KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert September 2019

Consumer Authentication

This report provides an overview of the market for Consumer Authentication products and services and provides you with a compass to help you to find the Consumer Authentication product or service that best meets your needs. We examine the market segment, vendor product and service functionality, relative market share, and innovative approaches to providing Consumer Authentication solutions.

by **John Tolbert**
jt@kuppingercole.com
September 2019

Content

Content of Tables

Content of Figures

Related Research

Advisory Note: Identity & Access Management/Governance Blueprint - 70839

Advisory Note: IAM Predictions and Recommendations 2014-2018 - 71120

Advisory Note: Cloud IAM: More than just Single Sign-On to Cloud Applications - 71031

Executive View: PingFederate 7 - 70801

Executive View: Salesforce Platform as a Service – Security and Assurance - 70751

Executive View: PingOne® - 70870

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 70949

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 70960

Leadership Compass: Access Management and Federation - 70790

Leadership Compass: Access Governance - 70735

Product Report: Microsoft Azure Active Directory - 70977

Scenario: Understanding Cloud Security - 70321

Scenario: Understanding Cloud Computing - 70157

Scenario: Understanding Identity and Access Management - 70129

Vendor Report: SecureAuth Corporation - 70260

1 Introduction

eCommerce businesses and other organizations that interact directly with end-users over the web are increasingly looking for better solutions for authenticating those users. Password authentication is not only insecure, but it leads to poor consumer experiences and is costly for businesses to maintain. Knowledge-based authentication is an even worse alternative. In order to deter fraud, comply with new regional and industry-specific regulations, and improve the customer experience, organizations are adopting Consumer Identity and Access Management (CIAM) solutions or enhancing their existing customer-facing IAM solutions with modular authentication services.

Most organizations have IAM products in place already. However, many are finding that their current solutions are not able to meet consumer expectations or security requirements.

There are a number of motivations driving businesses to enhance their authentication solutions:

- Improve consumer experiences
- Increase security
- Reduce fraud
- Preserve privacy
- Comply with regulations requiring strong or multi-factor authentication, such as AML (Anti-Money Laundering), EU PSD2, KYC (Know Your Customer), and NY CCR (New York cybersecurity law)

Consumer authentication services today are primarily leveraging mobile devices, particularly smartphones. Given the near ubiquity of these devices, it's not a surprise. Smartphones can serve as a second factor, or the "something you have" factor in Multi-Factor Authentication (MFA) scenarios.

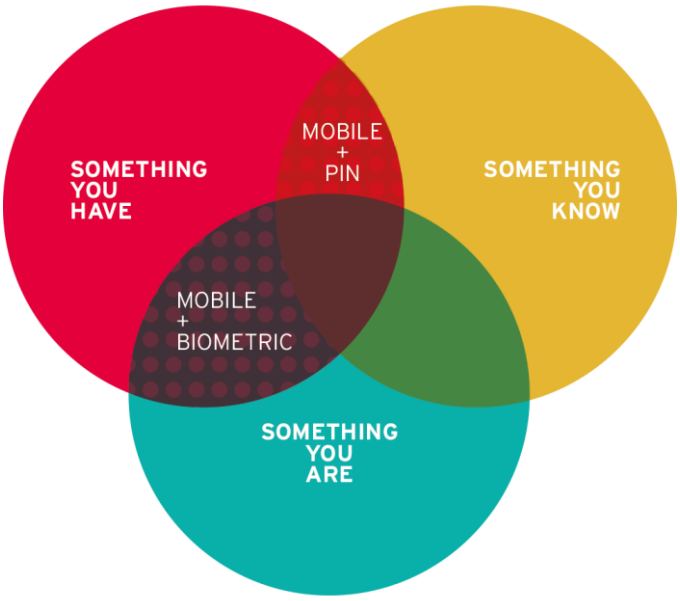


Figure 1: The Role of Mobile Devices in MFA

This KuppingerCole Leadership Compass provides an overview of the leading vendors in this market segment. Picking solutions always requires 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 customer and his requirements. However, this Leadership Compass will help identify those vendors that customers should look at more closely.

1.1 Market Segment

The Consumer Authentication market is growing, with some vendors offering mature solutions providing standard and deluxe features to support millions of users across every industrial sector. As will be reflected in this report, the solutions in this space are quite diverse. Some vendors have about every feature one could want in a consumer authentication service, while others are more specialized, and thus have different kinds of technical capabilities. For example, some smaller vendors are targeting the government-to-citizen (G2C) market as well as business-to-consumer (B2C). We sometimes see support for national e-IDs, x.509 certificates, and higher assurance authentication mechanisms in these vendors' products compared to the rest.

Furthermore, KuppingerCole research indicates that the particular market segments that vendors choose to target often has a direct effect on the type of features available in their consumer authentication solutions. Consumer authentication product or service vendors that are primarily pursuing retail and media companies as clients tend to not have the customer-driven pressure to support high assurance authentication and complex attribute-based access controls. This Leadership Compass will examine solutions that are available for both on-premise and cloud-based deployment.

Many vendors are taking an "API-first" approach to consumer authentication, which allows organizations with in-house expertise to extend their existing IAM infrastructure to accommodate consumer use cases better. The API-first approach also permits in-house developers to easily "bolt-on" authentication services to existing or legacy Line of Business applications, without necessarily investing in a full-size CIAM solution. Identity API platforms are not always completely assembled products and services. Rather, these platforms are collections of tools, code, and templates. Identity API platforms may contain many open source elements, and generally leverage well-known standards. KuppingerCole is also producing a Leadership Compass focuses on Identity API platforms.

1.2 Delivery models

In the Consumer Authentication market, solutions are offered as SaaS, or for on-premise or in-IaaS deployment. Pure-play SaaS solutions are multi-tenant by design. On the other side, Managed Service offerings are run independently per tenant. For SaaS offerings, the licensing model is often priced per user. For on-premise deployments, licensing costs can be measured in a variety of ways, such as per-user, per-server, or per transaction.

1.3 Required Capabilities

Typical requirements seen in RFPs regarding consumer authentication include:

- Deployment options: On-premise, cloud, or hybrid options.
- Social logins: Allow users to login via Facebook, LinkedIn, Twitter, Google, Amazon, etc.

- Multi-factor authentication mechanisms:
  - SMS OTP (still in use, but deprecated due to security problems)
  - Email / Phone OTP
  - Mobile push notifications
  - Mobile apps
  - Mobile SDKs that corporate customers can use to build stronger authentication into their own apps
  - Native mobile biometrics, such as Apple or Samsung implementations of fingerprint and facial recognition
  - Third-party biometrics
  - **FIDO® Certified** authenticators, including U2F, UAF, and 2.0
  - Wearable biometrics
  - Behavioral biometrics
  - Environmental authentication via IoT or SmartHome devices
  - USB or other hardware tokens (rare)
- Risk adaptive authentication and authorization: Evaluation of various factors at runtime or transaction-time, according to customer set policies, to determine if transactions should proceed, require additional attributes to be collected, or denied. Examples of data points often considered in adaptive authentication and authorization scenarios include, but are not limited to
  - Geo-location
  - Geo-velocity
  - IP address
  - User attributes
  - User behavioral analysis
  - Device identity and/or fingerprint
  - Device hygiene
  - Device reputation
  - Device jailbreak or root detection
  - Fraud risk intelligence, cyber threat intelligence, and compromised credential intelligence
- Account recovery mechanisms: Organizations needs to provide options and processes for recovering access to accounts when consumers registered authenticators are unavailable. For example, a consumer can't remember a password, or loses a smartphone or simply gets a new one. Consumers need flexibility in these cases, but businesses also need to ensure that the authenticator de-registration and re-registration methods are secure and adhere to their own policies.

The criteria evaluated in this Leadership Compass reflect the varieties of use cases, experiences, business rules, and technical capabilities required by KuppingerCole clients today, and what we anticipate clients will need in the future. The products examined meet many of the requirements described above, although they sometimes take different approaches in solving the business problems.

When evaluating the services, besides looking at our standard criteria of

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

We also considered a series of specific features. These functional areas, which are reflected in the spider charts for each company in Chapter 5 include:

APIs	APIs are increasingly available in consumer authentication solutions to provide tie-ins to existing IAM or IDaaS infrastructure, as well as to security services and external analytics solutions.
Authenticators	Types of authenticators supported, such as FIDO, MFA, SDKs, social logins.
Fraud/Threat Intel	Capability to consume and utilize 3rd-party fraud, threat, and compromised credential intelligence. Some vendors generate their own intelligence, based on activities within their own networks and client base. Generally, in-network intelligence concerns credentials that have been compromised within the vendor's ecosystem.
Mobile Security	Since most emphasis on consumer authentication is in the mobile area, this factor quantifies the use of mobile app security features; specifically, providing secure SDKs for mobile app development, Global Platform Secure Element / Trusted Execution Environment (SE/TEE) for Android devices and Secure Enclave for iOS devices. Some vendors utilize mobile app hardening services and mobile threat analytics to raise the assurance level for their customers.
Risk Analytics	Evaluation of user attributes behavioral analysis, environmental factors, fraud/threat intelligence, and other information to determine authentication and authorization levels required per transaction.

Scalability	Some solutions have massive scalability while others do not. Picking the right size vendor is an important consideration in RFPs. Not everyone needs the biggest and most scalable solutions. But if your business does, then understanding the scalability comparison and factors examined will be of paramount interest. The most scalable solutions are usually those which are based on micro-services architectures. Most are cloud-hosted, with the ability to spin-up and wind down additional virtual server instances to serve rapid increases in demand. This rating is influenced by many factors including number of customers, consumers, deployment models, multi-cloud utilization, geographic distribution, SLAs, and maximum number logins per second.

Each of the categories above will be considered in the product evaluations below. We've also looked at specific USPs (Unique Selling Propositions) and innovative features of products which distinguish them from other offerings available in the market. Features that are considered innovative are listed below.

- Support for standards such as GSMA Mobile Connect, FIDO Alliance, and Global Platform Secure Element (SE) and Trusted Execution Environment (TEE) standards.
- A comprehensive and consistent set of REST-based APIs for integrating with current IAM infrastructure.
- Advanced support for authentication mechanisms, especially mobile biometrics.
- Mobile app integration capabilities (SDKs).
- Integration with national e-IDs and passports.

Please note that we only listed a sample of features, and we consider other capabilities per solution as well when evaluating and rating the various consumer authentication solutions.

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 identifying 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

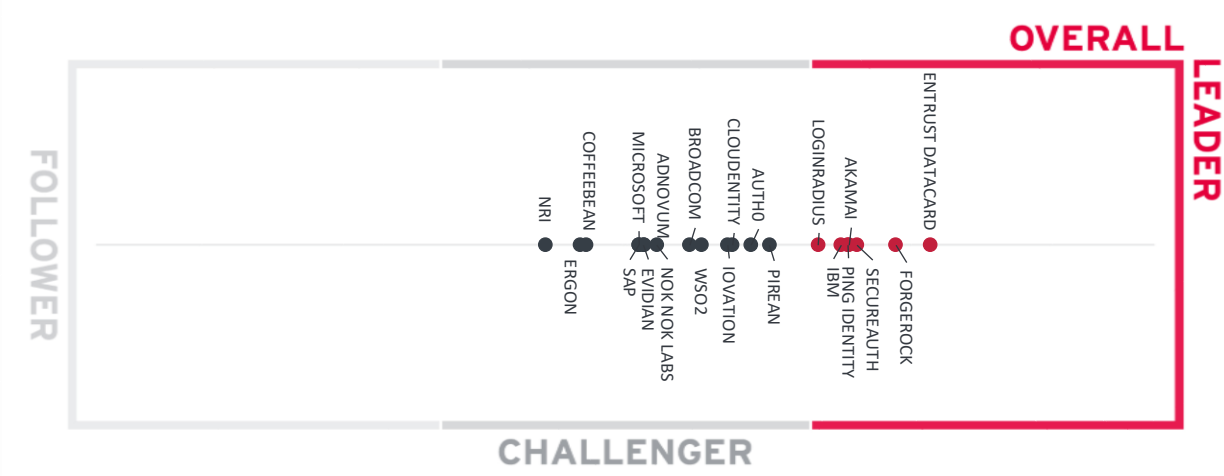


Figure 2: The Overall Leadership rating for the Consumer Authentication market segment

Entrust Datacard leads the pack, with ForgeRock, Akamai, SecureAuth, IBM, LoginRadius, and Ping Identity as Overall Leaders, showing strong ratings in all Leadership categories. These vendors provide comprehensive Consumer Authentication solutions to a large share of the market.

Interestingly, there are some significant differences in how these vendors deliver their solutions. Entrust Datacard and Ping Identity offer a full feature set for either on-premises or in the cloud. Akamai, IBM, and Login Radius solutions are cloud-delivered. ForgeRock and SecureAuth are on-premises but moving to full SaaS.

In the Challenger segment we see an even distribution across the main sequence. Pirean, iovation, and Cloudentity are not far from Leaders. Although they are not market leaders, their positions are bolstered by strong innovation. WSO2, Broadcom, and Auth0 are to the right of the midpoint. It is worthwhile to note that WSO2 utilizes an open source methodology, while Auth0 is developer-focused, and Broadcom is a strong traditional enterprise product. Rounding out the Challengers are AdNovum, Evidian, SAP, Microsoft, Nok Nok Labs, CoffeBean, Ergon, and NRI.

The Followers segment is empty, which shows that there a large number of very capable solutions in this consumer authentication solutions market.

Overall Leaders are (in alphabetical order):

- Akamai
- Entrust Datacard
- ForgeRock
- IBM
- Login Radius
- Ping Identity
- SecureAuth

Product Leadership is the first specific category examined below. This view is mainly based on the analysis of product/service features and the overall capabilities of the various products/services.

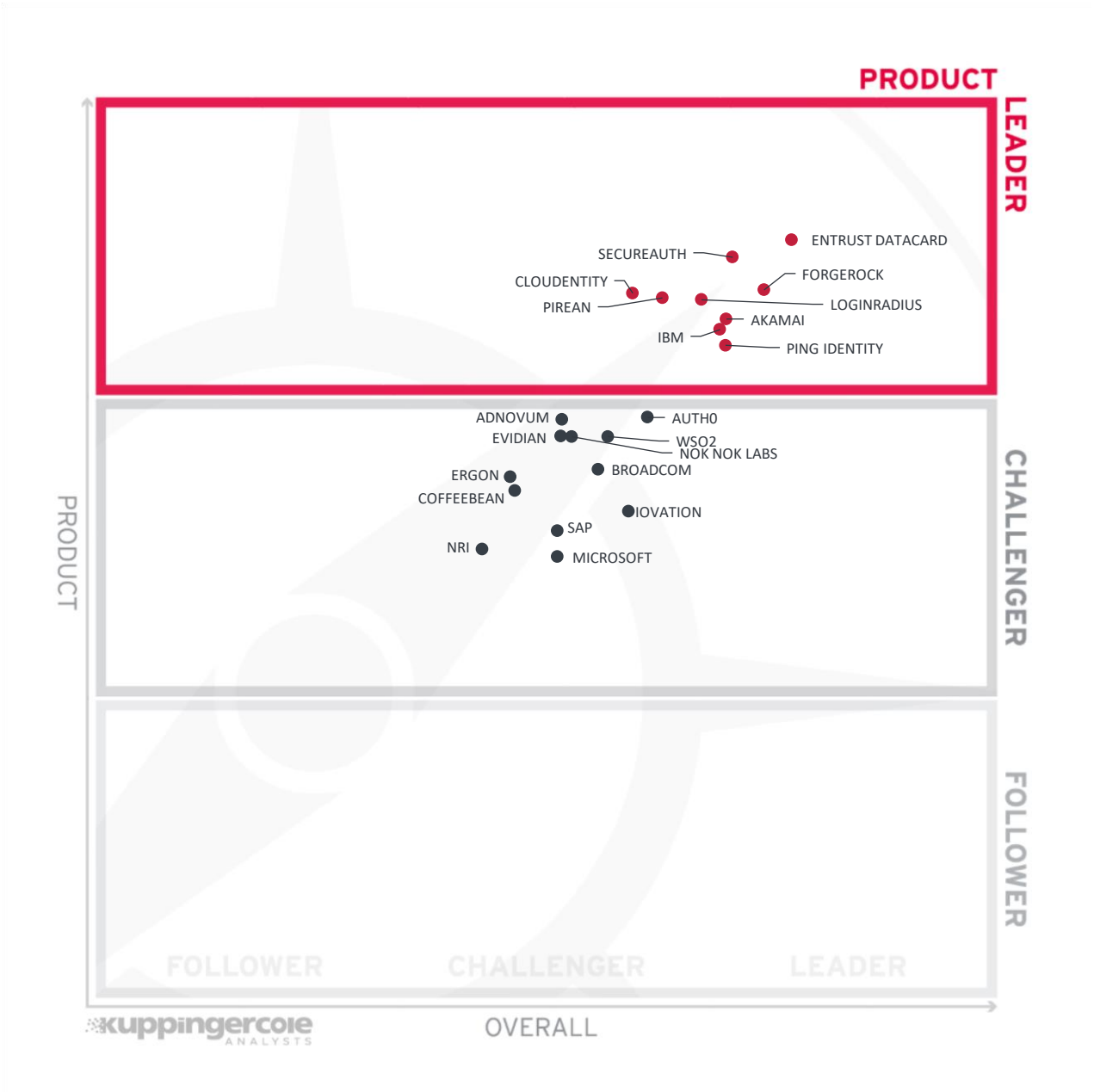


Figure 3: Product Leaders in the Consumer Authentication market segment

Product Leadership, or in some cases Service Leadership, is where we examine the functional strength and completeness of products/services. Entrust Datacard and SecureAuth are at the uppermost right space. Both companies have an excellent history of providing high security solutions.

Cloudentity is micro-services based for scalability. ForgeRock Identity Platform, while not offered as SaaS yet, can be run in IaaS, and offers much flexibility to customers. IBM has significant functionality with risk reduction with Trusteer. Pirean Access:One offers substantial functionality for a smaller vendor. LoginRadius has offers clients a turn-key SaaS solution. Akamai's acquisition of Janrain brought them a large number of consumer-facing customers which is well-positioned with Akamai's traditional services. Ping Identity offers full functionality to customers regardless of deployment model.

Many companies are clustered together at the top of the Challenger range: AdNovum, Auth0, Evidian, Nok Nok Labs, and WSO2. These products and services have a good mix of features that help them to excel in most areas of consumer authentication.

Following them, we find Broadcom, CoffeeBean, Ergon, iovation, SAP, NRI, and Microsoft.

The Follower segment is empty, due to the level of product maturity that each of the surveyed vendors has obtained.

Product Leaders (in alphabetical order):

- Akamai
- Cloudentity
- Entrust Datacard
- ForgeRock
- IBM
- Login Radius
- Ping Identity
- Pirean
- SecureAuth

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 about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested cutting-edge features, while maintaining compatibility with previous versions.

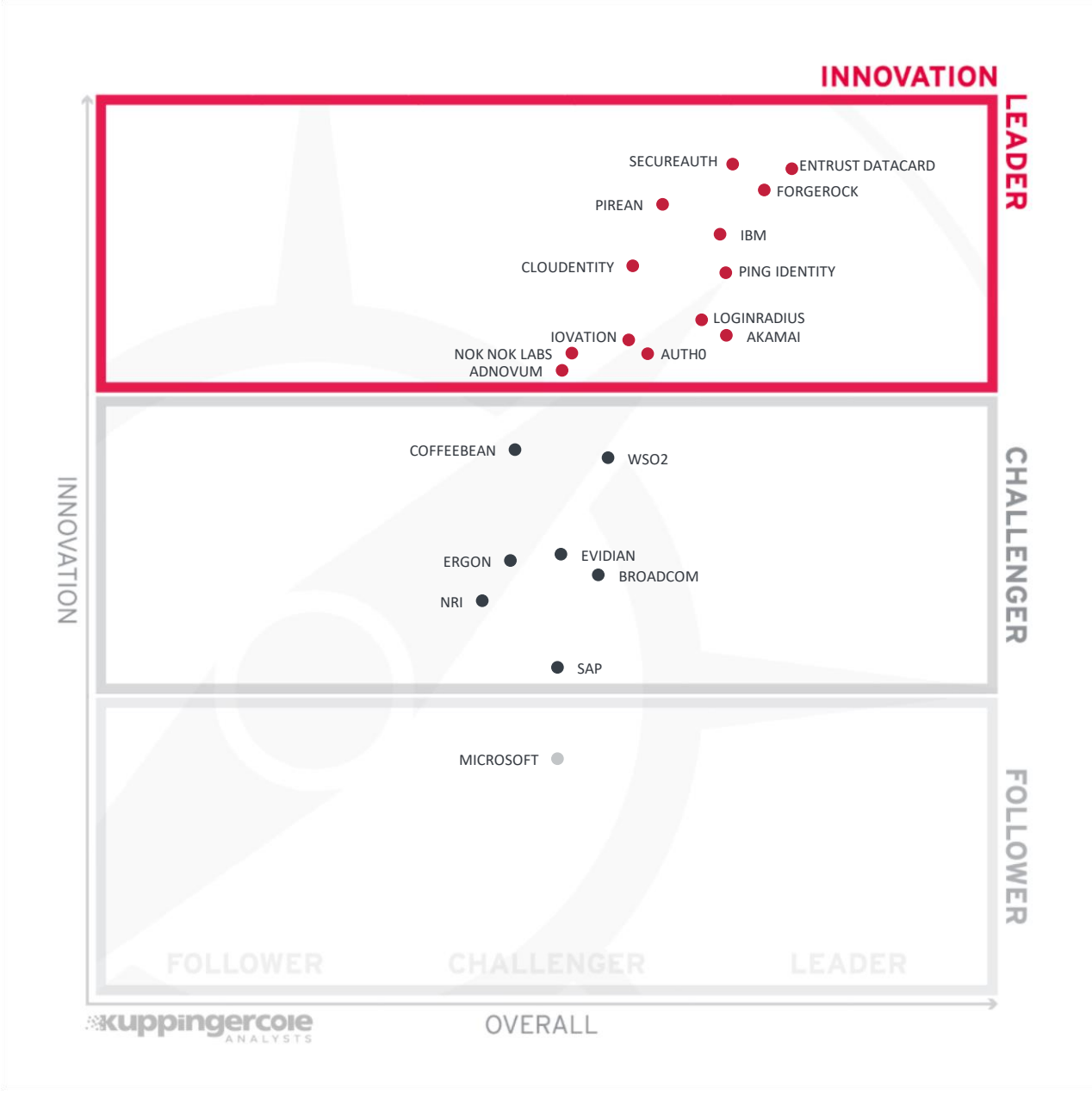


Figure 4: Innovation Leaders in the Consumer Authentication market segment

A sizable selection of vendors qualifies for Innovation Leader. The field is rapidly evolving, and business requirements are driving vendors to come up with new features to meet these requests. The top innovators are SecureAuth, Entrust Datacard, ForgeRock, Pirean, IBM, Cloudentity, and Ping Identity. We also see a second tier of innovation leaders just above the line: AdNovum, Akamai, Auth0, iovation, and LoginRadius.Two of the most important factors for innovation leadership are support for MFA variety,

particularly FIDO; and ability to generate in-network and/or consume 3rd-party threat intelligence sources for risk reduction.

CoffeeBean, WSO2, and Nok Nok Labs are in the top half of the Challenger segment. In the second half of the Challenger area, we find Evidian, Broadcom, Ergon, NRI, and SAP.

Microsoft appears in the Follower section.

Innovation Leaders (in alphabetical order):

- AdNovum
- Akamai
- Auth0
- Cloudentity
- Entrust Datacard
- ForgeRock
- IBM
- iovation
- LoginRadius
- Ping Identity
- Pirean
- SecureAuth

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

Figure 5: Market Leaders in the Consumer Authentication market segment

The Consumer Authentication market is growing, and there is still room for much more growth. Microsoft is at the pinnacle in terms of number of B2C customers, consumers served, and overall ecosystem.

Akamai, SAP, Ping Identity, Broadcom, Entrust Datacard, and ForgeRock are also Market Leaders. Each of these companies is well-established and have large numbers of customers, consumers, and strong support ecosystems.

Vendors are fairly evenly distributed across the Challenger block. Auth0, Evidian, IBM, iovation, Login Radius, SecureAuth, and WSO2 are in the top half. AdNovum, Cloudentity, Ergon, Nok Nok Labs, NRI, and Pirean are in the lower half.

Finally, we see CoffeeBean in the Followers section.

Market Leaders (in alphabetical order):

- Akamai
- Broadcom
- Entrust Datacard
- ForgeRock
- Microsoft
- Ping Identity
- SAP

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 6: 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 generally considered to be “overperforming” in the market. However, in this report we find a good mix of strongly capable large and specialty vendors above the dotted line.

The matrix shows a picture that is typical for evolving market segments, with a rather broad distribution of the various players across the quadrants and a weak correlation between Market Leadership and Product Leadership.

In the upper right box, we find Akamai, Entrust Datacard, ForgeRock, and Ping Identity. These vendors are leading in the innovation, product, and market ratings.

Below these, we find LoginRadius and IBM above the dotted line, with SecureAuth, Pirean, and Cloudentity in the box but below the line. The products and services represented here have excellent products with a lot of room for market growth.

On the other hand, in the center top box, we see Broadcom, Microsoft, and SAP having a significant market share but less robust in terms of product leadership.

In the center of the graphic we find AdNovum, Auth0, Ergon, Evidian, iovation, NRI, Nok Nok Labs, and WSO2. These all have respectable positions in both the Product Leadership and Market Leadership ratings and thus are interesting options to the leading vendors.

CoffeeBean is in the lower center. While they have a strong service, their marketing reach has been somewhat limited, but they have room to grow.

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. This distribution and correlation is tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

Figure 7: 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.

This chart shows a clustering along the line, which means the solutions have a balanced ratio of product capabilities and innovation. Many vendors are in the top right including Akamai, Cloudentity, Entrust Datacard, ForgeRock, IBM, LoginRadius, Ping Identity, Pirean, and SecureAuth are the technology leaders, with many advanced features.

AdNovum, Auth0, iovation, and Nok Nok Labs are just below the Technology Leaders in the center right box.

Many vendor solutions reside in the center of the chart: Broadcom, CoffeeBean, Ergon, Evidian, NRI, SAP, and WSO2. These products have a fairly even mix of innovation to product strength.

In the center left sector, we see Microsoft, who will be adding functionality to their service.

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, vendors which are highly innovative have a good chance for improving their market position. However, there is always a possibility that they might also fail, especially in the case of smaller vendors.

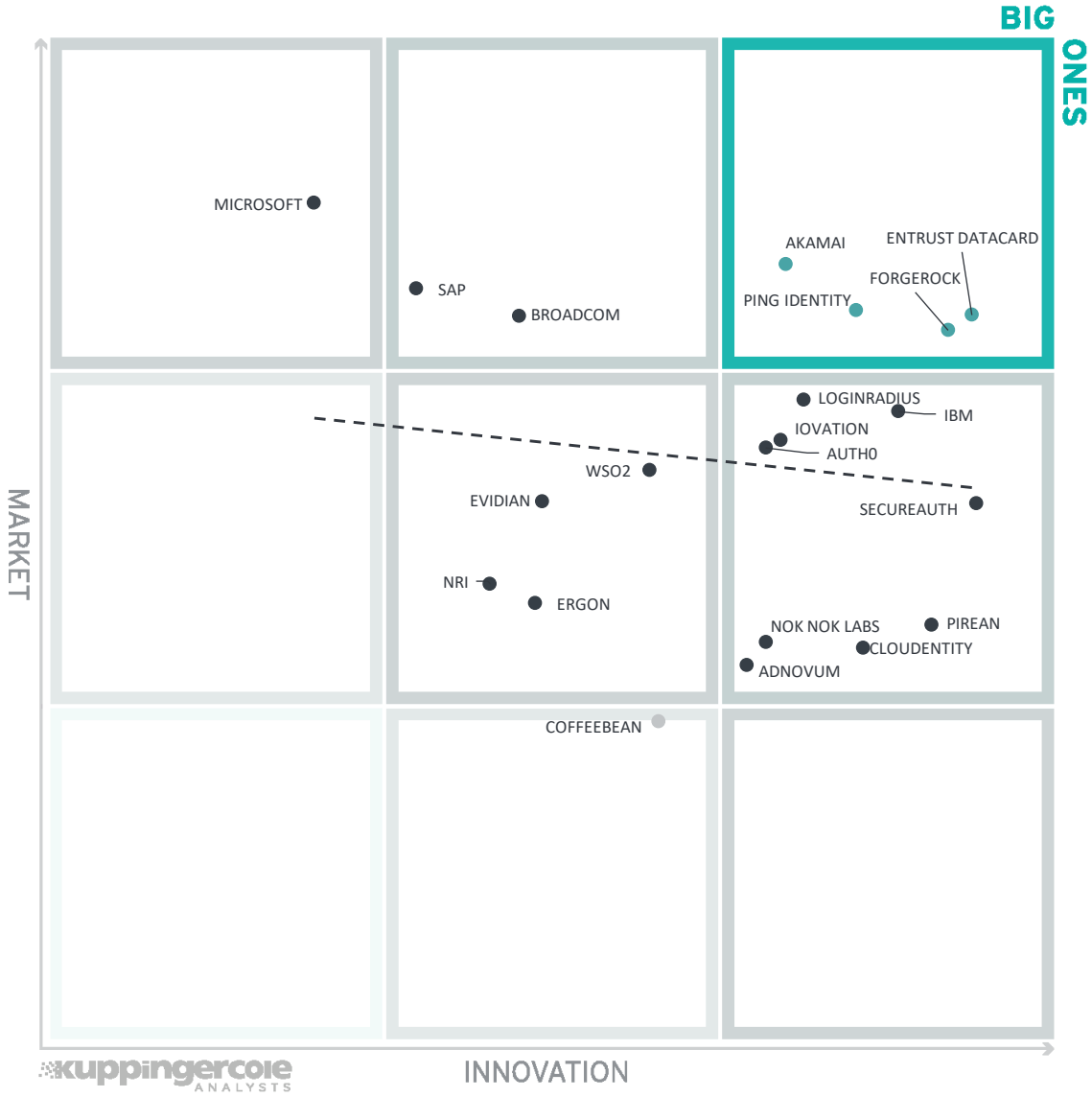


Figure 8: The Innovation/Market Matrix

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

Akamai, Entrust Datacard, ForgeRock, and Ping Identity occupy the top right sector, having both an excellent position in the market and presenting innovative capabilities to their customers.

The majority of solutions are found in the center right box. AdNovum, Auth0, Cloudentity, IBM, iovation, LoginRadius, Nok Nok Labs, Pirean, and SecureAuth, These chart positions indicate very strong innovation, but having less market share.

SAP, and Broadcom are also on top of the market, and are distributed across the top center box according to their relative innovation. Microsoft appears in the top left box, showing a commanding market share, but less innovation.

Fewer vendors than normal populate the center box. This shows a bias toward innovation in the consumer authentication market. In this section we see Ergon, Evidian, NRI, and WSO2.

CoffeeBean is found at the top of the lower center, offering some innovative features but not yet capturing a large share of the market.

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 Consumer Authentication. 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
ADNOVUM	strong positive	positive	strong positive	positive	positive
AKAMAI	strong positive	strong positive	strong positive	positive	positive
AUTH0	positive	positive	positive	positive	strong positive
BROADCOM	strong positive	positive	positive	positive	positive
CLOUDENTITY	strong positive	positive	positive	strong positive	positive
COFFEEBEAN	positive	positive	positive	neutral	neutral
ENTRUST DATACARD	strong positive	strong positive	strong positive	positive	positive
ERGON	positive	positive	strong positive	neutral	positive
EVIDIAN	positive	positive	strong positive	neutral	positive
FORGEROCK	strong positive	strong positive	strong positive	strong positive	positive
IBM	strong positive	positive	strong positive	positive	positive
IOVATION	strong positive	positive	neutral	neutral	positive
LOGINRADIUS	positive	positive	strong positive	positive	positive
MICROSOFT	positive	neutral	positive	neutral	positive
NOK NOK LABS	positive	positive	positive	positive	positive
NRI	positive	neutral	strong positive	neutral	neutral
PING IDENTITY	strong positive	strong positive	positive	strong positive	positive
PIREAN	strong positive	positive	positive	positive	positive
SAP	neutral	neutral	strong positive	neutral	positive
SECUREAUTH	strong positive	strong positive	strong positive	positive	strong positive
WSO2	positive	positive	positive	positive	neutral

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
ADNOVUM	strong positive	weak	strong positive	weak
AKAMAI	positive	strong positive	strong positive	strong positive
AUTH0	positive	strong positive	positive	positive
BROADCOM	neutral	positive	strong positive	positive
CLOUDENTITY	strong positive	weak	neutral	weak
COFFEEBEAN	positive	weak	weak	weak
ENTRUST DATACARD	strong positive	positive	strong positive	positive
ERGON	neutral	weak	strong positive	weak
EVIDIAN	neutral	neutral	strong positive	neutral
FORGEROCK	strong positive	strong positive	positive	strong positive
IBM	strong positive	strong positive	strong positive	strong positive
IOVATION	positive	positive	strong positive	weak
LOGINRADIUS	positive	strong positive	positive	positive
MICROSOFT	weak	strong positive	strong positive	strong positive
NOK NOK LABS	neutral	neutral	weak	Weak
NRI	neutral	weak	positive	Weak
PING IDENTITY	strong positive	strong positive	strong positive	positive
PIREAN	strong positive	neutral	positive	neutral
SAP	neutral	strong positive	strong positive	strong positive
SECUREAUTH	strong positive	neutral	positive	neutral
WSO2	positive	neutral	positive	positive

Table 2: Comparative overview of the ratings for vendors

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.

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 Consumer Authentication, we look at the following six areas:

APIs	APIs are increasingly available in consumer authentication solutions to provide tie-ins to existing IAM or IDaaS infrastructure, as well as to security services and external analytics solutions.
Authenticators	Types of authenticators supported, such as FIDO, MFA, SDKs, social logins.
Fraud/Threat Intel	Capability to consume and utilize 3rd-party fraud, threat, and compromised credential intelligence. Some vendors generate their own intelligence, based on activities within their own networks and client base. Generally, in-network intelligence concerns credentials that have been compromised within the vendor's ecosystem.
Mobile Security	Since most emphasis on consumer authentication is in the mobile area, this factor quantifies the use of mobile app security features; specifically, providing secure SDKs for mobile app development, Global Platform Secure Element / Trusted Execution Environment (SE/TEE) for Android devices and Secure Enclave for iOS devices. Some vendors utilize mobile app hardening services and mobile threat analytics to raise the assurance level for their customers.
Risk Analytics	Evaluation of user attributes behavioral analysis, environmental factors, fraud/threat intelligence, and other information to determine authentication and authorization levels required per transaction.

Scalability	Some solutions have massive scalability while others do not. Picking the right size vendor is an important consideration in RFPs. Not everyone needs the biggest and most scalable solutions. But if your business does, then understanding the scalability comparison and factors examined will be of paramount interest. The most scalable solutions are usually those which are based on micro-services architectures. Most are cloud-hosted, with the ability to spin-up and wind down additional virtual server instances to serve rapid increases in demand. This rating is influenced by many factors including number of customers, consumers, deployment models, multi-cloud utilization, geographic distribution, SLAs, and maximum number logins per second.

The spider graphs provide comparative 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 Consumer Authentication.

5.1 AdNovum NEVIS Suite

AdNovum was founded in 1988 in Switzerland. They have expanded around Europe and to Singapore as well. nevisAuth is a separately licensable product within the NEVIS Security Suite which includes components for complete IAM, IGA, and WAF. AdNovum's customer base is primarily in the DACH region, where they focus on medium to large enterprise customers, particularly in finance and insurance. Product is mostly deployed on-premises, but AdNovum hosts some single-tenant instances for some customers.

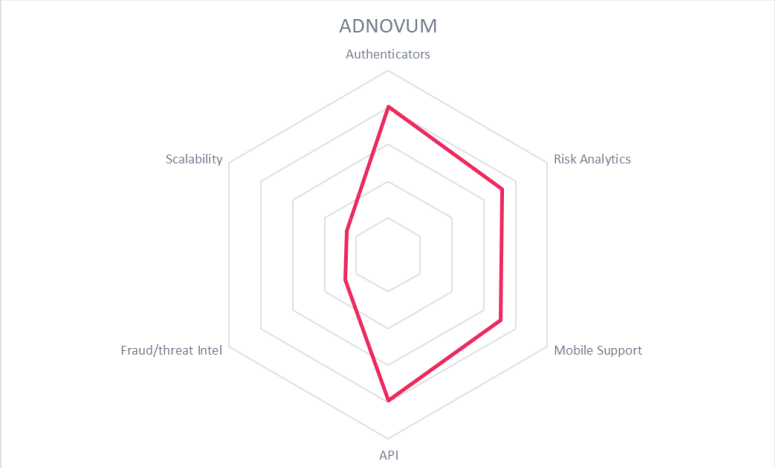
Strengths	Challenges
• Excellent selection of strong MFA mechanisms • High security solutions for finance, government, and insurance industries • Hardened mobile app and SDK	• Small customer base mostly localized in EU • Other than Arxan mobile analytics add-on, no 3rd-party threat intelligence consumption • Not available as SaaS

Table 3: AdNovum's major strengths and challenges

NEVIS supports many authentication mechanisms including Authy, FIDO UAF 1.1 face/fingerprint biometrics for both Android and iOS, BehavioSec for behavioral analytics and authentication, KBA, Kerberos, email/SMS OTP, Google Authenticator, mobile push notifications, SuisseID, VASCO tokens, and x.509. NEVIS also contains a FIDO UAF 1.1 Server. Mobile apps and SDK utilize SE/TEE or Secure Enclave. nevisAuth can accept social logins. SAML, OAuth, and OIDC are supported for federation and authorization. NEVIS provides a wide variety of account recovery options.

Administrators can create risk-based authentication policies which can require evaluation of device fingerprint/health/type, geo-location and geo-velocity, HTTP headers, IP address, and user and resource attributes. Extensive mobile security analytics are available as an add-on through Arxan. Risk factors can be weighted. Different actions can be required based on the outcome of the evaluation. At present, the solution does not integrate with 3rd-party cyber threat intelligence or compromised credential intelligence.

AdNovum can send event data to SIEM solutions. The risk engine is addressable via the REST API. nevisIDM or LDAP can serve as the user data repository.



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

Table 4: AdNovum's rating

AdNovum is a privately-owned Swiss IT company specializing in IT and security projects and has a strong DACH regional presence. The NEVIS product has excellent authentication options. Its risk analysis engine is more than adequate but would benefit from integration with additional 3rd party intelligence providers.

5.2 Akamai Identity Cloud (formerly Janrain)

Janrain was acquired by Akamai in early 2019. Janrain was launched in 2002 to provide user management and login capabilities for the social media market. Today the company has many large enterprise clients around the world serving 1.7 billion consumers across many sectors, including retail, entertainment, health, pharmaceutical, and finance. The Akamai suite of solutions is offered as a cloud-native multi-tenant service. Licensing is per managed user annually.

Strengths	Challenges
• Large enterprise customer base • 35+ social login types supported • Many security certifications • Impressive 99.998% uptime • Tight integration with Akamai security solutions	• No FIDO U2F/UAF/2.0 support • More authentication choices would be useful • Risk engine doesn't support device health assessments

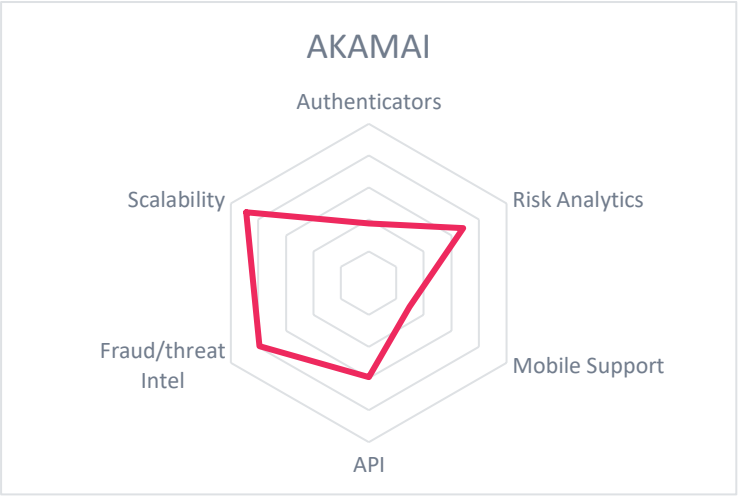
Table 5: Akamai's major strengths and challenges

Janrain was the pioneer in social network integration. Besides OIDC-based social and traditional logins, Akamai also supports these authentication and federation methods: mobile apps/biometrics, OAuth, SAML, and SMS OTP authentication. Akamai supports LDAP and SCIM for bulk import. An SDK which leverages SE/TEE and Secure Enclave allows customers to develop their own secure mobile apps.

The Akamai service has a robust risk engine which processes device fingerprint/history, geo-location and geo-velocity, IPs, and user attributes and history. Akamai Identity Cloud uses internal threat intelligence and compromised credential intelligence (Akamai IP Reputation) and Akamai's Bot Manager and Kona Site Defender to protect consumer accounts from fraud and identity theft. The solution can be extended with identity vetting service integration. The risk engine is configurable and addressable over APIs. External SIEM connections are possible, as is delegated administration. Akamai is ISO 27001:2013, ISO 27018:2014, SOC Type 2, HIPAA/HITECH, CSA Star Type 2, TRUSTe, and US-EU Privacy Shield certified.

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

Table 6: Akamai's rating



Akamai has quickly integrated Janrain's Identity Cloud into their service suite. The tie-ins with other Akamai products, particularly Bot Manager, IP Reputation, and Kona Site Defender, makes the Identity Cloud solution very appealing especially to finance, health care, retail, and media customers. Multiple security certifications and demonstrated high uptime show that Akamai Identity Cloud is mature and highly scalable, and thus should be seriously considered by organizations that need highly available and secure consumer authentication services.

5.3 Auth0

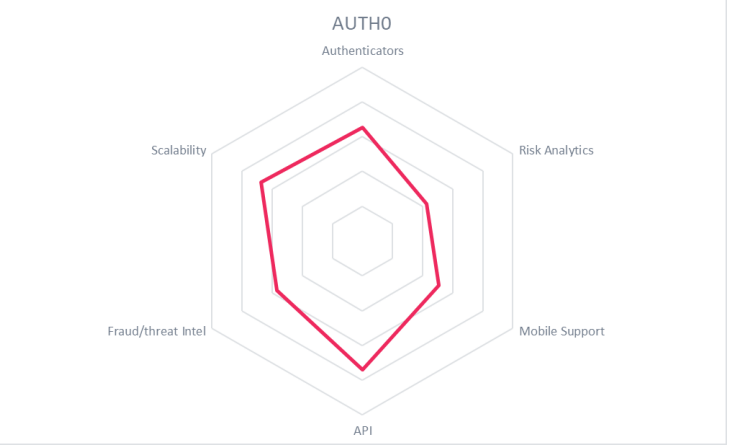
Bellevue, WA based Auth0 is a rapidly growing B2B, CIAM and B2E IAM solution provider. Founded in 2013, they have been pioneering API-driven identity services. Auth0 targets developers and provides code samples for developers to use in order to quickly build CIAM solutions, or to connect identity services to existing customer/consumer-facing applications. Auth0's services are cloud-hosted, with public or private options available. Auth0 licensing is based on active users per month.

Strengths	Challenges
• API-driven authentication services • Code snippets for copy-and-paste authentication services • Anomaly and breached password detection add-ons available • Rapid deployment	• Requires some coding expertise • Android apps don't use Global Platform SE/TEE • Risk engine is coarse-grained and lacks some device intelligence features • Risk engine not accessible via API

Table 7: Auth0's major strengths and challenges

Auth0 supports Duo, FIDO U2F, Google Authenticator, KBA, mobile apps/biometrics/push notifications/SDK, Mobile Connect, OIDC, OTP, SAML, social logins, and Yubikeys as authentication methods. Additional FIDO methods can be integrated with custom coding. Customer administrators can use MFA and set up delegated or role-based administration. Users can be provisioned in by LDAP or SCIM. Anomaly and Breached Password protection are elective services that Auth0 provides for better security. Auth0 offers email-based account recovery, but other options can be configured.

Risk factors that can be evaluated include geo-location/velocity, IP, user-agent, attributes, and history. Device health/reputation is not currently considered by the risk engine. Such sources can be developed and configured by clients as needed.



Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	strong positive

Table 8: Auth0's rating

Auth0 is a well-funded, high-revenue startup experiencing enormous growth. They identified a previously untapped audience in IAM: developers. They emphasize providing consumer authentication service through well-documented APIs. Auth0's successful business model challenges traditional IAM and CIAM delivery models. Auth0 is a strong contender in the consumer authentication space, especially for organizations that need quick-to-deploy solutions and those that have programming expertise alongside major consumer-facing applications should strongly consider Auth0 when doing RFPs.

5.4 Broadcom (formerly CA Technologies) Layer 7 Authentication

Well known for enterprise IAM, Broadcom's tightly integrated suite is also used for B2C authentication. Broadcom is promoting the legacy Layer 7 brand name for IAM solutions. The product is on-premise only and runs on Red Hat or SUSE Linux or Windows Servers. The Rapid App Security add-on provides a single SDK for authentication and connections to Layer7 Mobile API Gateway.

Strengths	Challenges
• Many strong authentication options • Robust risk engine for Consumer Authentication • Rapid App Security SDK and Mobile API Gateway integration	• Mobile app/SDK not built on SE/TEE • Cannot enforce MFA for admins • In-network threat intel bundled, but 3rd-party threat intelligence sources require customization

Table 9: Broadcom's major strengths and challenges

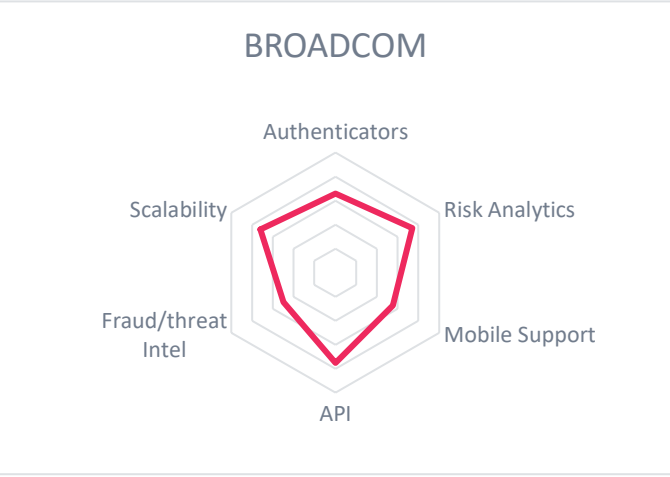
For authentication, Broadcom accepts FIDO, KBA, Mobile Push, OATH, Yubikeys, Google Authenticator, social logins, and native Apple and Samsung biometrics. Several 3rd-party authenticators interoperate with the platform. OAuth, OIDC, and SAML protocols are supported. KBA, Mobile Push, and `OTP are Broadcom's account recovery mechanisms.

The risk engine analyzes up to 200 different risk factors, including detailed device fingerprint and history, geo-location and geo-velocity, user attributes and behavioral profiling, root/jailbreak checks, and IMEI and SIM serial numbers on mobile devices. The management interface is intuitive and features a drop-down list style policy building tool. Different authentication methods and actions can be triggered based on very granular risk scores. Risk factors cannot be individually weighted. Third-party threat and fraud intelligence sources can be consumed via APIs but requires customization.

LDAP but not SCIM interfaces are available for provisioning. The product integrates with SIEM via syslog. Role-based and delegated administration models are supported.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 10: Broadcom's rating



Broadcom's Layer7 Authentication is widely deployed and highly scalable. Tight integration with other Broadcom products and good standards support enables it to fit well into complex IAM and CIAM deployments. The good selection of authenticators and granular risk engine make it suitable for environments where high security and authentication assurance is needed.

5.5 Cloudentity

Cloudentity is headquartered in Seattle. In 2014, Cloudentity parlayed their IAM expertise from Syntegrity into a full-featured CIAM and IDaaS solution. Their approach is cloud-first and a defining goal is scalability; thus, their offering is based on micro-services. 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 they offer a hosted service. Cloudentity has licensing options based on the number of micro-services used, rather than per-user.

Strengths	Challenges
• Micro-services architecture • Rapid deployments • API-driven consumer authentication platform • Integrated API gateway can share policies • Threat intel included in base service	• Small but growing North American customer base and support ecosystem • Admin UI and documentation needs improvement • Mobile apps for Android don't support SE/TEE

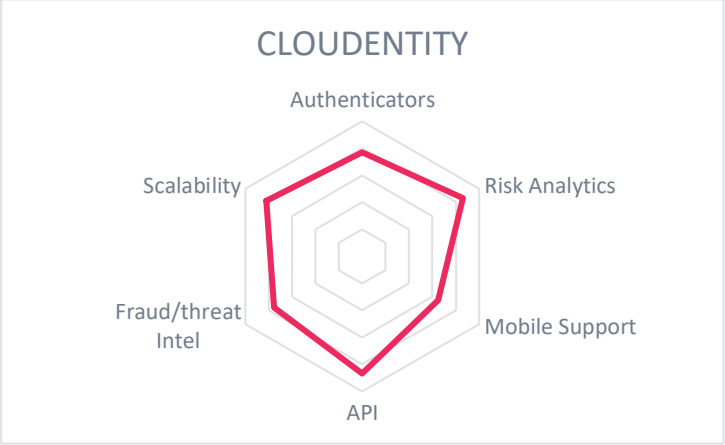
Table 11: Cloudentity's major strengths and challenges

For authentication and federation, Cloudentity supports FIDO UAF and 2.0/WebAuthN, Google Authenticator, JWT claims, KBA, mobile apps/push notifications/SDK, OIDC and social logins, OAuth, TOTP, and SAML. Cloudentity offers an SDK for mobile app development. Cloudentity's risk-adaptive micro-service provides comprehensive authentication, authorization and registration through policy management. APIs/SDKs are available for providing access control for micro-segmentation to extending permissions to API endpoints. LDAP and SCIM interfaces are available for provisioning. The product integrates with SIEM via Kafka, REST, or syslog. Users can recover accounts using alternate registered authenticators, proof-of-possession workflows or other initiated backchannel means.

Cloudentity's risk engine can consider IP, geo-location/velocity, device fingerprint/health/history/type, and user attributes/history. It can process external intelligence from Cylance, Crowdstrike, Imperva, RSA, and Secureworks. The fine-grained risk engine is addressable via API.

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

Table 12: Cloudentity's rating



Cloudentity represents the newest approach in IAM and CIAM; that is, making all services available via APIs. Cloudentity's micro-services architecture allows surge scalability across hybrid environments, and SecDevOps for secure deployments. Their customer base and support ecosystem are small and concentrated in the US but growing. Organizations that have a need to deploy and manage rapidly evolving infrastructures, or those that need controllable scalability should consider Cloudentity when shopping for consumer authentication solutions.

5.6 CoffeeBean Technology Identity and Access Platform

CoffeeBean started up in 2008 in California with a focus on increasing ROI in marketing solutions. They began developing their consumer identity and marketing solution in 2010. They are still privately held, but now have operations in Germany and a large development center in Brazil. CoffeeBean has a number of IT partners in various locations, but mostly in Brazil, for system integration and support for digital marketing. Licensing is a monthly fee based on number of contacts. CoffeeBean can be run on-premises, and they also host their solution as a SaaS for customers.

Strengths	Challenges
• FIDO U2F/UAF/2.0 clients and servers • Strong authentication for admins and consumers • One of few vendors actively engaged in South America	• Startup with small customer base • No SIEM connectors • Fraud/risk intel processing requires customization

Table 13: CoffeeBean's major strengths and challenges

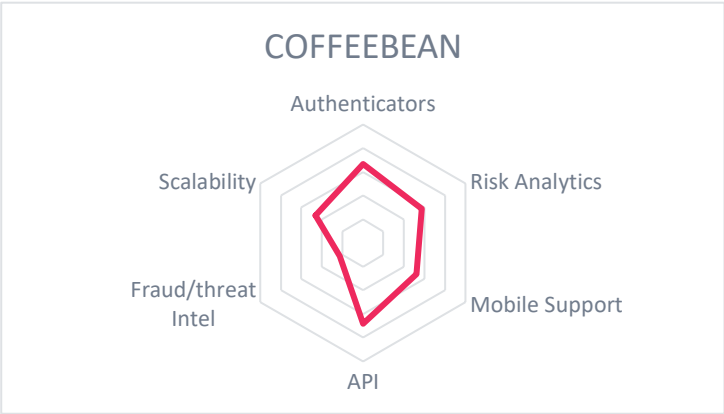
CoffeeBean's authentication options include Duo mobile, email/phone/SMS OTP, FIDO U2F/UAF/2.0, Google Authenticator, LastPass, and mobile apps, push, and biometrics; social logins including Facebook, Google, Instagram, LinkedIn, and Twitter. It is compatible with OAuth, OIDC, OpenID and SAML standards. CoffeeBean produces an SDK that customers can use for building mobile apps. LDAP or SCIM can be used for provisioning. Email, SMS, and WhatsApp can be used for account recovery.

In terms of risk factors, CoffeeBean can evaluate device fingerprint/history/type, geo-location and geo-velocity, IP, and user attributes and history. The risk engine can be customized to allow consumption of 3rd-party fraud/threat and KYC intelligence feeds. Risk engine outputs a granular risk score and is addressable via API.

The solution doesn't export data to SIEMs or security tools at present; nor does it support delegated administration.

Security	positive
Functionality	positive
Integration	positive
Interoperability	neutral
Usability	neutral

Table 14: CoffeeBean's rating



CoffeeBean is strongly focused on retail, hospitality, and finance industries. In addition to consumer authentication, CoffeeBean's solution integrates with on-premise captive Wi-Fi portals. Their presence in South America, both in terms of development center and sales target, is a plus for that region and for their own growth potential. CoffeeBean has rapidly added advanced functionality greatly improving its services and positioning. Companies that are looking for a consumer authentication solution that specializes in retail, hospitality, or finance, and who want to actively engage with consumers in shops should give CoffeeBean a look.

5.7 Entrust Datacard IntelliTrust / IdentityGuard

Entrust Datacard commands a large share of the global EMV market and has thousands of customers across the globe, serving millions of users, in both the B2C and B2E space. Entrust Datacard's IdentityGuard product is on-premises, IntelliTrust is SaaS; both provide the same functionality. Licensing is per-user or per-transaction.

Strengths	Challenges
• Large selection of secure authentication mechanisms • Sophisticated risk analytics engine • Integration with Cyber Threat Intelligence providers • Transaction Guard add-on service • Numerous security certifications	• No social login integration, although OIDC is supported • Splunk connector is available, but currently must export logs as .csv or use APIs to send to other SIEMs; syslog in work

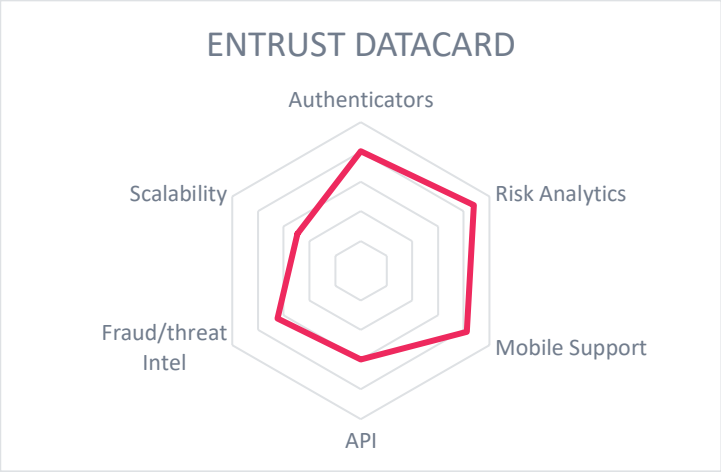
Table 15: Entrust Datacard's major strengths and weaknesses

Entrust Datacard supports a wide range of authenticators: biometrics such as MacOS X TouchID, FIDO U2F and 2.0, mobile apps/push notifications/SDK, OATH OTPs and tokens, and 3rd party authenticators including Feitian and Yubikey. Mobile apps/SDK leverage Global SE and TEE for Android, and Secure Enclave for iOS. OAuth, OIDC and SAML are supported for federation. Consumer accounts can have multiple strong authenticators registered, allowing for multiple secure account recovery options.

Entrust Datacard's risk engine can evaluate many risk factors, such as device fingerprint/health and history, geo-location, geo-velocity, IP, and user attributes/behavioral analysis. Admins can prioritize the factors in policies to require step-up authentication. The risk engine also can integrate with 3rd party fraud/risk intelligence sources such as iovation. Entrust Datacard also offers fraud reduction in Transaction Guard and mobile identity proofing and consumer onboarding services. The solution has API integration to Splunk or can send data as .csv to SIEM systems. It integrates with several MDM solutions. LDAP can be used for provisioning. SCIM will be supported in late 2019.

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

Table 16: Entrust Datacard's rating



Entrust Datacard has a feature-rich consumer authentication solution for either on-premise or SaaS. Social logins should be supported but are not, as the solution supports OIDC. The basic palette of services includes a large number of authenticators, an advanced risk engine, and industry-leading inclusion of cyber threat intelligence; optional services such as mobile ID proofing and Transaction Guard add real value. Entrust Datacard should be on the short list for organizations looking for secure consumer authentication capabilities.

5.8 Ergon Informatik Airlock

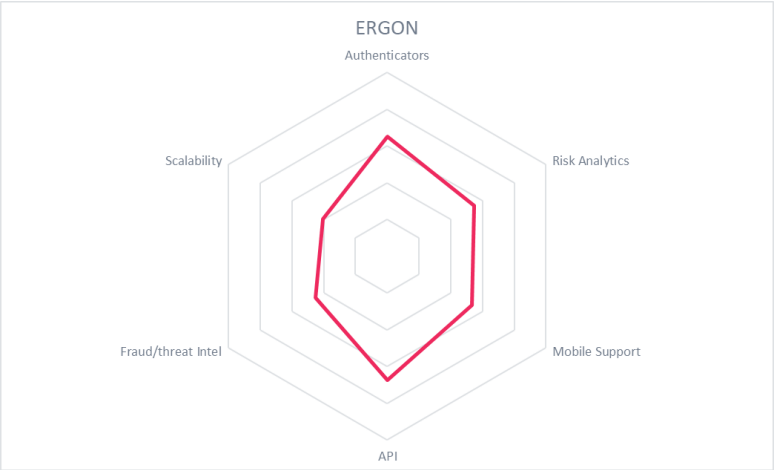
Ergon Informatik, maker of the Airlock Secure Access Hub, was founded in 1984 in Zurich. It is an employee-owned company with a strong history of providing IAM solutions in Europe to customers in a variety of industries, including finance. Hundreds of clients use Airlock Secure Access Hub to protect thousands of applications and millions of consumer identities. Licensing is an annual fee based on users and/or systems. It is available for on-premises deployment or in partner-hosted SaaS.

Strengths	Challenges
• Support for some specialty 3rd-party credentials • Integrated WAF • Threat intelligence and analysis included • Excellent account recovery options	• Risk engine doesn't support device health or history and is not accessible by developers • Customer base mostly localized in EU • Mobile SDK coming in November 2019 • FIDO not supported

Table 17: Ergon's major strengths and challenges

Ergon Airlock accepts the following consumer authentication types: CrontoPush (mobile push app), Google Authenticator, Grid cards, Kobil AST Suite, Kobil SecOVID, Mobile Signature Service ID, mTAN SMS, SMS OTP, social logins, Swiss Mobile ID, and Yubikeys. They partner with others for mobile apps and an SDK which can use SE/TEE for Android and Secure Enclave for iOS. OAuth, OIDC, and SAML are supported for federation. LDAP can be used for bulk provisioning. Multiple authenticators can be tied to a single account, providing multiple options for account recovery.

Ergon also supports policy-based adaptive authentication and transaction authorization. The risk engine can evaluate Airlock WAF fingerprint, browser fingerprint, device ID, geo-location, geo-velocity, IP address/reputation, SSO cookies, time/date, and user attributes/history. The risk engine is extensible and can be customized to process additional risk factors from Cronto and VASCO. Webroot threat intelligence is included in the base service; IBM Trusteer interoperability is available OOTB. Risk factors cannot be independently weighted and the engine itself is not addressable via API. User and WAF management functions are exposed through APIs.



Airlock can send data to SIEMs using CEF, ELK, syslog, and some custom connectors.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	neutral
Usability	positive

Table 18: Ergon's rating

Ergon has a somewhat smaller market share, localized mostly in Switzerland, but is expanding in the DACH region. Airlock supports some regional credentials, and the risk engine has been enhanced in the last year. Integration of threat intelligence is a plus. A mobile SDK and support for FIDO would be

beneficial. European enterprises seeking consumer authentication solutions with a bundled WAF for consumer application protection should take a look at Ergon Airlock Suite.

5.9 Evidian Web Access Manager

Evidian is a division of Atos, a large European IT service provider. The company provides a comprehensive portfolio in the area of IAM, as well as e-commerce, supply chain, and CRM support. Their WAM product contains the essential consumer authentication capabilities. It is integrated with other Evidian solutions in Identity Provisioning, Governance, and Enterprise Single Sign-On. It can be deployed on-premises or in IaaS, but they do not host it as multi-tenant SaaS (planned for 2020).

Strengths	Challenges
• Accepts many types of strong authenticators • Detailed browser and device "fingerprinting" for risk analysis • Secure mobile SDK	• FIDO support coming later in 2019 • Cannot compute geo-velocity as a risk factor • No OOTB connectors for fraud/threat intel

Table 19: Evidian's major strengths and challenges

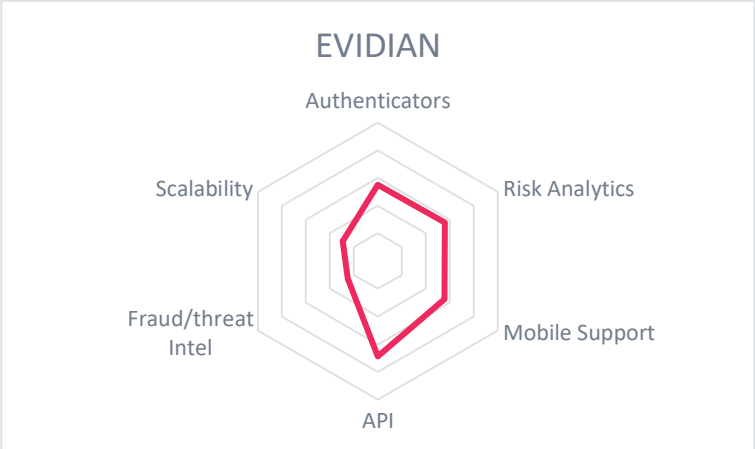
Evidian Web Access Manager is a mature solution for Consumer Authentication. It runs on various Linux, UNIX, and Windows Server versions. The product supports many authentication mechanisms, such as email/SMS OTP, Kerberos, mobile push, and social logins, as well as non-standard forms such as QR codes and grid cards. Their mobile SDK supports SE/TEE and Secure Enclave for Android and iOS. Support for FIDO authentication is planned for later in 2019.

The risk engine can evaluate many risk factors, such as browser and device fingerprints (but not device health), geo-location, IP address, and user attributes and history. Advanced user behavioral analysis is not available in the product yet. The product can be customized to accept risk scores from generated by 3rd-party intelligence sources. The risk engine performs coarse-grained scoring; admins can prioritize risk factors and choose assurance levels appropriate to requested resources.

Evidian's solution can provide data to SIEM via REST APIs. It works in conjunction with its own Identity Governance product. Evidian supports OAuth, OIDC, and SAML for federation to WAM or SaaS systems. It does not support delegated admin models explicitly.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	neutral
Usability	positive

Table 20: Evidian's rating



Evidian delivers a respectable offering in the area of adaptive authentication, particularly with a focus on accepting strong, two-factor authenticators for high assurance use cases. An increased

focus on APIs and FIDO support are planned in the next year. Built-in fraud/threat intelligence connectors and tweaks to the risk engine would strengthen the product.

5.10 ForgeRock Identity Platform

ForgeRock is a leading, venture-backed IAM vendor, headquartered in the US but with many offices around the world. ForgeRock supports most major IAM standards and is a significant contributor to several international standards organizations. Their Identity Platform serves both B2E and B2C markets. ForgeRock provides the tools that their clients can use to build robust consumer authentication deployments either on their own premises or in IaaS. A PaaS version is now available for developers.

Strengths	Challenges
• Very scalable • Wide array of authentication methods • Intelligent Authentication / AuthN Trees • Highly extensible to meet most any consumer authentication requirement	• Open Banking Sandbox is available as SaaS, but full authentication solution is not yet • No mobile SDK • Account recovery techniques are slated to be improved

Table 21: ForgeRock's major strengths and challenges

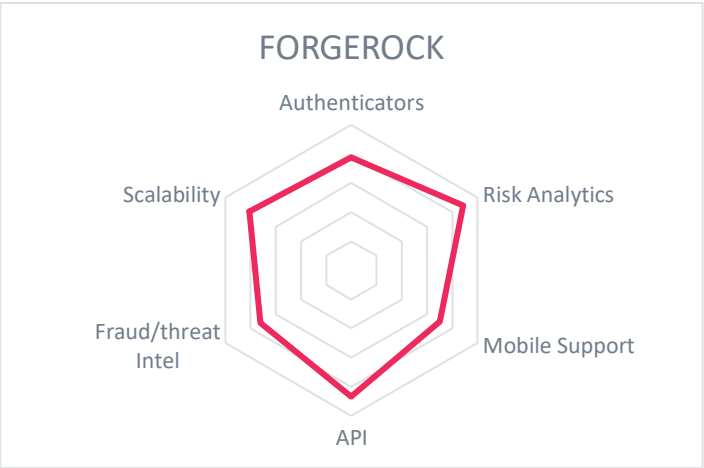
ForgeRock Identity Platform provides numerous choices for how consumers can authenticate using email/phone/SMS OTP, FIDO UAF/U2F/2.0, KBA, mobile apps/push notifications, Mobile Connect, OATH, and social logins. It supports OAuth, OIDC, and SAML for federation. CAPTCHA, email, and KBA can be used to reset usernames and passwords.

Identity Platform's risk engine can evaluate device fingerprints and type, geo-location and geo-velocity (customization needed), IP, and user attributes/history. It can be configured to consume any 3rd-party threat intelligence source, and connectors are available for 4IQ, Exabeam, ThreatMetrix, and VeriClouds. ForgeRock Identity Platform features an intuitive, flow-chart-based policy authoring tool called Intelligent Authentication. Authentication Trees allow customer admins to flexibly create policies in the GUI that meet the levels of assurance needed for sophisticated use cases. The details of designing complex, risk-adaptive authentication and authorization rules are abstracted by the interface. In the latest release, ForgeRock has introduced Registration Trees, which allows businesses to set up customizable registration flows, similar to Authentication Trees.

Identity Platform supports role-based and delegated administration. Identity Platform interoperates via standard protocols with just about any other security or identity infrastructure, including IGA, PAM, and SIEM solutions.

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

Table 22: ForgeRock's rating



ForgeRock Identity Platform serves hundreds of millions of consumers across hundreds of customers. With its support

for many authenticators, Authentication Trees policy builder, and configurable risk engine, ForgeRock Identity Platform should be on the short list for organizations looking for consumer authentication solutions.

5.11 IBM Cloud Identity

Cloud Identity is IBM's consumer authentication service, composed of the Trusteer Management Agent, Pinpoint Detect, Verify, Mobile SDK, and Rule Engine. IBM hosts Cloud Identity as a multi-tenant SaaS. The solution is based on a micro-services architecture. Licensing is per session, which can include login and various actions and transactions.

Strengths	Challenges
• Excellent administrative security • Large number of authentication options • Trusteer for built-in fraud reduction • FIDO 2.0 certification	• Obtaining threat and fraud intelligence outside of Trusteer requires customization • Account recovery options require customized development • Federation support requires add-ons

Table 23: IBM's major strengths and challenges

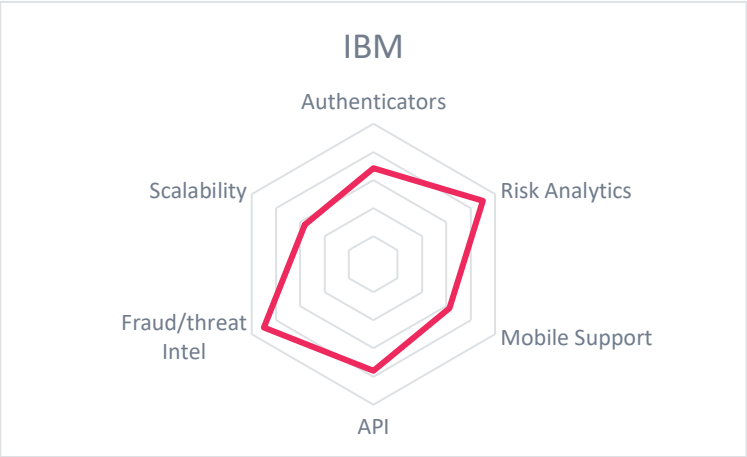
IBM provides self-registration and profile management features, and accepts a wide array of authenticators, including email/SMS OTP, FIDO U2F and 2.0, mobile apps/biometrics/push notifications, QR codes, social logins, and 3rd-party mechanisms via IBM Security App Exchange. Mobile apps and SDK use SE/TEE on Android and Secure Enclave on iOS for high security. It supports OIDC, OAuth, SAML, WS-Federation, and WS-Trust via add-ons. For provisioning, LDAP but not SCIM interfaces are available. Developers can access APIs to build account recovery mechanisms.

Cloud Identity integrates well with other IBM solutions in the Identity Governance, Security, and enterprise business application space. Cloud Identity also integrates with IBM's QRadar SIEM. Pinpoint Detect is the risk engine that processes device fingerprint/health/history, geo-location and geo-velocity, IP, and user attributes and history. Threat intelligence is provided by IBM Trusteer, which is backed up by IBM X-Force for deep threat analysis. It can interoperate with various 3rd-party identity proofing services.

Cloud Identity customers can delegate admin responsibilities and enforce MFA for administrators. Cloud Identity is FFIEC and SOC2 Type 2 certified.

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

Table 24: IBM's rating



IBM Cloud Identity is an advanced and highly integrated suite of solutions capable of meeting the most stringent security requirements. Organizations that are performing RFPs for consumer authentication services should fully evaluate Cloud Identity's extensive list of technical capabilities.

5.12 iovation

Portland, OR based iovation was founded in 2004. It was acquired by TransUnion in mid-2018. The company provides an integrated MFA and fraud reduction solution. iovation's SaaS intelligence services are used by many CIAM and IDaaS vendors as well as IAM operators. For consumer authentication, four services are available: ClearKey, LaunchKey, FraudForce, and SureScore. FraudForce and SureScore are licensed by transaction volume, and ClearKey and LaunchKey can be licensed per user.

Strengths	Challenges
• Industry-leading device intelligence service • Mobile SDK provides many biometric options • Excellent risk analysis • Massively scalable services • FraudForce, SureScore and ClearKey share a common API for authentication requests	• Lacking major IAM protocol support: FIDO, LDAP, OATH, OAuth, OIDC, SAML, and SCIM • Services not bundled for easy acquisition and licensing • No SIEM integration

Table 25: iovation's major strengths and challenges

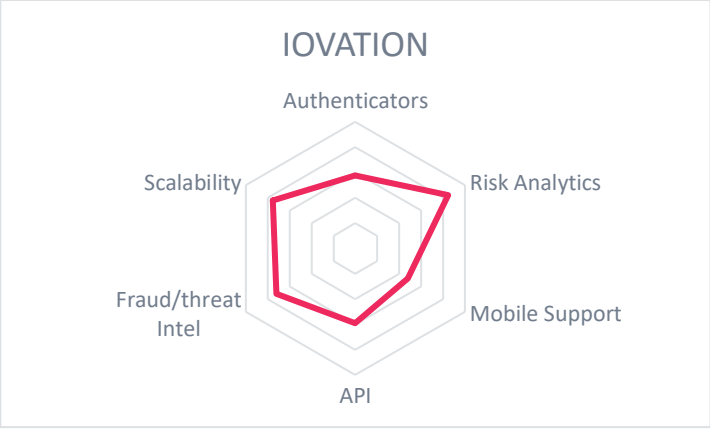
ClearKey provides basic device recognition and fraud indicator collection. LaunchKey supports KBA and provides mobile apps and an SDK that allows for the following methods: facial and fingerprint recognition, PIN, circle code, device factors, and wearable factors. All credentials are stored locally on the user's device. Mobile apps and SDK utilize mobile encryption. iovation does not support FIDO, OATH, OAuth, OIDC, and SAML currently. Consumer accounts are not provisioned by LDAP or SCIM.

The sophisticated risk engine can evaluate botnet activity, device fingerprints/health/history, geo-location and geo-velocity, IPs, root detection, transaction history, and user behavioral analysis. TransUnion's Identity Verification service is a valuable ID proofing option. It can also consume external fraud and threat intelligence from sources such as Cyren and Neustar. Customer admins can create very detailed authentication policies. The risk engine is highly configurable and addressable via API.

iovation is SOC2 and Privacy Shield certified. iovation supports role-based and delegated administration. Event data cannot be sent to SIEM or other security.

Security	strong positive
Functionality	positive
Integration	neutral
Interoperability	neutral
Usability	positive

Table 26: iovation's rating



iovation is a leading provider of high-quality threat intelligence to other IAM, CIAM, and IDaaS vendors. They also offer very robust and innovative consumer authentication services but are missing support for key IAM protocols. A mix of iovation services are required to deploy a full consumer authentication solution. Better packaging of these services would help iovation gain even more market share. iovation should be in the running for consumer authentication services RFPs and should be considered as an augmenting intelligence source for existing CIAM and IDaaS deployments.

5.13 LoginRadius Identity Platform

Established in 2011, LoginRadius is a VC-backed CIAM vendor based in Vancouver, Canada. The company provides consumer authentication services for enterprises around the world and has over 1 billion consumer identities under management. LoginRadius Identity Platform is primarily SaaS but can host in customers' private clouds and IaaS. Multiple licensing models are available, including annual or monthly fees based on registered or active users, plus service options.

Strengths	Challenges
• Many privacy and security certifications • Large customer base • MFA options for admins • FIDO 2.0 support	• Focused on high transaction volume customers • No device health assessment capability • Somewhat weak account recovery methods

Table 27: LoginRadius' major strengths and challenges

LoginRadius thus allows social logins from any OIDC-conformant identity provider. Other authentication mechanisms supported include Authy, FIDO U2F/UAF/2.0, Google Authenticator, mobile apps/biometrics/push notifications, Mobile Connect, and SMS OTP. Mobile apps and SDK utilize SE/TEE for Android and Secure Enclave for iOS. Users can be provisioned using LDAP or SCIM. KBA and OTP are available for account recovery.

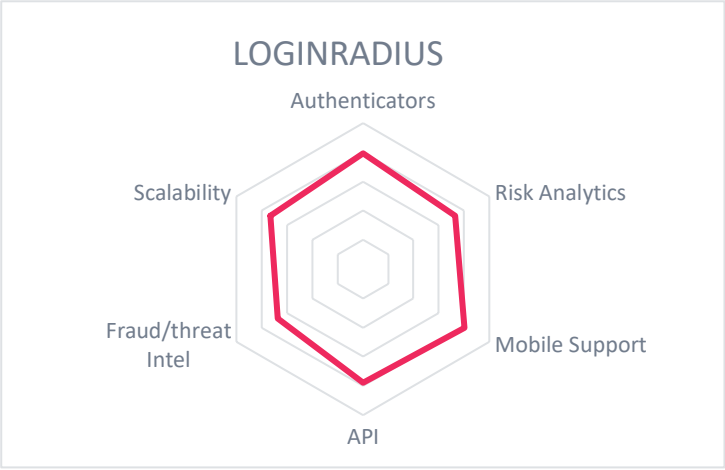
The risk engine can process device fingerprints/history, geo-location and geo-velocity, IPs, user attributes and history. It can also consume external fraud and threat intelligence from sources such as ThreatMetrix. Customer admins can create fine-grained authentication policies. The risk engine is addressable via API.

LoginRadius has obtained a large number of security and privacy certifications including CSA Star Level 2, ISO-27001:2013, SOC2 - Type II, ISO 27017, ISO 27018, NIST CSF Cyber Security Framework, US-EU Privacy Shield, and US-Swiss Privacy Shield.

LoginRadius supports role-based and delegated administration. Event data can be sent to SIEM or other security and identity analytics solutions.

Security	positive
Functionality	positive
Integration	strong positive
Interoperability	positive
Usability	positive

Table 28: LoginRadius' rating



LoginRadius' target market has evolved from SMBs to enterprises. Recent enhancements, especially the addition of stronger MFA methods such as FIDO 2.0 has positioned them to expand their market reach considerably. LoginRadius' service is global and is also highly scalable. Overall, the LoginRadius continues to increase its CIAM market share and deserves evaluation in consumer authentication RFPs.

5.14 Microsoft Azure Active Directory B2C

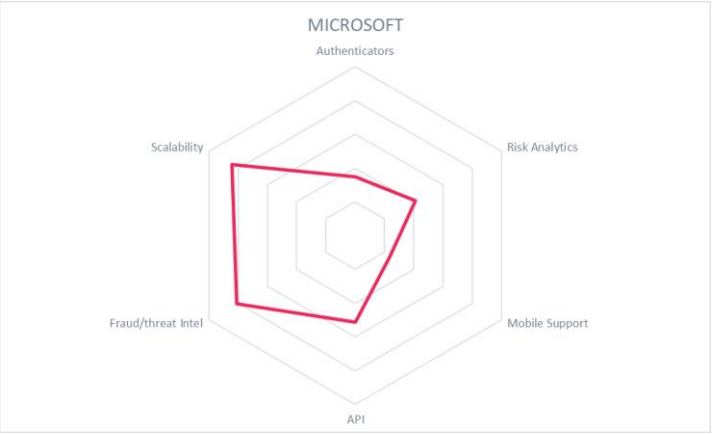
Microsoft Azure Active Directory B2C is a cloud-based identity and access management service focused on facilitating business to consumer applications. Built upon Microsoft Azure AD, the B2C offering is architected to scale and perform well with hundreds of millions of users and over one billion logins per day. Azure is one of the global leaders in the cloud infrastructure market, second only to Amazon's AWS. It is licensed by number of authentication events.

Strengths	Challenges
• Strong attack detection through robust cyber threat intelligence network • Resilient against cyber attacks • Strong MFA for admins • Robust role and delegated access models supported • Extreme scalability	• Risk engine does not evaluate some critical factors, particularly device intelligence • Support for 3rd-party fraud/threat intelligence requires extensive configuration • Mobile app/SDK does not use SE/TEE/Secure Enclave

Table 29: Microsoft's major strengths and challenges

Microsoft Azure AD B2C accepts KBA, mobile app/push notifications, SMS OTP, and social login authentication. Additional MFA options are available through partners. Microsoft has a mobile SDK for app development, but it does not use Global Platform SE/TEE for Android or Secure Enclave on iOS. Support for FIDO 2.0/WebAuthn should arrive later in 2019. Azure AD B2C also accepts OAuth, OIDC, and SAML. Azure AD B2C does not support LDAP and SCIM for provisioning. Email/phone and help desk calls are supported for account recovery. Account linking can also be configured for more account recovery options.

Microsoft customers benefit from the rich and comprehensive threat intelligence, compromised credential, and account protection services that are built-in to the Azure AD B2C offering. Azure AD B2C can consume external fraud and threat intelligence, although extensive configuration is needed. The risk engine evaluates a limited set of factors such as geo-location, geo-velocity, IP, and user attributes; however key factors such as device fingerprint/health/history, and user behavioral analysis are missing. The risk engine itself is not accessible via API. Security event info can be sent to external SIEMs.



Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 30: Microsoft's rating

Microsoft Azure AD B2C has the scalability and performance to meet business requirements but lacks some advanced authenticator options and risk engine sophistication that are found in other solutions. Given Microsoft's commitment to cloud services, we expect it to mature in time.

5.15 Nok Nok Labs S3 Authentication Suite

Nok Nok Labs is a privately held, venture-backed US company based in Palo Alto, California. It was founded in 2012 and is centered on providing secure B2C and B2E authentication services. Nok Nok Labs was a founding member of the FIDO Alliance. The company has over 100 patents owned or filed worldwide. The solution can run on-premises on RHEL 7 or CentOS 7, in IaaS in Docker containers, or in their hosted SaaS. Licensing is based on per-user annual subscription fees.

Strengths	Challenges
• FIDO Universal Server (U2F/UAF/2.0) • Strong mobile security utilizing SE/TEE and Secure Enclave • Modular, pure-play authentication service	• Risk engine cannot evaluate device history and reputation or other 3rd-party threat intelligence feeds • No security certifications • No support for social logins

Table 31: Nok Nok Lab's major strengths and challenges

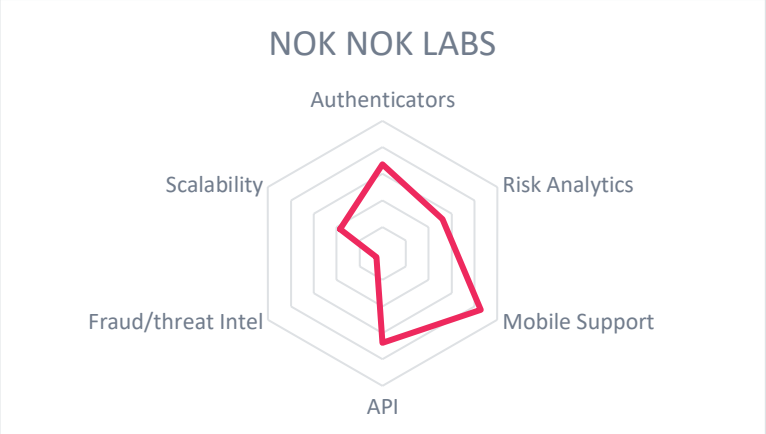
S3 Authentication Suite accepts Feitian tokens, FIDO U2F/UAF/2.0, Google Titan, mobile apps/push notifications, Mobile Connect, and Yubikeys. Nok Nok has a mobile SDK which utilizes SE/TEE for Android and Secure Enclave for iOS. S3 allows registration via FIDO but not LDAP or SCIM. It supports OAuth, OIDC, and SAML protocols. S3 has an account recovery platform that allows multiple registered authenticators per account.

S3 Authentication Suite has a risk engine which processes geo-location and geo-velocity, IP address, date/time, device fingerprint/health, and user attributes and history. Third-party behavioral biometrics, identity proofing services, and User Verification Index results can interoperate with S3; however, other external threat intelligence sources cannot be consumed at this time. The risk engine and its results are accessible via REST APIs. Admins can create flexible policies for step-up authentication or authorization.

S3 can export event data to SIEMs using Log4J appenders. The console allows for multiple admin roles and delegated administration.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 32: Nok Nok Lab's rating



Nok Nok Labs is focused on modernizing authentication. As a founding member of FIDO Alliance, Nok Nok has pioneered the implementation of all versions of FIDO specifications. With the exception of email/SMS OTP, authentication methods other than FIDO are mostly absent. The risk engine offers somewhat advanced functionality but needs to be able to intake 3rd-party threat intelligence sources. Organizations that want to offer consumers the latest passwordless technologies and can integrate with legacy dependencies should evaluate Nok Nok Labs S3 Authentication Suite.

5.16 NRI Secure Uni-ID Libra

NRI Secure Technologies, headquartered in Tokyo, provides security consulting and solutions. Uni-ID is their consumer authentication product, first developed in 2008 and relaunched as Uni-ID Libra in mid-2017. The product is licensed per named user and can be deployed on-premises or in IaaS. NRI also offers it as a hosted service in single-tenant mode.

Strengths	Challenges
• Large-scale deployments in leading Japanese auto, aviation, telecom, finance, and hospitality companies • Excellent IAM standards support • FIDO 2 Universal Server certified	• No sales or support presence outside of Japan • Mobile app SDK would benefit customers • Does not consume 3rd-party fraud or threat intelligence • Weak account recovery methods

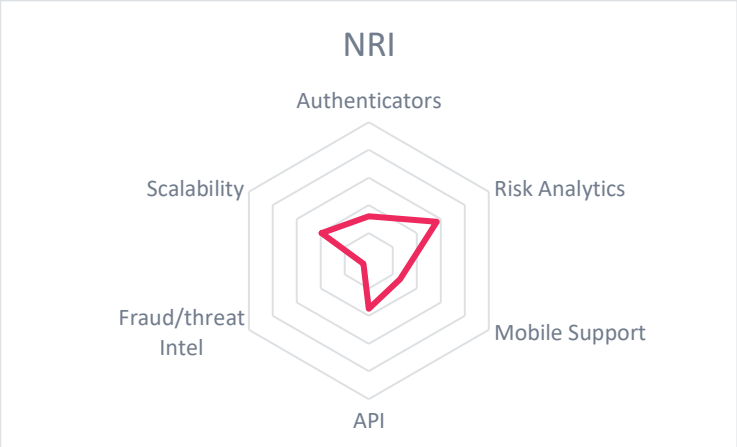
Table 33: NRI's major strengths and challenges

Uni-ID Libra accepts FIDO U2F/UAF/2.0, SMS OTP, and Facebook, Google, Slack, Yahoo Japan, Line, and Kakao Talk social logins. It supports OIDC and SAML. Admins can be required to use Google Authenticator for strong authentication. Consumers can self-register and can be provisioned from other systems using SCIM. LDAP is not supported currently. Email and help desk are the only supported account recovery methods.

Uni-ID Libra can interoperate with security tools such as Splunk and the ELK stack. The solution contains some risk-adaptive authentication capabilities, which include the evaluation of IP address device fingerprint, history, and type; geo-location and geo-velocity, and user behavioral analysis. The risk engine cannot be augmented with 3rd-party fraud or threat intelligence but does allow for compromised credential checks and brute-force password attack prevention.

Security	positive
Functionality	neutral
Integration	strong positive
Interoperability	neutral
Usability	neutral

Table 34: NRI's rating



NRI Uni-ID Libra has a mix of standard and advanced authentication options with some risk-adaptive features. They are almost exclusively focused on the Japanese market but have some very large customers deployments there. They have some customers with global deployments and have accordingly added GDPR compliant consent management features. NRI has significantly enhanced their product offering, as evidenced by the recent achievement of FIDO 2.0 certification. Adding MFA options, especially mobile authentication apps and SDKs that support biometrics would strengthen the solution. Organizations in Japan with consumer authentication needs should definitely consider NRI Uni-ID Libra.

5.17 Ping Identity

Ping Identity is a leading IAM and CIAM vendor, with a good reputation in identity federation and access management. PingFederate and PingID are their products for on-premise and hybrid consumer authentication deployments, while PingOne For Customers is their IDaaS offering. PingOne For Customers is licensed per active user, and PingFederate and PingID are licensed per managed user. Similar functionality is achieved regardless of the deployment model.

Strengths	Challenges
• Large selection of innovative MFA options • Excellent support for identity standards • OOTB threat intelligence integration • Sophisticated risk engine	• Some consumer authentication use cases require multiple Ping Identity products • FIDO 2 support requires PingFederate

Table 35: Ping Identity's major strengths and weaknesses

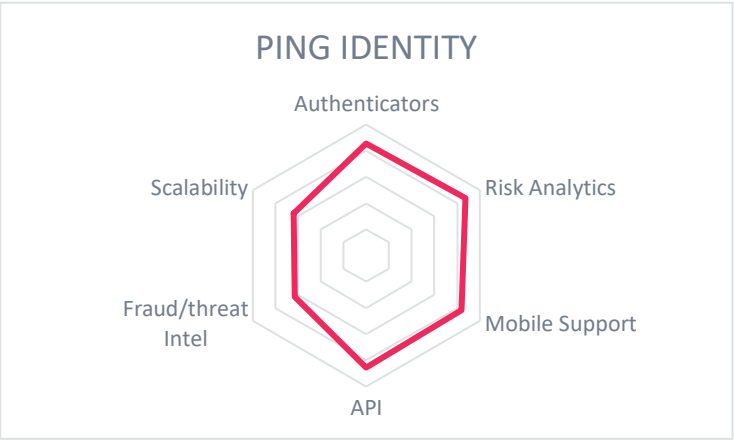
Ping Identity has developed and actively promoted passwordless authentication options for customers. PingID supports authentication methods such as Apple Watch, email/SMS/voice OTP, FIDO UAF biometrics (via partnership), mobile apps/push notifications, social logins, and Yubikey authentication mechanisms. Mobile apps run on both Android and iOS, using SE/TEE and Secure Enclave. They have a mobile SDK that allows customers to add MFA to their mobile apps. If used in conjunction with PingFederate, it can also support FIDO U2F/2.0 and all federation protocols. PingID integrates directly with Microsoft Active Directory Federation Server (ADFS) and Azure AD; and can use LDAP or SCIM for provisioning. Both Ping solution sets support multiple registered authenticators per account to facilitate account recovery.

The risk engine evaluates date/time, device fingerprint/health/history, geo-location and geo-velocity, IP address, root detection, and user attributes/history. Ping ID receives threat intelligence from ID Data Web, iovation, and ThreatMetrix. Threat intelligence may require additional licensing depending on source. Risk evaluation results are available via APIs.

Event data can be sent to SIEM over syslog. Role-based and delegated administration is supported.

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

Table 36: Ping Identity's rating



Ping Identity has strong support for IAM standards and excellent MFA variety. The risk engine has been greatly enhanced in the past year. For on-premise cases, combining relevant products into a single B2C package would help customers. Ping Identity products and services are mature and highly capable and should be considered for consumer authentication RFPs, particularly for companies that need customizability.

5.18 Pirean Access: One

Pirean was founded in 2002 with offices in London and Sydney. In 2018, Pirean was acquired by Exostar, an IAM and collaboration solutions provider for highly regulated industries such as Aerospace and Defense and Life Sciences. Pirean offers B2E and B2C IDaaS platform called Access: One. The product can be deployed either on-premises or in IaaS, and Pirean hosts it as a managed service. It is licensed by a measure of managed users, either monthly or annually. Modular design allows Authenticator-as-a-Service to be deployed without the full Access: One package.

Strengths	Challenges
• Large number of authenticators accepted • Excellently packaged discrete authentication service • Strong risk controls for high assurance environments • Well-designed REST API framework	• Currently small but expanding customer base and partner ecosystem • Limited visibility outside of UK, but growing • Scalability uncertain

Table 37: Pirean's major strengths and challenges

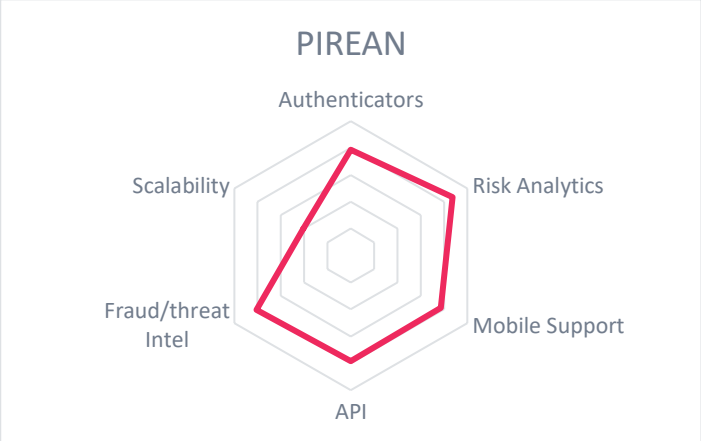
Pirean supports FIDO U2F/UAF/2.0, mobile apps and push notifications, Mobile Connect (via 3rd-party plug-in), native biometrics for Android and iOS, OATH TOTP, SMS OTP, and social logins for authentication. Apps and SDK use SE/TEE and Secure Enclave. It supports OAuth, OIDC, and SAML for federated authentication and authorization, and LDAP and SCIM for provisioning. API access is via JWT.

The risk engine is robust and can evaluate date/time, device fingerprint/health/history, geo-location and geo-velocity, IP address, root detection, and user attributes/history. Pirean supports STIX and TAXII, thus Access: One can be configured to query external services such as BAE Applied Intelligence, Experian Hunter, FireEye, IBM Trusteer, Palo Alto, ThreatMetrix for threat intelligence evaluation. APIs facilitate connections with identity vetting services. Admins can write flexible policies using a workflow interface.

Customers can send data to SIEMs over syslog or through OOTB connectors. The console supports role-based and delegated administration.

Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 38: Pirean's rating



Pirean's Access: One has a lot of advanced functionality in the mobile authentication and risk engine areas. Pirean is pushing the envelope with successful blockchain ID PoCs. Packaging Authenticator-as-a-Service enables rapid tech insertions. Customers needing high assurance consumer authentication with multiple fraud intelligence sources should carefully consider Pirean Access: One's capabilities.

5.19 SAP Customer Data Cloud

SAP Customer Data Cloud, formerly Gigya Identity Enterprise, is tightly integrated within the SAP platform. Their cloud-based service accommodates over 30 social logins and integrates with many SaaS vendors. Annual subscription licenses are based on the total number of contacts, which includes all unique records of customers, prospects, employees, and business partners.

Strengths	Challenges
• Large dedicated professional services team • High performance, supporting billions of consumer identities and tens of billions of transactions per month • Optional integration with identity vetting services • Tightly integrated with SAP HANA platform	• Strong authentication options needed • No support for FIDO • No OOTB integration with external threat intelligence • Licensing is by total number of contacts rather than active users • Weak account recovery methods

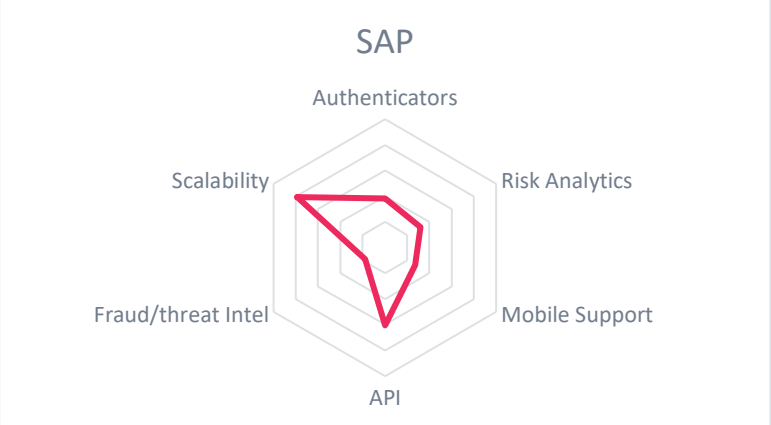
Table 39: SAP's major strengths and challenges

SAP supports OAuth, OIDC, and SAML. Consumers can authenticate with email/SMS OTP and Android/iOS biometrics. CAPTCHA can be used for step-up. SAP has OOTB integrations with Socure, Trulioo, and LexisNexis for identity verification. Network Protected Identity provides real-time analysis and alerting only on in-network credential compromises. It also has limited risk analytics capabilities, evaluating device IDs, IP addresses, locations, and blacklisted locations. Customer admins can configure 3rd-party threat intelligence consumption via APIs. FIDO authentication and other MFA options are not present yet. Email and KBA are the account recovery methods present.

SAP Customer Data Cloud has extensive password complexity and policy options available in the administrative interface. Customers can connect SAP Customer Data Cloud to external SIEMs using CEF or LEEF.

Security	neutral
Functionality	neutral
Integration	strong positive
Interoperability	neutral
Usability	positive

Table 40: SAP's rating



SAP has a global reach and continues to expand. Since the Gigya acquisition, SAP has made just a few significant improvements in the feature set as pertains to risk-adaptive consumer authentication. The solution needs stronger MFA options, particularly for mobile devices. The licensing scheme needs to be revamped. Organizations looking for SaaS-delivered consumer authentication solutions that don't require strong MFA options with granular risk controls may consider SAP Customer Data Cloud.

5.20 SecureAuth Identity Platform

SecureAuth merged with Core Security in late 2017 and then split away again in 2019. SecureAuth is known for high security solutions for B2E. SecureAuth Identity Platform is theirauthentication solution, which can be implemented as an appliance or virtual appliance or as SaaS service. The product is licensed annually per named user.

Strengths	Challenges
• Variety of MFA mechanisms supported, including some 3rd party biometrics • Broad support of federation and other IAM standards and protocols • Cyber threat intelligence integration • Large ecosystem of IAM partners	• No built-in directory currently, but can use any LDAP directory; self-contained directory on product roadmap • FIDO support planned

Table 41: SecureAuth's major strengths and challenges

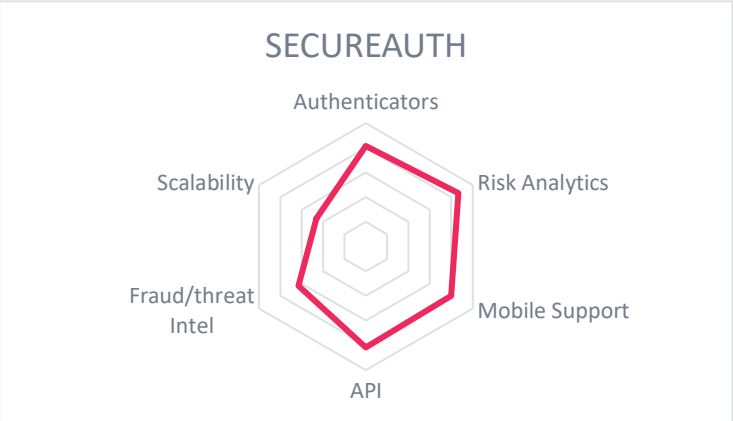
SecureAuth supports many forms of MFA: Android and iOS biometrics, behavioral biometrics, email/phone/SMS OTP, mobile apps protected in SE/TEE and Secure Enclave, mobile push notifications, OATH tokens, social logins, and Yubikeys. FIDO support is on the roadmap. It can integrate with identity repositories using LDAP, OIDC, and SAML. Any registered authenticator can serve as an account recovery mechanism, as well as KBA and help-desk resets.

The risk engine can evaluate device fingerprints/health, geo-location and geo-velocity, IPs, user attributes and behavioral analysis. SecureAuth Threat Service is a subscription service that provides threat intelligence to the risk engine for real-time fraud prevention and risk mitigation. SecureAuth Identity Platform can output granular risk scores for evaluation according to customizable policies allowing multiple actions. Fraud and threat intelligence from FireEye and NeuStar are integrated into Identity Platform's risk analysis.

It can also connect with any SIEM. They have achieved SOC2 Type 1 certification. Role and delegated administrative access models are supported.

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

Table 42: SecureAuth's rating



SecureAuth Identity Platform is a very strong product with its broad support of authenticators, granular risk engine, and threat intelligence utilization. Comprehensive FIDO support will make the solution even more compelling when it arrives. SecureAuth should be on the shortlist for any consumer authentication RFP, but especially for organizations needing high assurance and secure solutions.

5.21 WSO2 Identity Server

WSO2 was founded in 2005. They are an open source IAM/CIAM solution provider. Their emphasis is on providing identity services like authentication over APIs. The solution can be run on-premises, in IaaS, and they also offer a managed service capability. The product is licensed under the Apache 2.0 License and is supported under an annual subscription.

Strengths	Challenges
• Many pre-defined connectors for attribute providers and security services • Wide range of authenticators supported • Integrated adaptive risk engine • Strong IAM standards support • Extensible architecture • Open source code plus support model	• Risk engine does not process device health/history • No mobile SDK • No OOTB connectors for fraud/risk intelligence

Table 43: WSO2's major strengths and challenges

WSO2 Identity Server accepts email/SMS OTP, FIDO U2F, Google Authenticator, JWTs, Microsoft Authenticator, Mobile Connect, and social logins. They have connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, and others are in work. The solution does not have a mobile app or SDK. Identity Server also has a risk engine that can process device fingerprints and history, geo-location, geo-velocity, user attributes and behavioral analysis. Third-party intelligence can be imported and processed, but there are no pre-built connectors. WSO2 has good support for IAM standards, including OAuth, OpenID, OIDC, SAML, and WS-Fed. They support standards-based and just-in-time provisioning using LDAP and SCIM.

WSO2 does not support identity proofing services at present. Moreover, most all functions are exposed through APIs, allowing customer admins to build connectors and data feeds as necessary. Identity Server supports role-based but not delegated administration.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	neutral

Table 44: WSO2's rating

WSO2 is an established open source IAM integrator. Recently they have built more functionality for consumer-facing use cases, and as a result are rapidly gaining customers for their consumer authentication capabilities. Organizations that prefer open source with professional support solutions should consider WSO2 for their consumer authentication needs.

6 Vendors and Market Segments to watch

Aside from the vendors covered in detail in this Leadership Compass document, we also observe other vendors in the market that we find interesting. Some decided not to participate in this KuppingerCole Leadership compass for various reasons, while others are interesting vendors but do not fully fit into the market segment of Consumer Authentication or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 Amazon Cognito

Amazon offers some consumer authentication functionality with Cognito. 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. All services are exposed via APIs, meaning it would be categorized as more of a DIY CIAM solution as defined earlier in this report. 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.

6.2 Avatier

California-based Avatier is a growing IAM and CIAM vendor. Their focus is on rapid deployment of basic IAM services to customers. Avatier has mostly been deployed on-premise but is being run in IaaS by some customers. Avatier supports authentication mechanisms including Knowledge-based Authentication (KBA), email/phone/SMS OTP, and Microsoft Azure MFA. The Avatier mobile app features fingerprint, voice, facial recognition biometrics, but doesn't support FIDO. Avatier can accept social logins including Facebook, Microsoft, LinkedIn, Twitter, etc. SAML and OAuth are supported for federation. Users can self-register or be provisioned via LDAP or SCIM. Risk factor evaluation and adaptive authentication are not possible within the product today.

Avatier provides API access for ITSM and SIEM integration. KuppingerCole monitors Avatier and information about their other IAM products is available in other reports.

6.3 AvocoSecure Trust Platform

AvocoSecure is a privately-owned UK company offering Cloud and Adaptive Authentication services. Their product is called Trust Platform. Trust Platform is not derived from traditional IAM, but rather was built to UK government security standards for high assurance verification of consumer identities. AvocoSecure partners offer customer profile storage in cloud or hybrid installations. It is 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 also accepts federated login via SAML, OIDC, and OAuth.

Using a REST API, Trust Platform can feed data to SIEM systems and Splunk.

KuppingerCole will continue to monitor AvocoSecure and will include them in future publications.

6.4 Curity AB

Curity AB was founded in Stockholm in 2015. They are focused on integrating with and extending existing IAM solutions with authentication. Beyond passwords and KBA, Curity accepts mobile push notifications, many social logins, TOTP compliant hardware tokens, and x.509. Curity supports SAML, OAuth, and OIDC. It can function as a token exchange service, and in addition to the federation protocols, is capable of issuing JWT, PKCE, and PPID.

The solution is deployed on-premises but can run in containers. Since it interoperates with IAM systems, it does not have its own customer database or risk engine. It provides basic identity analytics reports, GUI, and API services.

KuppingerCole will track Curity's progress and report on them in the future.

6.5 Duo Security

Duo Security provides a scalable MFA solution that can support a small to enterprise-size user base. Duo Security focuses on reducing the complexity of user identity verification while monitoring the health of their devices before connecting them to the applications they use. Duo's Trusted Access platform is a fully multi-tenant SaaS 2FA security solution. Once a user's initial authentication event is processed by an organization, that organization can then delegate the verification of the user's second authenticator to Duo's Trusted Access platform. Duo offers range of second factor options such as biometrics, Duo Push, Duo Mobile passcodes, and SMS passcodes for mobile devices. Duo also supports FIDO U2F and most third-party HOTP-compatible hardware tokens. The solution can also integrate with certain wearables and biometrics.

Regarding risk engine capabilities, Duo can detect if the user's device software is up to date, if the disk is encrypted, if a screen lock is enabled, or if the device is managed or unmanaged. Duo further reduces risk by marking devices as trusted and binding them to the specific user. With this feature, stolen credentials and MFA can't be used to access an application from any other device.

Although we have covered them in the past, and have an Executive View available, Duo did not respond for this report.

6.6 Fusion Auth

FusionAuth is single-tenant CIAM solution that can be deployed on-premises or in a private cloud. Its self-hosted option is free for unlimited users and offers mobile and web MFA, social login connections, brute force password attack detection, APIs and Webhooks, customizable consumer data storage, admin UI for managing users, and detailed user search and reporting capabilities. Managed cloud hosting, technical support, and custom development options are available.

6.7 Singular Key

Singular Key offers a passwordless MFA service with developer-centric cloud-native authentication API & SDKs that facilitate deployment and allow users to select the authenticator types they prefer. The solution leverages relevant authentication standards such as FIDO.

The company is relatively new to the market but their cloud-native approach with a focus on end-user authenticator selection could prove appealing to consumer-facing businesses. The company has

integration with SMS providers, mobile identity document authentication, and various identity providers to provide secure and convenient phishing-resistant authentication options.

6.8 Swivel Secure

Swivel Secure was founded in 2000 and is headquartered in the UK. They support some standards-based authentication methods and they offer some proprietary authentication mechanisms. The on-premise version comes as an appliance and they also offer a hosted SaaS. The product is licensed per user on an annual basis.

Swivel Secure supports mobile push notifications, OATH tokens, and SMS OTP. The solution does not have a mobile SDK. Swivel Secure has mobile apps that implement several varieties of PIN-based authentication, such as a randomized floating keypad (PINPad) and a randomized character choice aligned to preset PIN (TURing image authentication). To understand better how these work, see the demo **here**. These apps do not use Global Platform SE/TEE or Secure Enclave. Consumers can be provisioned in from LDAP. The solution supports SAML but does not support OAuth or OIDC. A user portal enables consumers to provision devices and reset PINs themselves.

AuthControl Sentry's risk engine evaluates device history, but not fingerprints/health; geo-location and geo-velocity, user attributes and user history. The risk engine and policy builder are somewhat coarse-grained and are not accessible via API. AuthControl Sentry cannot accept feeds from any 3rd-party fraud or threat intelligence sources. It does not interoperate with identity proofing services.

AuthControl Sentry can send event data to SIEMs over syslog. Delegated administration is not supported.

Swivel Secure takes a different approach to consumer authentication. While some basic standards are supported, their emphasis has been to create easy-to-use MFA options that rely minimally on the user's ability to remember passwords. Additional authenticators and IAM standards should be supported, and the risk engine needs improvement: most importantly the ability to consume various forms of threat intelligence.

6.9 Ubisecure Identity Server

Based in Finland, Ubisecure offers an integrated product solution that delivers consumer authentication functionality. Most customers run Ubisecure on-premise on RHEL or Windows servers, but a few run it in the cloud, and they have a Canadian MSSP partner.

Ubisecure customers can authenticate with passwords, Mobile Connect, ETSI MSS, TUPAS, NemID, SMS OTP, OTP TAN, MeonTrust MePIN smartphone biometrics authenticator app, and all the major social logins plus VKontakte, Amazon, and GitHub. Ubisecure also supports Legal Entity Identifier (LEI). LEI is a global identifier for companies, specified by the EU eIDAS regulation, and endorsed by the G20. LEI is a new standard to aid in compliance for Anti-Money Laundering (AML) and Know Your Customer (KYC) initiatives. LEI is a 20-digit alphanumeric code. Ubisecure supports federation with SAML, OIDC, WS-Federation, and OAuth. It supports LDAP and REST for bulk provisioning. Ubisecure currently only looks at a small number of risk factors. It does not have the ability to utilize external cyber threat intelligence feeds.

For more information on Ubisecure, see our **Executive View**.

6.10 UXP Systems

Toronto, Canada based UXP Systems offers Consumer IAM features in their User Lifecycle Management (ULM) Identity and Access Management module. ULM can act as a federation hub providing access to multiple domains from a single digital ID. They support SAML, OAuth, and OIDC, and can access user attribute information in both LDAP and SQL databases. For mobile authentication, they support Mobile Connect. The platform also allows registration and authentication via social networks such as Facebook and Twitter. UXP Systems is focused on helping the telecommunications industry with digital transformation. KuppingerCole will monitor UXP Systems and possibly include them in reports in the future.

7 Methodology

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

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

7.1 Types of Leadership

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the Consumer Authentication market. These products deliver most of the capabilities we expect from Consumer Authentication solutions. 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 they become Overall Leaders by being above average in all areas.

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

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

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

7.2 Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

Security is measured by the degree of security within the product. Information Security is a key element and requirement in the KuppingerCole IT Model (#70129 Scenario Understanding IT Service and Security Management[1]). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Unresolved security vulnerabilities and hacks are also understood as weaknesses. This rating is based on the severity of such issues and the way vendors deal with them.

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

Functionality is a measure of three factors. One is what the vendor promises to deliver. The second is the state of the art in industry. The third factor is what KuppingerCole expects vendors 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 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 in which products within each vendor's portfolio interoperate with each other. 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. 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 credential can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability can have several elements. 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 related to interoperability and is 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 to ensure its importance is understood by both the vendor and the customer. As we move forward, simply providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability 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 good documentation can facilitate adequate accessibility. However, we have strong expectations that user interfaces will be logically and intuitively designed. Moreover, we expect a high degree of consistency across user interfaces of a product or different products of a vendor. We also believe that vendors should follow common, established approaches to user interface design.

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

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 highest potential for breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will 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 increase costs, but inevitably lead 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 is of highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns and will result in weak infrastructure.

7.3 Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

7.4 Rating scale for products and vendors

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

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

7.5 Inclusion and exclusion of vendors

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

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

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

8 Copyright

The Future of Information Security – Today

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

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

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

KuppingerCole Analysts AG
Wilhelmstr. 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com