KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert | February 2017

Adaptive Authentication

Leaders in innovation, product features, and market reach for Adaptive Authentication. Your compass for finding the right path in the market.

by **John Tolbert**
jt@kuppingercole.com
February 2017

Leadership Compass
Adaptive Authentication
By KuppingerCole

Content

Content Tables

Table of Figures

Related Research

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

Advisory Note: Trends in Authentication and Authorization - 71043

Scenario: The Future of Authentication - 70341

Blog: PSD II, Adaptive Authentication, and Multi-Factor Authentication

Webcast: Beyond Usernames and Passwords: 3 Steps to Modern Authentication

Blog: Authentication: Multi-Factor, Adaptive and Continuous

Blog: Not So Dead Yet: Why Passwords Will Survive All of Us

1 Management Summary

Identity and Access Management (IAM) systems have continued to evolve significantly over the last two decades. Increasing security and improving usability have both been contributing factors to this evolution. Data owners and IT architects have pushed for better ways to authenticate and authorize users, based on changing risks and newer technologies. Businesses have lobbied for these security checks to become less obtrusive and provide a better user experience (UX). One of these such enhancements is Adaptive Authentication.

Adaptive Authentication (AA) is the process of gathering additional attributes about users and their environments and evaluating the attributes in the context of risk-based policies. The goal of AA is to provide the appropriate risk-mitigating assurance levels for access to sensitive resources by requiring users to further demonstrate that they are who they say they are. This is usually implemented by "step-up" authentication. Different kinds of authenticators can be used to achieve this, some of which are unobtrusive to the user experience. Examples of step-up authenticators include phone/email/SMS One Time Passwords (OTPs), mobile apps for push notifications, mobile apps with native biometrics, FIDO U2F or UAF transactions, SmartCards, and behavioral biometrics. Behavioral biometrics can provide a framework for continuous authentication, by constantly evaluating user behavior to a baseline set of patterns. Behavioral biometrics usually involve collecting environment data (such as IP addresses, geo-location, nearby WiFi SSIDs, etc.), keystroke analysis, mobile "swipe" analysis, and even mobile gyroscopic analysis.

AA solutions can use multiple authentication schemes and authentication challenges presented to a user or service according to defined policies based on any number of factors, for example the time of day, the category of user, the location or the device from which a user or device attempts authentication. The factors just listed as examples can be used to define variable authentication policies which are often referred to as context- or policy-based AA. A more advanced form of AA uses risk-scoring analytics algorithms to first baseline regular access patterns and then be able to identify anomalous behaviour which triggers additional authentication challenges. This can be referred to as dynamic AA, yet it is difficult to categorise AA products into dynamic or static AA categories, since the strongest products are able to use a combination of both approaches. This is invariably a positive feature, as there are use cases where the use of either static or dynamic AA proves the most appropriate, and both approaches are not without their limitations.

A wide variety of adaptive authentication mechanisms and methods exist in the market today. Examples include:

- Re-authentication
- Knowledge-based authentication (KBA)
- Multi-factor authentication, also known as MFA (Smart Cards, USB authenticators, biometrics)
- One-time password (OTP), delivered via phone, email, or SMS
- Out-of-band (OOB) application confirmation
- Identity context analytics, including
  - IP address
  - Geo-location
  - Geo-velocity
  - Device ID
  - User Behavioral Analysis

Many organizations today employ a variety of Adaptive Authentication methods. Consider the following sample case. Suppose a user successfully logs in to a financial application with a username and password. Behind the scenes, the financial application has already examined the user's IP address, geo-location, and Device ID to determine if the request context fits within historical parameters for this user. Further suppose that the user has logged in from a new device, and the attributes about the new device do not match recorded data. The web application administrator has set certain policies for just this situation. The user then receives an email at their chosen address, asking to confirm that they are aware of the session and that they approve of the new device being used to connect to their accounts. If the user responds affirmatively, the session continues; if not, the session is terminated.

Going one step further in the example, consider that the user would like to make a high-value transaction in this session. Again, the administrator can set risk-based policies correlated to transaction value amounts. In order to continue, the user is sent a notification via the mobile banking app on his phone. The pop-up asks the user to confirm. The user presses "Yes", and the transaction is processed.

Adaptive authentication, then, can be considered a form of authorization. The evaluation of these additional attributes can be programmed to happen in response to business policies and changing risk factors. Since access to applications and data are the goal, adaptive authentication can even be construed as a form of attribute based access control (ABAC).

The story above is just one possible example. Adaptive authentication is being used today by enterprises to provide additional authentication assurance for access to applications involving health care, insurance, travel, aerospace, defense, government, manufacturing, and retail. Adaptive authentication can help mitigate risks and protect enterprises against fraud and loss.

There are a number of vendors in the Adaptive Authentication market. Many of them provide complete IAM solutions, and Adaptive Authentication is just one part of their overall solution. Other vendors have developed specialized Adaptive Authentication products and services, which can integrate with other IAM components. The major players in the Adaptive Authentication segment are covered within this KuppingerCole Leadership Compass.

This Leadership Compass provides an overview and analysis of the Adaptive Authentication solutions within the IAM market. These solutions are sometimes referred to as Contextual Authentication, or just Step-Up Authentication. This Leadership Compass will examine solutions that are available for primarily on-premise deployment.

Overall, the breadth of functionality is growing rapidly. Support for standard adaptive authentication mechanisms is now nearly ubiquitous in this market segment; and the key differentiators have become the use of new technologies to step up the user's authentication assurance level or to collect and analyze information about the user's session.

The entire market segment is mature but constantly evolving, due to innovations in authenticator technology and risk analysis engines. We expect to see more changes within the next few years. However, given the surging demand of businesses and the need to provide better security, many organizations must implement Adaptive Authentication if they have not already to help reduce the risk of fraud and data loss. 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 particular customer and their requirements. However, this Leadership Compass will help identifying those vendors that customers should look at more closely.

1.1 Overall Leadership

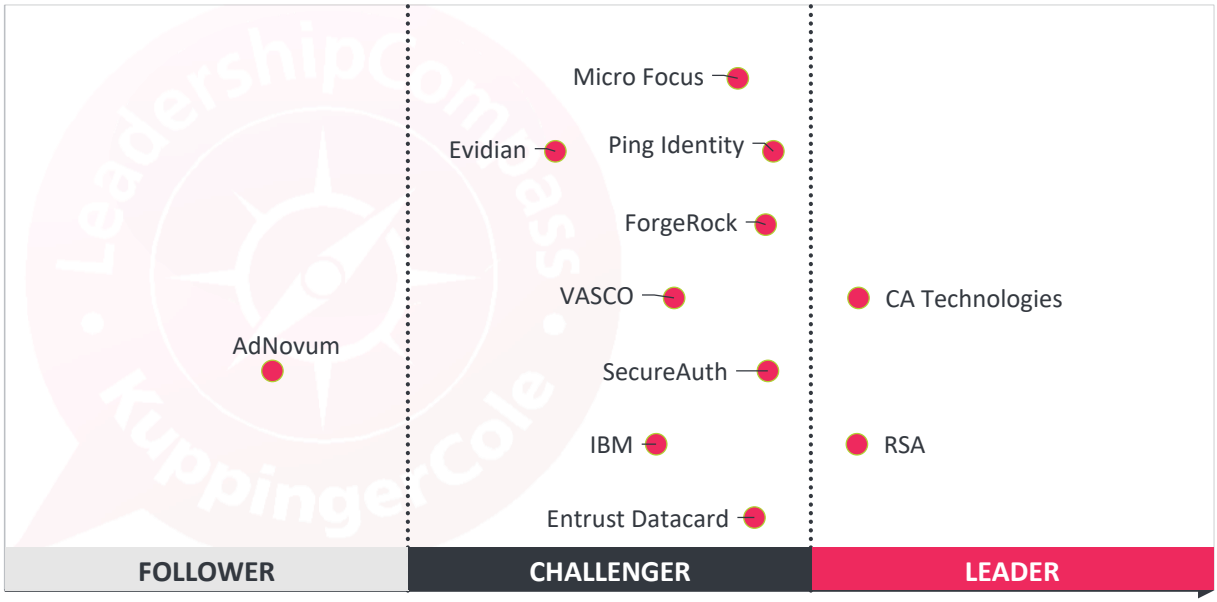


Fig. 1: Overall Leaders in the Adaptive Authentication segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Overall Leadership is the combined view on the three Leadership categories: Product Leadership, Innovation Leadership, and Market Leadership. This combined view provides an overall impression of our rating of the vendor's offerings in the AA market segment. Notably, some vendors benefit, for example, from a strong market presence while slightly lagging in other areas such as innovation.

Alternately, others may show their strength in the Product Leadership and Innovation Leadership, while having a relatively low market share or lacking a global presence. Thus, we strongly recommend looking at all Leadership categories and the individual analysis of the vendors and their products for gaining a comprehensive understanding of the players in this market segment.

In the market for Adaptive Authentication, we currently see two companies in the Leaders segment for Overall Leadership. These are CA Technologies and RSA as established players with strong offerings and large customer bases.

The Challenger segment is very crowded, with most vendors being placed in that segment. Here we find Entrust Datacard, ForgeRock, MicroFocus, PingIdentity, and SecureAuth. All of them are top challengers, and are almost leaders in this space. Evidian, IBM, Vasco Data Security, reside in the center of the Challenger segment. Each of these vendor's products have various strengths that make their solutions attractive to different kinds of customers.

AdNovum Informatik is found in the Followers section. Vendors may be placed in the Followers section for several reasons, such as small customer base or lack of global reach.

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. In a mature market, such as this, one vendor may excel at certain features, and only meet the minimum levels for others. To choose the right product, a thorough evaluation of organizational requirements and a mapping to the features provided by the vendors' products is mandatory.

1.2 Product Leadership

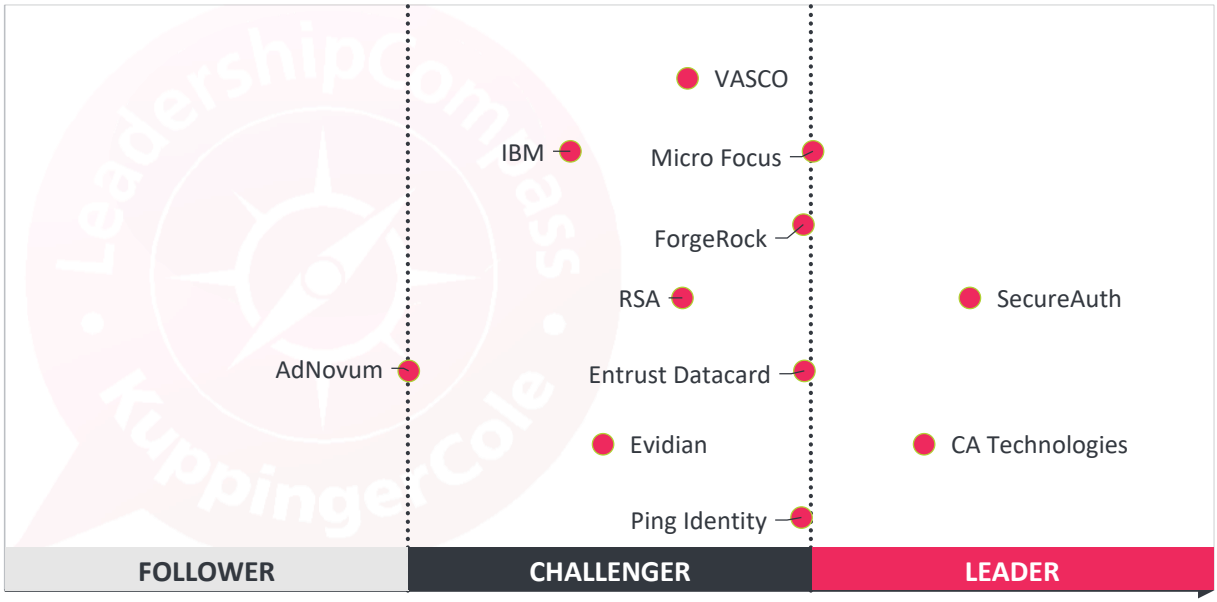


Fig. 2: Product Leaders in the Adaptive Authentication segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The second view we provide is about Product Leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

Here we see two companies placed in the Leaders segment: SecureAuth and CA Technologies. Both of them have mature and feature-rich product offerings.

At the top of the Challenger segment, we find Entrust Datacard, ForgeRock, MicroFocus, and PingIdentity. These products have most of the features we expect for this category. Rounding out the remainder of the Challenger section are Evidian, IBM, RSA, and Vasco Data Security. Again, each product has varying strengths and weaknesses across their feature sets that will merit attention from those conducting RFIs and RFPs.

AdNovum Informatik's Nevis suite is found on the border between Follower and Challenger.

In a mature market, such as this, one vendor may excel at certain features, and only meet the minimum levels for others. To choose the right product, a thorough evaluation of organizational requirements and a mapping to the features provided by the vendors' products is mandatory. There are sufficient examples where products that weren't "feature leaders" still were the better fit for specific customer scenarios.

1.3 Market Leadership

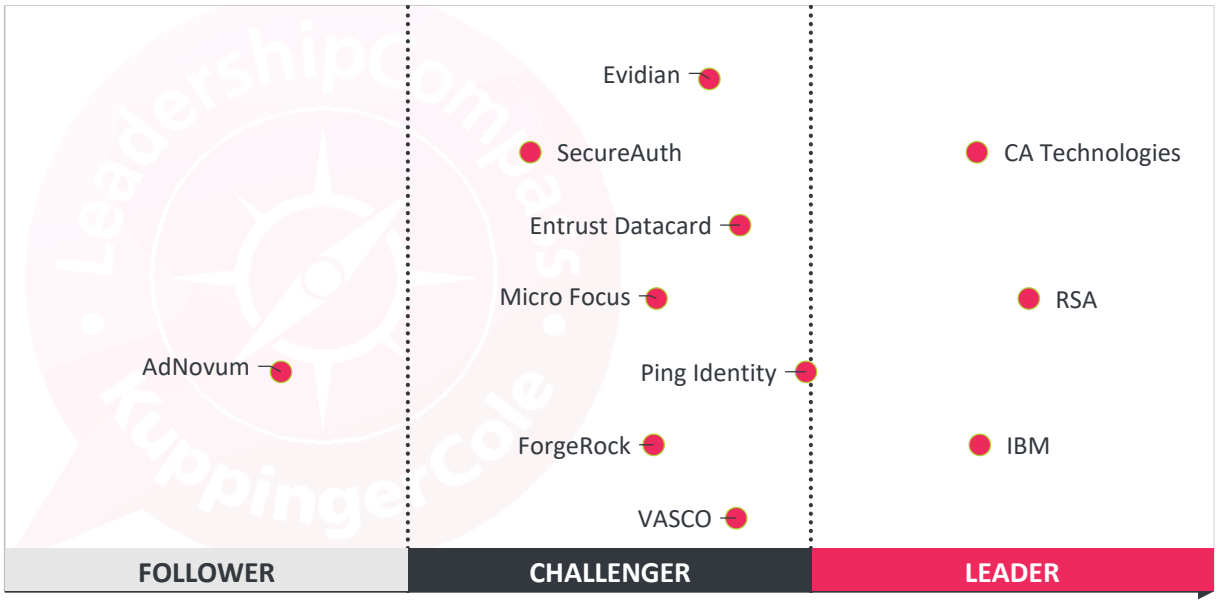


Fig. 3: Market Leaders in the Adaptive Authentication segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

We expect Market Leaders to be leaders on a global basis. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered Market Leaders. The same holds true for the vendor's partner ecosystem – without global scale in the partner ecosystem, we don't rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might be able to execute well in their "home base".

Small vendors are sometimes more directly involved in customer projects, which can be positive or negative. It can be negative if it leads the vendor to branch product development in ways that does not benefit all customers. Additionally, the success of projects depends on many other factors, including the quality of the system integrator. So even large vendors with a good ecosystem might sometimes fail in projects.

It is not surprising that the large and established software vendors dominate the Leaders segment. CA Technologies, IBM, and RSA all made it into the Leaders segment.

PingIdentity, with their recent acquisition of UnboundID, sits at the border of Leader and Challenger, and is considered as one of the top challengers. Entrust Datacard, Evidian, ForgeRock, MicroFocus, and Vasco Data Security are located in the top of the Challenger section. SecureAuth is found left of center in the Challenger segment. This means they command a sizable market share, but perhaps not the global reach, number of customers, or supporting integrators compared to the Leaders.

AdNovum Informatik is in the Followers section, due to a regional focus on sales and marketing.

It must be noted that this Market Leadership rating doesn't allow any conclusion about whether the products of the different vendors fit the customer requirements.

1.4 Innovation Leadership

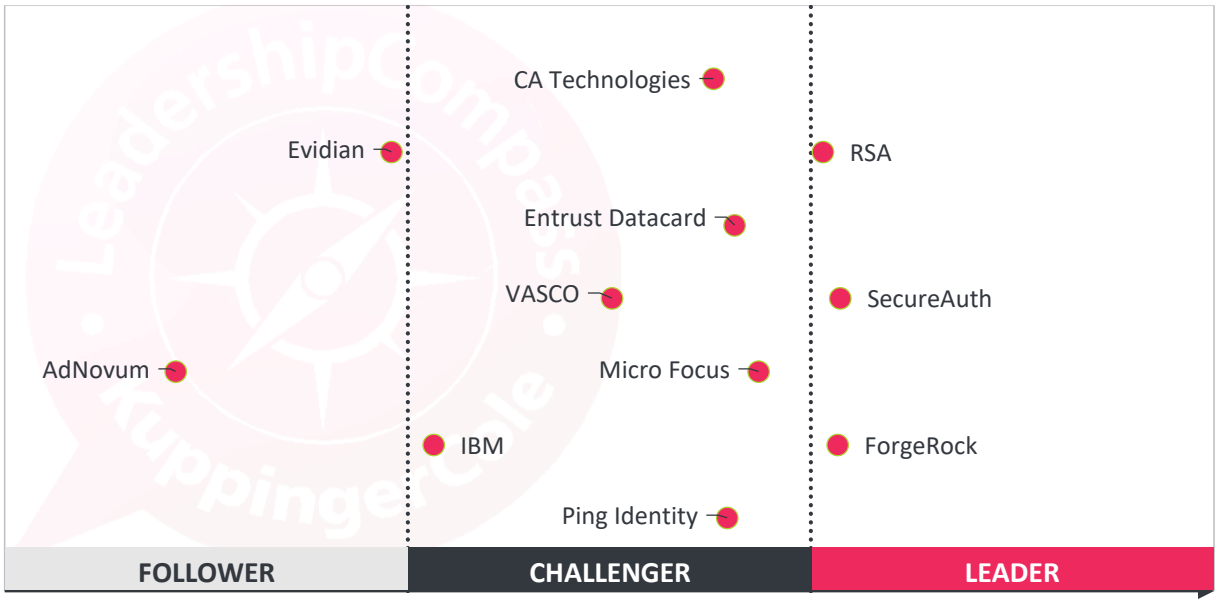


Fig. 4: Innovation Leaders in the Adaptive Authentication segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

The third angle we view when evaluating products is about innovation. Innovation is, from our perspective, a key distinction in IT market segments. Innovation is what customers require to receive new releases that meet new requirements. Thus, a look at Innovation Leaders is also important, beyond analyzing product features.

Here we see ForgeRock, RSA, and SecureAuth in front in the Leaders segment. Each showed significant innovation and strong support of the list of features we consider as innovative in the Adaptive Authentication market, such as good variety in multi-factor authentication methods and intelligent risk engines.

Entrust Datacard, MicroFocus, and PingIdentity reside in the upper third of the Challenger section, indicating that they show significant innovation in this market. CA Technologies, IBM, and VASCO Data Security are also found in the Challenger area, showing a moderate amount of innovative features in the products.

AdNovum Informatik and Evidian populate the Followers section. They have some innovative features; however, they lack support for some of the innovative features we'd like to see.

Again, in some cases products that appear more to the left of that figure do not necessarily fail in innovation but are focused on specific requirements or highly focused approaches.

Some vendors are more innovative than others with respect to new features, such as providing many different kinds of authentication methods, SaaS integration, and sophistication in their risk engines. Overall, this view reflects the fact that there is still a lot of innovation happening in the Adaptive Authentication market, with significant room for some of the vendors to enhance their offerings.

2 Methodology

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

It should be noted that it is inadequate to pick vendors based only on the information provided within this report. Customers must always define their specific requirements and analyze in greater detail what they need. This report does not 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.

We look at four types of leaders:

- Product Leaders: Product Leaders identify the leading-edge products in the particular market segment. These products deliver to a large extent what we expect from products in that market segment. They are mature.
- Market Leaders: Market Leaders are vendors which have a large, global customer base and a strong partner network to support their customers. A lack of global presence or breadth of partners can prevent a vendor from becoming a Market Leader.
- Innovation Leaders: Innovation Leaders are those vendors which are driving innovation in the particular market segment. They provide several of the most innovative and upcoming features we hope to see in the particular market segment.
- Overall Leaders: Overall Leaders are identified based on a combined rating, looking at the strength of products, the market presence, and the innovation of vendors. Overall Leaders might have slight weaknesses in some areas but become an Overall Leader by being above average in most 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 most areas.
- Challengers: This level identifies products which are not yet leaders but have specific strengths which might make them leaders in the future. Typically, these products are also mature and might be leading-edge when looking at specific use cases and customer requirements.
- Followers: This group contains products which lag in some areas, such as a containing a limited feature set or having only a regional presence. The best of these products might have specific strengths, making them a good or even best choice for certain use cases and customer requirements, but are of limited value in other situations.

In addition, we have defined a series of matrixes which:

- Compare ratings. For example, the rating for innovation against the rating for the overall product capabilities, thus identifying highly innovative vendors which are taking a slightly different path than established vendors. This also shows established vendors which no longer lead in innovation. These additional matrixes provide different viewpoints on the vendors, and should be considered when downselecting vendors in the vendor/product selection process or picking vendors for RFIs (Request for Information).
- Display different views by comparing the product rating to other feature areas. This is important because not all organizations need the same product features, depending on their current situation and specific requirements. Based on these additional matrixes, customers can evaluate which vendor best fits their current needs, but is also promising regarding its overall capabilities. The latter is important given that a product typically not only should address a pressing challenge but become a sustainable solution. Chosen solutions should address both immediate business needs as well as being good enough for the next steps and future requirements.

Thus, the KuppingerCole Leadership Compass provides a multi-dimensional view on vendors and their products.

Our rating is based on a broad range of input and a long experience in this market segment. The referenced input consists of experience from KuppingerCole advisory projects, feedback from customers using the products, product documentation, and vendor responses to a questionnaire sent out before creating the KuppingerCole Leadership Compass, plus a variety of other sources.

3 Product Rating

KuppingerCole, as an analyst company, regularly does evaluations of products and vendors. The results are, amongst other types of publications and services, published in the KuppingerCole Leadership Compass Reports, 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). Thus, providing a mature approach to security and having a well-defined internal security concept are key factors when evaluating products. Shortcomings, such as having no or only a very coarse-grained, internal authorization concept are understood as weaknesses in security. Known security vulnerabilities and hacks are also understood as weaknesses. The rating then is based on the severity of such issues and the way a vendor deals with them.

Functionality is measured in relation to three factors. One is what the vendor promises to deliver. The second is the state of the industry. The third factor is what KuppingerCole would expect the industry to deliver to meet customer requirements. In mature market segments, the state 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 interoperate with themselves. This detail can be uncovered by looking at what an administrator is required to do in the deployment, operation, management, and discontinuation of the product. The degree of integration is then directly related to how much overhead this process requires. For example: if each product maintains its own set of usernames and passwords for every person involved, it is not well integrated. Or, 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 user account can allow the admin to deal with all aspects of the product suite, then a better level of integration has been achieved.

Interoperability also can have several meanings. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or standards that are important outside of the product family. Extensibility is part of this and measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status to insure its importance and understanding by both the vendor and the customer. As we move forward, just providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy) for more information about the nature and state of extensibility and interoperability.

Usability refers to the degree in which the vendor enables 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 create adequate accessibility. However, overall we have strong expectations regarding well integrated user interfaces and a high degree of consistency across user interfaces of a product or different products of a vendor. We also expect vendors to follow common, established approaches to user interface design.

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

- Increased Administrative labor is the highest area of both cost and potential breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will only result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased Administrative Labor 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 of these areas will lead to inevitable identity and security breakdowns.

4 Vendor Rating

The following additional categories are considered in the vendor evaluation.

- Innovativeness
- Market position
- Financial strength
- Ecosystem

Innovativeness is measured as the capability to drive innovation in a direction which aligns with the KuppingerCole understanding of the particular market segment(s) the vendor is in. Innovation has no value by itself, therefore the innovation must provide clear benefits to the customer. Moreover, being consistently innovative is an important factor for building trust in vendors and their product roadmaps, because innovative vendors are more likely to remain leading-edge. KuppingerCole considers vendor support for standardization initiatives as a component of the innovativeness rating. Driving innovation without standardization frequently leads to vendor lock-in scenarios. Thus, active participation in international standards organizations adds to the positive rating of innovativeness.

Market position measures the position the vendor has in the market and related market segments. This is an average rating over all markets in which a vendor is active. Therefore, being weak in one segment doesn't necessarily lead to a very low overall rating. This factor considers the vendor's presence in major markets. The rating in market position is specific to the particular market segment analyzed in this KuppingerCole Leadership Compass, not related solutions. Thus, a very large vendor might not be a market leader in the particular market segment we are analyzing.

Financial strength is a measure of a vendor's financial health, in terms of profitability, revenue, and/or investment. In general, publicly available financial information is an important factor. Companies which are venture-financed are more likely to become an acquisition target, with potential risks to customers of not fulfilling the stated roadmap. If public information is not available, KuppingerCole evaluates other factors, such as financial information provided confidentially. Even while KuppingerCole doesn't consider company size to be a value in itself, financial strength is an important factor for customers when making decisions.

Ecosystem is a measure of the size of the vendor's partner base, including reseller channels, system integrators, and certified consultants (if applicable) and support specialists. This rating also assesses 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.

5 Vendor Coverage

KuppingerCole attempts to include all vendors within a specific market segment in their Leadership Compass documents. The scope of the document is global coverage, but may include vendors which are only active in regional markets such as the EU, North America, or the APAC region.

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.
- Decline to participate: Vendors may decide to not participate in our evaluation. KuppingerCole tends to include their products anyway, as long as sufficient information for evaluation is publicly available. This approach allows KuppingerCole to provide a more comprehensive and objective overview of leaders in the particular market segment.
- Lack of information: Products of vendors which don't provide the information we have requested for the Leadership Compass document will not appear in the document unless we have access to sufficient information from other sources.
- Borderline classification: Some products might have only a small overlap with the market segment we are analyzing. In these cases, we might decide not to include the product in that KuppingerCole Leadership Compass.

Our goal is to provide a comprehensive and objective view of the products in a market segment. KuppingerCole will provide regular updates on their Leadership Compass documents.

For this Leadership Compass document, almost all major vendors we approached responded to the questionnaire. The exception in this case was Oracle. We have included a brief analysis of Oracle Adaptive Access Manager due to the relevance of that product in Chapter 14.

Furthermore, there are a few point offerings in the market that have a limited market visibility and were not included in the leadership analysis for this KuppingerCole Leadership Compass. Some of these vendors are listed in the final section of this document and might become part of the next edition of this document, depending on how they evolve.

6 Market Segment

Adaptive Authentication is a niche within the IAM market. Many full stack IAM vendors provide Adaptive Authentication capabilities, built into their suites. These products and services will be examined below. Also, there are specialty products focused on Adaptive Authentication, which interoperate with Web Access Management (WAM) and Single Sign-On (SSO) systems. These too, will be included in this Leadership Compass.

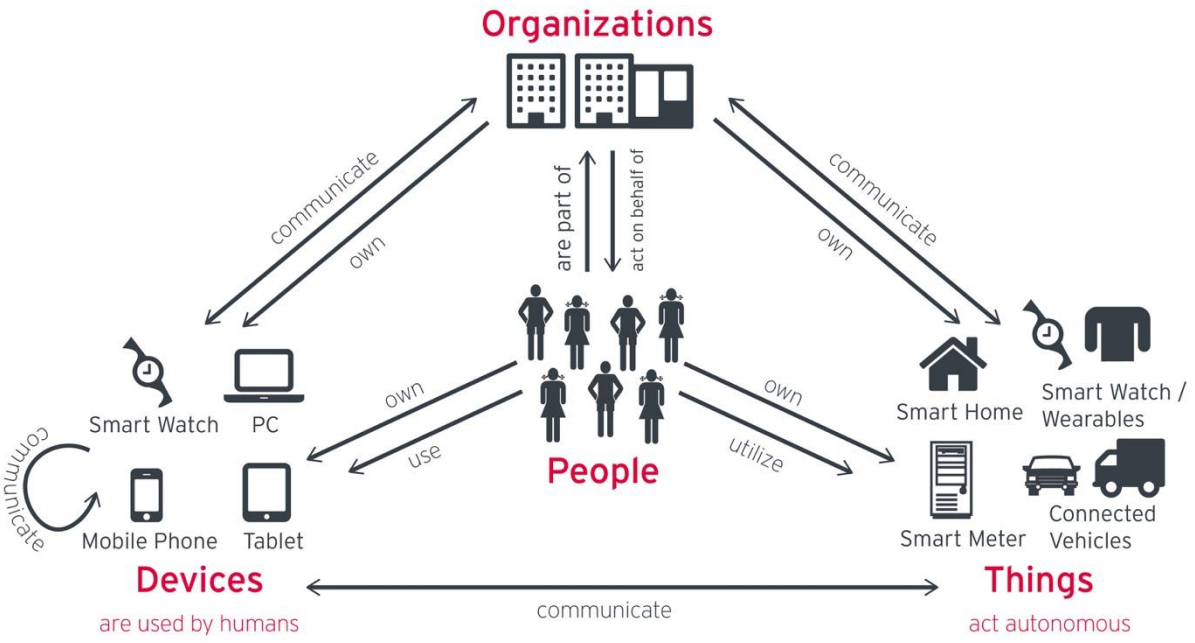


Fig. 5: Adaptive authentication means matching the right people to the right resources using the appropriate authenticators.

Various drivers have led to the development of adaptive authentication solutions. Organizations need to provide access to information, but also need to make sure that sensitive information is not exposed to the wrong users. Differing levels of authentication assurance must be computed in authorization and access control decisions. The risk management approach that pervades IT Security thinking today demands risk adaptive authentication within the IT architecture. Therefore, different types of authentication methods and authenticators are available on the market, and are integrated with risk analysis engines, the input from which is evaluated against enterprise policies. This approach allows deploying organizations to have flexibility to meet policy and regulatory requirements while providing users with more secure and/or more usable technologies for proving their identities.

Various technologies support all the different requirements customers are facing today. The requirements are:

- Deployment options: On-premise, cloud, or hybrid options. This Leadership Compass examines the major on-premise Adaptive Authentication products.
- Standard multi-factor authentication support: KBA, SmartCards, OTP
- New technology multi-factor authentication support: OOB mobile confirmation apps, FIDO UAF/U2F, and Biometrics
- Static rule configuration: by resource and user action on resource
- Identity context analytics with risk engine: IP address, geo-location, geo-velocity, device ID, user behavior,
- Threat intelligence integration: subscription to 3rd party services that identify malicious IP addresses, URLs, and compromised credentials

Adaptive Authentication is an outgrowth of yesterday's IAM systems. Many organizations are feeling and responding to the pressure to move away from just using usernames and passwords for authentication. While many strong authentication options have existed for years, such as SmartCards, it is not often feasible from an economic perspective to deploy SmartCards or other hardware tokens to every possible user of a system. Moreover, hardware tokens continue to have usability issues. The mix of authenticators and associated user attributes that most commercial Adaptive Authentication systems present are increasingly sufficient to meet the needs of higher identity assurance for access to sensitive digital resources and high-value transactions.

It is important to understand the primary use cases that drive the requirements for AA and MFA products, as most of the major market players in this space tend to develop solutions tailored for consumer or employee use cases. Some offerings are geared towards specific industry verticals.

A good AA or MFA solution needs to balance integration flexibility with simplicity. Today's newest offerings in this area provide multiple authentication mechanisms, including many mobile options; risk engines which evaluate numerous definable factors which can be gathered at runtime and compared against enterprise policies; and out-of-the-box (OOTB) connectors for the majority of popular on-premise and cloud enterprise applications.

Integration with existing IAM platforms should be a primary factor in selecting a suitable product. The advantages of taking a single-vendor approach are primarily due to the potential licensing cost savings that arise from negotiating product bundle discounts. The advantages gained from the imagined greater ease of integrating disparate products from the same vendor rarely offer the reduced complexity promised by sales. Most major solutions support popular identity store back-ends, generally LDAP but sometimes also SQL. While adaptive and multi-factor authentication may mitigate many authentication risks, no security solution is impenetrable. It is important to plan for rapid response measures when security breaches do occur. Even the best defensive systems can suffer breaches.

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.

7 Specific features analyzed

When evaluating the products, we focus on:

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- platform support

In addition to the aforementioned aspects, we consider several specific features. These include:

Multi-Factor Authentication

Often expressed as combining two or more of the following factors: something you know, something you have, and something you are. Knowledge-based authentication (KBA): Security questions and answers that are determined at registration time. KBA is sometimes used in cases where users have forgotten their passwords, and need to have them reset, or as a step-up authentication method. KBA is not recommended, as many of the answers to common questions chosen are not secrets.

OATH One Time Passwords (OTP): OATH standardizes the use of randomized, single use passwords based on cryptographic hashes. OTP delivery methods can be phone calls, email, or SMS (text) messages. As a more secure variation, OATH specifies time-limited OTPs, sometimes expressed as TOTP. Due to the fact that OTP implementations are not truly random, and attackers have discovered ways to circumvent OTP, some organizations such as US NIST have deprecated the use of OTP as a primary or step-up authentication method.

FIDO U2F and UAF: The FIDO Alliance has defined two standards for mobile and two-factor authentication. U2F applies to various hard token generators, whereas UAF works in conjunction with mobile devices, such as smartphones. The FIDO framework allows device and software manufacturers to utilize different technologies as the basis for authentication events, such as PINs, biometrics, and cryptography.

Mobile apps / push notifications: Service providers are increasingly building their own mobile apps for authentication and authorization. Mobile apps can offer a variety of authentication methods, from simple screen swipes to including biometrics (see below). Push notifications are a different type of mobile app which can be used as a second factor in authentication or to authorize transactions out-of-band.

Biometrics is the term applied to any security technology, usually employed for authentication and authorization, which functions by comparing registered measurements to run-time measurements. Examples of biometrics include fingerprint, face, voice, iris, and behavioral. Biometrics can be used as primary authenticators or as policy-invoked adaptive authentication mechanisms.

	SmartCards: Cards with small processors and secure storage devices that contain digital certificates and various user attributes. SmartCards can be used to facilitate the highest levels of authentication assurance. SmartCards are used for not only authentication, both as primary and adaptive authentication methods, but also for physical access and digital signatures.
Risk Engine	Factors such as IP address, device fingerprints, geo-location, geo-velocity, user behavior profiling
Cyber Threat Intelligence	Subscriptions to real-time feeds of known bad IP addresses, locations, proxies, malicious URLs, and compromised credentials
User Stores/Directories	LDAP, Active Directory, Azure Active Directory, SQL integration
Federation support	SAML 2.0, OAuth 2.0, OIDC, and others.
IAM integration	Integration of products within a suite; SSO
Security models	Strong authentication to admin functions, role-based administration, delegated administration, encryption, SIEM/RTSI integration, Identity Governance integration, Privilege Management integration
Deployment models	On-premise, cloud, or hybrid. On-premise is the model considered by this Leadership Compass.
Customization	The less you need to code and the more you can configure, the better – that's the simple equation we considered regarding customization. However, we also looked for features like a transport system to segregate development, test, and production environments. Notably, copying configuration files does not represent a transport system.
Multi tenancy	Given the increasing number of SaaS deployments, but also specific requirements in multi-national and large organizations, support for multi-tenancy is highly recommended.

The support for these functions is included with the evaluation of the products. 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.

8 Market Leaders

Based on our evaluation of the products, we've identified (as mentioned above) different types of leaders in the Adaptive Authentication market segment. The Market Leaders are shown in Figure 9.

We expect Market Leaders to be have a global sales and support network. Companies which are strong in a specific geographic region but sell little or nothing to other major regions are not considered Market Leaders. The same holds true for the vendor's partner ecosystem – without global scale in the partner ecosystem, we don't rate vendors as Market Leaders.

Market Leadership is an indicator of the ability of vendors to execute on projects. However, this depends on other factors as well. Small vendors might be able to execute well in their "home base".

Small vendors are sometimes more directly involved in customer projects, which can be positive or negative. It can be negative if it leads the vendor to branch product development in ways that does not benefit all customers. Additionally, the success of projects depends on many other factors, including the quality of the system integrator. So even large vendors with a good ecosystem might sometimes fail in projects.

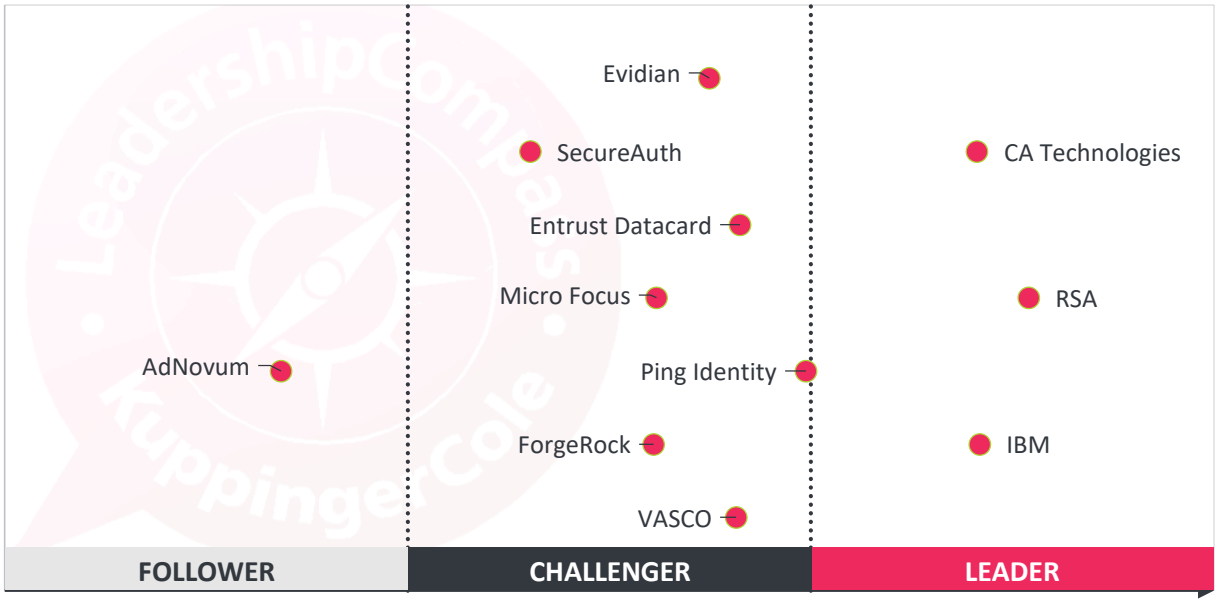


Fig. 6: Market Leaders in the Adaptive Authentication market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

It is not surprising that the large and established software vendors dominate the Leaders segment. CA Technologies, IBM, and RSA all made it into the Leaders segment.

PingIdentity, with their recent acquisition of UnboundID, sits at the border of Leader and Challenger, and is considered as one of the top challengers. Entrust Datacard, Evidian, ForgeRock, MicroFocus, and Vasco Data Security are located in the top of the Challenger section. SecureAuth is found left of center in the Challenger segment. This means they command a sizable market share, but perhaps not the global reach, number of customers, or supporting integrators compared to the Leaders.

AdNovum Informatik is in the Followers section, due to a regional focus on sales and marketing.

It must be noted that this Market Leadership rating doesn't allow any conclusion about whether the products of the different vendors fit the customer requirements.

Market Leaders (in alphabetical order):

- CA Technologies
- IBM
- RSA

9 Product Leaders

The second view we provide is about Product Leadership. That view is mainly based on the analysis of product features and the overall capabilities of the various products.

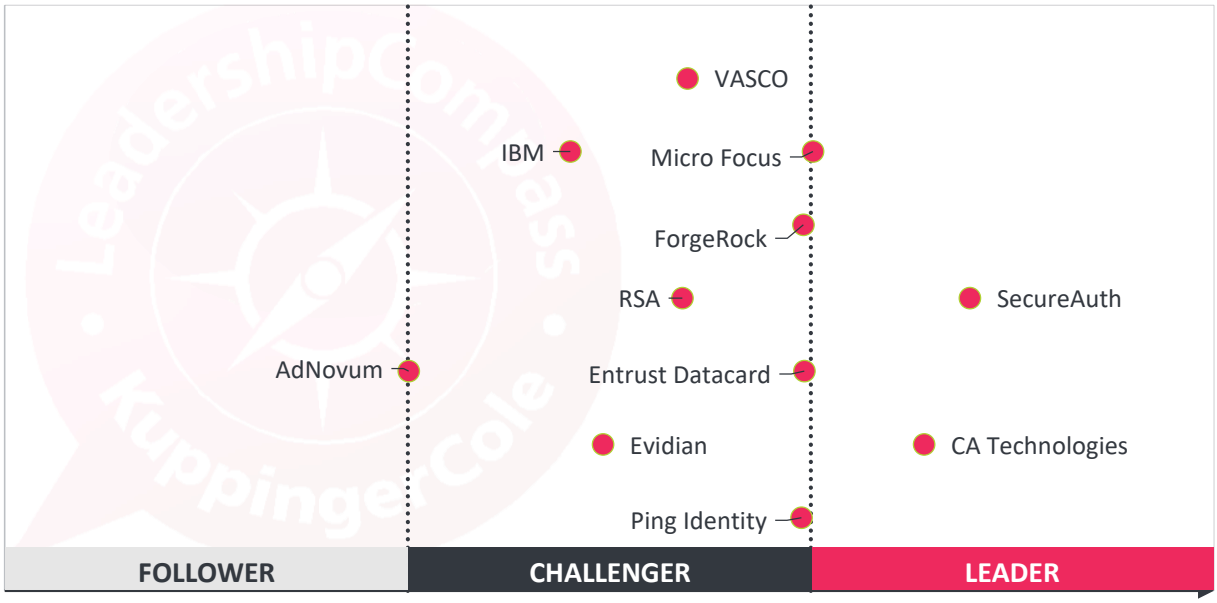


Fig. 7: Product Leaders in the Adaptive Authentication market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Here we see two companies placed in the Leaders segment: SecureAuth and CA Technologies. Both of them have mature and feature-rich product offerings.

At the top of the Challenger segment, we find Entrust Datacard, ForgeRock, MicroFocus, and PingIdentity. These products have most of the features we expect for this category. Rounding out the remainder of the Challenger section are Evidian, IBM, RSA, and Vasco Data Security. Again, each product has varying strengths and weaknesses across their feature sets that will merit attention from those conducting RFIs and RFPs.

AdNovum Informatik's Nevis suite is found on the border between Follower and Challenger.

In a mature market such as this, one vendor may excel at certain features, and only meet the minimum levels for others. To choose the right product, a thorough evaluation of organizational requirements and a mapping to the features provided by the vendors' products is mandatory. There are sufficient examples where products that weren't "feature leaders" still were the better fit for specific customer scenarios.

Product Leaders (in alphabetical order):

- CA Technologies
- SecureAuth

10 Innovation Leaders

The third angle we took when evaluating products was about innovation. Innovation is, from our perspective, a key distinction in IT market segments. Customers require innovation to receive new features that meet new requirements.

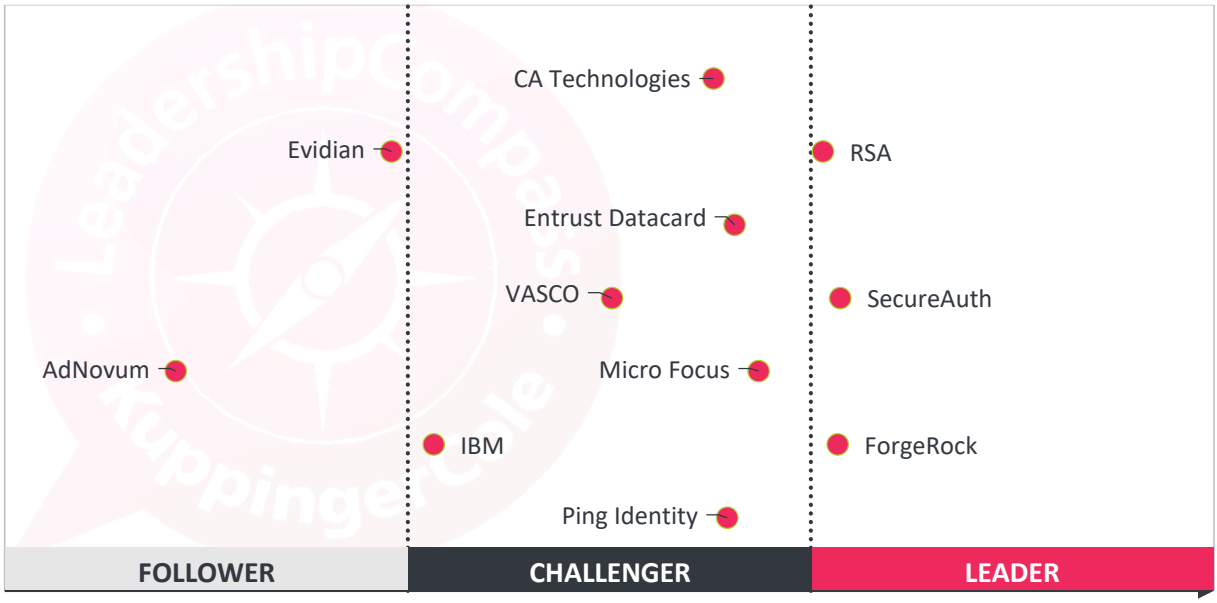


Fig. 8: Innovation Leaders in the Adaptive Authentication market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

Here we see ForgeRock, RSA, and SecureAuth in front in the Leaders segment. Each showed significant innovation and strong support of the list of features we consider as innovative in the Adaptive Authentication market, such as good variety in multi-factor authentication methods and intelligent risk engines.

Entrust Datacard, MicroFocus, and PingIdentity reside in the upper third of the Challenger section, indicating that they show significant innovation in this market. CA Technologies, IBM, and VASCO Data Security are also found in the Challenger area, showing a moderate amount of innovative features in the products.

AdNovum Informatik and Evidian populate the Followers section. They have some innovative features; however, they lack support for some of the innovative features we'd like to see.

Again, in some cases products that appear more to the left of that figure do not necessarily fail in innovation but are focused on specific requirements or highly focused approaches.

Some vendors are more innovative than others with respect to new features, such as providing many kinds of authentication methods, SaaS integration, and sophistication in their risk engines. Overall, this view reflects the fact that there is still a lot of innovation happening in the Adaptive Authentication market, with significant opportunity for some of the vendors to enhance their offerings.

Innovation Leaders (in alphabetical order):

- ForgeRock
- SecureAuth
- RSA

11 Product Evaluation

This section contains a quick rating for every product we've included in this KuppingerCole Leadership Compass document. KuppingerCole provides *Product Reports* and *KuppingerCole Executive View Reports*, providing detailed information regarding products described herein.

11.1 AdNovum Nevis

AdNovum, based in Switzerland, provides adaptive authentication with their Nevis Security Suite. The suite consists of various components for Web Access Management, Federation support, Web Application Firewall, authentication, and user management including delegated administration and self-registration, support for digital signatures, and an administrative console. All features are provided by separate components. However, these components are tightly integrated.

Strengths/Opportunities	Weaknesses/Threats
• Broad support for authentication mechanisms, including several national ID cards • Proven strength in various customer deployments • Additional uncommon features such as delegated administration and digital signature support	• Currently focused on few markets, including Switzerland, Germany, and Singapore, but following an expansion strategy into new markets • Still small but growing partner ecosystem

Table 1: AdNovum Nevis Security Suite major strengths and weaknesses.

The Nevis Suite is flexible in that it can be deployed on-premise, including appliance options, or as a fully multi-tenant cloud service. AdNovum supports UID/password, KBA, OATH, OTP, BioID, RADIUS, Kerberos, x.509, and Vasco tokens for authentication; SAML, OAuth, OIDC, and WS-Federation/Trust for federation; and national ID cards such as ePA and SuisseID.

Nevis Suite features Adaptive, Context-Aware Authentication (ACAA). The risk engine evaluates device fingerprints, geo-locations, and time-of-day in the current iteration. The product will include additional user behavioral analytics and support BehavioSec's behavioral biometrics later in 2017.

Upgrades and configurations can be moved through various test environments automatically or via the GUI. Nevis Suite uses Splunk forwarder or SNMP to send data to SIEM/RTSI systems. NevisReports can draw and information from the Suite. It also can integrate with business intelligence and data analytics solutions via syslog, ElasticSearch API, and REST API façade.

Security	neutral
Functionality	weak
Integration	neutral
Interoperability	neutral
Usability	neutral

Table 2: Nevis Suite rating.

The AdNovum Nevis Security Suite takes a different approach to adaptive authentication. The product has a well-defined architecture that is componentized. It provides several interesting and unique features, such as support for some national ID cards. The risk engine will benefit from additional factor evaluation, and this is planned. Another challenge is the small number of partners and the limited regional reach, being mainly focused on the Swiss and Singapore markets as of now. However, AdNovum does have an expansion strategy into further markets.

11.2 CA Technologies

CA Advanced Authentication is a solution that consists of two modular components – CA Strong Authentication for MFA and CA Risk Authentication for risk analysis. These components can be licensed and deployed jointly (as CA AA) or individually. Both components can be integrated with CA Single Sign-On via an out-of-the-box adapter to protect any web resource integrated into the SSO environment. The product has been adopted by a large number of customers.

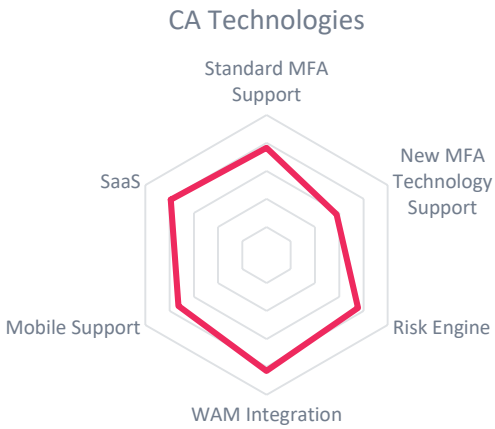
Strengths/Opportunities	Weaknesses/Threats
• Broad support for common authentication mechanisms • Proven strength in large number of enterprise customer deployments • Whitebox methodology for DeviceDNA™ fingerprinting and risk analytics • Fully multi-tenant cloud implementation • Integration with SaaS • Mobile support	• SIEM integration via Syslog; some integration with Splunk • No FIDO support yet

Table 3: CA Advanced Authentication major strengths and weaknesses.

CA Advanced Authentication is quite flexible: it is available as a standalone product, but also integrates with CA's and other IAM vendor's products. It can be deployed on-premise or in the cloud, where it is fully multi-tenant. Customers managing installations may easily promote configuration changes and version upgrades through their various environments.

The product provides capabilities for step-up authentication, including KBA and OTP (email, phone, and SMS). CA Advanced Authentication can also integrate with 3rd party products. Step-up authentication and/or authorization is also available via push notifications to the mobile app. CA is a sponsor member of the FIDO Alliance, and we expect to see FIDO protocol support in the medium term.

The risk engine analyzes up to 200 different risk factors. It also has user behavioral profiling that can trigger various authentication methods based on risk scores and facilitate continuous authentication. The product integrates with SIEM/RTSI via syslog, and with GRC and SRM systems via APIs.



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

Table 4: CA Advanced Authentication rating.

CA Advanced Authentication is a leader in the AA market, being mature and widely deployed. CA Technologies has a good partner base for that product and delivers leading-edge support for heterogeneous IT infrastructures. This makes the product a clear pick for shortlists when looking for an AA solution.

11.3 Entrust IdentityGuard

Datacard Group finalized their purchase of Entrust in early 2014. The merged company commands a large share of the EMV market, and now has taken a big step to a fully multi-tenant Cloud offering. Entrust Datacard has thousands of customers across the globe, serving millions of users, in both the B2C and B2E space. A significant portion of Entrust Datacard's customer base is banking/finance.

Strengths/Opportunities	Weaknesses/Threats
• Fully multi-tenant cloud • Large selection of innovative authentication mechanisms, including biometrics, OTP, OOB push • Standalone, but with Federation support and WAM integration available • Sophisticated risk analytics engine • Integration with Cyber Threat Intelligence providers	• Lacks integration with Service Request Management systems • Some solutions offered are specifically tailored for banking and finance, this can limit its appeal for use in other verticals

Table 5: Entrust IdentityGuard major strengths and weaknesses.

Entrust IdentityGuard is a full-featured adaptive authentication solution that supports a wide range of authenticators, including KBA, out-of-band push mobile apps, OATH OTPs, biometrics, and 3rd party authenticators. It also connects to WAM and federation systems via SAML, RADIUS, and Kerberos.

IdentityGuard's risk analytics engine can evaluate up to 50 different risk- related data points. Administrators can rate and weight the factors via policies. The product also allows user behavioral profiling. The risk engine also can integrate with 3rd party Cyber Threat Intelligence providers. Entrust has an aggressive schedule for on-boarding additional Cyber Threat Intelligence providers, giving it an edge in the security innovation area.

IdentityGuard can output data via syslog to SIEM and RTSI systems. It also offers integration to GRC partner SailPoint. It does not provide out-of-the-box integration with Service Request Management systems, which could be an issue for some potential deployments. Support for FIDO authentication is planned.

Security	positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 6: Entrust IdentityGuard rating.

Entrust IdentityGuard is well-rounded in the typical adaptive authentication feature set. Entrust is responsive to customer's requirements. Support for a large number of authentication mechanisms, an advanced risk engine, and industry-leading inclusion of cyber threat intelligence put IdentityGuard on the short list for organizations looking for adaptive authentication capabilities.

11.4 Evidian Web Access Manager

Evidian is a vendor based in France that is part of Groupe Bull, a large IT vendor and systems integrator. The company provides a comprehensive portfolio in the area of IAM. Their product for Web Access Management is named Evidian Web Access Manager, and it includes Context Aware Authentication. It is integrated with other Evidian solutions both in Identity Provisioning, Governance, and Enterprise Single Sign-On.

Strengths/Opportunities	Weaknesses/Threats
• Authentication proxy architecture facilitates integration of legacy applications • Supports social logins: Facebook, LinkedIn, Twitter, FranceConnect • Detailed device "fingerprinting" as risk factor	• Few system integration partners outside of EMEA • FIDO support not currently available but planned • Cyber threat intelligence integration not currently available but planned

Table 7: Evidian Web Access Manager major strengths and weaknesses.

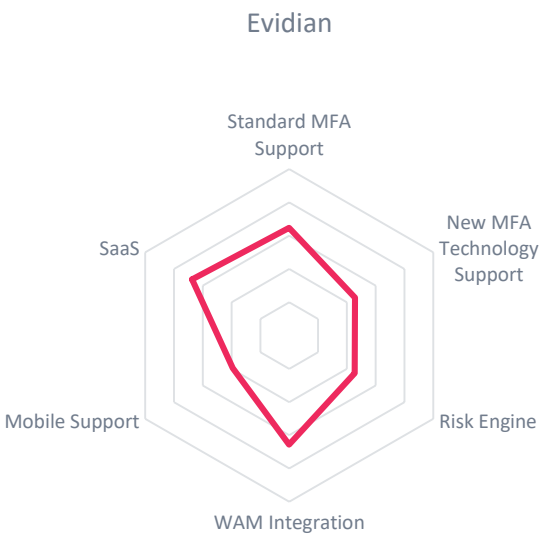
Evidian Web Access Manager is a mature solution for Adaptive Authentication. It runs on various Linux, UNIX, and Windows Server versions. All backend components such as databases are delivered with the product, making it a self-contained deployment. The product supports the main adaptive authentication mechanisms, such as email/SMS OTP and SmartCards. Evidian also accepts social logins, providing a wide range of entry points and step-up authentication options. Support for FIDO authentication is planned.

The risk engine can evaluate the common risk factors, such as device fingerprint, IP address, geo-location, and geo-velocity (could the user have reasonably traveled between last login location and current?). Advanced user behavioral analysis is not available in the product yet.

Evidian's Context Aware Authentication solution can provide data to SIEM/RTSI via REST APIs. It works in conjunction with its own Identity Governance product and Web Access Manager. Federated connections to other WAM systems via SAML, WS-Federation, OIDC, and OAuth are possible.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	neutral

Table 8: Evidian Web Access Manager rating.



Overall, Evidian delivers a respectable offering in Adaptive Authentication, particularly through its integration with its Web Access manager. There are a significant number of system integration partners in Europe, but few in other regions. Overall, the Evidian solution is an interesting alternative to the established players in the market and deserves evaluation in decision making processes.

11.5 ForgeRock Identity Platform

ForgeRock has become a leading vendor in the IAM space. While their products are open source, both their technology and support are enterprise grade. Their offering for Adaptive Authentication, called Adaptive Risk, is a separately licensed module available in Identity Platform. The Adaptive Risk module works in conjunction with ForgeRock Access Management.

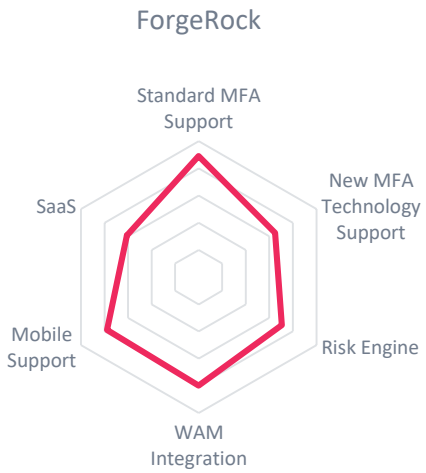
Strengths/Opportunities	Weaknesses/Threats
• Large scale B2C deployments • Integration with Physical Access Control Systems (PACS) • Wide array of authentication methods (from social logins to SmartCards) • Broad platform support • Fully multi-tenant cloud options • UMA support	• No OOTB integration with 3rd party Identity Governance products

Table 9: ForgeRock Identity Platform major strengths and weaknesses.

ForgeRock Identity Platform contains a strong web access management product with built-in adaptive authentication functionality. The core product supports many standards protocols, such as SAML, XACML, OIDC, OAuth2, and OATH; and many authentication mechanisms, including email/SMS OTP, mobile apps with "swipe" or TouchID. Third-party authenticators can be integrated as well. ForgeRock also allows adaptive authentication policies to protect access to non-HTTP resources, such as databases, VMs, and even physical resources, such as doors and gates.

Risk analysis takes place in the ForgeRock Access Management authorization engine, and can be invoked at any point during a session. The risk engine processes detailed device fingerprints, geo-location, and user and device history. Following the XACML model, the authorization can call out to and accept input from other risk engines, which are considered PIPs.

The product is very extensible and supports almost all applicable standards. It can output logs to SIEM/RTSI, and integrate with Privilege Management and Service Request Management systems. Identity Governance is part of ForgeRock Identity Platform.



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

Table 10: ForgeRock Identity Platform rating.

ForgeRock is venture-financed and currently investing heavily in product development. This results in both rapidly improving the already good capabilities of the product and has led to a large partner ecosystem on global scale. ForgeRock has a sizable list of customers with installations supporting up to 150 million external users. ForgeRock Identity Platform has many innovative features in the Adaptive Authentication space and should be considered in product evaluations.

11.6 IBM Advanced Access Control

IBM Security Access Manager integrates the formerly separate products IBM Tivoli Access Manager (TAM) and IBM Tivoli Federated Identity Manager (TFIM). The solution is delivered as a soft/virtual appliance as well as a hardware appliance. Adaptive Authentication capabilities are delivered via a separately licensed Advanced Access Control (AAC) module. Security Access Manager is required to run the AAC product.

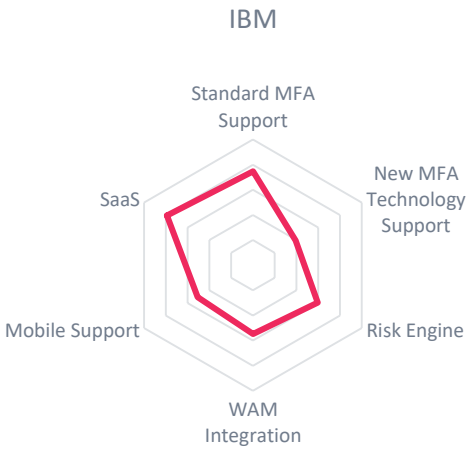
Strengths/Opportunities	Weaknesses/Threats
• Very large customer base, with large scale deployments • Strong integration with IBM identity solutions • Uses IBM Trusteer Fraud Prevention and MaaS Enterprise Mobility Management as risk inputs	• Limited OOTB MFA options • Limitations for multi-tenancy • Interoperability with other IAM solutions constrained to standard protocols • Requires IBM Security Access Manager (WAM)

Table 11: IBM Advanced Access Control major strengths and weaknesses.

IBM's AAC natively supports KBA, OTP, and certificate MFA. RSA, Nuance, Bio-Key, and Entersekt have demonstrated the ability to integrate their authenticators with IBM AAC. More mechanisms, especially mobile-based apps and OTP, will be supported in future releases. The solution can run on a number of OS and IaaS platforms. Though several MSPs run IBM Security Access Manager with AAC, the solution is not fully multi-tenant. AAC does provide MFA options to some common SaaS applications.

The risk engine evaluates basic parameters such as user attributes, device fingerprints, and IP addresses. The risk engine can receive input from Trusteer Fraud Prevention service. It measures current session information against baseline profiles of users' behavior. If deviations are detected, access can be permitted after successful step-up authentication is triggered by a Permit-with-Obligation response. Additionally, the risk engine can process data from IBM MaaS Enterprise Mobility Management reporting the ownership of mobile devices and detect if they are jabilbroken. IBM AAC does not take in cyber threat intelligence from sources other than these two IBM services.

IBM AAC integrates with IBM's QRadar for SIEM, IBM Privilege Management, and IBM Identity Governance. WAM support is included in the base Security Access Manager product. Federation is possible via SAML and OIDC.



Security	positive
Functionality	neutral
Integration	positive
Interoperability	neutral
Usability	positive

Table 12: IBM Security Access Manager with AAC rating.

Security Access Manager AAC is widely deployed and is highly scalable. IBM has a large system of partners and integrators. Some desirable advanced features are not present, specifically MFA options. The requirement to run Security Access Manager and tight integration to other IBM solutions means that AAC is a reasonable add-on, but for organizations with other IAM solutions and/or requirements for interoperability, it may not be a leading candidate.

11.7 MicroFocus Access Manager

MicroFocus' Access Manager is a widely deployed and mature WAM and federation solution. The Advanced Authentication module for adaptive authentication can be licensed separately from MicroFocus' Access Manager product.

Strengths/Opportunities	Weaknesses/Threats
• Large selection of innovative MFA options • Strong geo-location and geo-fencing capabilities • Integration with 3rd party cyber threat intelligence services	• Some scripting may be needed to pull external attributes

Table 13: MicroFocus Access Manager Advanced Authentication major strengths and weaknesses.

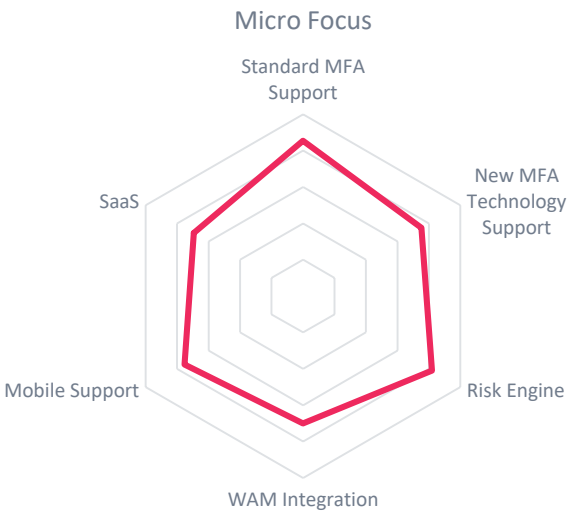
MicroFocus offers two editions: remote access for external users, which includes MFA options such as SMS OTP, OAuth 2, FIDO U2F, and mobile apps; and enterprise, which includes the remote access edition options plus SmartCards and biometrics. It is available as either a hardware appliance or a soft appliance. The Advanced Authentication module integrates with IDaaS such as Microsoft Azure AD, and manages access to common SaaS applications. It also supports many federation standards, such as SAML, OIDC, and WS-Federation.

The risk engine evaluates IP address, geo-location, device fingerprint, user attributes, and user profile baselines. Moreover, input from 3rd party threat management platforms can be received and processed by the risk engine.

MicroFocus integrates with Business Intelligence, Privilege Management, and Identity Governance systems via the REST API. It can also send data to SIEM/RTSI using syslog. Updates and configuration changes can be easily managed via the "Code Promotion" administrative feature.

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

Table 14: MicroFocus Access Manager rating.



Micro Focus has a large partner ecosystem on a global scale. The product is widely deployed, with a significant number of large-scale customer implementations. This product has many innovative features which may appeal to many customers. If advanced MFA options and integrating cyber threat intelligence into the risk engine is important, MicroFocus should be on the list of Adaptive Authentication products to consider.

11.8 PingIdentity

PingIdentity provides adaptive authentication using PingID, PingFederate, and Ping Access. Each product provides different capabilities, and can be licensed individually as necessary, or bundled. The Ping family of products can be run on-premise, in the cloud, or through PingOne cloud services.

Strengths/Opportunities	Weaknesses/Threats
• Large selection of innovative MFA options • Excellent support for identity standards • Highly scalable • Granular access control over data • Cyber Threat Intelligence integration	• No user behavioral analysis • Static rules-based risk engine

Table 15: PingIdentity major strengths and weaknesses.

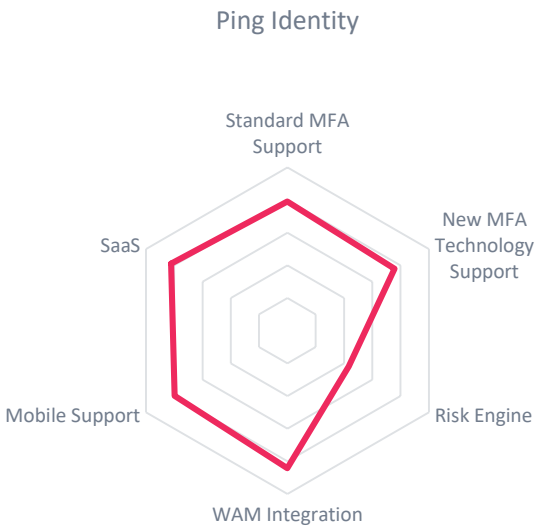
PingID supports email and SMS OTP, voice biometrics, AppleWatch, mobile push notification app, social logins, and Yubikey authentication mechanisms. PingFederate can also support FIDO U2F, RSA SecurID, RADIUS, SmartCards, and SAML federation. Ping products run on both Linux and Windows. PingID handles AA for RDP, SaaS, and VPN integration. Mobile apps run on both Android and iOS, and Mobile Device Management (MDM) integration is coming in a near-term release.

The risk engine evaluates IP address, geo-location, basic device fingerprint, and user attributes via static policies. For mobile devices, PingID can determine if devices are jail-broken. Geo-velocity will be a risk factor in future releases.

The Ping suite integrates with Splunk for Business Intelligence, CyberArk for Privilege Management (configured from CyberArk side), and SailPoint for Identity Governance. All three Ping products can send data to SIEM/RTSI using syslog. Updates and configuration changes can be easily managed via the administrative interfaces.

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

Table 16: PingIdentity rating.



PingIdentity products are widely used and are scalable. They have strong support for identity management standards. Adaptive authentication is achieved through the many MFA options included. The risk engine needs additional functionality, including support for user behavioral analysis, dynamic policies, and integration with 3rd party threat intelligence providers. The UnboundID acquisition brings additional scaling, greater cloud presence, and a focus on consumer identity management. UnboundID adds data governance and XACML-based fine-grained access controls at the resource level. The Ping products are mature and highly capable, and should be considered for adaptive authentication RFIs.

11.9 RSA Adaptive Authentication and SecurID Access

RSA is a major player in the security hardware and software markets. Their Adaptive Authentication product, part of the Fraud and Risk Intelligence suite, is a widely used solution, particularly in the financial industry, supporting hundreds of millions of users. RSA SecurID Access has some adaptive authentication capabilities, and will be indicated separately.

Strengths/Opportunities	Weaknesses/Threats
• Variety of MFA mechanisms supported, including 3rd party products and biometrics • Sophisticated and flexible risk engine • Integration with eFraudNetwork for additional intelligence in risk analytics • SecurID has FIDO U2F and Apple Watch support	• Lack of interoperability with IAM products • Limited integration with other RSA identity solutions • No federation support • May require consulting services for deployment and upgrades

Table 17: RSA Adaptive Authentication and SecurID major strengths and weaknesses.

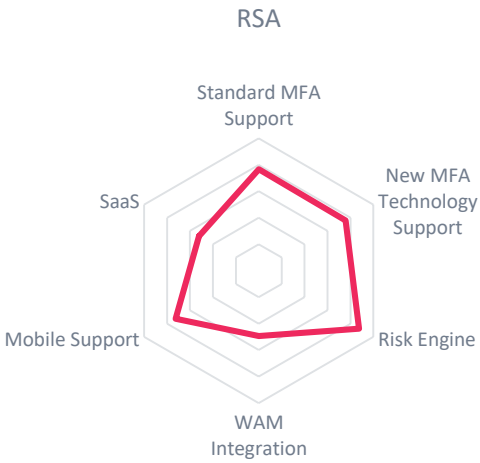
RSA Adaptive Authentication supports KBA, SMS OTP, Android and iOS biometrics, 3rd party biometrics, Eye-Verify biometrics, and mobile app OTP as MFA mechanisms. Administrators can stipulate that multiple authenticators are required via API calls and static policies. It can be deployed either on-premise or as SaaS. RSA SecurID supports FIDO U2F and Apple Watch.

The Adaptive Authentication product has extensive user behavioral profiling capabilities, based on users' historical interactions. The Adaptive Authentication solution receives input from the RSA eFraudNetwork service, which collects, compiles, and disseminates data on malicious activity attempts to reduce fraudulent transactions. The risk engine uses Naïve Bayesian machine learning algorithms to fine tune predictive capabilities for each customer. The risk engine can receive feeds from a variety of external threat intelligence sources, and can analyze the accuracy of each source and reports findings to administrators.

RSA Adaptive Authentication can work with RSA Archer, but integration with other RSA identity products is weak, and interoperability with other WAM systems is currently absent. RSA SecurID does have OOTB WAM support.

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

Table 18: RSA Adaptive Authentication and SecurID rating.



With over 8,000 customers serving more than 900 million users, RSA's products are very scalable. The Adaptive Authentication risk engine capabilities surpass the competition in terms of sophistication and flexibility. The lack of integration with other RSA products and the lack of interoperability with other vendors are drawbacks. However, if MFA and a powerful risk engine are top requirements, RSA should be at the top of the consideration list.

11.10 SecureAuth IdP

SecureAuth is a well-established vendor in the AA market. They have a large customer base, predominantly in North America. As their name implies, their strength is authentication. SecureAuth is an on-premise solution, including appliance and virtual appliances.

Strengths/Opportunities	Weaknesses/Threats
• Variety of MFA mechanisms supported, including some 3rd party products and biometrics • Broad support of federation and other IAM standards and protocols • Cyber threat intelligence integration • Large ecosystem of IAM partners	• No automated code and configuration migration tools

Table 19: SecureAuth IdP major strengths and weaknesses.

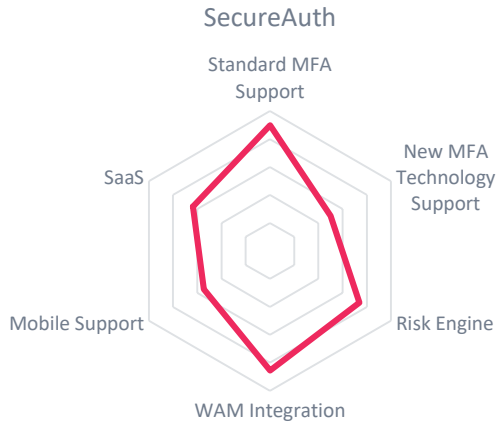
SecureAuth supports more forms of MFA than any other vendor: PIN, KBA, email/phone/SMS OTP, SmartCards, iOS and Android biometrics, behavioral biometrics, Mac OATH tokens, Yubikeys, Push notifications, federated logins, social logins, and more. It can front-end authentication to common SaaS applications, and integrate with any standards-based identity repositories, such as Ping Identity, Okta, RSA, and Microsoft Active Directory.

The risk engine can evaluate user attributes and user behavioral analysis, geo-location, geo-velocity, and device fingerprints. SecureAuth Threat Service is a subscription service that provides threat intelligence to the risk engine for real-time fraud prevention and risk mitigation.

SecureAuth integrates with SailPoint for identity governance. It can also connect with HP ArcSight, IBM QRadar, Splunk for SIEM/RTSI as well as Business Intelligence. SecureAuth partners with CyberArk for Privilege Management.

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

Table 20: SecureAuth IdP rating.



As a pure play adaptive authentication product, SecureAuth is one of the most compelling choices. Their broad support of innovative MFA, federation, and directory options is outstanding. Wide support of IAM standards allows interoperability with many other vendors' products. The ability to ingest threat intelligence in real-time is also a key differentiator. Lastly, the large partner ecosystem ensures that all the necessary IAM suite functions and integrations are possible. SecureAuth should be on the shortlist for any adaptive authentication RfI.

11.11 Vasco

Vasco is a global company with a history in identity management and electronic signatures. Their best known product, considered here, is DIGIPASS, which works in concert with IdentiKey. The products are available as both hardware appliance and virtual appliance. Vasco also offers its own cloud service.

Strengths/Opportunities	Weaknesses/Threats
• Good support of MFA mechanisms, including biometrics • Strong focus on mobile apps • Sophisticated risk analytics	• No support for 3rd party threat intelligence feeds • Needs interoperability with identity governance and privilege management products

Table 21: Vasco major strengths and weaknesses.

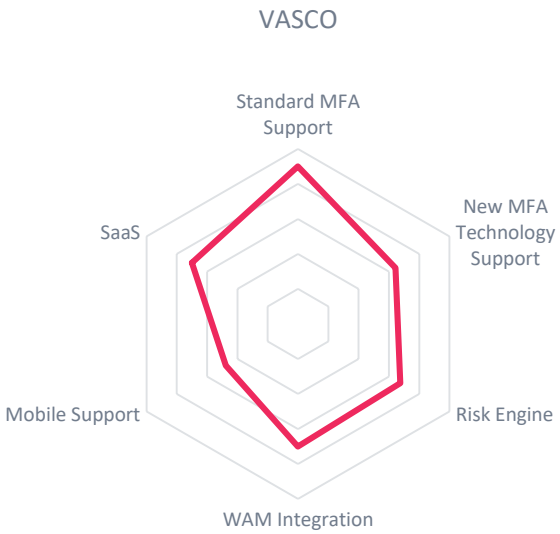
Vasco has good MFA support, including OATH OTP, Android and iOS touch biometrics, facial recognition biometrics, and mobile push notification apps. The IdentiKey federation server includes SAML, Kerberos, and RADIUS support. It integrates with many common identity repositories, such as Microsoft Active Directory, OpenLDAP, IBM Security Directory, and NetIQ Directory.

The risk engine can process up to 150 different factors, including the standard device fingerprint, IP address, geo-location, and proxy detection. It applies machine learning and neural network algorithms to user patterns to produce real-time risk scores. The product is fine-tuned for fraud prevention.

The Vasco products can send data to SIEM/RTSI via syslog or .csv files. They integrate with Identity Governance and Privilege Management solutions through SOAP APIs. Administrators can promote test configurations from development to production with automated tools.

Security	positive
Functionality	neutral
Integration	positive
Interoperability	positive
Usability	strong positive

Table 22: Vasco DIGIPASS and IdentiKey rating.



As an established identity management vendor, Vasco has a robust adaptive authentication offering. Their product suite includes many innovative features, as well as standard functions. They have a large customer base serving mid-sized user populations. Additional integration and interoperability with other IAM solutions may make the products more appealing.

12 Products at a glance

Based on our evaluation, a comparative overview of product ratings covered in this document is shown in table 23.

Product	Security	Functionality	Integration	Interoperability	Usability
AdNovum Nevis	neutral	weak	neutral	neutral	neutral
CA Technologies	positive	strong positive	strong positive	positive	strong positive
Entrust Datacard	positive	positive	positive	positive	positive
Evidian	positive	neutral	positive	positive	neutral
ForgeRock	positive	positive	strong positive	strong positive	positive
IBM Adaptive Access Control	positive	neutral	positive	neutral	positive
MicroFocus	strong positive	positive	positive	neutral	strong positive
PingIdentity	positive	positive	positive	strong positive	strong positive
RSA Adaptive Authentication	positive	strong positive	weak	neutral	strong positive
SecureAuth	strong positive	positive	strong positive	strong positive	strong positive
Vasco	positive	neutral	positive	positive	strong positive

Table 23: Comparative overview of the ratings for the product capabilities.

Table 24 provides an overview containing four additional ratings for the vendor, expanding 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	neutral	neutral	neutral	neutral
CA	positive	positive	strong positive	strong positive
Entrust Datacard	positive	neutral	positive	positive
Evidian	neutral	neutral	strong positive	positive
ForgeRock	strong positive	positive	strong positive	strong positive
IBM Adaptive Access Control	neutral	strong positive	strong positive	strong positive
MicroFocus	positive	neutral	positive	neutral
PingIdentity	positive	positive	strong positive	strong positive
RSA Adaptive Authentication	strong positive	strong positive	strong positive	strong positive
SecureAuth	strong positive	neutral	neutral	positive
Vasco	neutral	neutral	strong positive	positive

Table 24: Comparative overview of the ratings for vendors.

Table 24 requires additional explanation in the event a vendor received a "critical" rating.

In the category of *Innovativeness*, this rating is applied if vendors provide none or very few of the advanced features we sought in that analysis, such as support for multi-factor authentication, advanced risk engines, integration with other security products, and others. However, in this analysis all vendors scored at least neutral regarding this criterion.

The *critical* ratings are applied for *Market Position* specific to vendors which have very limited visibility (with the evaluated product and in general) 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 the category of *Financial Strength*, "critical" applies for vendors with a very limited customer base. 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. This rating applies in case of a lack of information about financial strength. It is also possible that vendors with better ratings might fail and disappear from the market.

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

12.1 The Market/Product Matrix

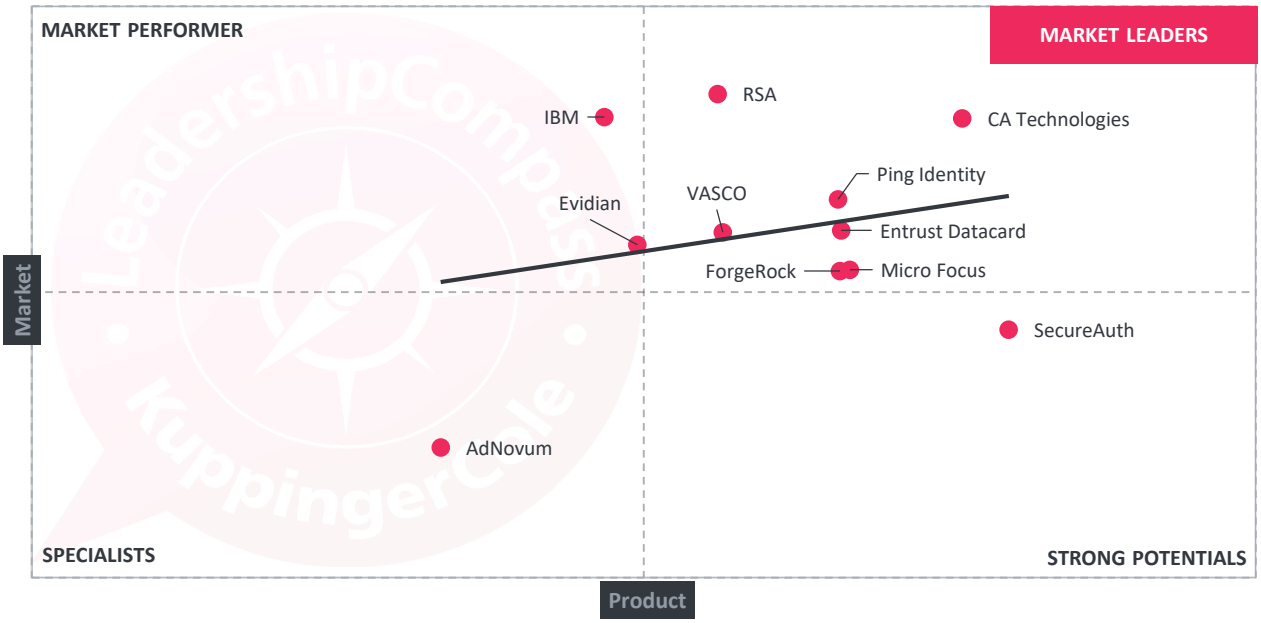


Fig. 9: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

We have compared the position of vendors regarding combinations of our three major areas of analysis, i.e. Market Leadership, Product Leadership, and Innovation Leadership.

These comparisons, for instance, use the rating in Product Leadership on the horizontal axis and relate it with the rating in other areas, which is shown on the vertical axis. The result is split into four quadrants. The upper right quadrant contains products with strength both in the product rating and in the second rating, in this case, market rating. The lower right quadrant contains products that are overall strong but are lacking in the dimension shown on the vertical axis.

For example, products that have strong technical capabilities but are relatively new to the market may currently have a small customer base. The upper left quadrant contains products which are typically below average in the product rating but have specific strengths in the second dimension of each matrix. They might be highly innovative or very mature and established, but not leading edge when looking at the product rating. Finally, the lower left quadrant contains products suffering on both axes. However, these products might have specific strengths that are highly valuable for some specific use cases.

This comparison shows which vendors are better positioned in our analysis of Product Leadership compared to their position in the Market Leadership. Vendors above the line are "overperforming" in the market. Often the overperformers are the very large vendors, while vendors below the line frequently are innovative but focused on specific regions.

We've defined four segments of vendors to help in classifying them:

Market Leaders: This segment contains vendors which have a strong position in our categories of Product Leadership and Market Leadership. These vendors have an overall strong to excellent position in the market.

Strong Potentials: This segment includes vendors which have strong products, as demonstrated by being ranked high in our Product Leadership evaluation. However, their market position is not as good. That might be due to various reasons, such as a regional focus or the fact that they are niche vendors in that market segment.

Market Performers: Here we find vendors which have a stronger position in Market Leadership than in Product Leadership. Typically, such vendors have a strong, established customer base because they are active in other markets.

Specialists: Specialists usually have specific strengths, but provide neither full coverage of all features which are common in the particular market segment, nor count among the software vendors with very large related product portfolios.

This chart shows an interesting distribution of the vendors. Due to the maturity of the market and vendor products, most of the solutions surveyed fit into the Market Leaders section of the chart. They are separated by degrees. We find CA Technologies, Entrust Datacard, ForgeRock, MicroFocus, PingIdentity, RSA, SecureAuth, and Vasco Data Security here.

SecureAuth is the only member of the Strong Potentials segment, with both excellent innovativeness and product leadership, but smaller market size.

Evidian and IBM make up the Market Performer category. AdNovum Informatik is the lone Specialist in this analysis.

12.2 The Product/Innovation Matrix

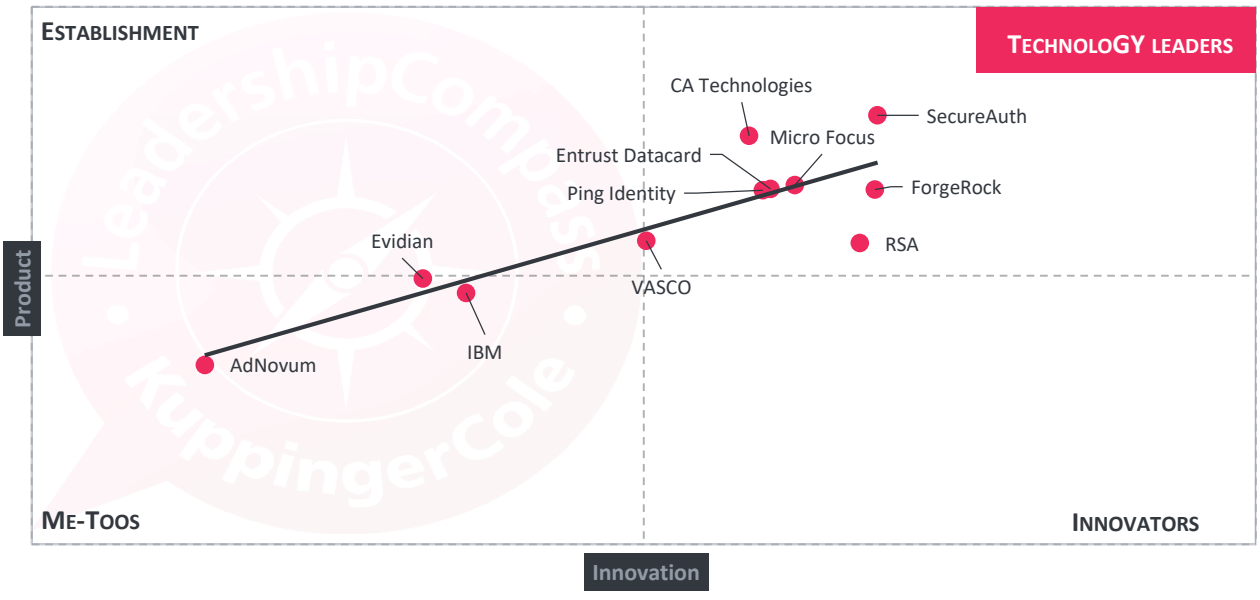


Fig. 10: The Product/Innovation Matrix. Vendors on the right are less innovative, while vendors on the left are, compared to the current Product Leadership positioning, more innovative.

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 few exceptions. This distribution and correlation is typical for mature markets with a significant number of established vendors.

We have four segments of vendors. These are:

Technology Leaders:	This group contains vendors which have technologies which have strong functionality and which show a good degree of innovation.
Establishment:	In this segment, we typically find vendors which have a relatively good position in the market but don't perform as well when it comes to innovation. However, there are exceptions if vendors take a different path and focus on innovations which are not common in the market, and thus do not count that strong for the Innovation Leadership rating.
Innovators:	Here we find highly innovative vendors with a limited visibility in the market. It is always worth having a look at this segment because these vendors might be a fit for specific customer requirements, especially those with advanced use cases.
Me-toos:	This segment mainly contains those vendors which are following the market in terms of functionality and innovation. There are exceptions in the case of vendors which take a fundamentally different approach to providing specialized point solutions. However, in most cases this is more about delivering what others have already created.

In this chart, most vendors are placed in the Technology Leaders segment, with a strong correlation of Innovation and Product rating. This is typical for more mature markets, where most vendors deliver a broad set of features, including at least a significant portion of the more innovative features.

In the analysis of this segment, we see many vendors in the upper right edge, indicating strength in both product capabilities and innovativeness, while others are more to the lower left, showing that these are not as strong in these ratings.

Vasco Data Security is located on the intersection of the "Technology Leaders" and the "Innovators" quarter. Evidian is on the dividing line between "Me-Toos" and "Innovators", while IBM and AdNovum are found in the "Me-Toos" section.

12.3 The Innovation/Market Matrix

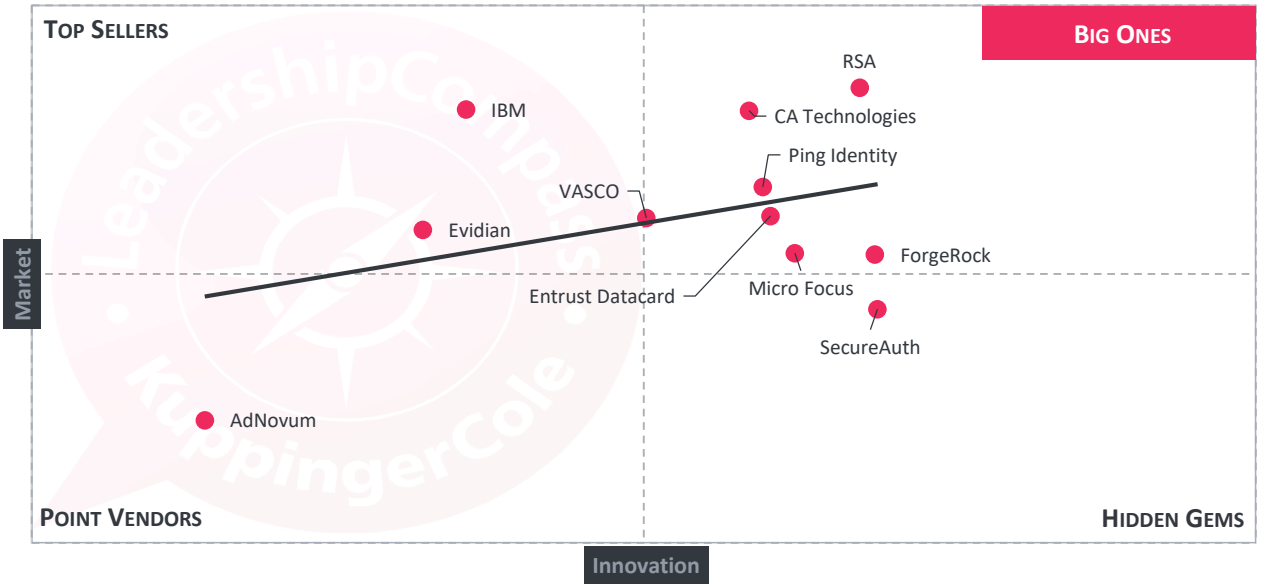


Fig. 11: The Innovation/Market Matrix. Vendors on the right are comparatively more innovative than those on the left. Vendors above the line have larger market shares, while vendors below the line have more opportunity to improve their market position.

The third comparison shows how Innovation Leadership and Market Leadership are related. Some vendors might perform well in the market without being Innovation Leaders. This might suggest 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. It is also possible that they might fail, especially in the case of smaller vendors.

The four segments we have defined here are:

Big Ones: These are market leading vendors with a good to strong position in Innovation Leadership. This segment mainly includes large software vendors.

Top Sellers: In this segment, we find vendors which have an excellent market position compared to their ranking in the Innovation Leadership rating. That can be caused by a strong sales force or by selling to a specific community of repeat customers, i.e., a loyal and powerful group of contacts in the customer organizations.

Hidden Gems: Here we find vendors which are more innovative than would be expected when looking at their Market Leadership rating. These vendors have a strong potential for growth; however, they may fail to meet their potential. Nevertheless, this group is always worth a look because of their innovativeness.

Point Vendors: In this segment, we find vendors which typically either have point solutions or which are targeting specific groups of customers such as SMBs. Point Vendor solutions may be focused on specific customers, and therefore not cover all requirements of all types of customers. Thus, they are not among the Innovation Leaders. However, these vendors might be attractive if their solution fits the specific customer requirements.

Here we see most of the companies surveyed being both highly innovative and having a strong position in the market. These Big Ones include CA Technologies, Entrust Datacard, ForgeRock, Micro Focus, PingIdentity, RSA, and VASCO Data Security.

SecureAuth is in the Top Seller category. Evidian are IBM are found in the Hidden Gem section, while AdNovum Informatik occupies the Point Vendor area.

13 Overall Leadership – the combined view

Finally, we've put together the three different ratings for Leadership, i.e. Market Leadership, Product Leadership, and Innovation Leadership and created an Overall Leadership rating. This is shown below in figure 12.

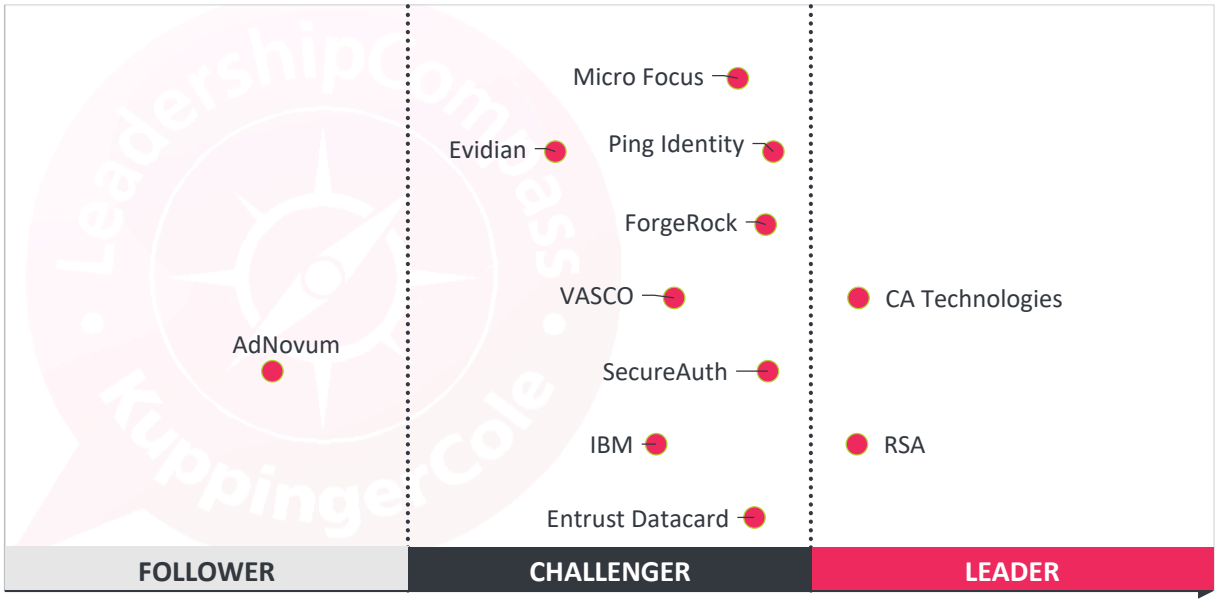


Fig. 12: The Overall Leadership rating for the Adaptive Authentication market segment [Note: There is only a horizontal axis. Vendors to the right are positioned better.].

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

In the market for adaptive authentication, we currently see two companies in the Leaders segment for Overall Leadership. CA Technologies and RSA are the established players with strong offerings and large customer bases.

The Challenger segment is very crowded, with most vendors being placed in that segment. Here we find Entrust Datacard, ForgeRock, MicroFocus, PingIdentity, and SecureAuth. All are top challengers, and are almost leaders in this space. Evidian, IBM, Vasco Data Security, reside in the center of the Challenger segment. Each of these vendor's products have various strengths that make their solutions attractive to different kinds of customers.

AdNovum Informatik is found in the Followers section. Vendors may be placed in the Followers section for several reasons, such as small customer base or lack of global reach.

Leadership does not automatically mean that these vendors are the best fit for a specific customer requirement. In a mature market such as this, one vendor may excel at certain features, and only meet the minimum levels for others. To choose the right product, a thorough evaluation of organizational requirements and a mapping to the features provided by the vendors' products is mandatory.

Overall Leaders are (in alphabetical order):

- CA Technologies
- RSA

14 Vendors and Market Segments to watch

Besides the vendors covered in this KuppingerCole Leadership Compass on Adaptive Authentication, there are several other vendors which either declined to participate in this KuppingerCole Leadership Compass, have only a slight overlap with the topic of this document, or are not (yet) mature enough to be considered in this document. This includes the following vendors:

14.1 CallSign

CallSign is a mobile multi-factor authentication solution. The security startup is headquartered in London, UK. CallSign is a mobile app that works on both Android and iOS. It uses biometrics and behavioral analysis to strongly authenticate users for both other mobile applications, as well as VPNs and SaaS applications. After installation on their smartphones, registered users can simply swipe a finger across the touchscreen to authenticate to apps or approve transactions.

CallSign currently offers integration with F5, Dropbox, G Suite, Juniper, Office365, and Salesforce. CallSign also licenses an SDK to allow implementers to develop customized application integration. The product also features a dashboard for enterprise reporting.

14.2 InWebo

InWebo, with offices in the US, France, and Germany, provides a multi-factor authentication solution that is deployable either on-premise or in the cloud. It is federation enabled, and processes RADIUS and SAML authentication.

For multi-factor authentication, InWebo provides mobile apps for OTP and Push notifications. The mobile app is used as a 2nd factor for browser access. The app generates keys, which the user subsequently can unlock via native biometrics (such as fingerprint swipe) or by entering a PIN. The same user actions are available for Push notification. The desktop application can also exchange keys and allow a user to unlock via a PIN. Once a user registers multiple devices with the InWebo service, the user can enter a single PIN to unlock any of their associated devices. InWebo brokers authentication to VPNs, SSO systems, common SaaS apps, and Windows login. The InWebo solution will be investigated further for possible inclusion in future KuppingerCole Leadership Compasses.

14.3 NokNok Labs S3 Authentication Server

NokNokLabs, a Silicon Valley based startup, has delivered a set of mobile-oriented products that perform adaptive authentication, in conformance with the FIDO UAF standards. The S3 Authentication server can run in the cloud or on-premise. The NokNok Authentication server interoperates with any other FIDO UAF client or authenticator. Examples of authenticator types include PIN-based, behavioral, and biometrics such as fingerprint, facial recognition, iris recognition, and voice recognition. The Authentication server allows administrators to write policies that determine which authenticators can be or are required to access relying party applications, both mobile and web-based. The Authentication server also provides federation options such as SAML and OIDC via connectors to PingIdentity's PingFederate and IBM's Security Access Manager.

The S3 Authentication Suite and SDKs allow implementers to not only take advantage of existing FIDO authenticators, but also to build their own mobile, out-of-band solutions. NokNok is positioning this product as a more secure alternative to OTPs, thus it does not support OTPs. The SDKs also utilize secure development components, such as Trusted Platform Modules, Global Platform Trusted Execution Environment and Secure Elements for Android devices, and Secure Enclave for iOS. Apps created using the NokNok SDK can gather and transmit the following types of risk factors from mobile devices: geo-location, geo-velocity, device ID, Android device health indicators, and shared device indicators. These risk factors can be evaluated by the NokNok Authentication server.

NokNokLabs may be considered a leading edge vendor in the FIDO UAF market, which is directly relevant to adaptive authentication. The Authentication server also integrates with WAM and SSO systems via federation. However, it does not provide full backward compatibility with other adaptive authentication types, and it does not yet integrate with other IAM products, such as identity governance, privilege management, etc. We expect that NokNokLabs' products will be included in future KuppingerCole Leadership Compasses.

14.4 One Identity Cloud Access Manager

One Identity is a leading IAM vendor, with a broad portfolio for identity and access management. Part of this portfolio is One Identity Cloud Access Manager. While the name indicates a cloud-based solution, the product is, in fact, an on-premise solution for Web Access Management and Identity Federation.

Cloud Access Manager is a well-thought-out solution with features such as risk-based policy decisions and integrated support for MFA both as a service and on-premises (through One Identity's Defender offerings).

14.5 Oracle Adaptive Access Manager

Oracle Adaptive Access Manager, or OAAM, is a component of their Identity Management Middleware suite. It works in conjunction with Oracle Access Manager (OAM) and Oracle Entitlements Server. The entire suite is designed as an on-premise solution. OAM contains the policies and web access management functions. OAAM provides the step-up authentication and risk engine features. OAAM supports password, KBA, SMS OTP, and virtual authenticators.

The virtual authenticator approach is unique. One option for virtual authentication is server-based: the server presents images or phrases that the user chose at registration time, then asks the user to confirm that the image or phrase is correct at authentication time. Other options include images inscreen based

keyboards and numeric pads, in which users enter their PINs, passwords, or passphrases via mouse. The entry of passwords, PINs, or passphrases is protected since normal man-in-the middle attacks would fail.

OAAM's risk engine can process device fingerprints and do comparative analysis on user behavioral profiles.

Oracle was invited to participate in this Leadership Compass, but declined. We will likely include them in future research.

14.6 Ubisecure

Ubisecure is a leading provider of digital certificates and extends its portfolio into other areas. Ubisecure is different from most other solutions in the market in its focus on service providers instead of end-user organizations. Thus, the feature set concentrates on the specific requirements for these groups of users. However, we see the product also as an interesting solution for end-user organizations.

Ubisecure has shown commitment to innovation by enabling advanced mobile-based biometric authentication. The primary focus of the product is supporting service providers in providing controlled access for customers or citizens, which also serves well for use cases of large organizations that need to support consumer and customer access. The product supports a broad range of authentication methods, including banking cards and national ID cards.

14.7 United Security Providers AG

USP AG is a Swiss-based vendor of security solutions. Their Secure Entry Server combines access management, federation, authorization, network access control, and web application firewall functionality. It is available for cloud or on-premise deployment, and comes as a hardware appliance if desired. The SES supports X.509 certificate, Kerberos, Integrated Windows Authentication, ELCARD, MobileTAN/SMS OTP, YubiKey, SuisseID, Google Authenticator, RSA SecurID, Safenet, Vasco, MobileID, and SAML 2.0 authentication. SES can store and read attributes from LDAP, Active Directory, RADIUS, and other user repositories.

The web application firewall feature can prevent the following types of attacks: OWASP Top10, SQL Injection, Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), AJAX/JSON web threats, Layer 4-7 DoS and DDoS, Brute force attacks, Sensitive information leakage, Session hijacking, session fixation, Buffer overflows, Replay attacks, and many more.

United Security Providers AG's SES suite takes an innovative approach to access management and adaptive authentication. KuppingerCole will track USP AG and include their products in future publications.

15 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**

Kuppinger Cole Ltd.
Sonnenberger Strasse 16
65193 Wiesbaden | Germany

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