KuppingerCole Report

LEADERSHIP COMPASS

by John Tolbert | October 2018

Cloud-based MFA Solutions

This report provides an overview of the market for Cloud-based Multi-Factor Authentication (MFA) Solutions and provides you with a compass to help you to find the service that best meets your needs. We examine the market segment, vendor service functionality, relative market share, and innovative approaches to providing Cloud-based MFA Solutions.

by **John Tolbert**
jt@kuppingercole.com
October 2018

Leadership Compass
Cloud-based MFA Solutions
By KuppingerCole

Content

List of Tables

List of Figures

Related Research

Executive View: Entrust IdentityGuard for Enterprise – 71321
Executive View: ForgeRock Identity Platform – 70296
Executive View: Idaptive (formerly Centrify) Next-Gen Access Platform – 79036
Executive View: Microsoft Azure Information Protection – 72540
Executive View: Microsoft Azure Stack – 72592
Executive View: OneGini Connect – 79031
Executive View: One Identity Safeguard – 79042
Executive View: Ping Identity's PingDirectory – 70294
Executive View: Ping Identity's PingOne – 70288
Executive View: Symantec CloudSOC™ – 70615
Executive View: Symantec Advanced Threat Protection – 71155
Leadership Brief: Why Adaptive Authentication Is A Must – 72008
Leadership Brief: Mobile Connect – 71518
Leadership Brief: Transforming IAM – not Panicking – 71411
Leadership Compass: Adaptive Authentication – 71173
Leadership Compass: Adaptive Authentication – 79011

1 Introduction

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 business and security risks as well as the availability of newer technologies. Businesses have lobbied for these security checks to become less obtrusive and provide a better user experience (UX). Many organizations are opting to deploy these capabilities in conjunction with their Identity-as-a-Service (IDaaS) solutions or as part of a "cloud-first" strategy.

Cloud-based MFA is the process of using a SaaS solution to gather additional attributes about users and their environments and evaluate the attributes in the context of risk-based policies. The goal of Cloud MFA 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 involves keystroke analysis, mobile "swipe" analysis, and even mobile gyroscopic analysis.

Cloud MFA 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. A more advanced form of Cloud MFA uses risk-scoring analytics algorithms to first baseline regular access patterns and then be able to identify anomalous behavior which triggers additional authentication challenges. This can be referred to as dynamic Cloud MFA, yet it is difficult to categorize Cloud MFA products into dynamic or static Cloud MFA 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 Cloud MFA proves the most appropriate, and both approaches are not without their limitations.

A wide variety of Cloud-based MFA mechanisms and methods exist in the market today. Examples include:

- Knowledge-based authentication (KBA)
- Strong/Two-Factor or Multi-Factor Authentication (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 and device health assessment
  - User Behavioral Analysis (UBA)

Many organizations today employ a variety of 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.

Cloud-based MFA, 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, Cloud-based MFA can even be construed as a form of attribute-based access control (ABAC).

The story above is just one possible example. Cloud-based MFA 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. Cloud-based MFA can help mitigate risks and protect enterprises against fraud and loss.

There are a number of vendors in the Cloud-based MFA market. Many of the vendors have developed specialized Cloud-based MFA products and services, which can integrate with customers' on-site IAM components or other IDaaS. The major players in the Cloud-based MFA segment are covered within this KuppingerCole Leadership Compass.

Overall, the breadth of functionality is growing rapidly. Support for standard Cloud-based MFA mechanisms and the requisite identity federation are 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.

1.1 Market Segment

This 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 either Cloud-based MFA or on-premises Adaptive Authentication if they have not already to help reduce the risk of fraud and data loss.

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.

1.2 Delivery models

In this Leadership Compass, we consider cloud-based solutions only. See the recently released KuppingerCole Leadership Compass on Adaptive Authentication for similar solutions available for on-site deployment.

1.3 Required Capabilities

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

- Support multiple authenticators such as;
  - Smart Cards, USB tokens
  - Mobile apps and push notifications
  - x.509
  - Biometrics
  - OTP: phone, email, and SMS
- Integrate with IAM systems
- Perform real-time risk analysis of behavioral and environmental factors
- Support federation via OAuth2, OIDC, and SAML
- Facilitate compliance with existing and emerging regulatory frameworks, particularly EU GDPR and PSD2 (Revised Payment Service Directive)
- Adhere to policy-based access controls model so that IT departments and Line of Business application owners can define risk appropriate authentication rules
- Integrate with security intelligence and forensic systems
- Provide administrators with management dashboards and configurable reporting
- Allow for delegated and role-based administration

- Consider threat intelligence: subscription to 3rd party services that identify malicious IP addresses, URLs, patterns of fraud, and compromised credentials

Cloud-based MFA is an evolution 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 Cloud-based MFA 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 Cloud MFA and AA 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 Cloud 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. All Cloud MFA solutions, almost by definition, require and support identity federation. 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.

When evaluating the services, besides looking at the aspects of

- overall functionality
- size of the company
- number of customers
- number of developers
- partner ecosystem
- licensing models
- core features of Cloud-based MFA technology

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

Basic Authenticators	Username/password: the most basic form, not recommended. 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 SMS OTP implementations are not truly random, and attackers have discovered ways to circumvent SMS OTP, some organizations such as US NIST have deprecated the use of SMS OTP as a primary or step-up authentication method.
Advanced Authenticators	FIDO 2.0, 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. FIDO 2.0 is the latest iteration and will likely surpass U2F and UAF in adoption in the years ahead. SmartCards have 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. Other types of hardware tokens employ similar technologies in different form factors, such as RSA SecurID and Yubikeys.

	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.
Mobile support	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. The ratings for mobile support include whether or not a product adheres the Global Platform Secure Element (SE) and Trusted Execution Environment (TEE) for Android, and whether or not the product utilizes Secure Enclave in iOS.
Risk Analysis	Factors such as IP address, device fingerprints, device health assessment geo-location, geo-velocity, integration of 3rd-party threat intelligence, user behavior profiling
Threat Intelligence	Subscriptions to real-time feeds of known bad IP addresses, locations, proxies, malicious URLs, and compromised credentials
SSO	Single sign-on, generally to on-premise or LOB applications, using federation standards
SaaS integration	Use of federation technologies such as OAuth, OIDC, and SAML to allow authenticated users to seamlessly access popular SaaS applications.

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

Please note that we only listed major features, but also considered other capabilities as well when evaluating and rating the various Cloud-based MFA products.

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

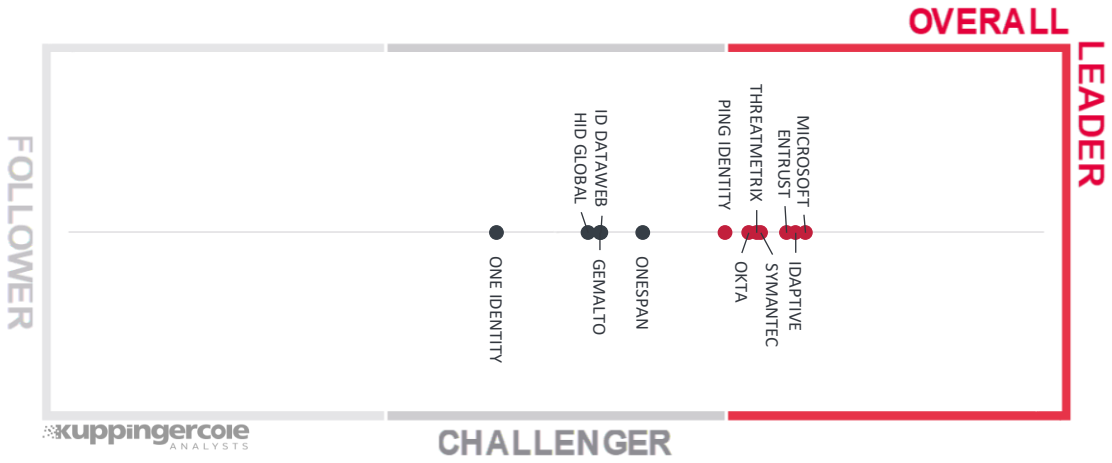


Figure 1: The Overall Leadership rating for the Cloud-based MFA market segment

We find several companies in the Leader section. Microsoft, Idaptive, and Entrust are at the top, showing strong ratings in all Leadership categories.

Okta, Ping Identity, Symantec, and ThreatMetrix are also in the Leader area. All seven of these companies have strong cloud-based MFA offerings which need to be compared carefully when conducting product evaluations. Each one has particular strengths, and overall, they have excellent MFA capabilities.

In the Challenger segment, Gemalto, HID Global, ID Data Web, and OneSpan, are all near the boundary with the Leader section. Each one of these vendors takes a slightly different approach, and as such, has somewhat different areas of focus for their Cloud MFA offerings. Rounding out the Challenger block are HID Global and One Identity.

Overall Leaders are (in alphabetical order):

- Entrust Datacard
- Idaptive
- Microsoft
- Ping Identity
- Okta
- Symantec
- ThreatMetrix, a LexisNexis Risk Solutions Company

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

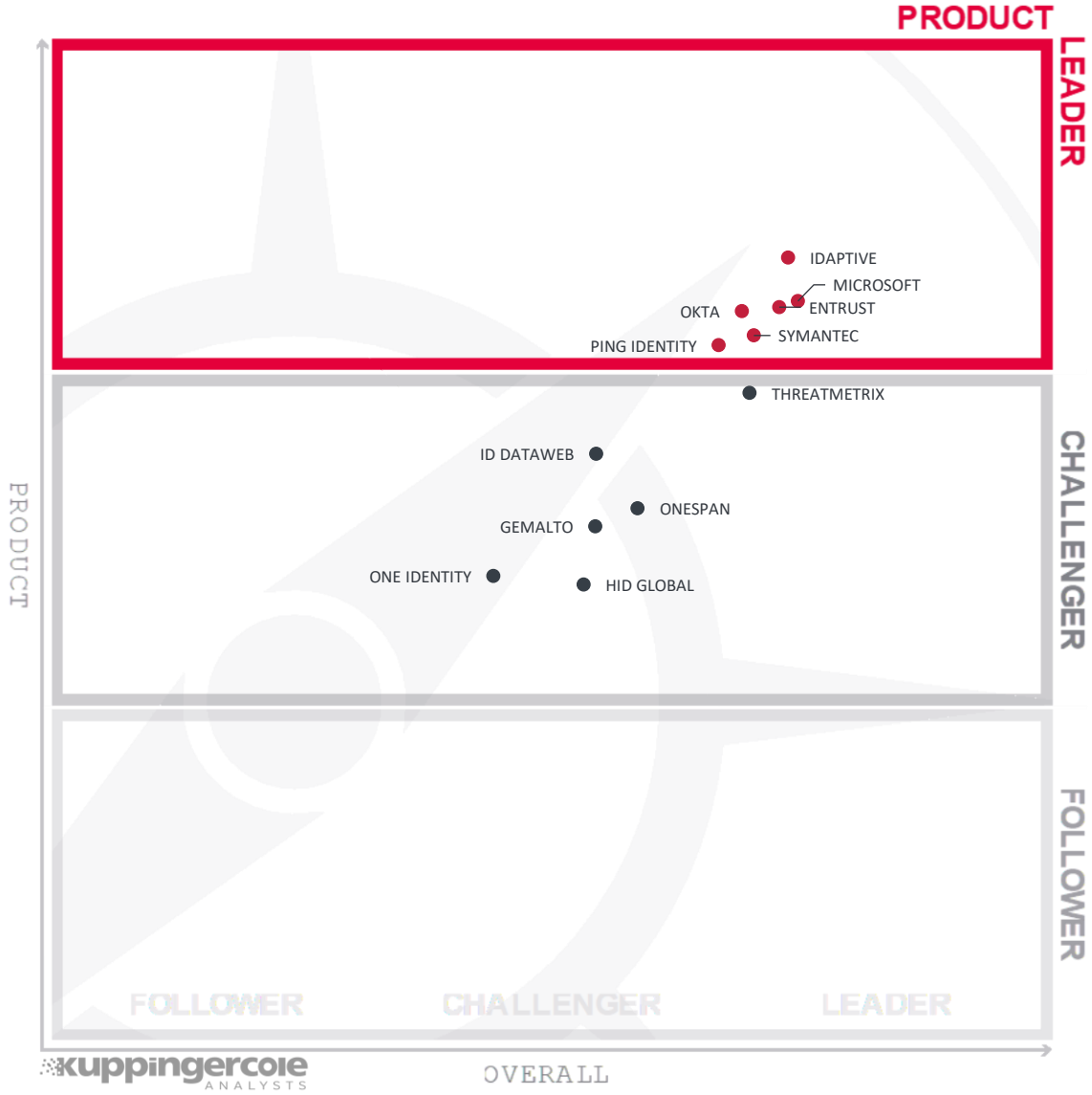


Figure 2: Product leaders in the Cloud-based MFA market segment

Product Leadership, or in this case, Service Leadership, is where we examine the functional strength and completeness of services. Idaptive is at the high point, sharing the leadership section with Microsoft, Entrust Datacard, Okta, Ping Identity, and Symantec. For this Leadership Compass, the breadth of authenticator support along with configurability and usefulness of the adaptive risk engine are key differentiators. The vendors in the top spots have much to offer in both of those categories.

In the Challenger section, ThreatMetrix is at the top, followed by ID Data Web, which is approaching the upper ranks. ThreatMetrix' intelligence services drive it to the top of the Challenger segment, while ID Data Web has numerous identity and attribute validation sources. Next up we see Gemalto, HID Global, One Identity, and OneSpan, which are also Challengers in the Cloud-based MFA market.

Product Leaders (in alphabetical order):

- Entrust Datacard
- Idaptive
- Microsoft
- Okta
- Ping Identity
- Symantec

Next, we examine **innovation** in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested cutting-edge features, while maintaining compatibility with previous versions.

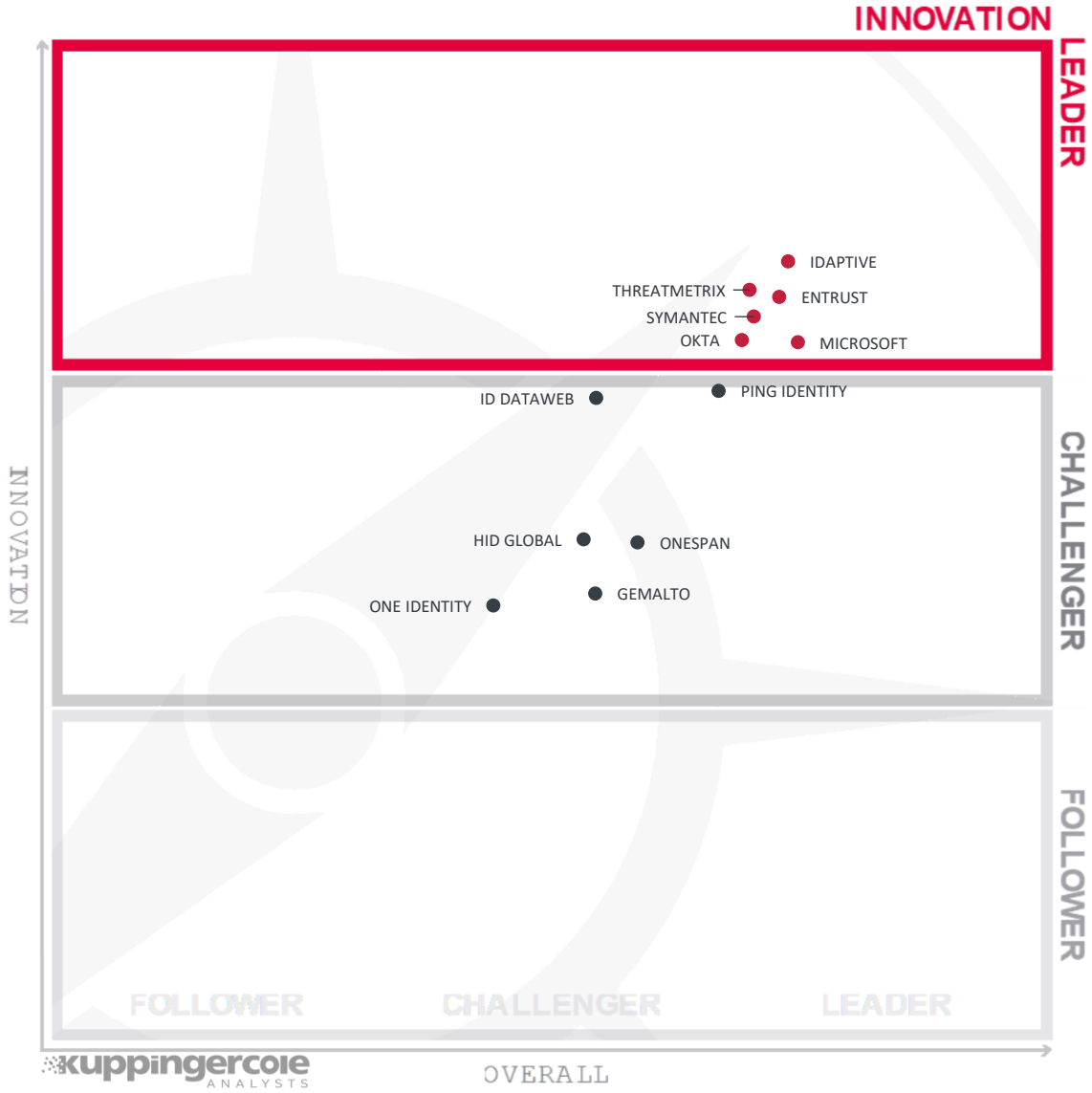


Figure 3: Innovation leaders in the Cloud-based MFA market segment

When looking at Innovation Leadership, Idaptive is slightly ahead of all others, based on excellent support for leading edge authentication techniques, risk analysis, and ability to process threat intelligence. Closely following (in alphabetical order) are Entrust Datacard, Microsoft, Okta, Symantec, and ThreatMetrix, constantly delivering new features at customer request. In addition to being an innovator in cloud-based MFA, ThreatMetrix is a leading provider of threat intelligence to other vendors in this space.

In the Challenger segment, we see ID Data Web and Ping Identity on the verge of becoming Leaders. Each of these vendors has made significant enhancements to their products that address real business needs, and both support the expected as well as emerging standards. In the remainder of the Challenger block, in alphabetical order, we find Gemalto, HID Global, One Identity, and OneSpan. They are building in more baseline functionality and we expect them to improve in the months ahead.

The Followers section is empty, indicating that all participating vendors are working to add innovative features at different paces.

Innovation Leaders (in alphabetical order):

- Entrust Datacard
- Idaptive
- Microsoft
- Okta
- Symantec
- ThreatMetrix, a LexisNexis Risk Solutions Company

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

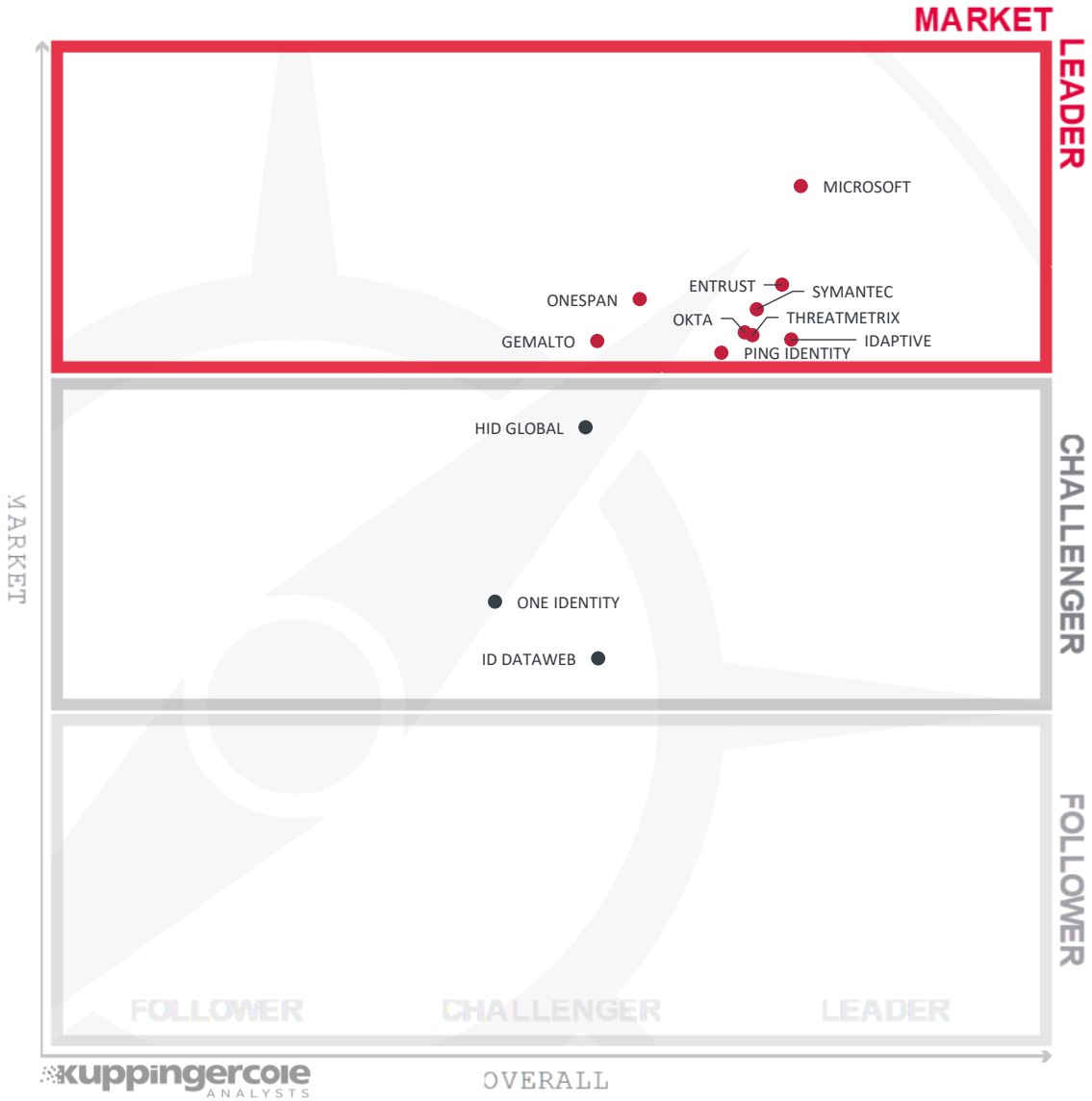


Figure 4: Market leaders in the Cloud-based MFA market segment

Microsoft is the Market leader, due to its large global customer base, partner and support network.

Entrust Datacard, Gemalto, Idaptive, Okta, OneSpan, Ping Identity, Symantec, and ThreatMetrix are also Market Leaders. They each also have hundreds to thousands of customers around the world, supporting millions of users, with large and experienced partners for implementations and support.

We find HID Global at the top of the Challenger segment. They have captured large numbers of customers and have a very good support ecosystem. HID Global's PACS business also helps drive their

expansion in this market. One Identity and ID Data Web complete the Challenger section of the Market Leadership analysis.

Market Leaders (in alphabetical order):

- Entrust
- Gemalto
- Idaptive
- Microsoft
- Ping Identity
- Okta
- OneSpan
- Symantec
- ThreatMetrix, a LexisNexis Risk Solutions Company

3 Correlated View

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

3.1 The Market/Product Matrix

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

Figure 5: The Market/Product Matrix. Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership.

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

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

In the upper right box, we find Microsoft, Entrust Datacard, and Symantec above the line. These vendors are leading in both the product and market ratings.

Below these, we find Idaptive, Okta, and Ping Identity which are product leaders but have slightly less market share than expected given the strength of their service.

On the other hand, in the center top box, we see Gemalto, OneSpan, and ThreatMetrix, having a significant market share although not counted amongst the Product Leaders.

In the center of the graphic, we find HID Global, ID Data Web, and One Identity. These all have respectable positions in both the Product Leadership and Market Leadership ratings and thus are possible alternatives to the leading vendors.

3.2 The Product/Innovation Matrix

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

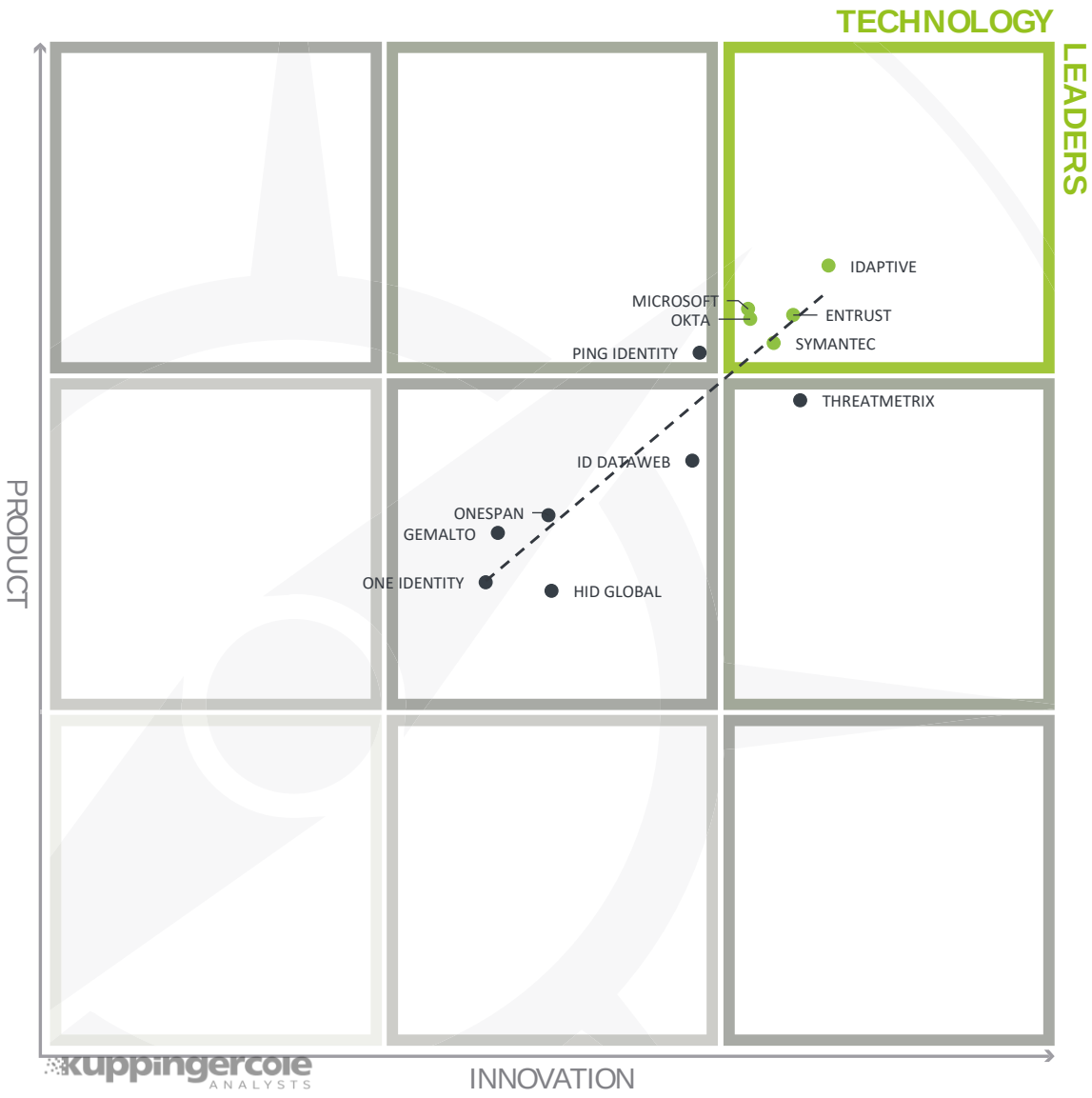


Figure 6: The Product/Innovation Matrix. Vendors below the line are more innovative, vendors above the line are, compared to the current Product Leadership positioning, less innovative.

In this chart, Idaptive, Microsoft, and Okta are above the line in the Technology Leader position. Entrust and Symantec lie directly on the line in the Technology Leaders upper right box.

ThreatMetrix is just below the Technology Leaders, indicating that they have a highly innovative service with room to grow.

Most vendor services reside in the center of the chart: Gemalto, HID Global, ID Data Web, One Identity, and OneSpan. Ping Identity is in the top center, which shows good product leadership but slightly less innovation.

3.3 The Innovation/Market Matrix

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

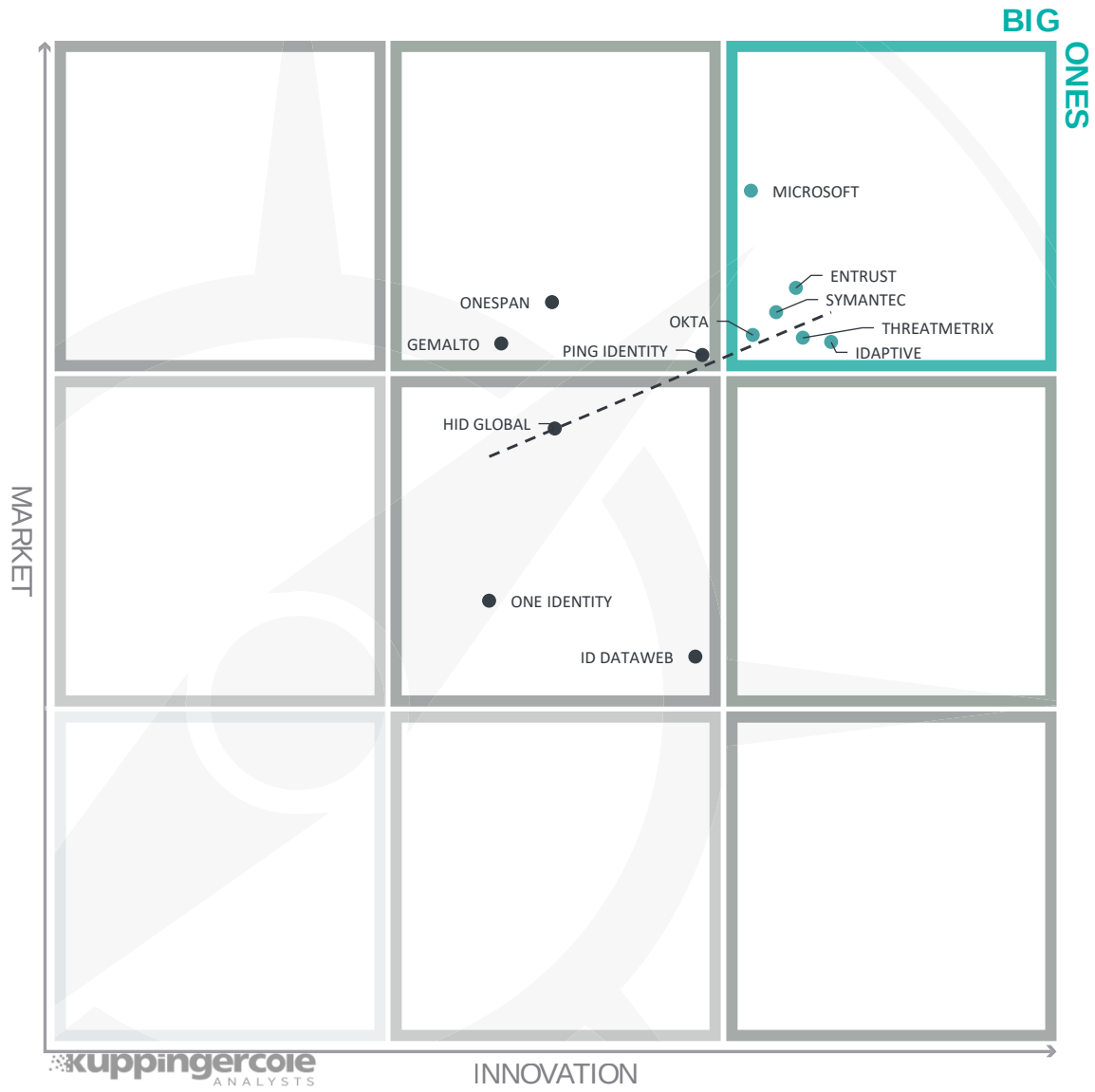


Figure 7: The Innovation/Market Matrix

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

Microsoft is above the rest, showing enormous market share.

Idaptive, Entrust Datacard, Okta, Symantec, and ThreatMetrix are also on top of the market, and are distributed across the top center box according to their relative innovation.

Gemalto, OneSpan, and Ping Identity are in the top center, with more market share than relative innovation.

The remaining services fall into the center of the chart: HID Global, ID Data Web, and One Identity.

4 Products and Vendors at a glance

This section provides an overview of the various products we have analyzed within this KuppingerCole Leadership Compass on Cloud-based MFA. Aside from the rating overview, we provide additional comparisons that put Product Leadership, Innovation Leadership, and Market Leadership in relation to each other. These allow identifying, for instance, highly innovative but specialized vendors or local players that provide strong product features but do not have a global presence and large customer base yet.

4.1 Ratings at a glance

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

Product	Security	Functionality	Integration	Interoperability	Usability
ENTRUST	strong positive	strong positive	strong positive	positive	strong positive
GEMALTO	strong positive	neutral	positive	strong positive	neutral
HID GLOBAL	positive	positive	weak	neutral	positive
IDAPTIVE	strong positive	strong positive	strong positive	strong positive	strong positive
ID DATAWEB	strong positive	positive	neutral	strong positive	positive
MICROSOFT	positive	positive	positive	strong positive	positive
OKTA	strong positive	positive	strong positive	strong positive	strong positive
ONE IDENTITY	positive	positive	weak	weak	strong positive
ONESPAN	strong positive	positive	positive	positive	positive
PING IDENTITY	positive	positive	positive	strong positive	positive
SYMANTEC	strong positive	positive	positive	positive	strong positive
THREATMETRIX	strong positive	strong positive	strong positive	positive	neutral

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
ENTRUST	strong positive	strong positive	strong positive	positive
GEMALTO	neutral	neutral	strong positive	strong positive
HID GLOBAL	positive	neutral	strong positive	positive
IDAPTIVE	strong positive	positive	positive	positive
ID DATAWEB	positive	weak	weak	neutral
MICROSOFT	positive	positive	strong positive	strong positive
OKTA	positive	strong positive	neutral	positive
ONE IDENTITY	neutral	weak	positive	positive
ONESPAN	neutral	positive	strong positive	strong positive
PING IDENTITY	positive	positive	positive	neutral
SYMANTEC	positive	positive	strong positive	strong positive
THREATMETRIX	positive	positive	strong positive	positive

Table 2: Comparative overview of the ratings for vendors

Table 2 requires some additional explanation regarding the “critical” rating.

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

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

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

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

5 Product/service evaluation

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

5.1 Entrust Datacard IntelliTrust

Entrust Datacard commands a large share of the global EMV market and has thousands of customers across the globe, serving millions of users, in both the B2C and B2E space. Entrust Datacard uses multiple data centers in the US and EU, with plans to expand to APAC and LatAM in 2018.

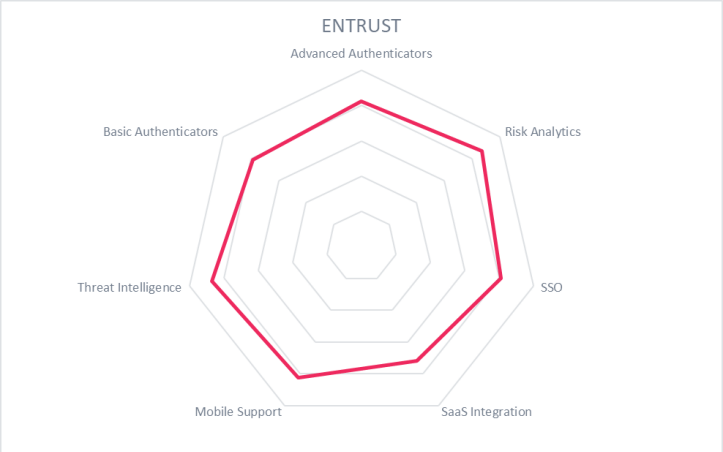
Strengths	Challenges
• Virtual Smart Card – NIST 800-157 Support; works with physical access control systems and IoT • Large selection of innovative authentication mechanisms • Sophisticated risk analytics engine • Integration with Cyber Threat Intelligence providers	• Lacks integration with Service Request Management systems • Splunk support OOTB; other SIEM support via .csv or API; syslog not currently supported

Table 3: Entrust Datacard's major strengths and weaknesses

Entrust Datacard IntelliTrust supports a wide range of authenticators, including CAC/PIV/Smart Cards, FIDO U2F keys, Kerberos, mobile push apps, OATH OTPs, RADIUS, biometrics, and 3rd party authenticators. Mobile apps which leverage Secure Elements and Trusted Execution Environment are available. It also enables connections to SaaS WAM via OAuth, OIDC, and SAML. Entrust offers a Mobile Smart Card solution, adhering to NIST 800-157 Derived PIV Credentials, which allows organizations with Smart Card deployments to issue parallel strongly vetted, high assurance credentials for use on mobile devices as a backup for physical cards and as a key for physical access controls (over NFC).

IntelliTrust's risk analytics engine can evaluate up to 50 different risk factors, such as device fingerprint and health, geo-location, geo-velocity, IP address, and user attributes. Admins can weight risk factors. Policies can be created per application/user/group, or globally. The service also performs user behavioral profiling. The risk engine also can integrate with 3rd party fraud/risk Intelligence providers, such as Iovation.

IntelliTrust can integrate with Splunk OOTB and can also export logs as .csv files. APIs allow integration with other systems. Entrust partners with SailPoint for IGA functionality. Entrust is a FIDO Alliance member, and more support for FIDO is planned.



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

Table 4: Entrust Datacard's rating

Entrust IntelliTrust has an innovative feature set for customers who need high security. Support for a large number of authenticators, virtual smart cards, an advanced risk engine, and industry-leading inclusion of cyber threat intelligence put Entrust on the short list for organizations looking for cloud-delivered MFA capabilities.

5.2 Gemalto SafeNet Trusted Access and Authentication Service

Gemalto, founded in 2006 in France and currently headquartered in the Netherlands, delivers IAM, encryption, and big data tools. It is also the world's largest maker of SIM cards. In late 2017, Thales launched a bid to acquire Gemalto. The Authentication Service is run from 6 public cloud data centers largely concentrated in EU.

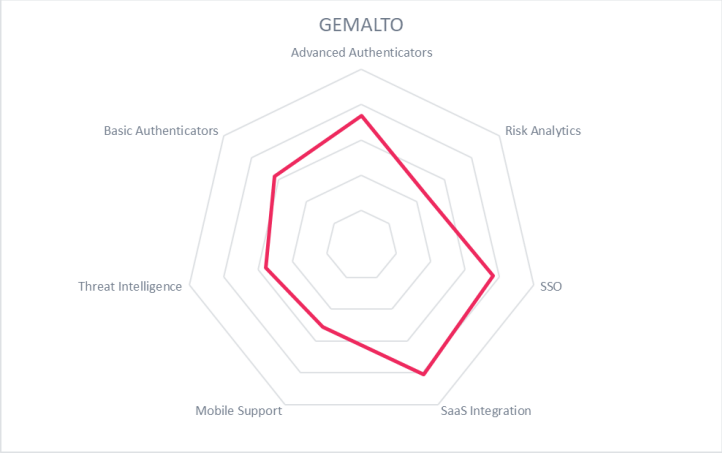
Strengths	Challenges
• Global customer base • Large, worldwide support ecosystem • Strong emphasis on eIDAS, GDPR, and PSD2 compliance • Excellent support for token-based authenticators, including national IDs	• Risk engine cannot process geo-velocity, device health, or user history; risk scores not available via API • No 3rd party threat intelligence integration • FIDO not supported

Table 5: Gemalto's major strengths and weaknesses

For authentication methods Gemalto accepts CAC/ CBA-based National ID/ PIV/Smart cards, email/phone/SMS OTPs Kerberos, Google Authenticator, mobile apps and push notifications (no SE/TEE support), RADIUS, RSA SecurID, x.509, and Yubikeys. Gemalto does not yet support FIDO, but it does offer a secure mobile SDK. It also enables connections to SaaS WAM via OAuth, OIDC, and SAML. LDAP can be used for provisioning, but not SCIM.

Gemalto's risk analytics engine can consider the following risk factors: application types, device fingerprint/ID, device history, device type, geo-fencing, geo-location, IP address/network, software signatures, and user attributes. Administrators can rank the factors in policies to require step-up authentication. Risk engine output is not accessible by customers. Gemalto does not integrate with 3rd party compromised credential/fraud/risk intelligence sources.

Gemalto can send data to SIEM systems. The solution supports delegated admin and RBAC. Gemalto's services can interoperate with IGA, PAM, and other SSO systems only via standards protocols, no connectors available. IDaaS and SaaS interoperability is possible using OIDC or SAML.



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

Table 6: Gemalto's rating

Gemalto's cloud-based MFA solutions cover the basics well. The risk engine needs some enhancements, such as accepting 3rd party intelligence and being able to compute geo-velocity. Gemalto's strong reputation in encryption and token technologies, plus their global support and partner ecosystem make them a competitive choice in the cloud MFA market.

5.3 HID Global

HID Global is part of ASSA Abloy, which is headquartered in Sweden. ASSA Abloy is a publicly-traded conglomerate that also produces many physical access control products. HID Global offers products in identity management, smart card readers, citizen identity, asset tracking, and mobile authentication. The adaptive authentication solution considered here is composed of 4 products: ActivID Authentication Solution, HID Approve (mobile authentication solution), HW tokens, and HID Risk Management Solution.

Strengths	Challenges
• PACS integration • MobileID for citizen-to-government apps • Some built-in identity vetting applications • Detailed device fingerprinting	• 3rd party fraud/threat intelligence links require customization • Missing integration with IGA, PAM, and SIEM • Coarse-grained rule engine editor

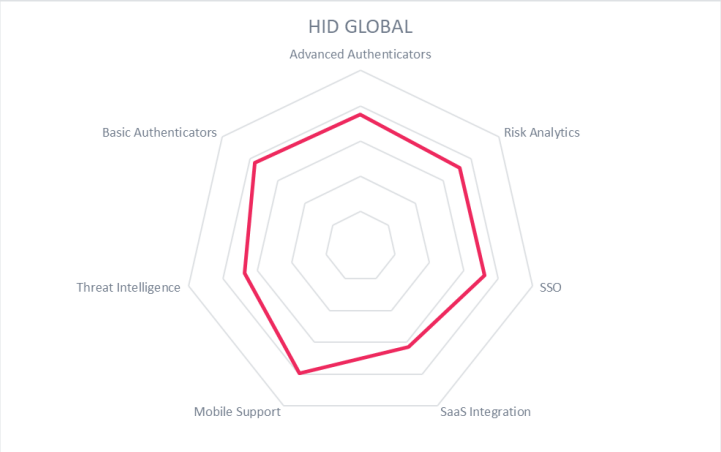
Table 7: HID Global's major strengths and weaknesses

To achieve full AA capabilities as outlined earlier, HID Global's solution requires the four products listed above. For SSO the solution supports SAML, OIDC, and OAuth2. HID Global supports behavioral analytics, email/phone/SMS OTP, FIDO U2F, Lumidigm fingerprint biometrics, mobile apps which can utilize SE/TEE if installed, mobile push, and CAC/PIV/PKI/Smart Cards for authentication. HID Global also allows adaptive authentication policies to protect physical resources, such as doors and gates.

The risk engine processes device fingerprints (up to 150 parameters, including less common ones such as IMEI and list of paired Bluetooth devices), device health assessments, geo-location, geo-velocity, jailbreak detection, and user and device history. The service can be configured to analyze external feeds of compromised credential, fraud, or threat intelligence. Administrators can craft policies that prioritize risk factors, generate granular risk scores, and prompt for step-up authentication as needed.
The product supports SCIM and LDAP for provisioning. It lacks the ability to send data to SIEM and has no native connectors to IGA or Privilege Management systems. The management console is intuitive, and it is easy for administrators to drill down to details within the dashboard.

Security	positive
Functionality	positive
Integration	weak
Interoperability	neutral
Usability	positive

Table 8: HID Global's rating



HID Global's product suite can help governments and businesses meet demanding requirements in the areas of identity vetting, mobile ID, and strong authentication assurance. PACS integration is an innovative plus, not found in many Cloud MFA solutions. Additional protocol support would improve interoperability with other identity and security solutions. A more fine-grained risk engine rules editor and the ability to more easily integrate

credential/fraud/threat intelligence would enhance the product as well. The mix of identity vetting and PACS integration features makes this solution an interesting alternative in the market.

5.4 Idaptive (formerly Centrify)

Idaptive (formerly Centrify), well-known for its privilege management and cross-platform identity solutions, also offers MFA as SaaS. Idaptive's MFA functionality as considered here is distributed amongst its Idaptive Application Services, Idaptive Endpoint Services, and Idaptive Infrastructure Services. Their robust multi-cloud approach utilizes 22 data centers on 4 continents.

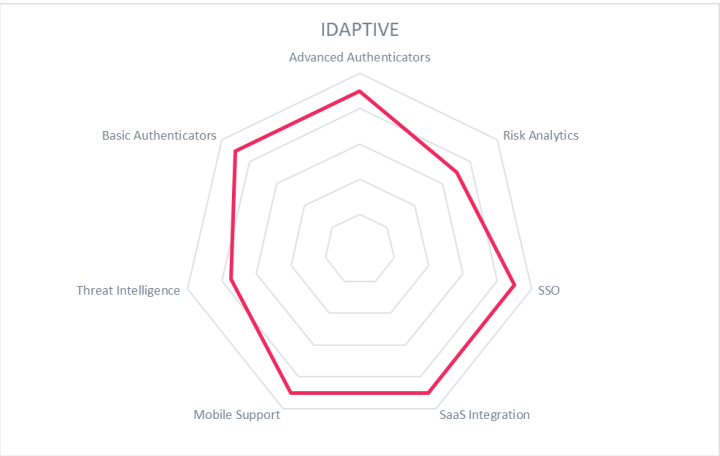
Strengths	Challenges
• Supports NIST 800-157, x.509 credentials on mobile devices • Excellent selection of strong MFA mechanisms • Sophisticated risk analytics for high security • CCM, Privacy Shield, SOC 2 Type 2 certifications	• Though they are global, tech support is generally limited to English • Risk factors are rated by algorithms, not configurable by customers

Table 9: Idaptive's major strengths and challenges

Idaptive supports an enormous number of MFA options: CAC/PIV/SmartCards, DUO, email/phone/SMS OTP, federated logins, mobile apps (protected in SE/TEE), mobile push notifications, OATH tokens, RADIUS, RSA SecurID, social logins, x.509 Derived Credentials, Yubikeys, 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. They also support LDAP and SCIM for out-provisioning, although provisioning into Idaptive services is unnecessary.

The risk engine can evaluate device fingerprints and health assessments, geo-location, geo-velocity, IMEI, IPs, user attributes and behavioral analysis. Idaptive leverages Palo Alto threat intelligence feeds and calls against "haveibeenpwned" for compromised credential information. Idaptive can output granular risk scores allowing configurable actions but doesn't allow customers to weight risk policies individually.

Idaptive supports granular roles, delegated admin models, and has its own privilege management service. It can interoperate with SIEMs via REST APIs or syslog.



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

Table 10: Idaptive's rating

Idaptive has a great track record in helping customers to meet complex IAM requirements. Their cloud-based MFA solution is world class, offering great reliability, scalability, and geographical distribution. Their solutions

support a range of use cases, up to those needing the highest levels of authentication assurance. Idaptive should be on the short list for any cloud-based MFA RFP.

5.5 ID Data Web Attribute eXchange Network (AXN)

ID Data Web was founded in 2011 outside the Beltway in Northern Virginia as a spin out of Criterion Systems, an IT services firm specializing in cyber security for US government. ID Data Web received a US NSTIC grant in 2012 to implement the Attribute eXchange Network (AXN), a service for credential federation and attribute verification. AXN has since grown into a full-fledged IDaaS with MFA options. Their service is delivered via a single public cloud provider hosted in data centers in Europe and the US.

Strengths	Challenges
• Highly configurable risk engine that allows step-up authentication and other non-interactive ID / attribute verification processes • Built-in identity vetting connectors • Excellent IAM standards support	• Small but rapidly growing customer base • Centered on US enterprises with global coverage requirements

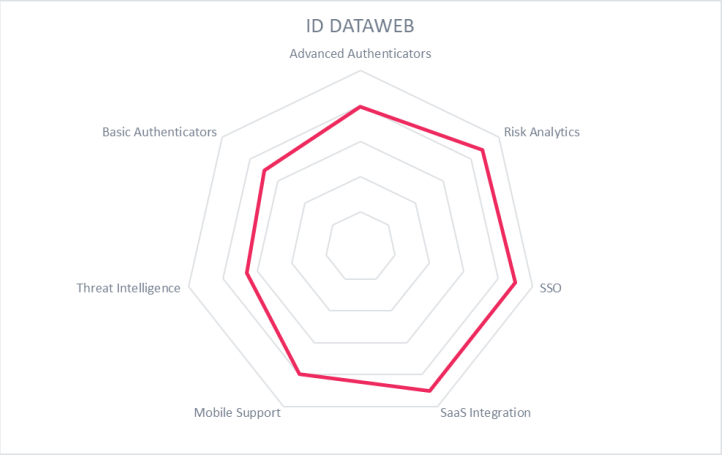
Table 11: ID Data Web's major strengths and weaknesses

Users can authenticate to AXN with biometrics, CAC/PIV/Smart Cards, Duo, email/phone/SMS OTP, FIDO UAF and U2F clients, mobile push notifications, social logins, Symantec VIP, x.509, and Yubikeys. The solution also supports OAuth, OIDC, and SAML. ID Data Web offers a secure mobile SDK, but no Android or iOS apps at this time. AXN supports provisioning over LDAP and SCIM. ID Data Web's risk engine can evaluate device fingerprints and health assessments, device history, geo-location, geo-velocity, IPs, user attributes and history. ID Data Web leverages ThreatMetrix global fraud consortium feeds, as well as its own in-network security intelligence. AXN can output granular risk scores allowing configurable actions to mitigate fraud including step-up authentication or a number of other ID verification or attribute validation processes. Risk evaluation results are also accessible via a RESTful API. Customer admins can design policies with custom weighted risk factors. Writing and editing policies is straightforward in the admin interface.

AXN can interoperate with IDaaS, IGA, and SaaS apps over OIDC, SAML, and SCIM protocols. There are no connectors for PAM solutions at present. AXN allows for both delegated and RBAC admin models. ID Data Web can send data to SIEMs and has connectors for QRadar and Splunk.

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

Table 12: ID Data Web's rating



AXN offers a good variety of authenticator choices. It has a highly configurable risk engine that allows for much more than just step-up authentication. It was built to interoperate with many credential and authoritative attribute sources. Though it is young in the

market, it is growing and adding capabilities rapidly. Customers in the financial industry and governments may find the built-in identity vetting and attribute validation functions especially useful. ID Data Web's AXN is worth a look when looking for cloud-based MFA solutions.

5.6 Microsoft Azure AD

Microsoft Azure Active Directory is their well-known cloud-based identity and access management service. The adaptive authentication offering is architected to scale and perform well with almost 1 billion users and 8 billion logins per day. Cloud services have been one of the primary drivers in Microsoft's business portfolio. Azure is one of the global leaders in the cloud infrastructure market, second only to Amazon's AWS, with more than 30 major data centers across the globe.

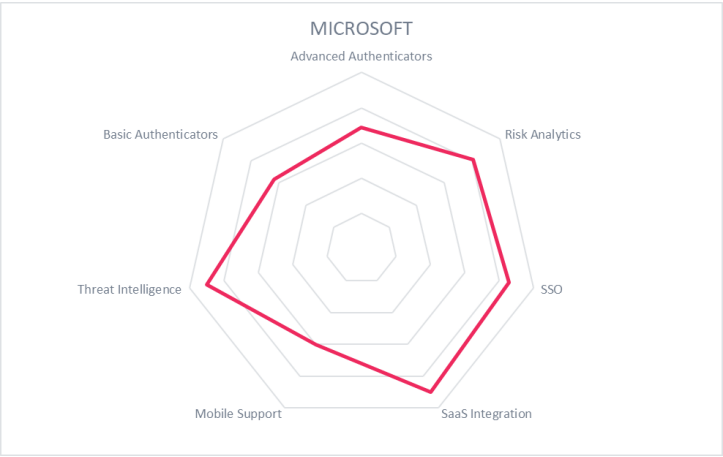
Strengths	Challenges
• Massive scalability, global reach, and excellent language support • Strong support for IAM standards • Very good attack detection through internal cyber threat intelligence network • Resilient against cyber attacks	• FIDO support planned • Needs more fine-grained administrative capabilities for user & policy management • Should ingest more device-side risk info

Table 13: Microsoft's major strengths and weaknesses

Microsoft AAD offers fairly broad authenticator support, including CAC/PIV/Smart Cards, mobile apps using SE/TEE, mobile push notifications, RADIUS, RSA SecurID, social logins, SMS OTP, and x.509. It does not offer a mobile SDK, and FIDO support is coming. OAuth, OIDC, SAML, and SCIM protocols are supported for interoperability.

The integrated risk engine can evaluate cookies, certificate-based device fingerprints for Azure AD joined and InTune managed devices, geo-location, geo-velocity, IPs, user attributes and behavioral analysis. Microsoft generates and analyzes an enormous amount of in-network threat intelligence as well as receives 3rd party sources, which are used to inform risk decisions on behalf of clients. Microsoft's internal ML determines the weighting of factors. Customer administrators can write complex conditional access policies. The management console permits some RBAC and delegated admin capabilities.

Microsoft has tight integration with other Microsoft identity and security services, such as Privileged Identity Manager and Cloud App Security. It can be configured to output security event data to Splunk or other security analytics systems. Strong protocol conformance allows the service to interoperate with many SaaS or other IDaaS solutions.



Security	positive
Functionality	positive
Integration	positive
Interoperability	strong positive
Usability	positive

Table 14: Microsoft's rating

Microsoft Azure AD has the scalability to meet the most demanding performance requirements and has great internal threat intelligence processing that significantly benefits customers. Some omissions in the feature set are likely to be addressed in upcoming enhancements. This service should definitely be considered when looking for AA and cloud MFA solutions.

5.8 Okta Adaptive Multi-Factor Authentication

Okta platform offers an adaptive MFA service in conjunction with their multi-tenant enterprise IDaaS solution. Okta has a focus on security, with FedRAMP (US), ISO 27001, SOC 2 Type 2, ISO27018, and CSA Star Level 2 certifications. All Okta services run on a single IaaS platform in multiple data centers in the EU and US.

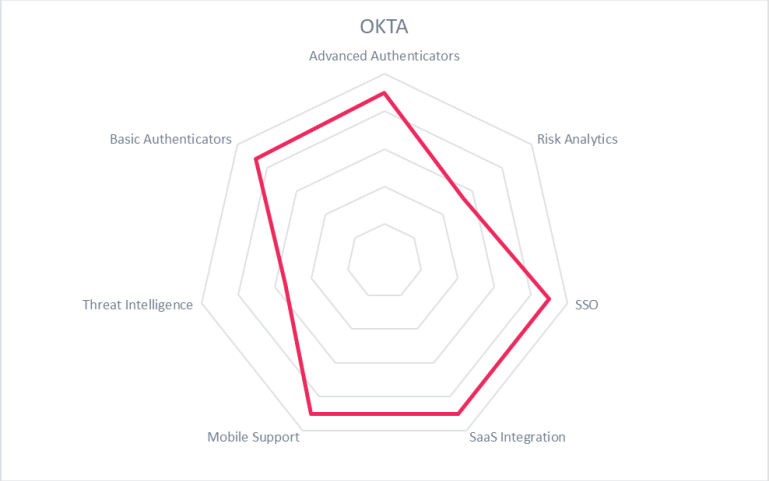
Strengths	Challenges
• Very large enterprise customer base • Wide array of authenticator options • Accepts 3rd party threat intelligence	• Heavily centered on North American market • Risk engine is in a "black box" – no API access

Table 15: Okta's major strengths and weaknesses

The Okta Platform accepts CAC/PIV/Smart Cards, Duo, FIDO U2F, Kerberos, mobile apps (utilizing SE/TEE and Secure Enclave), mobile push notifications, RADIUS, RSA SecurID, social logins, SMS/email/phone OTP, x.509, Symantec VIP, and Yubikeys. It supports federated authentication/authorization via SAML, OIDC, and OAuth. They offer a mobile SDK.

Okta's adaptive risk engine can evaluate device fingerprint and health assessment, geo-location, geo-velocity, IP reputation, user attributes and history. Its risk engine can receive intelligence about breached credentials and other cyber threats, and can then be configured to require step-up authentication or other actions from the methods listed above. Customer admins can select which risk factors and behaviors are evaluated, and what response is triggered based on them. Output from the risk engine is not available to customer administrators.

The flexibility of Okta platform allows it to accept user information from many standard sources, such as Microsoft AD, and allows Okta to integrate with many SaaS apps or any database. Okta does accept LDAP and SCIM provisioning, and can interoperate with IGA and PAM solutions. RBAC and delegated admin models are configurable. Okta can send data to SIEMs or other analytics systems.



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

Table 16: Okta's rating

Okta Platform does focus on security, scalability, and performance. While it does have a reasonable support ecosystem in the EU, the majority of its customers are in North America. The variety of authenticators supported, including high assurance options, as well as the protocol support and ease of integration with SaaS vendors make it worth considering on cloud MFA RFPs.

5.9 One Identity Starling 2FA

Originally founded in 2000, One Identity became a distinct legal entity of Quest Software in 2017. The company is a leading IAM vendor with multiple on-premise product lines moving more into the cloud for service delivery. The service considered here is Starling 2FA, which is hosted in two data centers, one in the EU and one in the US.

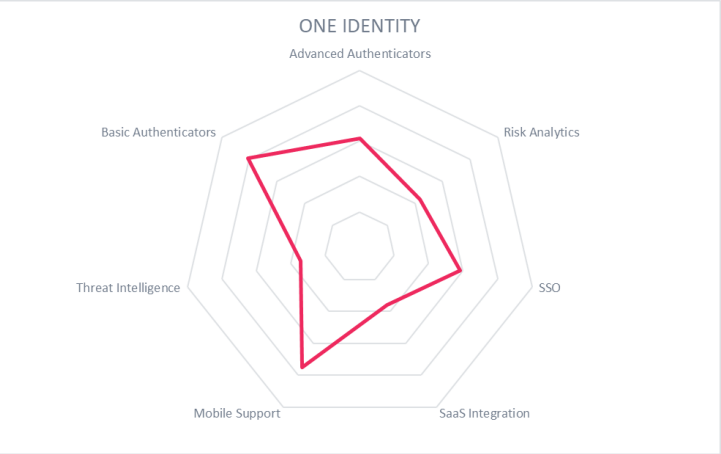
Strengths	Challenges
• Good selection of authenticators, particularly token-based	• No FIDO support or mobile SDK • No processing of 3rd party compromised credential or threat intelligence • Risk engine not addressable via APIs • No connectivity to external IGA, PAM, or SIEM systems

Table 17: One Identity's major strengths and weaknesses

One Identity's Starling service provides the following authentication options: CAC/Smart Cards, Duo, Kerberos, mobile apps (utilizing SE/TEE and Secure Enclave), mobile push notifications, RADIUS, RSA SecurID, some social logins, SMS/phone OTP, and Yubikeys. It supports federated authentication and authorization via SAML, OIDC, and OAuth; and provisioning over LDAP but not SCIM.

One Identity Starling's risk analytics engine can evaluate quite a few different risk factors, such as device fingerprint and health, geo-location, geo-velocity, IP address/network, and user attributes and history. Administrators can weigh the factors in policies to require step-up authentication. The risk engine cannot currently integrate with 3rd party fraud/risk Intelligence providers, but it does in-network risk analysis between customers. The risk engine is not addressable from APIs.

The solution does not interoperate with external IGA or PAM systems. Starling supports RBAC but not delegated admin models. The service cannot connect to SIEM or security analytics services.



Security	positive
Functionality	positive
Integration	weak
Interoperability	weak
Usability	strong positive

Table 18: One Identity's rating

One Identity Starling provides a basic MFA service with good support for token-based authentication. It has a reasonably sophisticated but opaque risk analytics facility. The service needs additional features to better compete in the market, especially regarding threat intelligence and interoperability with core IAM, IGA, and security functions.

5.10 OneSpan (formerly VASCO) Intelligent Adaptive Authentication

VASCO has been re-named OneSpan. The cloud service considered here is OneSpan's Intelligent Adaptive Authentication based on its open architected Trusted Identity platform. Most customers are in the banking and financial service industry. As a solution provider for finance, they have pre-defined rulesets available for regulatory compliance (i.e. GDPR, PSD2), and common fraud schemes.

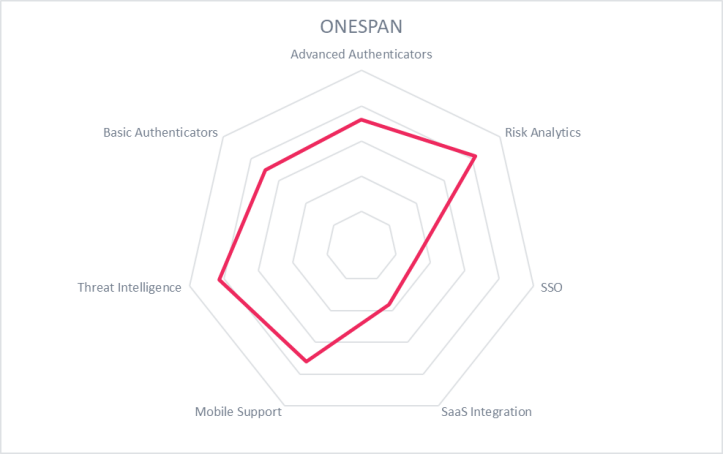
Strengths/Opportunities	Weaknesses/Threats
• Strong focus on mobile authentication, including biometrics, secure apps, SDK, etc • Sophisticated risk analytics that combines pre-configured rules with ML models to detect fraud in real-time • Digital signature and ID verification	• 3rd party threat intelligence feeds must be manually configured • Needs additional protocol support for interoperability

Table 19: OneSpan's major strengths and weaknesses

OneSpan has good mobile support: Android/iOS touch biometrics, facial recognition biometrics, mobile apps and a mobile SDK. Android-based apps utilize SE/TEE for high security and application shielding. OneSpan Mobile Security Suite supports FIDO UAF; Digipass SecureClick implements FIDO U2F. FIDO 2.0 clients/server and SDK are on the near-term roadmap. Token-based authenticators such as Gemalto, RSA SecurID, Smart Cards, and Yubikeys work with OneSpan. Additionally, OneSpan's mobile security suite offers additional features such as encrypted client/server communications channel, application shielding for secure mobile applications and real-time data extraction and conditioning.

The risk engine can process more than 150 different factors, including device fingerprint and health assessment, IP address, geo-location, geo-velocity, IMEI numbers, jailbreak detection, proxy detection, user attributes/history and other contextual data. Customers can write policies prioritizing risk factors that drive real-time authentication workflows.

OneSpan can send event data to SIEMs via syslog. They integrate with IGA and PAM solutions through SOAP APIs. Administrators can promote test configurations from development to production with automated tools.



Security	strong positive
Functionality	positive
Integration	positive
Interoperability	positive
Usability	positive

Table 20: OneSpan's rating

OneSpan's emphasis is on their software-based Intelligent Adaptive Authentication, Risk Analytics and Mobile Security solutions. ESignLive, now OneSpan Sign, provided a strong and growing digital signature solution. The acquisition of DealFlo further enhances the e-Signature offering and adds key ID verification and digital account opening capabilities. SAML 2.0 and OIDC protocol support is coming soon and will extend interoperability options. Companies in the financial space should consider OneSpan for their adaptive authentication with advanced risk analytics and mobile app security requirements.

5.11 Ping Identity Ping ID

PingIdentity has been a pioneer in identity federation since its inception in 2002. PingFederate was the flagship product, but Ping has expanded and carries a number of IAM/CIAM products and services. Ping ID is their cloud MFA offering. The service is hosted by a single public IaaS provider in APAC, EU, and the US.

Strengths	Challenges
• Large selection of innovative MFA options • Excellent support for identity standards • Wide use case support, including Windows login and a mobile SDK for consumer apps • OOTB Cyberthreat Intelligence integration	• Risk engine does not factor geo-velocity • Static rules-based risk engine

Table 21: Ping Identity's major strengths and weaknesses

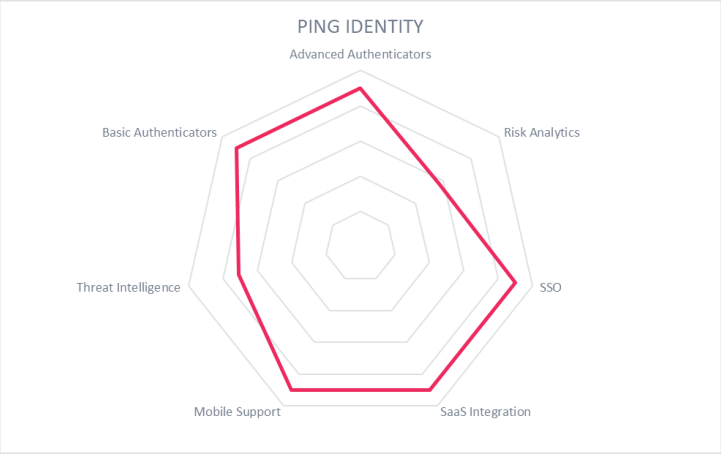
PingID supports authentication methods such as Apple Watch, Kerberos, SMS/email/voice OTP, FIDO UAF biometrics (via partnership), mobile apps/push notifications, social logins, and Yubikey authentication mechanisms. If used in conjunction with PingFederate, it can also support FIDO U2F, RSA SecurID, Symantec VIP, Duo Access, RADIUS, CAC/PIV/Smart Cards, x.509, and all federation protocols. Mobile apps run on both Android and iOS, using SE/TEE and Secure Enclave. They have an SDK for creating secure mobile apps. PingID comes with OOTB connectors for VPNs, on-premises and SaaS applications, Web SSO, RADIUS, Remote Desktop, SSH, and Windows Login for end user devices and Windows servers. PingID also integrates directly with Microsoft Active Directory Federation Server (ADFS) and Azure AD. PingID speaks both LDAP and SCIM for in- and out-provisioning.

The risk engine evaluates device fingerprint and health assessment, geo-location, IP address, and user attributes via static policies, and user history. For mobile devices, PingID can determine if devices are rooted/jail-broken. For device posture evaluation, PingID also integrates out of the box with MDM vendors such as MobileIron, Airwatch, and Microsoft InTune. Geo-velocity is not supported at this time. Ping ID receives threat intelligence from Threatmetrix. Risk evaluation results are not available via APIs.

Ping ID integrates with CyberArk for PAM and SailPoint for IGA. Event data can be sent to SIEM over syslog. Interoperability with AD, AAD, other IDaaS and SaaS apps is handled through PingFederate.

Security	positive
Functionality	positive
Integration	positive
Interoperability	strong positive
Usability	positive

Table 22: Ping Identity's rating



PingIdentity has strong support for IAM standards and excellent MFA variety. The risk engine needs additional features, including support for user behavioral analysis, dynamic policies, and the ability to compute geo-velocity. Though Ping ID is the main service considered here, to achieve full functionality customers may need to run PingFederate also. PingID and PingFederate are mature and highly capable and should be considered for Cloud MFA RFIs.

5.12 Symantec VIP

California-based Symantec, well-known for cybersecurity and information security solutions, also is a provider of IAM services, including cloud-delivered MFA and an associated threat intelligence service. Symantec VIP can also work in conjunction with their DLP, Encryption, and CASB services to provide fine-grained access control to data, based on DLP metatags as well as user information. Symantec uses a single public IaaS provider with an undisclosed number of locations to deliver the VIP service.

Strengths	Challenges
• VIP + CASB + DLP for most granular access control • High quality threat intelligence feeds • Many high assurance authenticators accepted	• Missing FIDO and OAuth support • Delegated administration model is not supported

Table 23: Symantec's major strengths and weaknesses

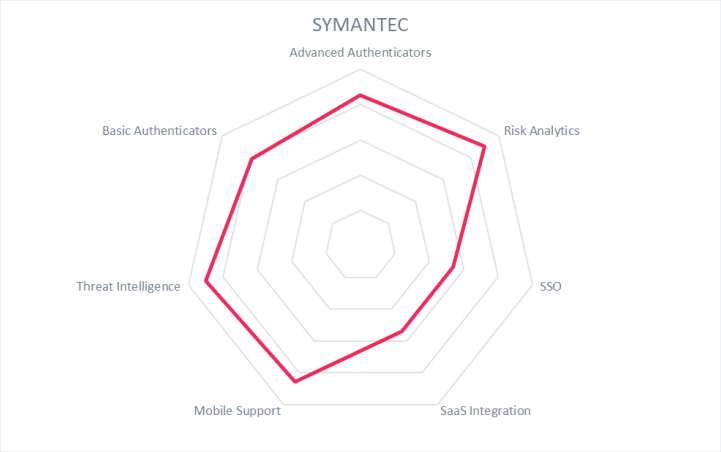
Symantec VIP accepts many authenticator types including Kerberos, mobile apps and push notifications, OATH OTPs, RADIUS, RSA SecurID, x.509, Symantec U2F keys, and Yubikeys. Mobile apps which leverage SE/TEE and a secure mobile SDK are available. While it can do SAML, it doesn't support OAuth; LDAP is supported for provisioning, but not SCIM.

VIP's adaptive risk engine can evaluate device fingerprint / health assessment / type, geo-location, geo-velocity, IP reputation, user attributes and history. VIP receives intelligence about breached credentials and other cyber threats from Symantec's Global Intelligence Network, and can then be configured to require step-up authentication or other actions from the methods listed above. Risk engine output is accessible to customers via API, and admins can create very granular policies based on that output.

Symantec VIP can interoperate with IGA, PAM, and SaaS systems (limited to SAML). The service allows for RBAC but not delegated administration. VIP can integrate with Symantec SIEM and other security services. Symantec offers an identity vetting service, ID Analytics, which can help reduce fraud for consumer-facing applications.

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

Table 24: Symantec's rating



Symantec has a number of high security features that make it attractive for enterprise customers that need high assurance for workforce and contractors, as well as some identity vetting functions that are useful for B2C deployments. Support for FIDO would strengthen the offering. Overall, Symantec VIP should definitely be considered in cloud MFA RFPs.

5.13 ThreatMetrix MultiFactor Authentication

ThreatMetrix was recently acquired by LexisNexis Risk Solutions. ThreatMetrix is known for its threat intelligence services, which cover device, domain, email, IP address, and network reputation data. It consumes its own services as well as offers the information as a service to clients and other IDaaS vendors. Though the service is cloud-based, no specific information was provided regarding the IaaS platforms used or locations in which it is deployed.

Strengths	Challenges
• Excellent device, identity, and threat intelligence • Highly configurable adaptive risk engine • Good selection of authenticators • ID proofing and attribute provider interop	• Weak administrative security (password-based) • FIDO support coming • LDAP and SCIM support needed for more IAM interoperability

Table 25: ThreatMetrix' major strengths and weaknesses

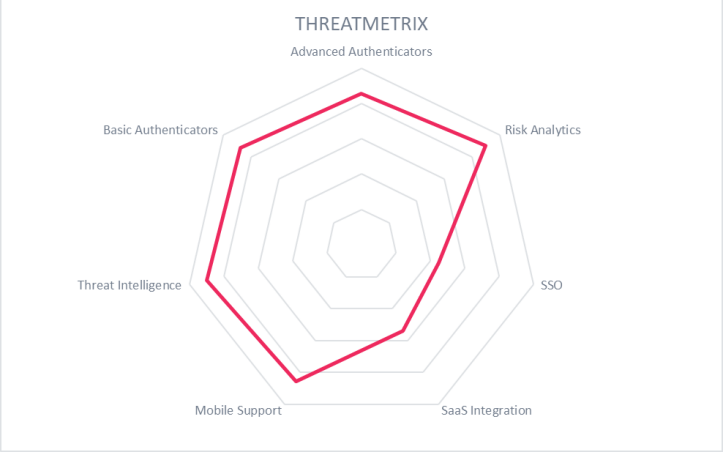
ThreatMetrix supports a wide range of authenticators for users, including CAC/PIV/Smart Cards, Duo, email/phone/SMS OTP, Kerberos, mobile push apps, RADIUS, RSA SecurID, social logins, and Yubikeys. They do not provide mobile authentication apps, but they do offer a secure mobile SDK. FIDO is not currently supported. It also enables connections to SaaS via OIDC and SAML. ThreatMetrix can pull extended ID attributes about government-issued identifiers, DOB, addresses, relatives, digital reputation, device IDs, geolocations, social networks, account numbers, payment instruments, vehicles, biometrics, associated user names. It does not support LDAP or SCIM.

ThreatMetrix is synonymous with device-based risk intelligence. Its risk analytics engine can evaluate many risk factors, such as device fingerprint/health/history/type, geo-location, geo-velocity, IP address/network, and user attributes and history. Their intelligence services run the gamut from compromised credential to fraud risk detection. Administrators can rank the factors in policies to require step-up authentication. Risk scoring is extractable via REST APIs.

ThreatMetrix does not interoperate directly with Microsoft AD or AAD, but it can support IDaaS platforms and enables federation to SaaS apps. It doesn't interoperate with IGA but can be called by PAM systems. The console allows for RBAC and delegated admin models. It doesn't interoperate with SIEM solutions.

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

Table 26: ThreatMetrix' rating



ThreatMetrix provides top-of-the-line intelligence which is a key ingredient in cloud MFA solutions today. While it needs additional protocol support, the quality of its intelligence coupled with MFA offerings make it a compelling choice.

6 Vendors and Market Segments to watch

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

6.1 AvocoSecure

AvocoSecure is a privately-owned UK company offering Cloud and Adaptive Authentication services. Their product is called Trust Platform. Trust Platform is not derived from traditional IAM, but rather was built to UK government security standards for high assurance verification of consumer identities. AvocoSecure partners offer customer profile storage in cloud or hybrid installations. It is available either as a cloud-based service or can be directly integrated into customer's on-premise environments. Trust Platform accepts username/password, SMS OTP, and social logins from Facebook, Twitter, Microsoft, LinkedIn, and Google. It also accepts federated login via SAML, OIDC, and OAuth.

Using REST API, Trust Platform can feed data to SIEM/RTSI systems and Splunk. At present, there are no interfaces to external CRM, marketing, or Big Data style analytics programs. However, Splunk can be used for rudimentary identity and marketing analysis.

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

6.2 CA Technologies

CA Identity Portfolio comprises Identity Management and Governance, Privileged Access Management, Single Sign-On, Advanced Authentication, and Directory products. The Rapid App Security add-on provides a single SDK for authentication and connections to CA Mobile API Gateway. The product can be deployed on-premise, and is featured in our Leadership Compass Adaptive Authentication.

6.3 Duo Security

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

Regarding risk engine capabilities, Duo can detect if the user's device software is up to date, if the disk is encrypted, if a screen lock is enabled, or if the device is managed or unmanaged. Duo further reduces risk

by marking devices as trusted, and binding them to the specific user. With this feature, stolen credentials and MFA can't be used to access an application from any other device.

Although we have covered them in the past, and have an Executive View available, Duo did not respond for this report. We expect that they will be covered in the next update of Leadership Compass Cloud-based MFA Solutions.

6.4 IBM

IBM Security Access Manager (SAM) is their tightly integrated adaptive authentication package. SAM can run on a hardware or virtual appliance, either on-premises or in IaaS environments. The same capabilities are available in IBM Cloud Identity as SaaS. IBM's Trusteer Pinpoint service (cloud-delivered and licensed separately) can provide a wealth of fraud reduction and vetted threat data to inform SAM's decisions. Since IBM SAM is also offered for on-premises, it is covered in our Leadership Compass Adaptive Authentication.

6.5 Iovation

Portland, OR based Iovation was founded in 2004. It was acquired by TransUnion in May of 2018. The company provides an integrated MFA and fraud reduction solution.

Iovation's intelligence services are used by many CIAM and IDaaS vendors as well as IAM operators. We will follow Iovation and include them in future reports.

6.6 NokNok Labs Strong Authentication SaaS

NokNokLabs, a Silicon Valley based startup, has delivered a set of mobile-oriented products that perform adaptive authentication, in conformance with the FIDO UAF and 2.0 standards. The service allows customers to deploy any FIDO UAF certified authenticators of their choice, and leverage NokNokLabs' authentication service. Customer admins can write risk adaptive policies that evaluate factors such as device ID, geo-location, geo-velocity, etc. Their Strong Authentication SaaS can then act as a front-end to other popular SaaS apps that understand OIDC and SAML, or for on-premises solutions such as ForgeRock, IBM SAM, and PingFederate.

We expect that NokNokLabs' products will be included in future KuppingerCole Leadership Compasses.

6.7 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 RSA® Fraud and Risk Intelligence Suite, is a widely used solution, particularly in the financial industry, supporting over one billion end users. RSA SecurID Access, which is part of the Identity Suite, has some adaptive authentication capabilities as well. This solution can run on-premise or in the cloud.

The RSA Adaptive Authentication Multi-Credential Framework enables the creation of plug-ins to support CAC/PIV/National ID/Smart Cards, Duo, Google Authenticator, Kerberos, OIDC, RADIUS, SMS OTP, x.509, Yubikeys and any FIDO U2F authenticator. RSA Adaptive Authentication Mobile SDK supports Android/iOS biometrics, including fingerprint and Face ID, and 3rd-party biometrics via the Multi

Credential Framework. Administrators can stipulate that multiple authenticators are required via static policies.

RSA's risk engine can evaluate device IDs/fingerprints, geo-location, geo-velocity, IP addresses, and other common factors. RSA's eFraudNetwork, a global shared repository of fraud intelligence feeds RSA risk engine deployments to significantly reduce transaction fraud risk. Real-time cyber threat intelligence or data from 3rd party solutions can be integrated with the RSA Adaptive Authentication Eco-System feature.

RSA Adaptive Authentication can work with RSA Archer via Case Management API. RSA SecurID Access, which is targeted at B2E, supports hard/soft tokens, FIDO, SMS, and mobile push, as well as integration with WAM/SSO systems, SaaS apps, PAM solutions, firewalls, and VPNs.

RSA was fully evaluated in the Leadership Compass on Adaptive Authentication. For details, please see that document.

6.8 United Security Providers Secure Entry Server

USP 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 SES suite takes an innovative approach to access management and adaptive authentication. KuppingerCole will track USP and include their products in future publications.

7 Methodology

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

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

7.1 Types of Leadership

We look at four types of leaders:

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

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

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

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

7.2 Product rating

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

KuppingerCole uses the following categories to rate products:

- Security
- Functionality
- Integration
- Interoperability
- Usability

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

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

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

Interoperability can have several elements. We use the term "interoperability" to refer to the ability of a product to work with other vendors' products, standards, or technologies. In this context, it means the degree to which the vendor has integrated the individual products or technologies with other products or

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

standards that are important outside of the product family. Extensibility is related to interoperability, and is measured by the degree to which a vendor allows its technologies and products to be extended for the purposes of its constituents. We think Extensibility is so important that it is given equal status to insure its importance is understood by both the vendor and the customer. As we move forward, simply providing good documentation is inadequate. We are moving to an era when acceptable extensibility will require programmatic access through a well-documented and secure set of APIs. Refer to the Open API Economy Document (#70352 Advisory Note: The Open API Economy[2]) for more information about the nature and state of extensibility and interoperability.

Usability refers to the degree in which the vendor enables the accessibility to its technologies and products to its constituencies. This typically addresses two aspects of usability – the end user view and the administrator view. Sometimes good documentation can facilitate adequate accessibility. However, we have strong expectations that user interfaces will be logically and intuitively designed. Moreover, we expect a high degree of consistency across user interfaces of a product or different products of a vendor. We also believe that vendors should follow common, established approaches to user interface design.

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

- Increased People Participation—Human participation in systems at any level is the highest area of cost and highest potential for breakdown for any IT endeavor.
- Lack of Security, Functionality, Integration, Interoperability, and Usability—Lack of excellence in any of these areas will result in increased human participation in deploying and maintaining IT systems.
- Increased Identity and Security Exposure to Failure—Increased People Participation and Lack of Security, Functionality, Integration, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes and breakdowns. This will create openings for attack and failure.

Thus, when KuppingerCole evaluates a set of technologies or products from a given vendor, the degree of product Security, Functionality, Integration, Interoperability, and Usability which the vendor has provided is of highest importance. This is because lack of excellence in any or all areas will lead to inevitable identity and security breakdowns, and will result in weak infrastructure.

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

7.3 Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position
- Financial strength
- Ecosystem

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

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

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

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

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

7.4 Rating scale for products and vendors

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

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

7.5 Spider graphs

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

These functional areas, which are reflected in the spider charts for each company in Chapter 5 include:

Basic Authenticators	Username/password: the most basic form, not recommended. 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.
Advanced Authenticators	FIDO 2.0,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. FIDO 2.0 is the latest iteration and will likely surpass U2F and UAF in adoption in the years ahead. SmartCards have 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. Other types of hardware tokens employ similar technologies in different form factors, such as RSA SecurID and Yubikeys. 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.

Mobile support	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. The ratings for mobile support include whether or not a product adheres the Global Platform Secure Element (SE) and Trusted Execution Environment (TEE) for Android, and whether or not the product utilizes Secure Enclave in iOS.
Risk Analysis	Factors such as IP address, device fingerprints, device health assessment geo-location, geo-velocity, integration of 3rd-party threat intelligence, user behavior profiling
Threat Intelligence	Subscriptions to real-time feeds of known bad IP addresses, locations, proxies, malicious URLs, and compromised credentials
SSO	Use of federation standards for Single-Sign-On to on-premises applications
SaaS integration	Use of federation technologies such as OAuth, OIDC, and SAML to allow authenticated users to seamlessly access popular SaaS applications.

The spider graphs provide comparative information by showing the areas where products are stronger or weaker. Some products show gaps in certain areas, while being strong in other areas. These might be a good fit if only specific features are required. Other solutions deliver strong capabilities across all areas, thus commonly being a better fit for strategic decisions on Cloud-based MFA.

7.6 Inclusion and exclusion of vendors

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

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

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

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

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

8 Copyright

The Future of Information Security – Today

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

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

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

KuppingerCole Analysts AG
Wilhelmstrasse 20-22
65185 Wiesbaden | Germany

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