner ecosystem and growing unwillingness of organizations to adopt open source software options for security. Their product suite has two distinct components: OpenIAM Identity Manager delivering Identity Provisioning and auditing capabilities, and the OpenIAM Access Manager providing access management including identity federation, web-based access management, and SOA security.

OpenIAM supports integration with their solutions via a service-based API and both REST and SOAP options are available. Their RESTful web services APIs support authentication, authorization, user provisioning, user search, and password resets. Their SOAP API integration services provide access to authentication provider, files, policy, users, roles, resources and mail services.

6.14 Oracle – Identity Cloud Service

Oracle is both a leading software vendor and a leading cloud service provider. Their platform is built from the ground up for IDaaS requirements in mind as well as giving good support to hybrid environments. Oracle Identity Cloud Service is a compelling offering targeted at enterprise customers and provides good above-baseline features in addition to a promising roadmap.

The Oracle Identity Cloud Service REST APIs not only give good support for cloud standards such as OAuth, OpenID Connect, and SCIM 2.0 for API-based integration but also offer support for securely managing resources, identities and configuration data. Social, MFA and even Adaptive API are also given. Oracle Identity Cloud Service provides an appealing offering to customers with a promising roadmap.

6.15 Salesforce – Identity Platform

Salesforce.com is a well-established player in the SaaS market, primarily known for its CRM (Customer Relationship Management) offering. Over the years their portfolio has significantly expanded and now provides digital identity as an integral part of the Salesforce platform. Salesforce Identity is not only the IAM foundation for Salesforce but is also offered to customers as IDaaS and for CIAM solutions.

The Salesforce Identity platform support supports SAML, OpenID, OpenID Connect, OAuth APIs for authentication. Salesforce Identity also allows for delegated administration via API calls to subscriber web services. Salesforce was a significant contributor to the SCIM provisioning protocol, and thus supports versions 1.1 natively and 2.0 via an Apex package for creating and synchronizing identities. In addition, Salesforce provides API access via SOAP, REST, Bulk, Streaming, and other custom APIs. Whether REST or SOAP is used, both utilize the same data model. Salesforce Identity provides both analytics features and reports, making the raw data available to 3rd party analytics applications via REST APIs.

6.16 SAP – Cloud Identity Platform

SAP is one of the world's largest software company headquartered in Germany. Since entering the cloud market five years ago, it has quickly grown to offer many SaaS solutions. The SAP Cloud Identity is one such service, allowing their customers to integrate their identities with other SAP services such as their SAP HANA Cloud Platform Identity Authentication and SAP HANA Cloud Platform Identity Provisioning solutions. The SAP Cloud Identity service fits well into the Cloud User and Access Management categories of the IAM market and adds the capabilities of managing external users in a cloud-based directory, controlling access, registering external users, to name only a few examples.

The SAP supports Cloud Identity platform give APIs for authentication, such as the ability to configure credentials for HTTP basic authentication or to set certificates for authentication. Other APIs includes the use of REST APIs to send an invitation via email, and user management REST APIs for user registration as well as retrieving user information, deactivation or deletion of the user. SCIM REST APIs are also provided to manage user or groups. Currently, only SAML and OAuth APIs are available for federated use cases.

6.17 SecureAuth – SecureAuth IdP

SecureAuth is a well-established provider of a set of identity management solutions covering Multi-Factor Authentication, Risk-based Adaptive Authentication, Single Sign-On, and User Self-Service, and SecureAuth's IdP is their primary integrated IAM and CIAM solution set. SecureAuth was founded in 2005, is based in Irvine California, and has a large customer base, primarily in North America.

SecureAuth's IdP functionality can be embedded into a custom application via their authentication APIs. The SecureAuth's authentication APIs allow the validation of user IDs, passwords, PINs, soft tokens and more. The APIs also enable the generation of OTPs and can analyze a user's access attempts using a device or browser fingerprinting, or other adaptive and biometrical means. Adaptive Authentication features are provided via APIs to allow administrators to evaluate behavioral biometrics, such as typing sequences or mouse movements via API. APIs are also given for Advanced identity analytics, although requiring 3rd party applications.

7 Related Research

Executive View: Auth0 Customer Identity Management – 71053
Executive View: Auth0 Authentication Service – 71325
Executive View: Centrify Next-Gen Access Platform – 79036
Executive View: ForgeRock Identity Platform – 70296
Executive View: ForgeRock Access Management – 71316
Executive View: iWelcome IDaaS and CIAM – 70298
Executive View: iWelcome Identity & Access Management as a Service – 71205
Executive View: Janrain Identity Cloud® – 70845
Executive View: Okta Cloud IAM Platform – 70887
Executive View: Ping Identity PingOne – 70288
Executive View: Ping Identity's PingFederate – 70284
Executive View: Pirean Consumer IAM Platform – 70223
Executive View: ViewDS Cobalt – 70851
Executive View: Ubisecure Identity Server – 70838
Executive View: WSO2 App Manager – 71296
Executive View: WSO2 Identity Server – 71129
Leadership Compass: Access Governance & Intelligence – 71145
Leadership Compass: Access Management and Federation – 71147
Leadership Compass: Adaptive Authentication – 71173
Leadership Compass: CIAM Platforms – 79059
Leadership Compass: Cloud-based MFA Solutions – 70967
Leadership Compass: Dynamic Authorization Management – 70966
Leadership Compass: Identity Provisioning – 71139
Leadership Compass: Identity as a Service: Single Sign-On to the Cloud (IDaaS SSO) – 71141
Leadership Compass: Identity as a Service (IDaaS B2E) – 70319
Whitepaper: ForgeRock: The Effect of GDPR on Customer Relations – 73000
Whitepaper: Ping Identity solutions for Customer Identity and Access Management – 70289
Whitepaper: Pirean: Orchestrated Identity for Meeting IAM & CIAM Requirements – 70225

Methodology

About KuppingerCole's Leadership Compass

- Types of Leadership
- Product rating
- Vendor rating
- Rating scale for products and vendors
- Inclusion and exclusion of vendors

Copyright

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

KuppingerCole Analysts, 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**.

^ top