KuppingerCole Report

LEADERSHIP COMPASS

By John Tolbert

February 09, 2021

Enterprise Authentication Solutions

This report provides an overview of the Enterprise Authentication Solutions market and provides you with a compass to help you to find the solution that best meets your needs. We examine the Enterprise Authentication market segment, product/service functionality, relative market share, and innovative approaches to providing modern solutions in this space.

By **John Tolbert**
jt@kuppingercole.com

Content

1 Introduction

As the number and severity of data breaches rise, businesses, governments, and other organizations seek to improve the authentication experience and raise assurance levels to mitigate against continuously evolving threats. Cyber-attacks put personal information, state secrets, trade secrets, and other forms of intellectual property at risk. Increasing security and improving usability are the twin goals of enterprise authentication upgrade projects. 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). Legacy IAM systems sometimes struggle not only to meet changing business requirements but also to keep up with the latest authentication technologies. Many enterprises are choosing to augment their IAM systems by logically separating authentication from the IAM stack and utilizing discrete services that offer Multi-factor Authentication (MFA) with extensible risk analysis features informed by various types of intelligence. 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.

MFA is the employment of multiple methods of determining that a user is who they are purporting to be in the context of an access request. Risk-adaptive authentication is the process of gathering additional attributes about users and their environments and evaluating those attributes in the context of risk-based policies. The goal of risk-based adaptive authentication 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 and/or the acquisition of additional attributes about the user, device, environment, and resources requested. 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, Smart Cards or other hardware tokens, and behavioral biometrics. FIDO Alliance is a leading organization that develops and promotes standards for strong authentication methods.

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. These methods generally require the use of client-side agents, either standalone or embedded into applications as SDKs.

Enterprise Authentication services can present multiple authentication schemes, methods, and challenges to a user or service according to defined policies based on any number of factors, for example, the time of day, the attributes of the user, their location, or the device from which a user or service attempts authentication. The factors just listed as examples can be used to define variable authentication policies. User Behavior Analysis (UBA) employs risk-scoring analytics algorithms to first baseline regular access

patterns and then be able to identify anomalous behavior which can trigger additional authentication challenges or attribute collection.

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

- Strong/Two-Factor or Multi-Factor Authentication devices, such as Smart Cards, mobile strong assurance credentials (e.g., Derived PIV credentials or other solutions which provide parallel x.509 certificates issued to mobile devices), USB authenticators, biometrics, etc.
- One-time passwords (OTP), delivered via phone, email, or SMS,
- Out-of-band (OOB) application confirmation, usually involving mobile phones,
- Identity context analytics, including
    - IP address
    - Geo-location
    - Geo-velocity
    - Device ID and device health assessment
    - User Behavioral Analysis (UBA)

The method of Knowledge-based authentication (KBA), or asking “security questions”, is still used by some organizations, though it should be deprecated due to its inherent security weaknesses. Many organizations today employ a variety of risk-based authentication methods. Consider the following sample case. Suppose a user in the finance department successfully logs into her laptop using local credentials. In order to connect to enterprise resources, she must then authenticate to her company’s VPN, which requires entering a separate username/password combination. Behind the scenes, the authentication server examines the user’s IP address, geo-location, device ID, and health assessment to determine if the request context meets criteria set forth in security policies and fits within historical parameters for this user. Though it appears that username/password is the one and only gate, these other checks provide some additional contextual assurance.

Going one step further in the example, consider that the employee needs to make a high-value bank transaction in an online banking application. Entry to the banking app may be brokered by Single Sign-On (SSO - typically SAML, OAuth, or JWT) features in her enterprise IAM, and may not require a visibly distinct authentication event. A bank transfer like this is a task within her scope and role as defined by attributes in the user identity repository. However, the bank administrator has set a risk-based policy correlated to transaction value amounts, and in this case, the requested payment value exceeds the policy limits. In order to continue, the user is sent a notification via a mobile banking app on her phone, which had been previously registered with the bank. The pop-up asks the user to confirm. The user presses “Yes”, and the transaction is processed.

Authentication and the related identity and context assurance values, then, can be considered a pre-cursor

to authorization. The evaluation of these additional attributes can be programmed to happen in response to business policies and changing risk factors.

The story above is just one possible permutation among thousands. Risk-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. Risk-based MFA can help protect enterprises against fraud and loss.

“Passwordless” is a popular term among the Enterprise Authentication vendors today. Some passwordless options have been around for a while but are starting to be implemented more at enterprises and even consumer-facing businesses. Passwordless options include the aforementioned biometrics and mobile push apps as well as simple possession of registered devices and x.509 certificates. Passwordless can also mean the evaluation of contextual risk factors without interrupting the user flow (in happy path flows).

Account recovery must also be considered for IAM and especially authentication solutions: when users forget passwords, lose credentials, or change devices, they need ways to get access to their accounts. Account recovery techniques include Knowledge-Based Authentication (KBA; but it is recommended to avoid this method as it is usually even less secure than password authentication), email/phone/SMS OTP, mobile push notifications, and account linking. Help desk assistance may also be needed on occasion, but it is a costly measure.

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

Overall, the breadth of functionality is still growing. Support for a variety of MFA mechanisms, evaluation of user and contextual attributes, 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. Device identity, fingerprint, health assessments, and intelligence are increasingly considered important factors to evaluate, as well as UBA, resource attributes, identity proofing, and other forms of intelligence collection. Machine Learning (ML) detection models may also be used to detect and classify outliers in device and user intelligence.

1.1 Market Segment

This market segment is mature and common feature sets are stable, but vendors are frequently introducing innovations in authenticator technologies and risk analysis engines. We expect to see this trend continue in the future. However, given the surging demands of businesses and the need to provide better security, many organizations must implement risk-based Enterprise Authentication solutions to augment IAM systems if they have not already to help reduce the risk of fraud and data loss.

Enterprise Authentication solutions are an evolution and differentiation of yesterday's IAM systems. Many organizations are responding to the pressure to move away from just using usernames and passwords for authentication. Strong authentication options, such as Smart Cards or other hardware tokens, have existed for years. However, such solutions have historically been complex and costly to deploy and administer. Moreover, hardware tokens continue to have usability issues. The mix of authenticators and associated user attributes that most commercial Enterprise Authentication systems present are increasingly sufficient to meet the needs of higher identity assurance for access to sensitive digital resources and high-value transactions.

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

A good Enterprise Authentication solution needs to balance integration flexibility with simplicity. Today's offerings in this area provide multiple authentication mechanisms, including many mobile options and SDKs; risk engines that evaluate numerous definable factors that can be gathered at runtime and compared against enterprise policies; and out-of-the-box (OOTB) connectors for the majority of popular on-premises and cloud-hosted 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 products from the same vendor rarely offer the reduced complexity promised by sales. All Enterprise Authentication solutions, almost by definition, require and support identity federation. While these solutions may mitigate many security 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.

Picking solutions always requires a thorough analysis of specific customer requirements and a comparison with available product and/or service 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 to identify those vendors that customers should look at more closely.

1.2 Delivery models

In the Enterprise Authentication market, solutions are offered as SaaS, PaaS, and for on-premises deployment. Pure-play SaaS solutions are often multi-tenant by design. On the other side, Managed Service

offerings are run independently per tenant. For SaaS offerings, the licensing model is often priced per user, either active users in a given time period or by the total number of registered users. For managed services or PaaS, the licensing costs can be per instance or per managed identity. The cloud-delivered variants sometimes charge per-session fees. For on-premises deployments, licensing costs can be measured in a couple of different ways, such as per-user or per-server.

1.3 Required Capabilities

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

- Support multiple authenticator types, such as:
  - Smart Cards, USB tokens, and older form factor hardware tokens
  - Mobile apps and push notifications
  - x.509 certificates
  - Biometrics, especially mobile biometrics leveraging native OS capabilities
  - OTP: HOTP/TOTP over phone, email, and SMS
- Availability of mobile SDK for customers to write their own secure apps; optional use of Global Platform Secure Element for credential storage and Global Platform Trusted Execution Environment (TEE) for safe mobile app execution
- Adhere to policy-based access controls model so that IT departments and Line of Business application owners can define risk-appropriate authentication rules
- Perform run-time risk analysis of behavioral and environmental factors
- Enforce configurable actions including permit, step-up authentication, deny, lock account/device, etc.
- Integrate with legacy IAM systems, usually via cookie support
- Support identity federation via OAuth2, OIDC, JWT, and SAML
- Integrate with SIEM, SOAR, UBA, and other security systems
- Provide administrators with management dashboards and configurable reporting
- Allow for delegated and role-based administration within the solution
- Process relevant threat intelligence in real-time: using customer's internal, vendor ecosystem collected information, and/or subscriptions to 3rd party services that identify aberrant user behavior, compromised credentials, etc.

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

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

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

- Support for standards such as FIDO Alliance, and Global Platform Secure Element and Trusted Execution Environment standards.
- Advanced support for authentication mechanisms, especially FIDO, mobile, and behavioral biometrics and mobile SDKs.
- Advanced provisioning capabilities, such as Just-in-Time SAML and SCIM standard support.
- A comprehensive, secure, and well-documented set of REST-based APIs, Webhooks, and/or WebAuthn to allow access to data by 3rd-party identity and security analytics tools.
- Highly configurable built-in reporting functions.

Please note that we only listed a sample of features, and we consider other capabilities per solution as well when evaluating and rating Enterprise Authentication solutions

2 Leadership

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

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

- Product Leadership
- Innovation Leadership
- Market Leadership

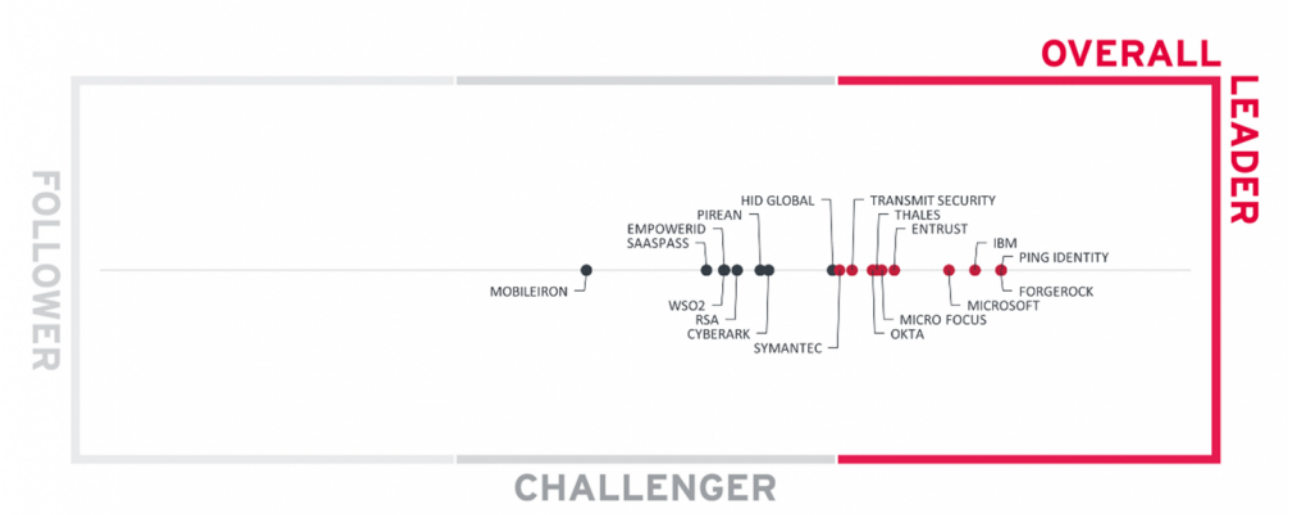


Figure 1: The Overall Leadership rating for the Enterprise Authentication market segment

The Enterprise Authentication market segment continues to grow in size and number of vendors. There is a wide range of vendor types. The overall leaders in this edition of the report are ForgeRock, Ping Identity, IBM, Microsoft, Entrust, Micro Focus, Thales, Okta, Transmit Security, and Symantec. The leaders include a mix of IAM specialist heavyweights, venerable full-service IT software and hardware companies, and

authentication specialists. Though many have offered products for on-premises for decades, each has a strong cloud component to its solution set now.

Challengers are distributed across the center and include HID Global, CyberArk, Pirean, RSA, EmpowerID, WSO2, SAASPASS, and MobileIron. Similarly, we see a mix of vendor types here: IAM specialists, IT stack vendors, and a few who are focused on specific areas related to enterprise authentication.

The Follower section is empty, which shows that a certain level of maturity in terms of product and market size is necessary to be competitive in Enterprise Authentication.

Overall Leaders are (in alphabetical order):

- Entrust
- ForgeRock
- IBM
- Micro Focus
- Microsoft
- Okta
- Ping Identity
- Symantec
- Thales
- Transmit Security

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

Figure 2: Product Leaders in the Enterprise Authentication market segment

Product Leadership, or in some cases Service Leadership, is where we examine the functional strength and completeness of services.

The Product Leaders in Enterprise Authentication are Ping Identity, ForgeRock, IBM, Transmit Security, Okta, Micro Focus, Microsoft, Entrust, Pirean, EmpowerID, and Symantec. Each of their products contains a sufficient level of innovation and delivered product vision to merit standing at the top of the rating.

We find that Challengers are clustered mostly in the upper third of the chart. At the top and nearly among the leaders we see CyberArk, Thales, SAASPASS, WSO2, RSA, and HID Global. These vendors have a

good set of capabilities in their products and services. MobileIron appears in the lower section of the Challenger block.

The Follower section is empty in this iteration of this report.

Product Leaders (in alphabetical order):

- EmpowerID
- Entrust
- ForgeRock
- IBM
- Micro Focus
- Microsoft
- Okta
- Ping Identity
- Pirean
- Symantec
- Transmit Security

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 and other cutting-edge features, while maintaining compatibility with previous versions.

Figure 3: Innovation Leaders in the Enterprise Authentication market segment

Innovation Leaders are those vendors that are delivering cutting edge products, not only at customer request but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. The Innovation Leaders in Enterprise Authentication are ForgeRock, Ping Identity, Transmit Security, IBM, Pirean, Micro Focus, Entrust, Microsoft, and Okta. There is a strong correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

The top Challengers are HID Global, EmpowerID, Thales, SAASPASS, WSO2, Symantec, and CyberArk. In

the second half of the Challenger area, we see RSA and MobileIron. These companies also have some specific innovations that make their offerings attractive to their customers, but both need to shift their emphasis to deploying newer technologies.
No Followers appear in the Innovation Leadership ranking.

Innovation Leaders (in alphabetical order):

- Entrust
- ForgeRock
- IBM
- Micro Focus
- Microsoft
- Okta
- Ping Identity
- Pirean
- Transmit Security

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

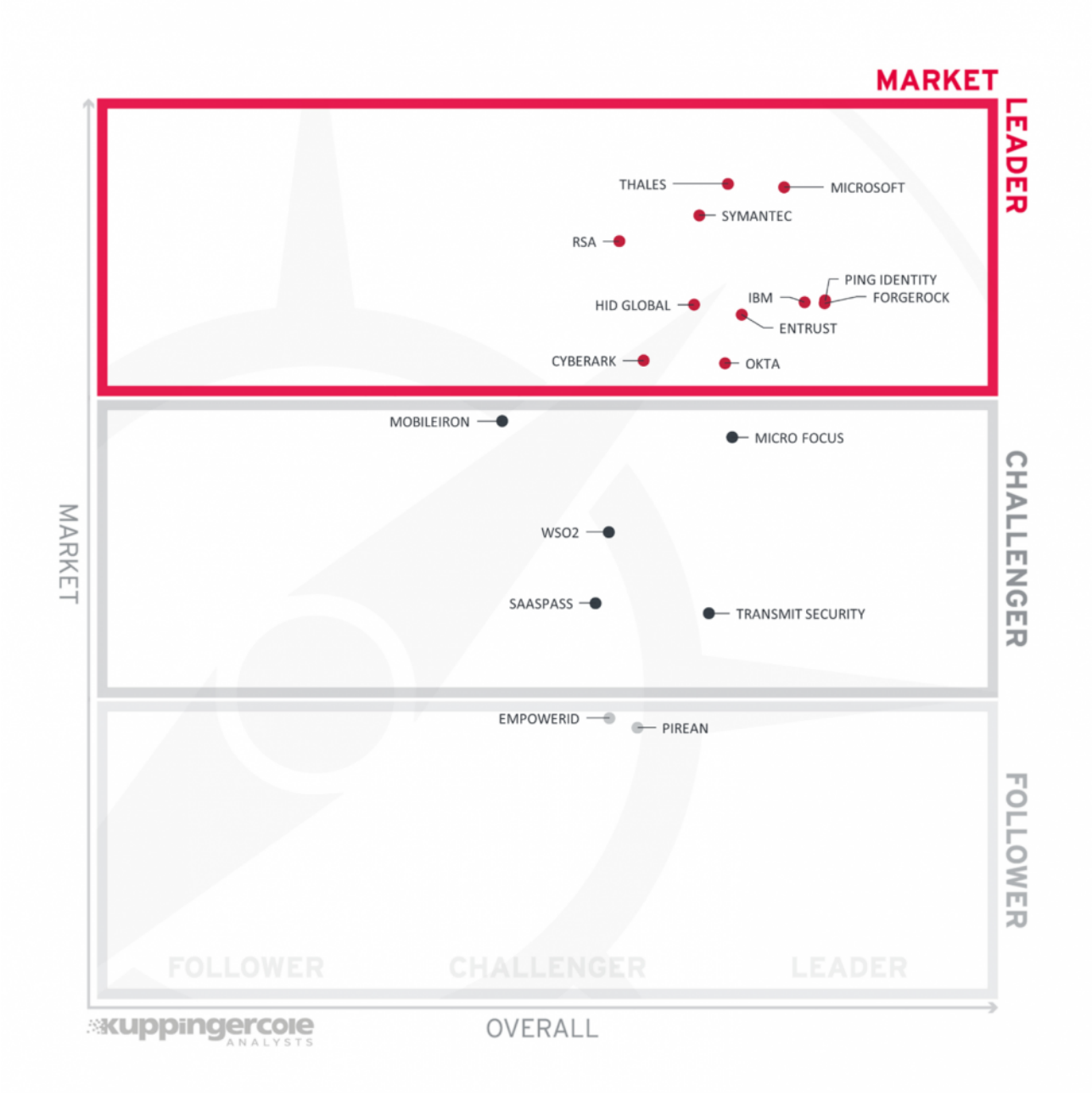


Figure 4: Market Leaders in the Enterprise Authentication market segment

Market Leadership is a combined measure of customers, managed users, partners, the geographic distribution of customers, support, and partners, and overall financial position. The Market Leaders in Enterprise Authentication are Thales, Microsoft, Symantec, RSA, Ping Identity, IBM, ForgeRock, HID Global, Entrust, CyberArk, and Okta. These are well-known names in the IAM space and have size and presence in the Enterprise Authentication segment to justify their leadership ranking.

The top Challengers are MobileIron and Micro Focus. WSO2, SAASPASS, and Transmit Security are also found in the Challenger section.

EmpowerID and Pirean are Market Followers, which, given the size of the overall market, shows a good chance for growth.

Market Leaders (in alphabetical order):

- CyberArk
- Entrust
- ForgeRock
- HID Global
- IBM
- Microsoft
- Okta
- Ping Identity
- RSA
- Symantec
- Thales

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. 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.

3.1 The Market/Product Matrix

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

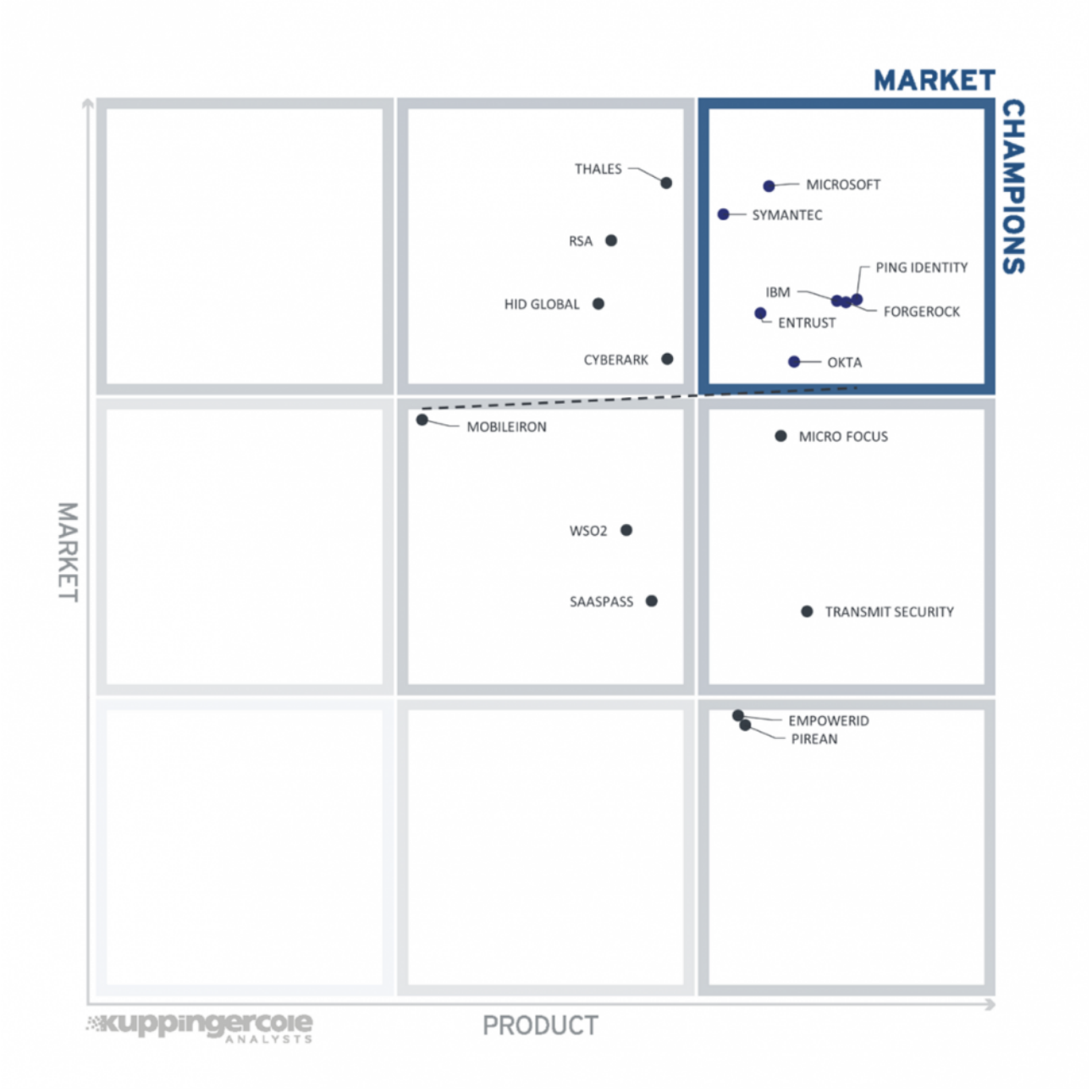


Figure 5: The Market/Product Matrix.

This chart shows how well vendors are doing in the market relative to product strength. 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.

The Market Champions in this report are Microsoft, Symantec, Ping Identity, IBM, ForgeRock, Entrust, and Okta. Each is a strong player in IAM and/or IDaaS in general, and it is no surprise that their robust authentication products and services have wide adoption.

To the left of the Market Champions in the top center box, we see Thales, RSA, HID Global, and CyberArk.

These companies are doing very well in terms of market share.

In the right center box find Micro Focus near the edge of Market Champions, with a good product and concomitant percentage of market share. Transmit Security is also in the right center but below the midpoint, showing that their feature-rich offering has opportunities for additional growth.

MobileIron, WSO2, and SAASPASS are in the center of the chart. These too have good products and services, perhaps missing a few functions compared to the leaders. All appear below the line which indicates that their market positions could likely increase.

Lastly, we have EmpowerID and Pirean in the bottom right. Their products are more feature-complete than their current market standing might suggest.

3.2 The Product/Innovation Matrix

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

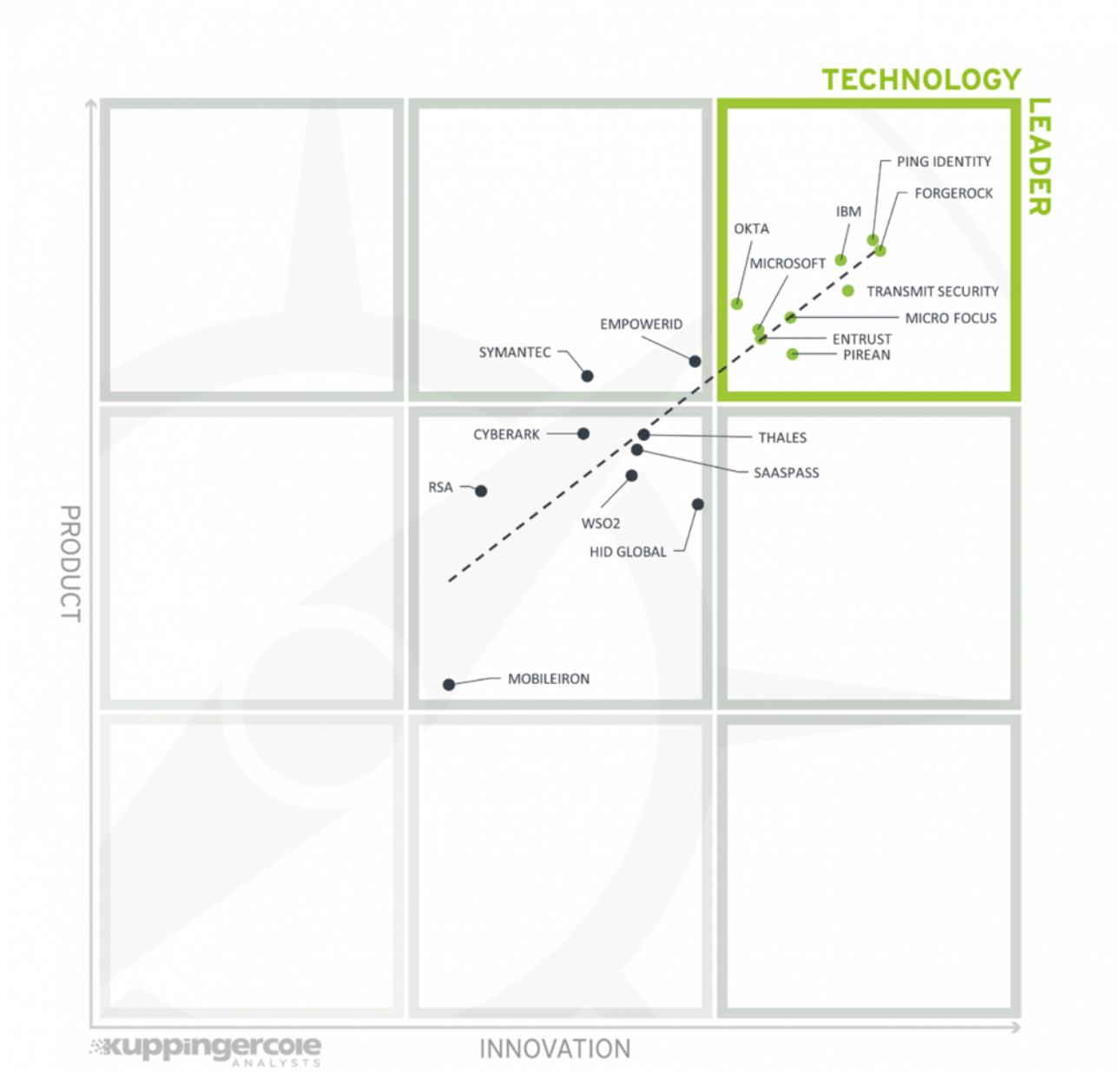


Figure 6: The Product/Innovation Matrix.

The Technology Leaders are Ping Identity, ForgeRock, IBM, Transmit Security, Okta, Micro Focus, Microsoft, Entrust, and Pirean. The vendors in the top left show a correlation between high scores for product completeness and vision. There is a range of company types here, though: IT stack vendors, IAM specialists, and cloud-native service providers. Delivering authentication solutions from the cloud, both as IaaS instances and via SaaS, has moved from being innovative to expected functionality in a contemporary product. However, we see that technical advancements born in the cloud, such as containers, orchestration, and micro-services architecture, are important areas for further innovation in enterprise authentication services.

EmpowerID and Symantec are in the top center above the line. Their products offer most of the functions that organizations look for in enterprise authentication, but with slightly less innovation.

CyberArk, Thales, SAASPASS, WSO2, RSA, HID Global, and MobileIron are in the center of the chart. Their ratios of product completeness to innovative vision are fairly closely aligned, but somewhat behind the Technology Leaders.

3.3 The Innovation/Market Matrix

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

Figure 7: The Innovation/Market Matrix.

Finally, we consider the intersection of Innovation and Market Position. The Big Ones are Microsoft, Ping Identity, IBM, ForgeRock, Entrust, and Okta. These companies are being rewarded by the market for the level of innovation they provide in their products and services.

Thales, Symantec, RSA, HID Global, and CyberArk are to the left of the Big Ones in the top center. Each has a substantial market share plus reasonably innovative approaches to enterprise authentication.

In the right center, Micro Focus appears near the upper border while Transmit Security is below. Both possess a significant number of innovations and have room to progress toward becoming a Big One.

MobileIron, WSO2, and SAASPASS are in the center box, indicating a moderate amount of innovation and market share.

Pirean is in the lower right. It is a younger company with a good amount of innovation that has not had time to capture an appropriate amount of the market. EmpowerID is in the lower center, having a smaller market share and just slightly less innovation.

4 Products and Vendors at a glance

This section provides an overview of the various products and/or services we have analyzed within this KuppingerCole Leadership Compass on Enterprise Authentication. This overview goes into detail on the various aspects we include in our ratings, such as security, overall functionality, etc. It provides a more granular perspective, beyond the Leadership ratings such as Product Leadership, and allows identifying in which areas vendors and their offerings score stronger or weaker. Details on the rating categories and scale are listed in chapter 7.2 to 7.4.

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	Interoperability	Usability	Deployment
CyberArk Identity Security Platform	●	○	●	●	○
EmpowerID	●	○	●	●	●
Entrust Identity	●	○	○	●	●
ForgeRock Identity Platform	●	●	●	●	●
HID Global Authentication Platform	●	○	○	○	○
IBM Security Verify	●	●	●	●	●
Micro Focus Authentication	○	●	○	○	●
Microsoft Azure Active Directory	●	●	●	●	●
MobileIron Zero Sign-On	○	●	●	○	●
Okta Identity Cloud	○	●	●	●	●
Ping Intelligent Identity Platform	●	●	●	●	●
Pirean Access: One	●	○	○	○	○
RSA SecurID Access	●	○	●	○	○
SAASPASS IAM	●	○	○	○	○
Symantec VIP	●	●	○	○	○
Thales SafeNet Trusted Access	●	○	○	○	○
Transmit Security Enterprise IAM Platform	●	●	○	●	○
WSO2 Identity Server	●	○	●	○	○
Legend		● critical	● weak	● neutral	○ positive	● strong positive

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

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

Vendor	Innovativeness	Market Position	Financial Strength	Ecosystem
CyberArk	positive	strong positive	strong positive	positive
EmpowerID	positive	neutral	positive	weak
Entrust	strong positive	strong positive	strong positive	positive
ForgeRock	strong positive	strong positive	positive	strong positive
HID Global	positive	positive	strong positive	positive
IBM	strong positive	strong positive	strong positive	strong positive
Micro Focus	strong positive	positive	strong positive	neutral
Microsoft	strong positive	strong positive	strong positive	strong positive
MobileIron	neutral	positive	positive	strong positive
Okta	strong positive	strong positive	strong positive	positive
Ping Identity	strong positive	strong positive	strong positive	strong positive
Pirean	strong positive	neutral	positive	neutral
RSA Security	weak	strong positive	strong positive	strong positive
SAASPASS	positive	positive	neutral	neutral
Symantec	neutral	strong positive	strong positive	strong positive
Thales	neutral	strong positive	strong positive	strong positive
Transmit Security	strong positive	positive	neutral	positive
WSO2	positive	positive	neutral	positive
Legend	critical	weak	neutral	positive	strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/service evaluation

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

Spider graphs

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

- Authenticators
  This category represents the breadth of authenticators supported, as detailed in Chapter 1.
- Mobile SDK
  Many organizations utilize mobile SDKs to create their own authenticators. This category rates the presence of mobile SDKs in vendor solutions as well as the depth of and security afforded by the features available to customers.
- Intel sources
  This category includes various forms of intelligence available for the risk analytics engine to process, including device intelligence, user behavioral analysis, user identity assurance levels, and credential intelligence for B2B2C use cases. Credit is given when vendors provide these capabilities within their own platforms and also for providing customers with the opportunity to add feeds and subscriptions on their own.
- Risk engine
  This category represents the collection of functions provided by the vendor for receiving the various forms of intelligence, processing the sets of relevant information, and providing usable outputs for customer applications and infrastructure. Features considered here include complexity and customizability of policies, depth and granularity of available output options, the rationale provided to customers for individual transaction processing decisions, and the use of Machine Learning algorithms in assessing intelligence sources and input.
- Scalability
  Picking the right size vendor is an important consideration in RFPs. Not everyone needs the biggest

and most scalable solutions, but if your business does, then understanding the scalability comparison and factors examined will be of paramount interest. The most scalable solutions are usually those which are based on modern distributed architectures. This rating is influenced by many factors including the architecture of the vendor solution, the number of customers supported, size of B2E implementations, and deployment models available. For SaaS-delivered solutions, multi-cloud utilization, geographic distribution, SLAs, and maximum supported number of transactions per second are considered.

- App connectors
  This category evaluates the number of pre-built connectors and token exchange services that customers can use to facilitate integration with on-premises, legacy, and SaaS-delivered apps.
- Identity/security fabric
  This category evaluates how well each product adheres to Identity and Security Fabrics. Micro-services architectures are the modern approach and best fit for Identity and Security Fabrics paradigms. This category, therefore, is a measure of the APIs, pre-built connectors, and standards support for which customers can use to facilitate integration with other IAM solutions including IGA and PAM as well as security tools such as SIEM and SOAR.

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

5.1 CyberArk

CyberArk was established in 1999 in Boston and is listed on the NASDAQ. They acquired Idaptive, a spin-off of Centrify, in mid-2020. Their combined offerings are considered here. CyberArk offers a range of IAM solutions, including their Privileged Access Management (PAM) solution. CyberArk is a SaaS-delivered product, and it is hosted in AWS in a large number of data centers around the world. For connectivity to an on-prem Active Directory, installation of CyberArk software is required on a Windows machine on the customer network. Identity Security Platform is licensed by the number of registered users per annum.

CyberArk supports Aegis, Authy, DeepNet, Derived PIV credentials, Duo, Google, LastPass, Microsoft, Okta, OneSpan Mobile, SAASPASS, SafeNet, and Symantec VIP apps; Android/iOS biometrics and mobile push apps; FIDO U2F/2.0 tokens; CAC/PIV cards, Duo, Feitian, Google Titan, Kensington, OneSpan DigiPass, RSA SecurID, Smartcards, Symantec VIP, Thetis, and Yubikey tokens. They have an SDK that supports C#, Java, PHP, and Python, but none for mobile; however, their UEM product can collect device intelligence if installed. CyberArk supports JWT, Kerberos, OAuth, OIDC, RADIUS, and SAML tokens/protocols. With customization, other methods can be accommodated as well. Users can be provisioned via SCIM, custom APIs, and self-registration. Customers can use all the standard methods for account and credential recovery.

CyberArk uses a mix of supervised and unsupervised ML algorithms to evaluate more than 60 different risk signals including device intel from external sources, user attributes from connected repositories, and user history and behavioral analysis. CyberArk does not use behavioral biometrics. Third-party intelligence sources such as Have I Been Pwned and Palo Alto Cortex Data Lake are consumed, but there are no connections to identity vetting services. The administrative interface allows for policy creation using drop-down lists.

CyberArk has REST APIs (not versioned), Webhooks, and supports WebAuthn for application integration. CyberArk provides over 2000 application templates for SaaS apps and 24 built-in custom API connectors for apps such as AWS, Box, Concur, DocuSign, Dropbox, Google Workspace, NetSuite, Microsoft 365, Salesforce, ServiceNow, Slack, WebEx, and Zendesk. In addition, CyberArk also provides a SCIM connector that can provision to hundreds of other SaaS applications that support SCIM. CyberArk can send event data to SIEMs in syslog format and has OOTB connectors for IBM QRadar, Micro Focus ArcSight, and Splunk. Exabeam, Micro Focus ATAR, Palo Alto XSOAR, and Siemplify SOAR products have API level interoperability with CyberArk. The Identity Security Platform has deep integration with CyberArk PAM and has a robust implementation of delegated access control.

CyberArk is SSAE SOC 2 Type 1 & 2 certified environments. The solution is UK Cyber Essentials and G-Cloud certified. CyberArk is also certified for US FBI Criminal Justice Information Services, US DOD Cloud Security Model, US FedRAMP, and US FISMA. Adding a mobile SDK and updating the policy authoring UI to include natural language and flow-chart style input would be beneficial for some customers. CyberArk offers a secure and scalable authentication service and should be considered in RFPs by organizations with those requirements.

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

CYBERARK®

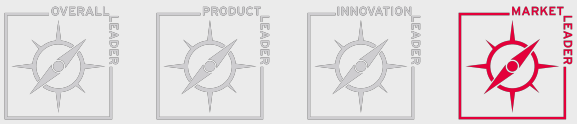
Strengths

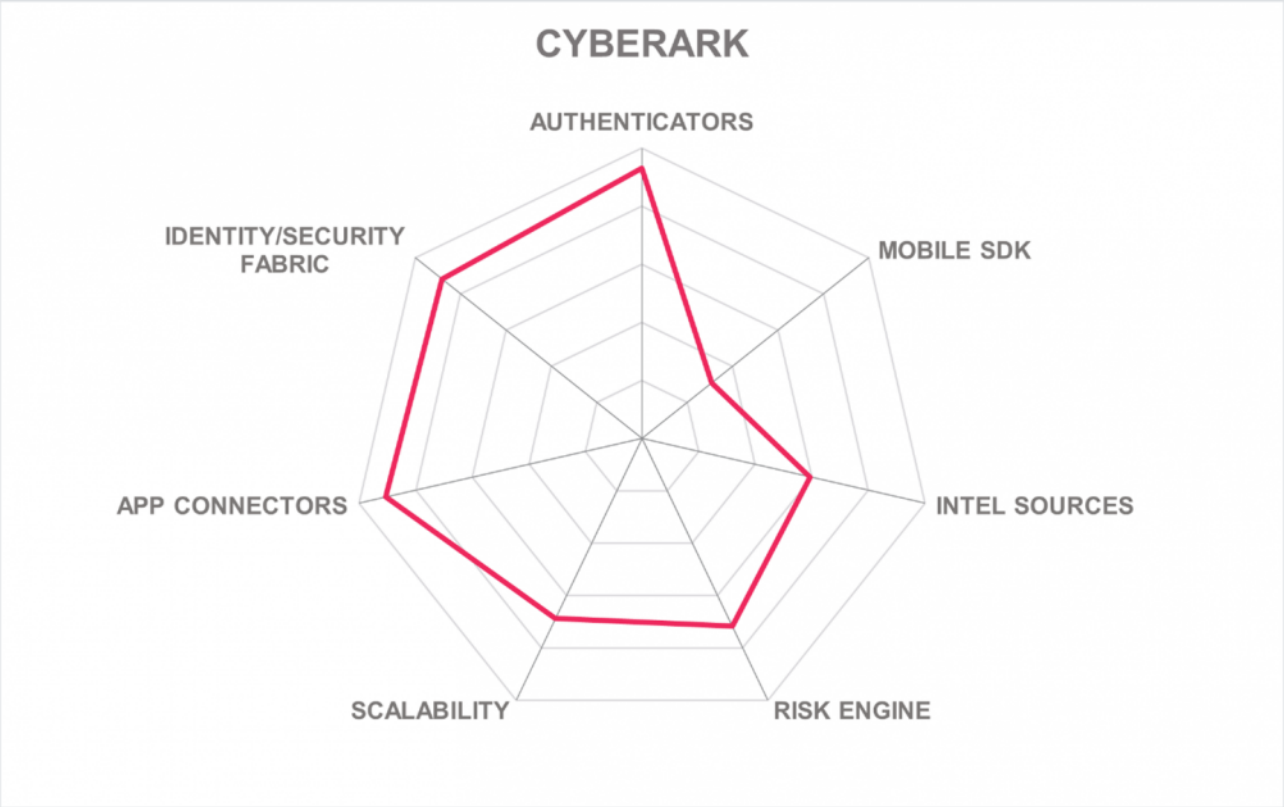
- Large selection of authenticators accepted
- Credential and threat intel bundled
- Risk engine powered by ML detection
- FIDO 2.0 support
- Integration with CyberArk PAM
- Many security certifications

Challenges

- No mobile SDK, but customers can use their UEM product to collect device intel
- UBA is utilized but no behavioral biometrics usage
- Policy authoring UI would benefit from natural language or flow-chart input techniques

Leader in




CYBERARK
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.2 EmpowerID

EmpowerID was founded in Ohio in 2005. They are privately held and have offices in the DACH region of the EU as well. In addition to the products listed above that are considered here, EmpowerID has access management, IGA, and lifecycle risk management solutions. These components can be installed on-premises on Windows and/or various flavors of Linux, or in any IaaS as Docker containers. EmpowerID hosts a managed service with data localization in Microsoft Azure. The products are licensed according to the number of monthly active users.

In terms of authenticators, EmpowerID supports Aegis, Authy, DeepNet, Duo, Google, LastPass, Microsoft, MobileConnect, Okta, SAASPASS, and SafeNet apps; Android/iOS biometrics and mobile push apps; FIDO U2F/2.0 tokens and Windows Hello; Duo, Feitian, Google Titan, OATH, OneSpan DigiPass, RSA SecurID, Smartcards, Symantec VIP, and Yubikey tokens. SDKs covering .NET, Java, JavaScript, and Xamarin are available. The mobile SDK can collect a good range of device intel signals. Protocols accepted include RADIUS, SAML, OAuth, OIDC, and JWT. All major account recovery procedures are supported. LDAP, SCIM, cloud-specific APIs, and self-registration can be used for provisioning.

The risk engine can process device intelligence (except device health), and identity assurance from Equifax and RSA Security. Behavioral biometrics are not supported. Admins can create granular policies with complex workflows as needed. Output to downstream authorization engines is configurable.

EmpowerID exposes all major functions via APIs: Kafka, OData, REST, SOAP, Webhooks, and Websockets methods; and CSV, JSON, and XML formats. EmpowerID provides connectors for major SaaS apps such as Box, Google Workspace, Microsoft 365, Salesforce, SAP Ariba and SuccessFactors, ServiceNow, Slack, and Zendesk. Interoperability with other IAM, IGA, and PAM products is primarily achieved via standards, but additional customizations are possible through the Workflow Studio.

ABAC/PBAC/RBAC administrative models are embedded. EmpowerID can send info to SIEMs using CEF and syslog. There is no support for SOAR at present. EmpowerID claims and/or attests to the following security standards and certifications: FIPS 140-2 and 197, NIST 800-57, HIPAA, ISO/IEC 14402/27001/27018, and multiple OpenID profiles. EmpowerID's workflow management approach facilitates customization when needed. The admin UI could be extended to support flow-chart and/or natural language type policy authoring. These alignments and certifications will appeal to customers in certain regulated industries and others that have strict security requirements.

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

empowerID

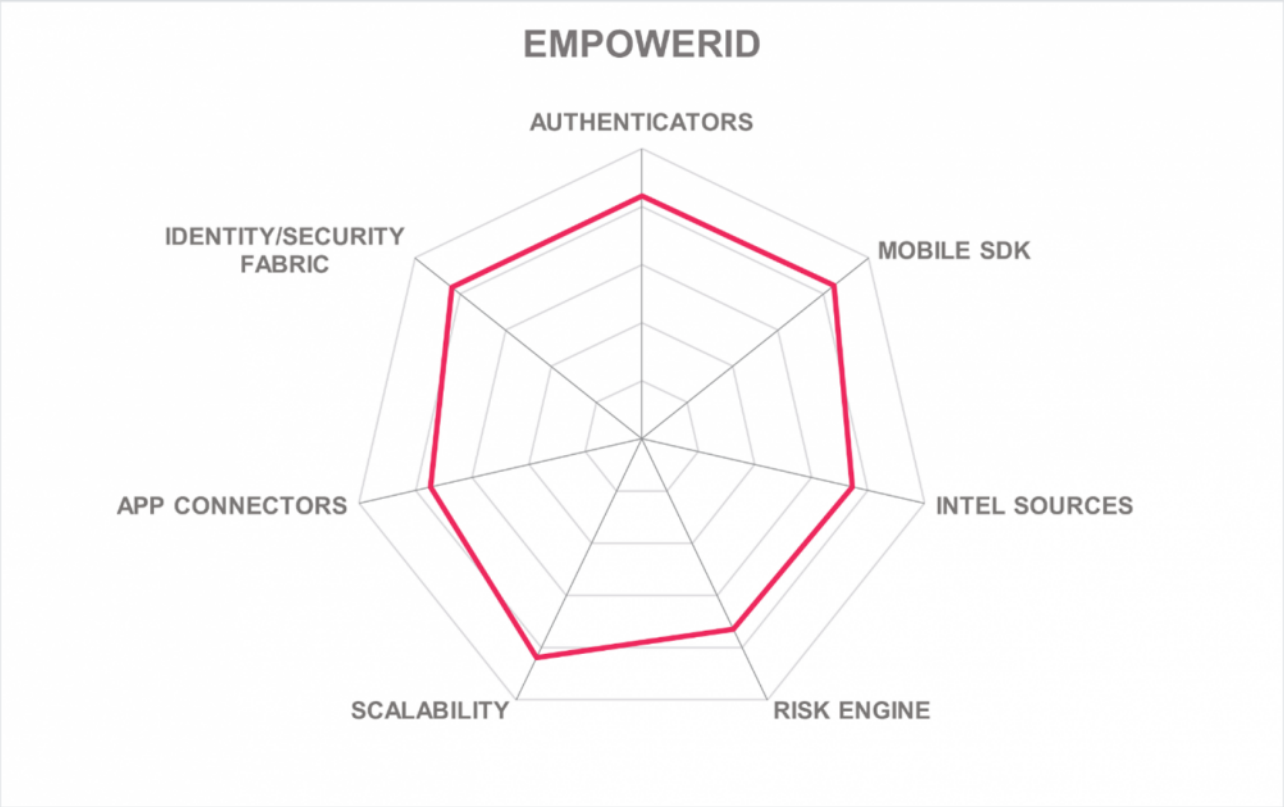
Strengths

- Flexible deployment options with data localization
- Microservices architecture
- Multi-faceted API implementation
- Good selection of authenticators

Challenges

- Admin UI could be modernized
- Device health not collected by mobile SDK
- Behavioral biometrics not supported

Leader in


EMPOWERID
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.3 Entrust

Privately held Entrust, formerly known as Entrust Datacard, was founded in 1969. Entrust Identity is the unified authentication portfolio: IntelliTrust is the IDaaS version, the former Identity Guard is now Identity Enterprise, and SMS PASSCODE is now known as Identity Essentials. Entrust Identity serves B2B/C/B2B2C and G2C use cases. Entrust has a substantial HSM, PKI, and integrated document signing business as well. Entrust Identity can be deployed on-premises on CentOS, RHEL, or Windows; on IaaS in AWS, Azure, or GCP; and they offer it as SaaS hosted in their own data centers and AWS. Moreover, some MSSPs operate Entrust Identity for their customers. Data can be regionalized to the US or EU. Licensing options include active or registered users per time period and per-transaction.

Entrust accepts multiple authentication methods, including Authy, their own Entrust app and Derived PIV credentials app, Google Authenticator; grid cards and QR codes; Android/iOS biometrics and mobile push apps; CAC/PIV, Feitian, Google Titan, Smartcards, Yubikey, or any OATH compliant hardware tokens. Relevant protocols supported include JWT, Kerberos, OAuth, OIDC, RADIUS, and SAML. Entrust offers a secure mobile SDK that can harvest some device intel parameters. LDAP but not SCIM can be used for bulk provisioning. All major account recovery methods are available.

Entrust Identity risk engine evaluates device (including iovation's device reputation service), environmental, and user attributes. Entrust offers remote onboarding and identity proofing via the use of mobile biometrics with sophisticated liveness detection and document verification. Administrators can write policies that incorporate 3rd-party intelligence with moderate granularity. The policy authoring UI is modern and intuitive.

API methods supported include REST, SOAP, and WebAuthn; and JSON and XML data formats. Entrust provides connectors for SaaS apps such as Box, Citrix, Google Workspace, Jira, Microsoft 365, Salesforce, Tableau, Taleo, WebEx, and Zoom. Entrust interoperates with BeyondTrust, Centrify, CyberArk, ForgeRock, HashiCorp, Microsoft Azure AD, and similar IAM/IGA/PAM solutions. RBAC and delegated admin models are supported. SIEM connections can be configured over APIs as .csv file transfers, but syslog is not available. SOAR integrations have not yet been developed.

Entrust Identity is aligned with ISO 27001 but not independently certified. Other pertinent security certifications have not been obtained yet. Crypto elements do use Entrust's FIPS 140-2 compliant toolkits. Improvements for the risk engine and signals intelligence are on the roadmap. The inclusion of a mobile biometrics and document verification app for remote onboarding and identity vetting is both innovative and useful. Moreover, Entrust's work on passwordless and proximity-based authentication and logout utilize leading-edge technologies and address critical use cases. Entrust Identity is a solution worth serious consideration by organizations looking for modular enterprise authentication services.

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

Entrust Datacard®

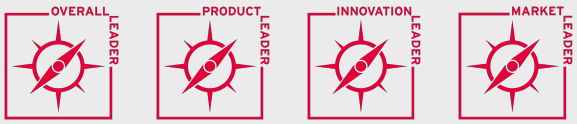
Strengths

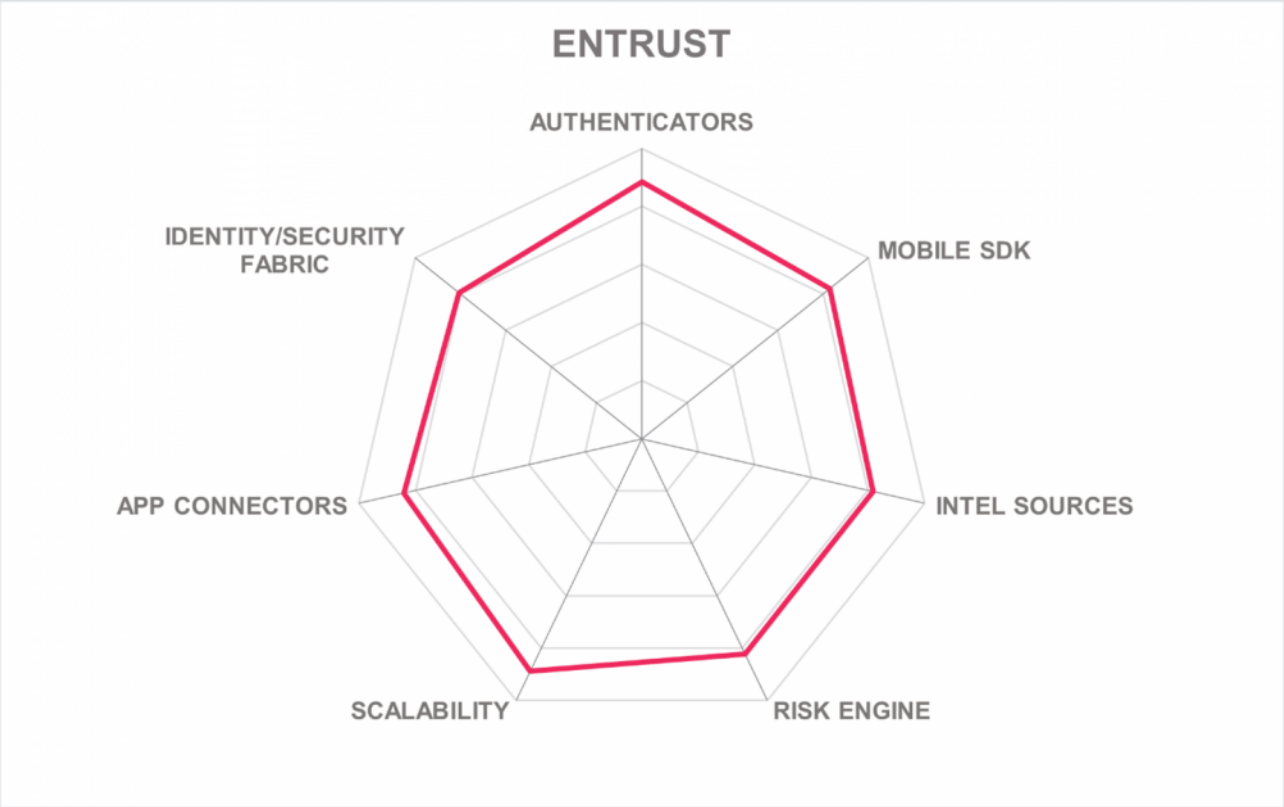
- Remote identity proofing and employee onboarding via a mobile app with biometrics and liveness detection
- High assurance credential issuance
- Derived PIV / Smartcard on mobile app support
- Mobile phone to PC proximity authentication and logout
- Excellent admin interface

Challenges

- Additional device intel features are on the long-term roadmap
- Behavioral biometrics not present but planned
- Syslog not supported, but SIEM integration can be configured

Leader in




ENTRUST
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.4 ForgeRock

ForgeRock is a leading venture-backed IAM vendor, headquartered in the Bay Area but with many offices around the world. ForgeRock supports most major IAM standards and is a significant contributor to several international standards organizations. Their Identity Platform serves both B2E and B2C markets. It is part of a full suite of IAM products including Access Management, Directory Services, Identity Management, IoT/Edge Security, Identity Gateway, Identity Governance, and Privacy & Consent Management. ForgeRock Identity Platform runs on-premises on most Linux variants, in any IaaS environment, in hybrid environments, or as SaaS in GCP in 20 regions. Several large MSPs run ForgeRock Identity Platform as their identity solution. Licensing is by the number of quarterly/annually active or registered users.

ForgeRock supports Authy, BehavioSec, DeepNet, Derived PIV credentials, Duo, Entrust, Google, LastPass, Microsoft, Miracl, NokNokLabs, OneSpan, SAASPASS, SafeNet, ThreatMetrix, Yoti apps; Android/iOS biometrics and mobile push apps; FIDO U2F/UAF/2.0 tokens; CAC/PIV cards, Duo, Feitian, Google Titan, OneSpan DigiPass, OATH (any), RSA SecurID, Smartcards, Symantec VIP, and Yubikey tokens. ForgeRock offers a secure mobile SDK for customer application development. The SDK can harvest some device intel, and customers can extend that as needed. ForgeRock supports JWT, Kerberos, OAuth, OIDC, RADIUS, and SAML tokens/protocols. With customization, any other method can be accommodated as long as its API is available and documented. Users can be provisioned via LDAP, SCIM, or self-registration. Customers can use all the standard methods for account and credential recovery.

ForgeRock's risk engine can evaluate a full range of device and credential intelligence, including multiple 3rd-party sources that can be plugged in via ForgeRock's Marketplace. User history and behavioral analysis input are also consumable by the risk engine. Callouts to identity vetting services are possible via the Marketplace. The admin interface is intuitive and features flow chart style authentication policy creation and maintenance.

Identity Platform has optimal API accessibility, supporting OData, REST, RPC, SOAP, WebAuthn, Webhooks, and Websockets, and CSV/JSON/XML formats. Many SaaS app connectors are present, such as Adobe Campaign Manager, Google Workspace, Hubspot, Marketo, Microsoft 365, Salesforce CRM, SAP, ServiceNow, Workday, etc. ForgeRock can send event data to SIEMs over CEF or syslog. Identity Platform provides IGA features, and through standards support can interoperate with other IAM and PAM solutions as needed. ABAC/RBAC and delegated access models are supported for customer administrators.

ForgeRock is certified and/or attested with CSA Star Level 1, ISO 27001, and has several OpenID profile certifications. ForgeRock Identity Platform allows customers to implement high, medium, and low-security models as needed. The ability to add in identity proofing and fraud and threat intelligence is a plus for advanced enterprise authentication use cases. ForgeRock's SaaS presence is smaller than some, but we expect it to ramp up quickly, thereby providing the same flexibility for customers who may not have the in-house resources to run the on-premises, hybrid, or IaaS versions. ForgeRock Identity Platform is well-suited to tackle most any set of authentication requirements and should be near the top of RFP shortlists.

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

FORGEROCK

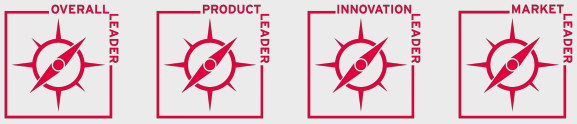
Strengths

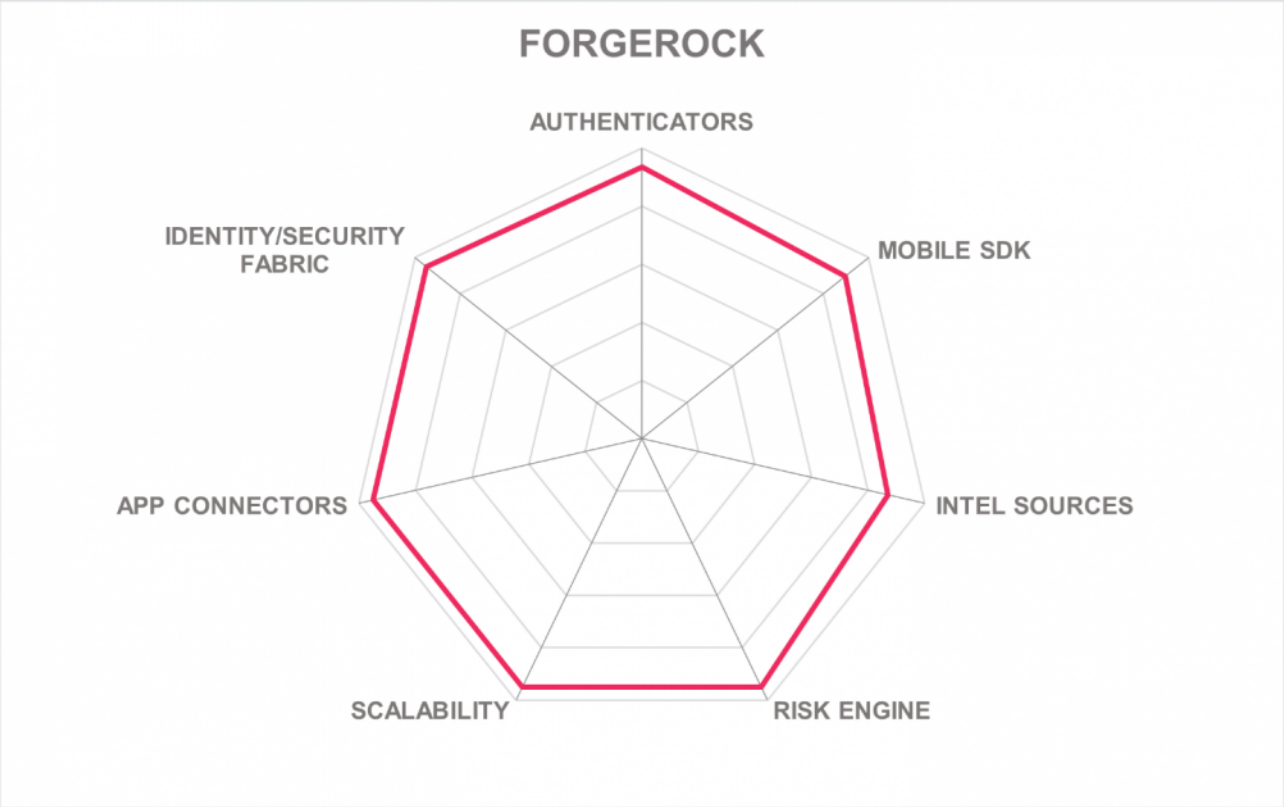
- Wide array of authenticators supported
- Maximum flexibility, exposure, and documentation of APIs
- Highly scalable microservices architecture
- Intuitive flow-chart style management and policy authoring interface
- Easy to add-in credential and device intel services via Marketplace

Challenges

- A latecomer to SaaS deployment model; smaller footprint compared to cloud-native vendors
- Very flexible but requires more expertise to implement and manage on-prem and IaaS instances
- SDK could support more device intel attributes without requiring customization

Leader in




FORGEROCK
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.5 HID Global

HID Global is a subsidiary of ASSA ABLOY Group AB of Stockholm. HID Global's US headquarters is in Austin, TX. HID Global has IAM solutions, and also makes physical access controls systems, RFID tags and readers, biometric readers, smart cards, passports, and some national identity cards, card readers, and mobile apps capable of remote identity verification. Their intersection of IAM, biometrics, and SDK allows them to perform identity card issuance for a number of organizations. HID Global Authentication Platform runs on-premises on CentOS, Debian, and Windows; in AWS, Azure, or Oracle Cloud; or as SaaS in AWS in 3 regions. MSPs also operate HID Global Authentication Platform. Licensing is by the number of quarterly/annually registered users.

HID Global supports Derived PIV credentials, Google, and Microsoft authenticator apps as well as their own; Android/iOS native biometrics and mobile push apps; FIDO U2F/2.0 tokens; CAC/PIV cards, Feitian, Google Titan, HID Crescendo, OATH (any), Smartcards, Symantec VIP, and Yubikey tokens. HID Global Authentication devices, such as the desktop fingerprint readers, can directly integrate with Microsoft Windows Hello for passwordless authentication. HID Global offers a secure mobile SDK for customer application development. The SDK can collect a good range of device intel attributes, and it can be extended. HID Global supports JWT, Kerberos, OAuth, OIDC, RADIUS, and SAML tokens/protocols. Users can be provisioned via LDAP, SCIM, some proprietary cloud APIs, and self-registration. Customers can use all the standard methods for account and credential recovery.

The risk engine in Authentication Platform can evaluate a full range of device intelligence, including device health and history. External sources of compromised credential intelligence are not evaluated. Behavioral biometrics are available. User history and behavioral analysis input is also consumable by the risk engine. HID Global is also in the identity assurance verification and credential issuance business. Government and enterprise customers can utilize HID Global for authoritative attribute lookups, remote document verification, and electronic credential assignment. The administrative interface is intuitive and allows customers to build risk-adaptive authentication policies.

For APIs, HID Global supports REST, SOAP, WebAuthn, Webhooks, and Websockets, and CSV/JSON/XML formats. HID Global does not provide OOTB connectors for SaaS apps, but customers can configure federation. HID Global can send event data to SIEMs via syslog. The solution can interoperate with IGA systems using standard protocols, but there is no explicit interoperability with PAM solutions. RBAC and delegated access models are supported for customer administrators.

HID Global attests and/or has certified on FIPS 140-2, ISO 27001, and SOC 2 Type 1. SOC2 Type 2 status is in work. HID Global has been a strong player in the government and enterprise workforce IAM for years. The inclusion of identity vetting and credentialing services is a valuable differentiating factor in their solution. The platform has some innovative features but is also lacking some features that some customer prospects may find essential. Organizations in highly regulated industries, with high security requirements, and those with physical access controls integration requirements should consider HID Global.

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

HID®

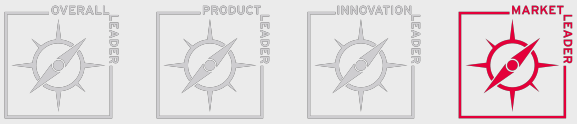
Strengths

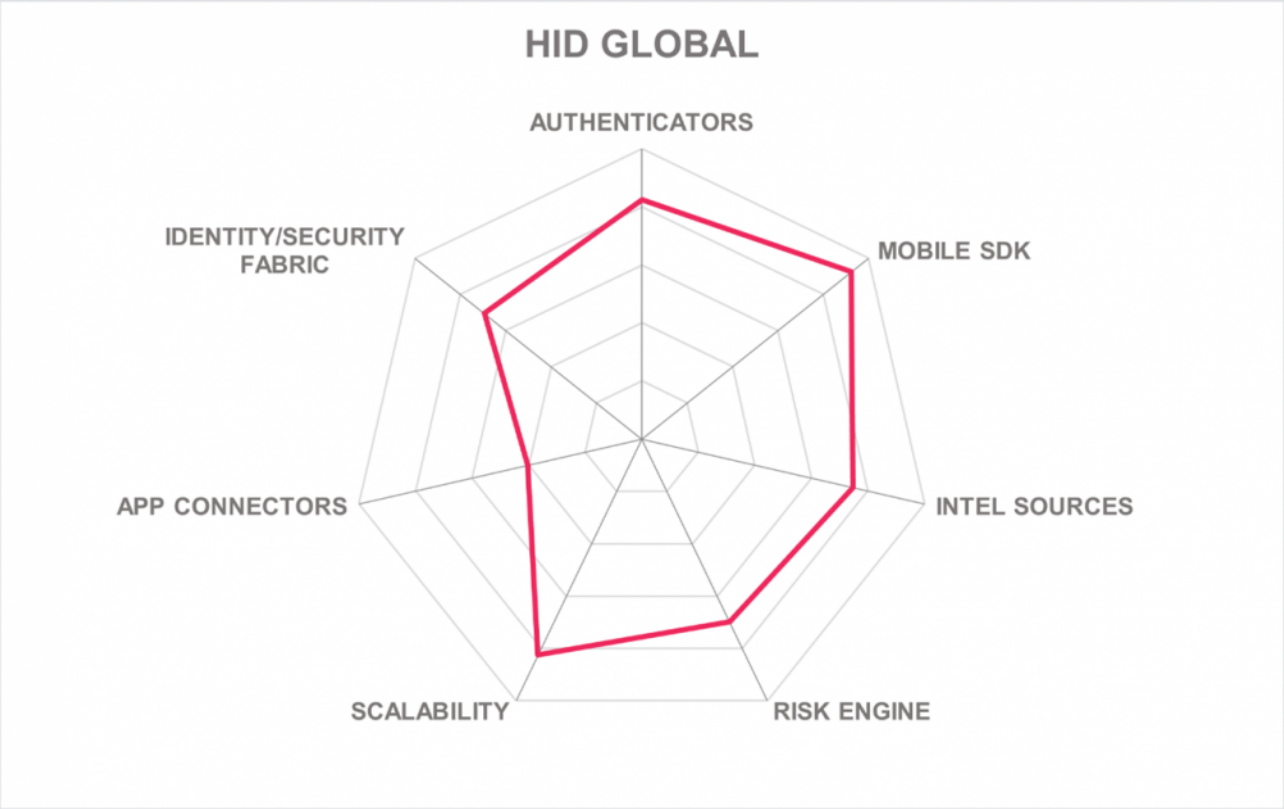
- FIDO 2.0 certified
- Hardware token manufacturer; supplier to OEMs
- Has identity assurance and strong credentialing capabilities
- Easy-to-use flow-chart style management and policy authoring interface
- Comprehensive device intelligence can be collected using secure SDK
- Risk engine can output to payment processing services

Challenges

- Risk factors cannot be separately weighted in policies
- Risk engine does not interoperate with external authorization systems
- No OOTB connectors for SaaS apps
- No PAM interoperability

Leader in




HID GLOBAL
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.6 IBM

IBM has renamed and branded their IAM and IDaaS solution to Security Verify from Cloud Identity. It can be used for B2B, B2C, and B2E use cases. The SaaS version is fully multi-tenant and highly scalable. IBM hosts its SaaS in their own data centers as well as in AWS. Security Verify is available for on-premises deployment, running on Windows and most types of Linux, and can be installed in any IaaS platform. The solution is based on a micro-services architecture. Licensing models include monthly active users, monthly/quarterly/annual registered users as well as per-session and per-node options. With customers and partners across the globe, IBM is a major player in the market.

IBM accepts a long list of authentication mechanisms, including Aegis, Authy, Derived PIV credentials, Google, LastPass, Microsoft, Okta, and SAASPASS; mobile push notifications and Android/iOS biometrics; FIDO U2F/2.0; CAC/PIV, Duo, Feitian, Google Titan, Kensington, OATH (any), OneSpan DigiPass, RSA SecurID, Smartcards, and Yubikey hard tokens. Protocols understood include JWT, Kerberos, OAuth, OIDC, RADIUS, SAML, and WS-Fed/Trust. IBM provides a secure mobile SDK that collects the normal range of device intelligence signals. Users can be provisioned using LDAP, SCIM, and self-registration. All major account recovery types are available, and customers can configure others via APIs.

Native integration with Trusteer gives Security Verify comprehensive device intelligence features, which, along with user attributes, history, UBA, and behavioral biometrics are processed by its granular risk engine. Moreover, external sources of intelligence can be piped in by customers. The authentication policy management interface uses the drop-down list approach.

Security Verify has well-documented and versioned APIs including support for REST, SOAP, Websockets, and WebAuthn as well as CSV/JSON/XML formats. IBM also supports decentralized identity integration with Sovrin. IBM provides numerous OOTB connectors to quickly integrate Security Verify with a variety of SaaS apps covering data analytics, marketing, messaging, office automation, IT automation, developer tools, etc. Security Verify interoperates with CA, Okta, OneLogin, and Ping Identity IDaaS; and CyberArk, IBM Secret Server, and Thycotic PAM solutions. Security Verify can send event data to SIEMs over syslog and has integration with IBM QRadar and Resilient SOAR. ABAC/RBAC and delegated access models are supported for customer administrators.

IBM Security Verify is designed for scalability. It is ISO 27001/27018 certified, PCI-DSS Level 1, and SSAE 18 SOC 2 Type 2 attested. Additional certifications for various government/cloud security programs may make the solution even more appealing for certain customers. Advanced device intelligence capabilities are available via the SDK and within the IBM Trusteer suite of products. Organizations that are looking for mature, highly scalable, and secure enterprise authentication solutions built on state-of-the-art micro-services architecture should put IBM on the list of solutions to consider.

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

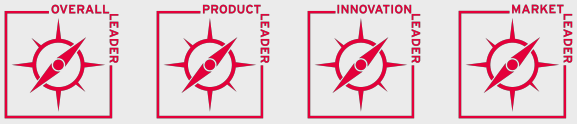
Strengths

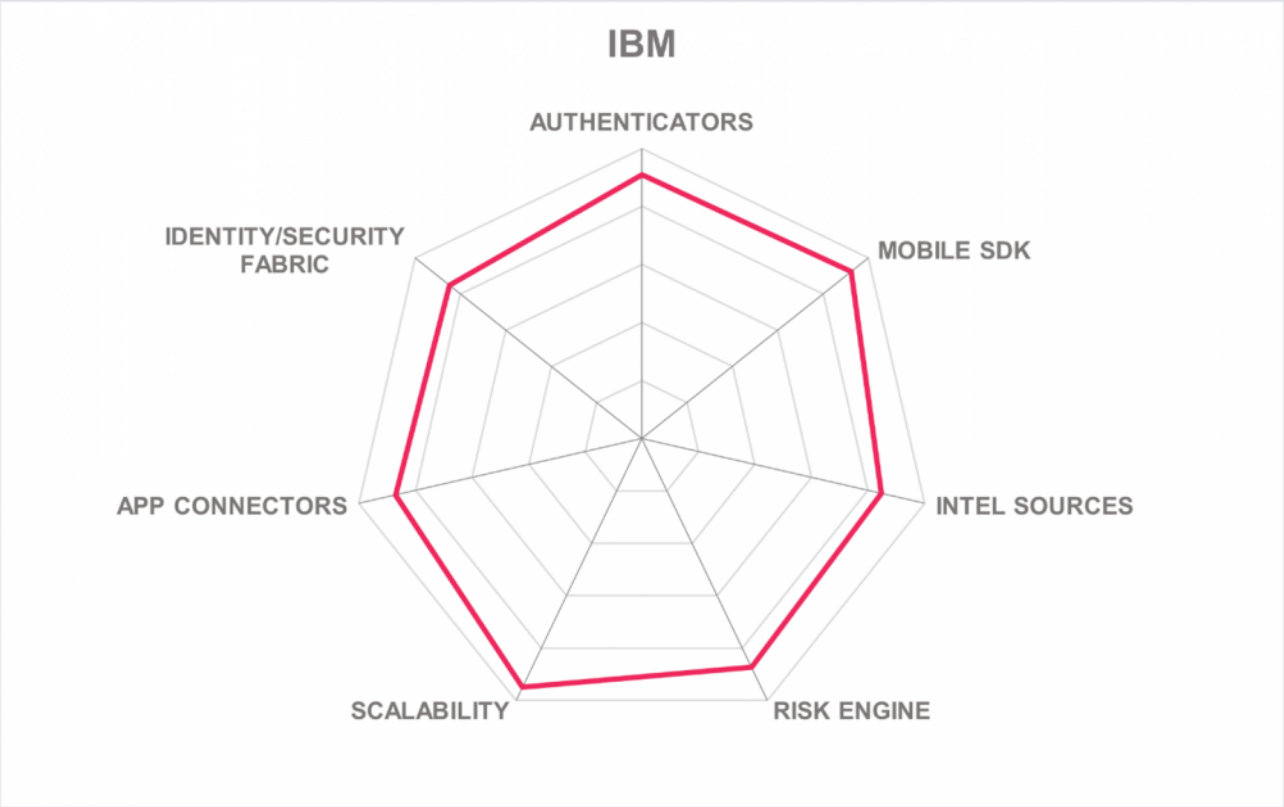
- Impressive selection of authentication mechanisms supported
- Highly scalable micro-services architecture
- Excellent and well-documented APIs for maximum extensibility
- High-quality device intel capabilities
- FIDO and OpenID (multiple profiles) certified

Challenges

- Multiple licensing models
- Webhooks are not supported
- IBM may want to consider pursuing governmental cloud and security certifications

Leader in




IBM
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.7 Micro Focus

Micro Focus is an IT software vendor with products covering many aspects of security and IAM, as well as application development, collaboration platforms, and IT operations. Micro Focus' global HQ is in the UK, and they have offices around the world. The Authentication product is Docker-based and can be installed on-premises on Windows or most Linux variants; and on AWS, Azure, or GCP IaaS. Micro Focus also hosts the solution as SaaS on AWS in EU and NA regions, and other MSPs utilize the product also. Licensing is by the number of active or registered users per time period or per login.

Micro Focus supports the following authenticator types: Authy, Derived PIV credential apps, Duo, Google, LastPass, Microsoft, SAASPASS, and SafeNet; mobile push notifications and Android/iOS biometrics; FIDO U2F/UAF/2.0; CAC/PIV, Duo, Feitian, Google Titan, Kensington, OATH (any), RSA SecurID, Smartcards, Symantec VIP, and Yubikey hard tokens. Proprietary non-OATH token types may require customization. Protocols supported include JWT, Kerberos, OAuth, OIDC, RADIUS, and SAML. Micro Focus provides a secure mobile SDK that collects a wide range of device intelligence signals including detailed info on device health. Users can be provisioned using LDAP, SCIM, and self-registration. All major account recovery types are available.

The Micro Focus risk engine can assess device intelligence, environmental attributes, user attributes/history and UBA, and additional cyber threat intelligence via their Interset solution. Authentication policies are set in the administrative interface, which utilizes both drop-down policy element lists and some guided natural language input.

Micro Focus provides multiple API access methods including REST, RPC, SOAP, Webhooks, and WebAuthn, in JSON and XML formats. API versioning is supported, and security can be augmented with the Micro Focus Secure API Manager product. Micro Focus offers many OOTB connectors to a wide range of apps including accounting, office automation, collaboration, IT operations and service management, HR, and CRM. Micro Focus Authentication interoperates with other IAM, IDaaS, IGA, and PAM solutions via standard protocols. It can communicate with SIEMs via CEF and syslog. ABAC, RBAC, and delegated admin models are supported.

Micro Focus' Access Management suite is Common Criteria EAL 3+ certified. Crypto components are FIPS 140-2 compliant. FIDO U2F and OpenID certifications have been achieved. Micro Focus is somewhat late to offer the solution as SaaS but they expect high performance in the cloud. Micro Focus has good standards support and organizations looking for modular authentication services may want to consider them, especially those which have requirements for EAL 3+ certifications.

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

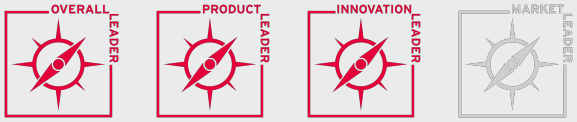
Strengths

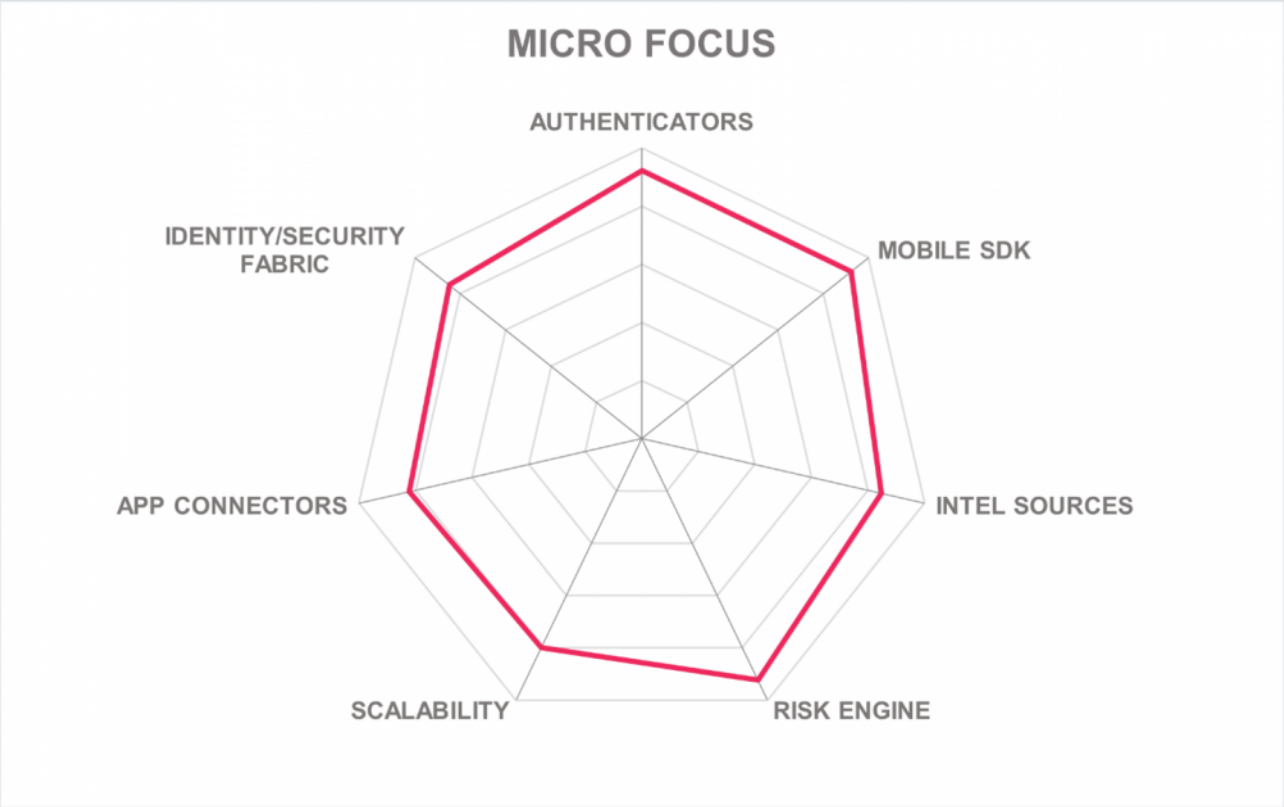
- FIDO certified
- Large selection of connectors to business apps
- SDK enables collection of broad set of device intelligence signals
- Integration with Micro Focus security tools such as ArcSight and Interset

Challenges

- Admin UI could be improved
- Entered SaaS authentication market late

Leader in




MICRO FOCUS
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.8 Microsoft

Redmond, WA headquartered Microsoft is well-known for operating systems, office automation, and cloud infrastructure. Azure Active Directory (Azure AD) is the product that provides enterprise authentication capabilities from their Azure cloud. Azure AD is delivered via dozens of data centers operating globally. Active Directory itself can be installed on-premises on Windows servers as well. Moreover, Active Directory can be installed on any IaaS that can run Windows servers. Licensing for Azure AD is according to numbers of monthly active users, or by numbers of registered per monthly/quarterly/annually.

Microsoft Azure AD accepts Aegis, Authy, DeepNet, Derived PIV credentials, Duo, Entrust, Google, LastPass, their own Microsoft app, Okta, OneSpan, SAASPASS, and SafeNet apps; Android/iOS biometrics and mobile push apps; FIDO U2F/2.0 support is integrated into Windows Hello and the Edge browser; hardware authenticators such as CAC/PIV cards, Duo, Feitian, OATH (any), RSA SecurID, Smartcards, Symantec VIP, and Yubikey tokens are supported as well. AAD also works with JWT, Kerberos, OAuth, OIDC, RADIUS, SAML, and WS-Fed. Microsoft Authentication Library (MSAL) offers multi-language support for developers to create desktop, mobile, and service applications; however, this does not allow for collecting device intel signals. Users can be provisioned by LDAP, SCIM, cloud-specific APIs, and self-registration. All account recovery mechanisms are present.

The Azure AD risk engine can consider device intel harvested from Microsoft Intune. Azure AD can access user attributes, history, and behavioral analysis. Behavioral biometrics are not supported. Microsoft has excellent built-in compromised credential intelligence and can support integrations with identity vetting services. Microsoft Graph ‘riskyUsers’ API is a premium feature for which additional charges are incurred. Risk engine output is somewhat coarse-grained and does not interoperate with 3rd-party authorization services. The administrative interface utilizes both drop-down lists and guided natural language input for policy creation.

Microsoft Azure AD has comprehensive support for API access including REST, RPC, SOAP, OData, Webhooks, and WebAuthn methods and CSV, JSON, and XML formats. APIs are versioned. Connectors for analytics, business management, collaboration, CRM, ERP, ITSM, and many other applications can be found in the marketplace. Azure AD has many IGA and lifecycle management functions, and it interoperates with Imprivata, Omada, Saviynt, and others. PAM functions are available and Azure AD works with other PAM vendors. Azure AD can send event data to SIEMs via CEF and syslog, and there are a number of SOAR integrations possible. The admin console supports MFA and RBAC.

Azure AD is built on Microsoft Azure, which has obtained an impressive list of security certifications, such as CSA Star, ISO 27001/27018, SSAE 18 SOC 2 Type 1/2, and many country-specific security certifications. FIDO 2 and OpenID profiles are certified as well. Given the size and distribution of data centers, Azure AD can scale to meet the requirements of any organization. The functional gaps outlined above are planned to be addressed in future updates. Microsoft Azure AD should be on the shortlist for any organization looking for robust enterprise authentication services.

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

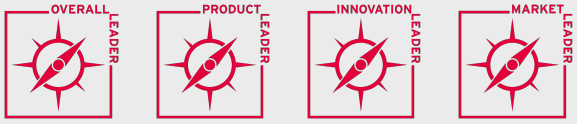
Strengths

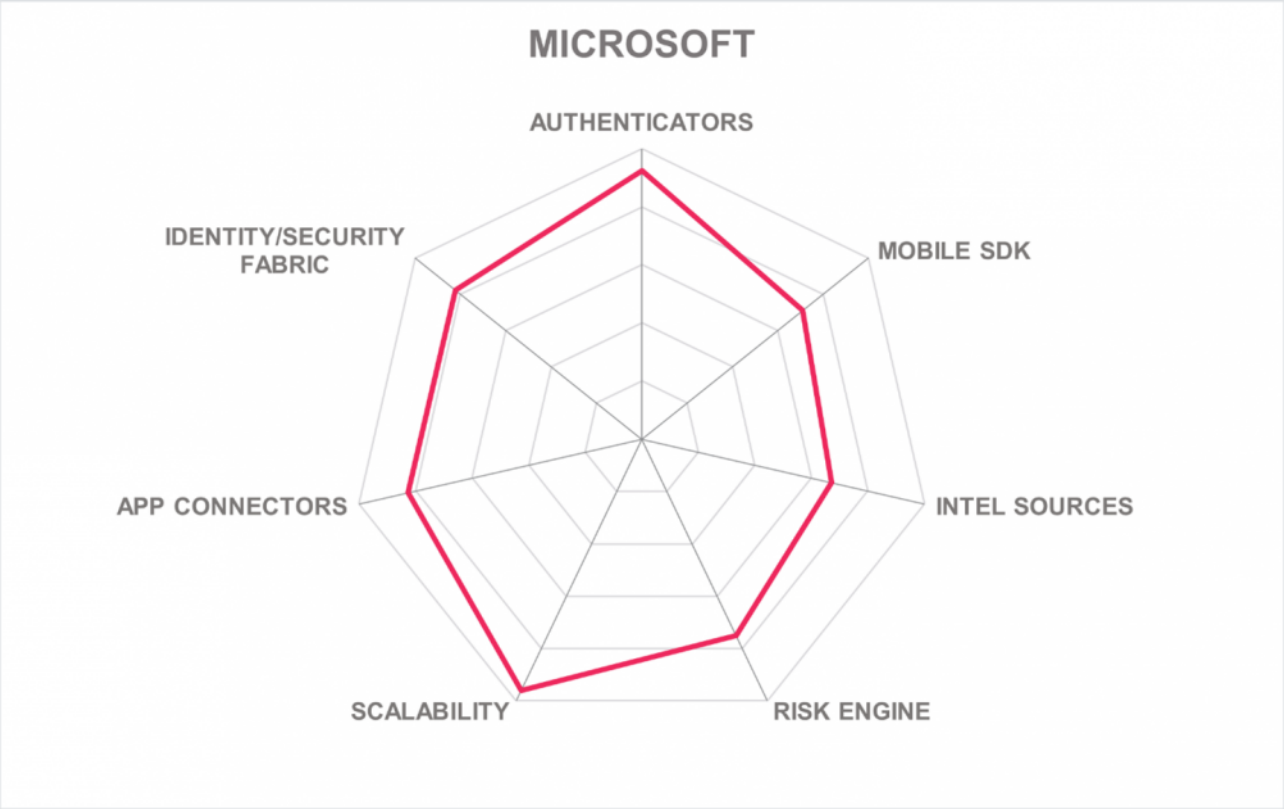
- Extreme scalability
- Flexible deployment and authenticator options
- Global Platform TEE support on Android
- Integration with Intune for device management
- Many SaaS connectors

Challenges

- Behavioral biometrics not included in the platform
- Advanced identity protection features are available in premium licenses at an extra cost
- Coarse-grained risk engine output

Leader in




MICROSOFT
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.9 MobileIron

MobileIron was founded in the Bay Area in 2007. Zero Sign-On is their authentication product, and they also have UEM and Mobile Threat Defense solutions. Ivanti announced its intent to acquire MobileIron in September 2020. MobileIron runs Zero Sign-On as SaaS from AWS and their own facilities, distributed globally. Licensing is determined by numbers of registered users per time period.

In addition to their own mobile app, MobileIron supports Derived PIV credentials and Google Authenticator, and Android and iOS biometrics. Their app is compliant with FIDO UAF/2.0. Kerberos and SAML are supported. MobileIron provides an SDK integrated with their UEM product such that device intel parameters can be collected. Users can be provisioned with LDAP but not SCIM, but self-registration is possible. The account recovery mechanisms available are email OTP/link and self-initiated recovery including encryption key codes.

The risk engine can consume signals from the SDK plus some environmental attributes; however, geo-location and geo-velocity are not computed. User attributes can be considered, but history and UBA cannot. Behavioral biometrics are not part of the feature set. There are no connectors to identity vetting, or compromised credential or threat intelligence sources. The policy interface uses drop-down lists and guided natural language input, but it does not allow policy import, weighting of risk factors, or output of risk scores to other systems. The risk engine itself is not addressable via API.

The API methods supported are REST and SOAP, and the formats accepted are JSON and XML. APIs are not versioned for compatibility. MobileIron provides connectors for Box, Concur, Dropbox, Google Workspace, Microsoft 365, SAP, Salesforce, ServiceNow, Tableau, and Workplace apps; IDaaS connectors for Microsoft AAD, Okta, OneLogin, and Ping Identity. It can interoperate with IGA but not PAM solutions. MobileIron can output event data to SIEMs over CEF and syslog. RBAC and delegated admin models are supported.

MobileIron has attested/certified to CSA Star Level 1, ISO 27001, and US FedRAMP. Crypto components comply with FIPS 140-2. MobileIron partners with Zimperium for incident response. MobileIron, as the name implies, focuses on mobile security and identity. Organizations that are looking for mobile-based authentication solutions and that do not have lots of other app or hardware token authentication solutions to support may want to consider MobileIron.

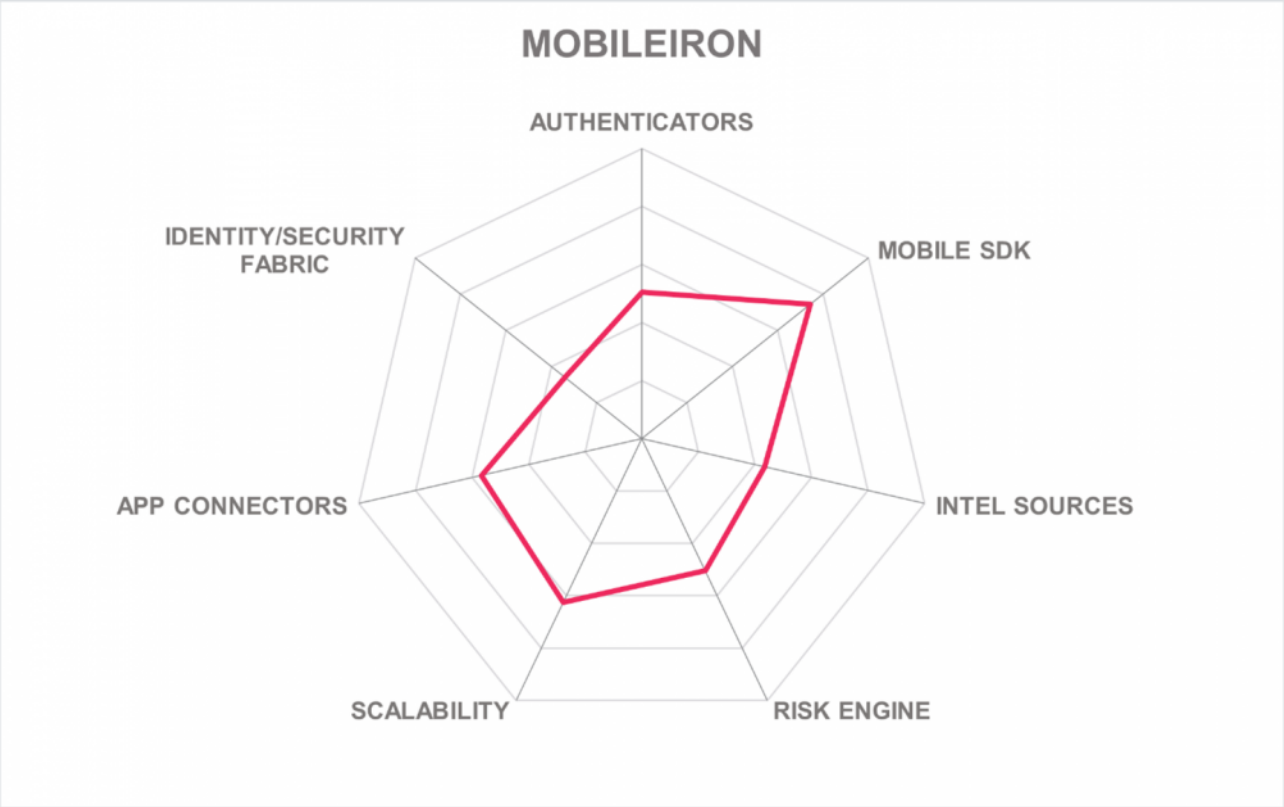
Security	●●●●○
Functionality	●●●○○
Interoperability	●●○○○
Usability	●●●●○
Deployment	●●●○○

Strengths

- Focus on mobile authentication, including secure mobile SDK
- Support for Derived PIV credentials
- Integration with UEM product
- Straightforward licensing scheme

Challenges

- Authenticator and account recovery selection tightly aligned to mobile
- JWT, OAuth, and OIDC not supported
- Risk engine does not evaluate geo-location/velocity or UBA
- Behavioral biometrics not included
- Coarse-grained risk engine does not allow policy import or risk score export


MOBILEIRON
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.10 Okta

Okta, founded in 2009 in San Francisco, is a leading IDaaS provider. Their Identity Cloud solution is SaaS-delivered, operating out of multiple globally distributed AWS data centers, as well as FedRAMP certified data centers. Lightweight connectors for directory synchronization can be run on-prem or in any IaaS. Licensing is on a per-user per-month basis for Okta Workforce Identity products.

Okta accepts Authy, DeepNet, Derived PIV Credentials, Duo, Google, LastPass, Microsoft, their own Okta Verify app, OneSpan Mobile ES, and SafeNet app authentication; Android and iOS biometrics; FIDO U2F/2.0; CAC/PIV cards, Duo, Feitian, Google Titan, Kensington, any OATH compatible, OneSpan DigiPass, RSA SecurID, Smart Cards, Symantec VIP, Thetis, Yubikey hardware authenticators and custom SAML/OIDC connectors. Okta has a mobile SDK that can collect some device intel parameters and that securely stores credentials. More advanced device intel-gathering features are planned for future releases. Okta interoperates with Jamf, Intune MDM, MobileIron, VMware Workspace ONE, and other device management solutions to check for device management status. Account takeover protection is facilitated by connectors to bot management, ID proofing, and fraud risk intel feeds. Okta Risk-based Authentication and Okta ThreatInsight check for login anomalies and large-scale password spray/brute force attacks. Protocol support includes JWT, Kerberos, OAuth, OIDC, RADIUS, SAML, and WS-Fed. Users can self-register or be bulk provisioned in via AD, LDAP, and SCIM. All normal account recovery methods are present.

Okta's Risk-based Authentication can evaluate some device intel, user attributes and history, environment, geo-location, geo-velocity, threat-feed , and behavioral analysis from multiple sources, but behavioral biometrics are not supported yet. Risk-based authentication policies can be built using their factor sequencing approach, which allows customers to prioritize certain risk factors in the chain, and which then can yield different outcomes based on risk scoring. The admin interface facilitates the creation and execution of complex workflows which can include automation of tasks with connected directory services and SaaS apps.

Okta supports REST API with versioning, Webhook, and WebAuthn interfaces and JSON format. **OOTB connectors are available** for more than 6,500 applications. Okta interoperates with multiple IAM solutions, including IGA and BeyondTrust, Centrify, CyberArk, and Thycotic for PAM. Okta also provides PAM-like capabilities via the Advanced Server Access Product. MFA and RBAC for customer admins are configurable, however, ABAC and delegated admin models are in the near-term roadmap. Okta can send event information to SIEMs using syslog.

Okta has attested or obtained a large number of security and performance certifications: CSA Star Level 2, ISO 27001 and 27018, SSAE SOC 2 Type 2, and US FedRAMP. Crypto components adhere to FIPS 140-2. Okta was an early cloud-native IDaaS and enterprise authentication solution provider, and that maturity in the market is reflected by high scalability and a plethora of connectors that make deploying their services easy. Any organization that is looking for enterprise authentication solutions, particularly those with complex applications or a large number of applications to support should consider Okta Identity Cloud.

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

okta

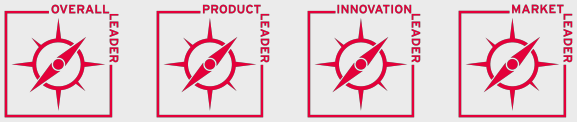
Strengths

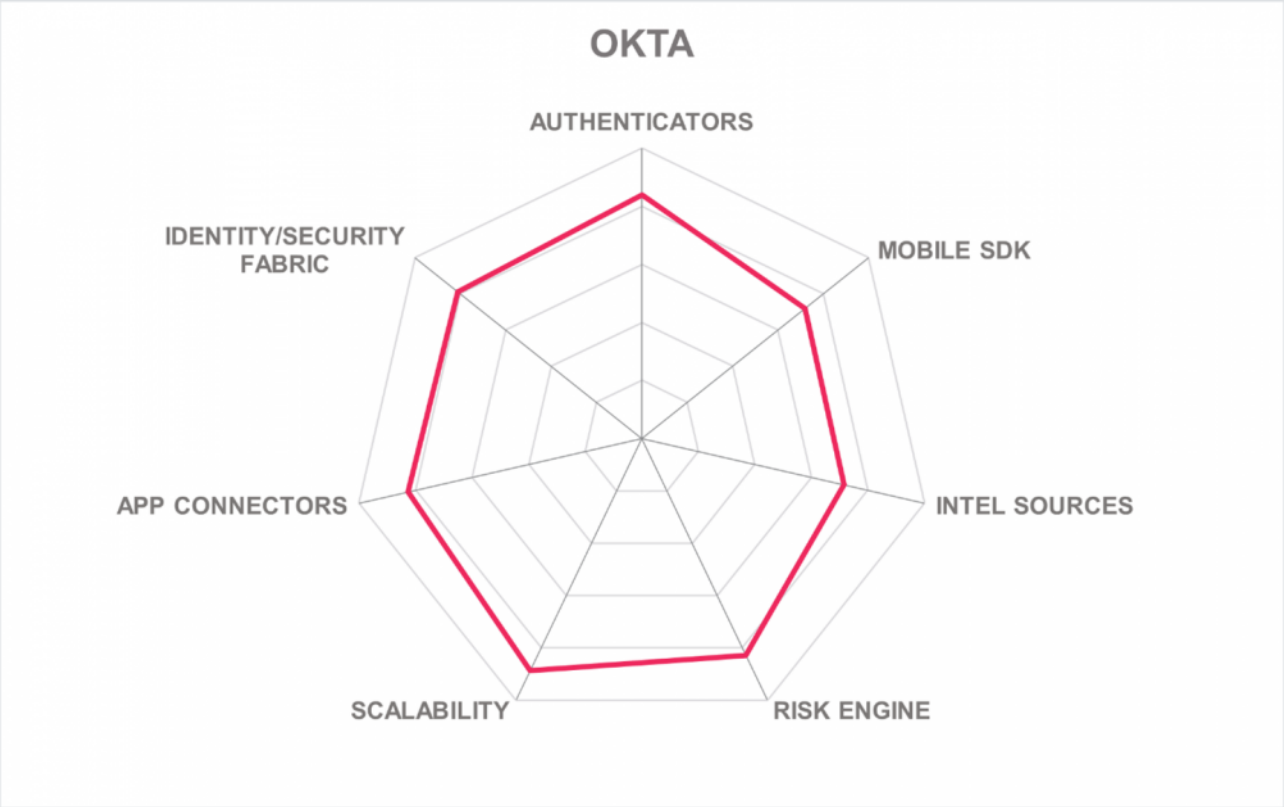
- Highly scalable cloud-delivered services
- Large range of MFA types supported
- Native and 3rd-party identity context integrations (IP reputation, device context) for password spray and brute force detection, etc.
- Multiple security certifications
- Connectors for thousands of apps

Challenges

- Limited device intel but enhancements are on the roadmap
- Behavioral biometrics not currently supported
- ABAC and delegated access control models not supported

Leader in




OKTA
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.11 Ping Identity

Ping Identity has been a trailblazer in identity federation and access management since it was established in 2002. Ping Identity has grown substantially and went public on NYSE late in 2019. Ping Intelligent Identity is available for both on-premises and cloud deployment. In addition, Ping has a full suite of IAM and API security products for CIAM and B2B2C use cases. Their solutions can run on-premises; in any IaaS environment, with support for Docker and Kubernetes; and they run it as a fully multi-tenant SaaS using multiple regions of AWS. The solution is licensed by the number of active users per time period.

Ping Intelligent Identity Platform users can authenticate with Aegis, Authy, DeepNet, Derived PIV credentials, Duo, Google, LastPass, Microsoft, OneSpan, SAASPASS, SafeNet Authenticators, email/phone/SMS OTP; Android/iOS native biometrics; FIDO U2F/2.0; CAC/PIV cards, Duo, Feitian, Google Titan, Kensington, any OATH compatible, OneSpan DigiPass, RSA SecurID, Smart Cards, Symantec VIP, Thetis, and Yubikey hardware authenticators. JWT, OAuth, OIDC, RADIUS, and SAML are supported. Ping provides an SDK to embed MFA features into any mobile app, collecting a large set of device intel attributes, and utilizing high-security features such as SE and TEE for Android. Ping has integrations with ID Data Web, Interset, iovation, and ThreatMetrix for additional intelligence. All relevant forms of account recovery and linking are supported. Bulk provisioning and bi-directional synchronization are possible via LDAP and SCIM, and self-registration and data management are possible for consumers. This solution can serve as an identity bridge to IDaaS, SaaS, and on-premises AD, IAM, and SSO implementations.

Ping's Intelligent Identity Platform has a much-enhanced risk engine that processes the full gamut of device intelligence, user attribute/history/behavioral analysis (through the new PingOne Risk Management service), and other threat intelligence signals. Partnership with Secured Touch brings behavioral biometrics capabilities to the solution. The admin interface facilitates policy authoring using drop-down lists, guided natural language input, plus flow chart representations. Risk engine output, though accessible via secure APIs, is still somewhat coarse-grained.

Ping Intelligent Identity Platform features support for REST, SOAP, WebAuthn, Webhooks, and Websockets using CSV, JSON, or XML formats. PingIntelligence for APIs is a separately sold product for monitoring and protecting APIs, and PingDataGovernance (also separately licensed) can be used for fine-grained, dynamic authorization to APIs. Ping Identity also provides customers with OOTB connectors for more than 1,500 applications in their marketplace. The Ping Intelligent Identity Platform can interoperate with Active Directory, IBM, Oracle Access Manager, RSA SecurID, SailPoint, and SiteMinder IAM stacks; CyberArk, OneIdentity, and Saviynt PAM systems. ABAC/RBAC and delegated access control models are supported.

Ping Identity self-certified with CSA and certifies/attests with ISO 27001 and SSAE SOC 2 Type 2. Their on-premises and SaaS solutions are highly scalable and offer maximum flexibility to customers in terms of support for standards as well as innovation for cutting edge use cases. Any type of organization that is in need of enterprise authentication services should consider the Ping Intelligent Identity Platform as a potential solution.

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

Ping Identity

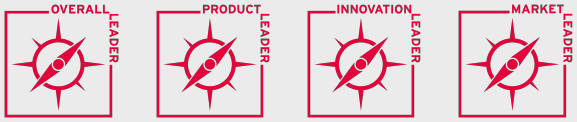
Strengths

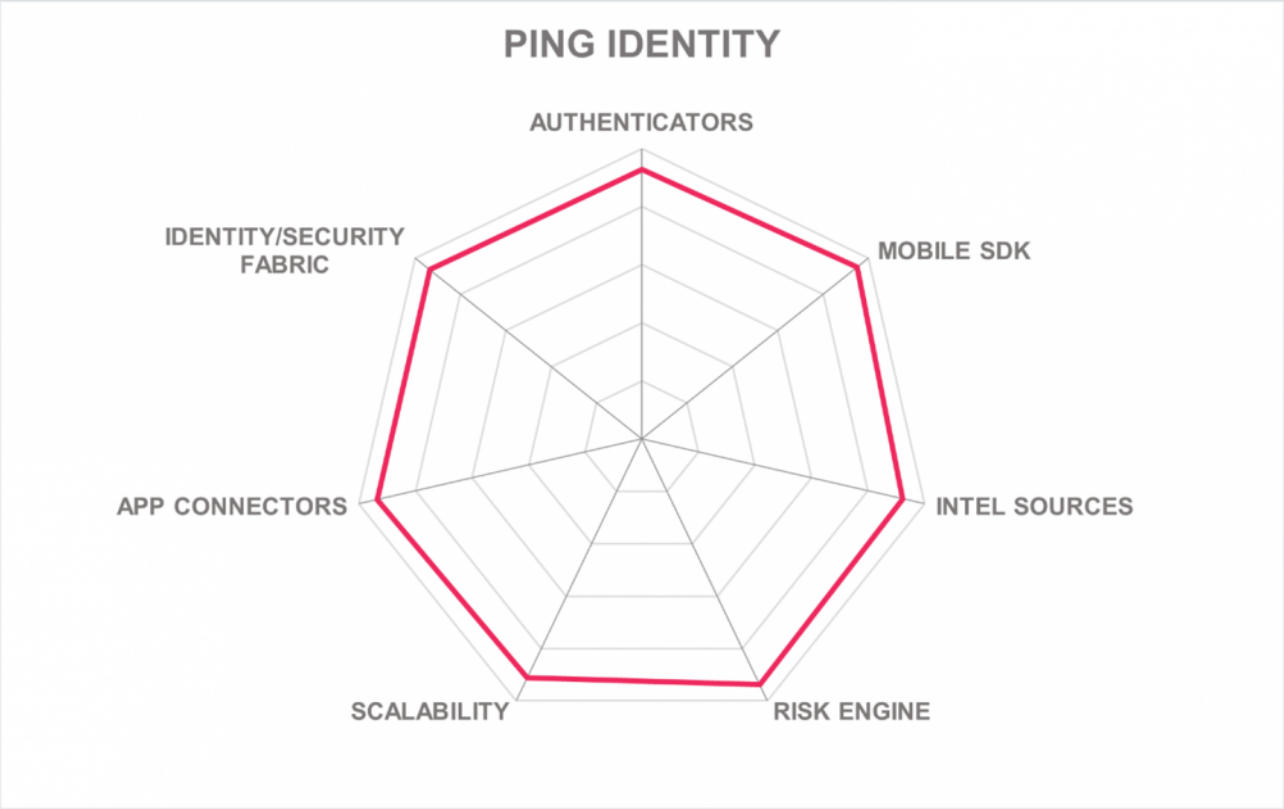
- Impressive selection of authentication mechanisms
- Secure mobile SDK with excellent device intel features
- Built-in and extensible threat intelligence
- Support for nearly all relevant standards
- Secure API access for all functions

Challenges

- Some useful functions are packaged and sold separately, such as PingOne Risk Management for UBA functionality
- Low/medium/high risk engine output may not be sufficient for the most complex use cases
- Behavioral biometrics should be built into mobile SDK

Leader in




PING IDENTITY
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.12 Pirean

Pirean was founded in 2002 with offices in London and Sydney. In 2018, Pirean was acquired by Exostar, an IAM and collaboration solutions provider for highly regulated industries such as Aerospace & Defense and Life Sciences. In July 2020, Exostar was acquired by Thoma Bravo. Pirean provides an IDaaS platform called Access: One which can be used for B2B/B2C/B2B2C/B2E use cases. The product can be deployed in containers either on-premises or in IaaS on AWS, Azure, GCP, or IBM Cloud; and Pirean hosts it as a managed service in AWS and IBM in multiple regions. Pirean can also host consumer profiles in the cloud for their customers. It is licensed according to monthly active users.

Pirean supports Authy, Duo, Google, Microsoft Authenticators; native biometrics for Android and iOS; FIDO U2F/UAF/2.0; and for hardware authenticators, any OATH compliant model and Duo, Feitian, Google Titan, Kensington, OneSpan DigiPass, RSA SecurID, and Yubikeys. Pirean also has a secure mobile SDK that customers can use to build into their own apps, and it can harvest device intelligence from consumer devices. Access: One can be configured to query external services such as Experian Hunter for credential and fraud intelligence. It supports JWT, OAuth, OIDC, and SAML for federated authentication and authorization (including API access); and self-registration, LDAP, and SCIM for provisioning. All standard account recovery mechanisms are present.

The risk engine is granular and can evaluate a large set of attributes against policies, including device intel and user attributes/behavior/history. Behavioral biometrics are not supported at this time, however. Authentication and authorization policies of variable depth can be composed in the admin interface, which is limited to the drop-down list approach. Risk scores are not output to 3rd-party applications.

Access: One supports REST APIs, SOAP, WebAuthn, Webhooks, and Websockets; and CSV, JSON, and XML data exchange formats. Pirean can interoperate with Active Directory and IBM IAM solutions; IBM and SailPoint IGA systems; and BeyondTrust, CyberArk, and Thycotic PAM systems. Access: One can send data to SIEMs over syslog or through OOTB connectors. ABAC/RBAC and delegated access models are supported.

Pirean’s strong feature set is the result of providing solutions for heavily regulated industries that require strict security. Pirean has attestations/certifications for AU IRAP, UK Cyber Essentials Plus and G-Cloud. Access: One also is aligned with ISO 27001 and attests to SSAE 18 SOC 2 Type 1 and 2. Given their growth and backing, we expect Pirean to increase its market share. Organizations with the need for strong security for their workforces and partners should consider Pirean Access: One.

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

Access: One

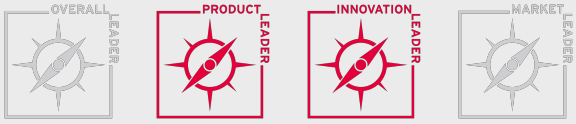
Strengths

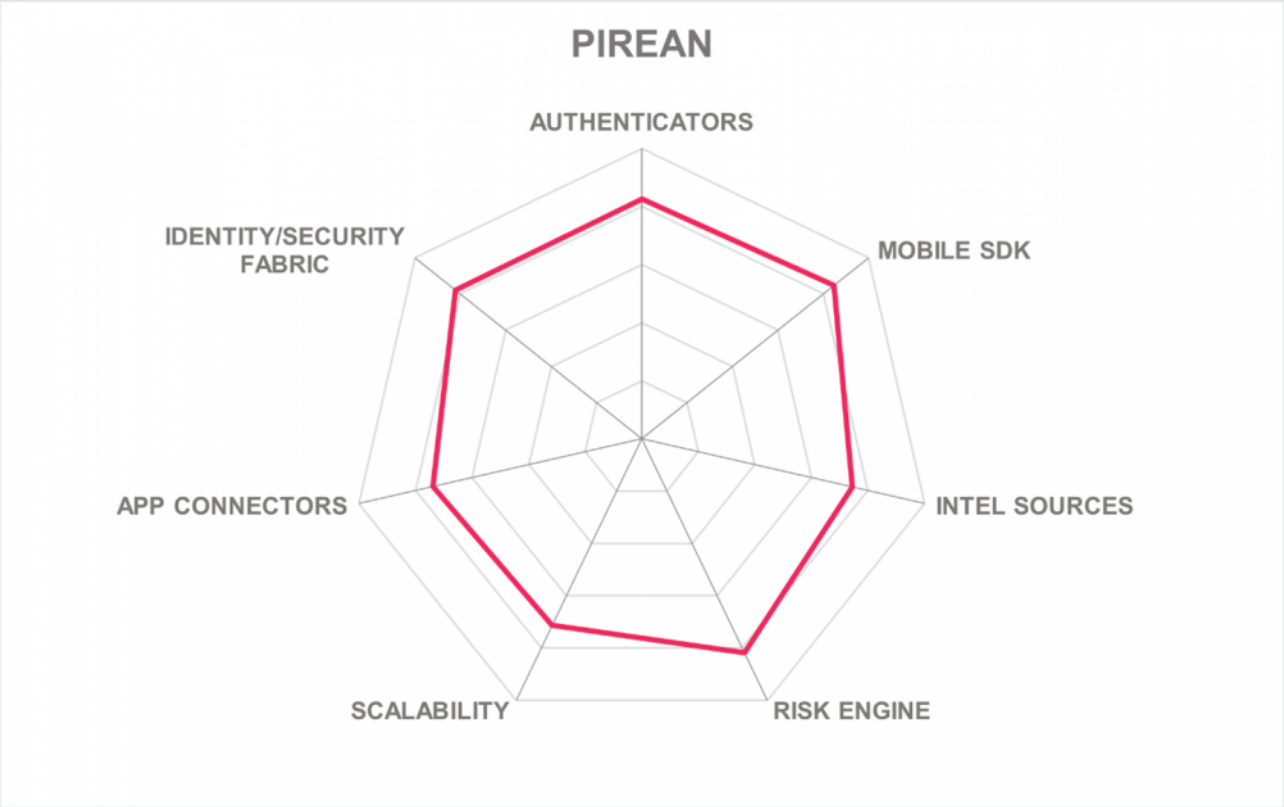
- Good selection of authenticators
- Built-in compromised credential intelligence
- Some high-security certifications
- Secure mobile SDK

Challenges

- Small but growing vendor, quite well geographically distributed
- Partner ecosystem needs to expand
- FIDO and OpenID certifications in work
- Risk engine does not output to other applications

Leader in




PIREAN
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.13 RSA Security

RSA was founded in 1982 and is headquartered in Bedford, MA. RSA Security was divested from Dell Technologies and acquired by a consortium of private investors led by Symphony Technology Group in September 2020. RSA will operate independently. RSA has products spanning Risk Management, Cybersecurity, Identity Management, and Fraud Prevention. RSA SecurID Access is the product considered here for Enterprise Authentication services. RSA SecurID Access can be deployed on-premises; in Amazon or Azure IaaS; and RSA hosts it as SaaS in Azure in multiple globally distributed data centers as well. The RSA Adaptive Authentication product is sold separately and primarily leverages cloud-hosted services. Licensing costs depend on the number of registered users per time period.

In addition to their own well-known authenticators, RSA SecurID Access accepts mobile push notifications; Android and iOS biometrics; BLE/NFC/USB FIDO U2F & 2.0 compliant devices, and CAC/PIV, Duo, Feitian, Google Titan, Kensington, OneSpan DigiPass, Smart Cards, Symantec VIP, Thetis, and Yubikey hardware tokens. RSA Adaptive Authentication offers a *mobile SDK that collects mobile device identifiers and indicators for the presence of emulators or rooted devices. In addition, the mobile SDK offers biometric face and fingerprint authentication methods.* JWT, OAuth, OIDC, RADIUS, and SAML are understood. LDAP and Just-In-Time SAML are used for account provisioning. All standard account recovery mechanisms are present.

The risk engine can pull a few additional device attribute types beyond those listed for the SDK, and user attribute and history lookups are supported. RSA SecurID Access can interoperate with other SIEMs over its API, but these feeds require customization at the API layer. Behavioral biometrics are not supported. Risk engine output is very granular. The risk engine is enhanced with ML detection models. The admin interface is drop-down style for policy building; however, customers can build complex rules with per-factor weightings.

REST API (with versioning), RPC, SOAP, and WebAuthn methods are available for communication, and JSON format is supported. Integrations for SaaS apps including Microsoft O365, Oracle eBusiness and PeopleSoft, ServiceNow, Slack, Tableau, and WorkDay are available. RSA SecurID Access has connectors for Azure AD, IBM, Ping Identity, Okta, OneLogin, and Oracle IAMs; and BeyondTrust, CyberArk, ManageEngine, One Identity, Thycotic, and Wallix PAMs. SecurID can act as a secure token exchange service but does not support Single Sign-Off.

RSA attests/certifies to CSA Star Level 1 and SSAE SOC 2 Type2. RSA is moving toward US FedRAMP certification and the SaaS will run in Microsoft Azure GovCloud. Relevant components of RSA SecurID Access are FIPS 140-2, FIPS 197, and NIST 800-57 compliant. RSA solutions tend to be scalable and addressed to high-security customer requirements. RSA SecurID Access and RSA Adaptive Authentication provide good hardware-based authentication methods and have a good risk engine, however, the product line is in need of some feature upgrades and re-packaging.

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

RSA

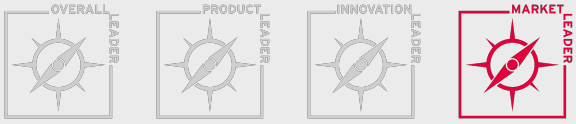
Strengths

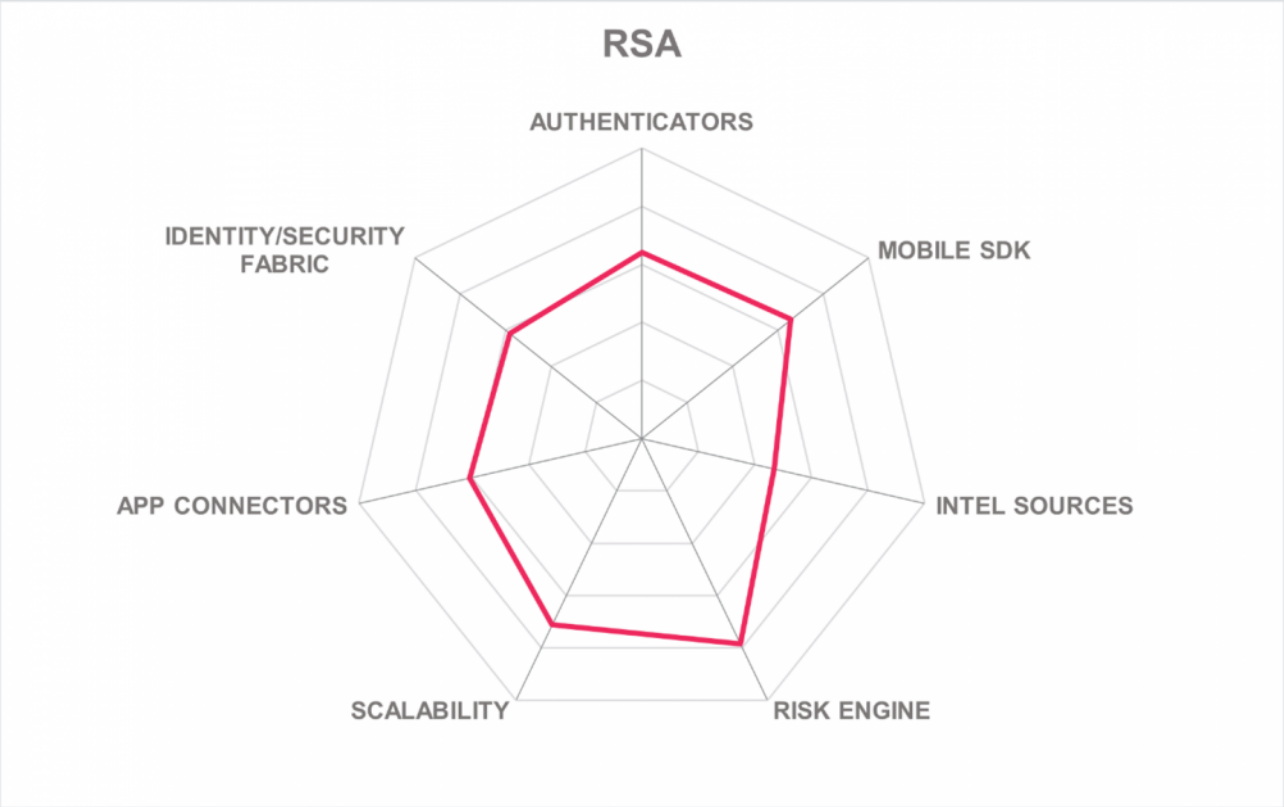
- FIDO U2F & 2.0 certified; includes support for BLE/NFC/USB devices
- Large selection of PAM integrations
- Robust, ML-enhanced risk engine
- Adaptive Authentication product is integrated with RSA eFraudNetwork

Challenges

- Limited 3rd-party app-based authentication
- Optimal functionality requires licensing both SecurID and Adaptive Authentication products
- External SIEM connections require custom coding

Leader in




RSA
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.14 SAASPASS

Privately held SAASPASS was formed in 2013 in San Francisco. Their product portfolio is centered on providing modern, passwordless authentication services. As their name implies, they host their cloud-based solution for customers in their own facilities, AWS, and GCP. The data centers that provide the SaaS are globally distributed. Customers can also install it in any IaaS and it can run on-premises on Windows and all major flavors of Linux as VMs. Licensing is by the number of monthly/quarterly/annual active users.

In addition to their own app, SAASPASS accepts Aegis, Authy, DeepNet, Duo, Google, LastPass, Microsoft authenticator apps. SAASPAAS also accepts mobile push notifications, native biometrics on Android and iOS, FIDO U2F/2.0, and the following hardware tokens: Duo, Feitian, Google Titan, Kensington, any OATH type, OneSpan DigiPass, RSA SecurID, Smart Cards, Symantec VIP, Thetis, and Yubikey.

SAASPASS offers a mobile SDK that can extract major device intel attributes. Behavioral biometrics are supported. SAASPASS has full protocol support including Kerberos, JWT, NTLM, OAuth, OIDC, RADIUS, SAML, and TACACS. LDAP and SCIM can be used for in-provisioning, as well as from other IDaaS and user self-registration. All pertinent account recovery methods are covered.

SAASPASS' risk engine considers a wide variety of data points from device intel and user attributes/history/behavioral analysis. There are no connections to identity vetting services. The risk engine allows policy import, and the admin GUI allows for drop-down, guided natural language input, and flow-chart style policy authoring. Risk factors can be weighted by customers, and the outcomes map to five risk levels, which can trigger different actions. The risk engine is not directly accessible over APIs and does not output to external authorization systems.

API support includes REST, SOAP, and Websockets, and CSV/JSON/XML formats. They offer connectors for many SaaS apps such as Adobe, AWS, Azure, Box, Checkpoint, Citrix, DocuSign, DropBox, GCP, Google Suite, Juniper, Microsoft O365, Palo Alto, Salesforce, Slack, Smartsheet, Zendesk, and Zoho. SAASPASS interoperates with any SAML-based IAM or IGA system including Okta, Ping Identity, Sailpoint, Saviynt, etc.; and BeyondTrust, Centrify, CyberArk, ManageEngine, One Identity, and Thycotic for PAM. SAASPASS can send event data to SIEMs over CEF and syslog. There is support for RBAC/ABAC and delegated admin models.

SAASPASS has attested to and/or achieved a number of important security certifications: CSA Star Level 4, ISO 27001/27018, and SSAE SOC 2 Type 2; German BSI C5, UK Cyber Essentials Plus, UK G-Cloud, US CJIS, and US FISMA; and relevant components comply with FIPS 140-2 and 197, NIST 800-57 and 800-171 (DFARS). SAASPASS offers good scalability and has globally distributed operations. Any organization that is looking for modular authentication services or needs to add-on passwordless capabilities to an existing IAM infrastructure may want to take a look at SAASPASS capabilities in this area.

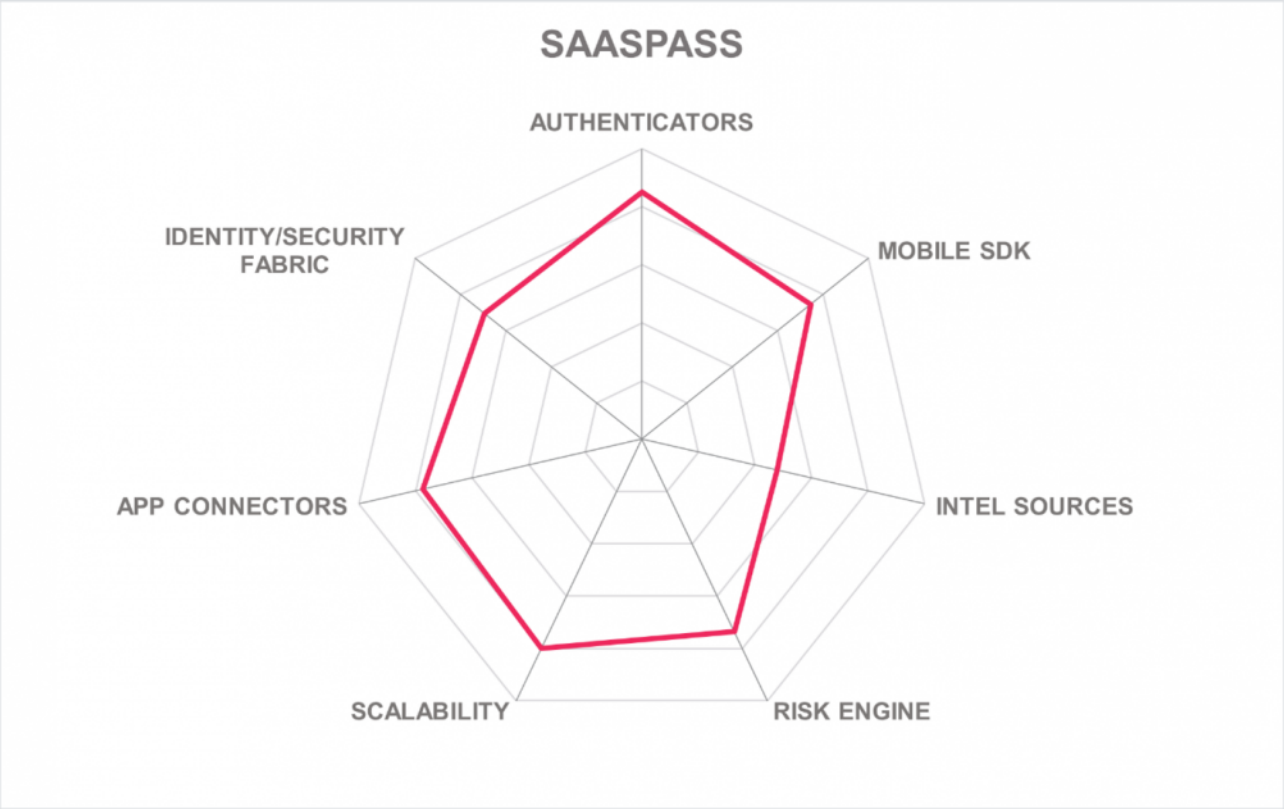
Security	● ● ● ● ●
Functionality	● ● ● ● ○
Interoperability	● ● ● ● ○
Usability	● ● ● ● ○
Deployment	● ● ● ● ○

Strengths

- Flexible deployment models
- Good selection of authenticators and SaaS app connectors
- Focused on passwordless authentication
- SDK gathers broad device intel
- Risk engine covers most major factors

Challenges

- Risk engine is not addressable via API and does not output to 3rd-party solutions
- No connectors to identity vetting services
- Smaller company but a growing global footprint


SAASPASS
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.15 Symantec

Symantec, now a division of Broadcom, has a long history in cybersecurity and IAM. Symantec offers their VIP authentication, Advanced Authentication, and SiteMinder as components for creating enterprise authentication services; and has products comprehensively covering endpoint, network, cloud, data, and web security. Advanced Authentication and SiteMinder are available for on-premises deployment on CentOS, RedHat, and Windows, any IaaS, and they host as SaaS from GCP in US data centers. Symantec VIP is SaaS. The licensing models are based on the number of quarterly/annually active users and/or per-login/session.

Symantec accepts Aegis, Authy, Duo, Google, LastPass, Microsoft, Okta, OneSpan, SafeNet, and their own authenticator apps. The combined solutions also accept mobile push notifications, Android & iOS native biometrics and FIDO U2F authenticators. Beyond their eponymous hardware devices, Symantec accepts Duo, Feitian, OneSpan DigiPass, RSA SecurID, SmartCards, and Yubikeys. Symantec does offer a mobile SDK for customer app development which can gather a wide range of device attributes. Kerberos, JWT, OIDC, RADIUS, and SAML protocols are supported. LDAP and SCIM can be used for bulk provisioning, and user self-registration is allowed. A standard variety of account recovery methods are possible.

Symantec VIP's risk engine can evaluate a broad spectrum of device and environmental attributes, including device ID, history, health, etc. User history and behavioral analysis are supported. Third-party behavioral biometrics can be integrated with customization. Callouts to identity vetting services are possible if configured over APIs, and customers can avail themselves of Symantec's Global Intelligence Network for threat intel. Moreover, customers can configure and consume other threat intelligence feeds if desired.

Policy import in JSON format is permitted, but the admin interface uses dated drop-down lists for policy construction. Large customers use APIs to control the system externally, and APIs are preferred by DevOps driven administration processes. The risk engine is addressable over APIs, but the risk engine output is limited to specifying one action per policy evaluation event.

API access includes REST, RPC, and SOAP; and CSV, JSON, and XML formats are understood. Symantec provides OOTB connectors for multiple SaaS apps such as Atlassian, Box, Brainshark, Concur, DocuSign, Dropbox, Freshdesk, Jive, Marketo, Qualtrics, Salesforce, ServiceNow, WebEx, Zoho, and Zoom. The solution set can interoperate with IBM, Microsoft ADFS and Azure AD, PingFederate, and Okta IAM; and works with CyberArk and Symantec PAMs. RBAC and delegated admin models can be used. Symantec can send event data to SIEMs over CEF and syslog.

Symantec has SSAE SOC 2 Type 2 certification for cloud service, FIDO U2F 1.0/1.1, and FIPS 140-2 for crypto components. Reported performance statistics are above average. Symantec has a good reputation for product security. Organizations with other Broadcom and Symantec products may want to consider the Symantec suite of Advanced Authentication, SiteMinder, and VIP for enterprise authentication services.

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

Symantec

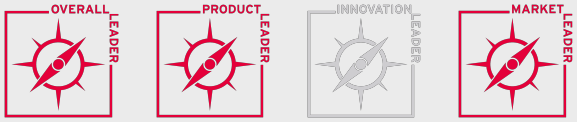
Strengths

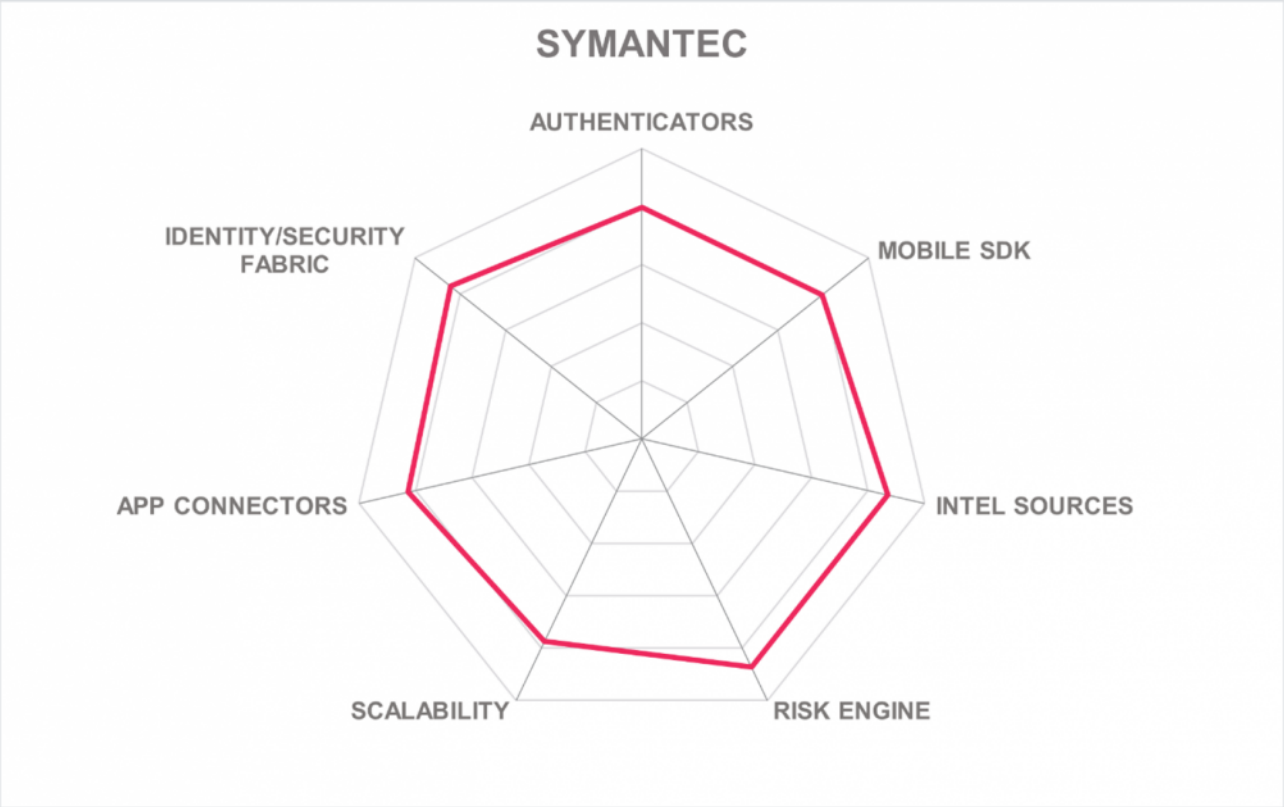
- Mobile SDK collects full range of data types
- Threat intel from Symantec Global Intelligence Network, other sources can be plumbed in as well
- Good mix of authenticators available
- Flexible deployment options
- Externally authored policies can be imported in JSON format

Challenges

- Policy authoring interface could be modernized to use natural language input or flow chart methods
- Requires multiple products for full-service deployment
- FIDO 2/WebAuthn not supported, although it is on the roadmap for VIP Authentication Hub
- Additional OOTB connectors for SaaS apps would be useful

Leader in




SYMANTEC
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.16 Thales

Thales is a global leader in the aerospace, defense, and transport industries. Thales also has cybersecurity and IAM products, including the heritage Gemalto and SafeNet/Vormetric lines, which are considered in this report. The SafeNet solutions can be installed on-premises on Ubuntu and Windows; in IaaS as VMs; and Thales hosts SaaS in AWS with data centers located in the EU and NA. Many different licensing options are available.

SafeNet accepts Aegis, Authy, Duo, Google, Okta, SAASPASS, and of course SafeNet app-based authenticators; x.509, mobile push notifications, phone OTP, and Android & iOS biometrics; FIDO 2.0; and CAC/PIV, Feitian, Google Titan, any OATH-based, RSA SecurID, Smart Cards, Thetis, and Yubikey hardware authenticators. Only a subset of options is available for admin authentication. Thales offers a mobile SDK but device intel collection is limited and is not exposed to customers for risk factor weighting. Kerberos, OAuth, OIDC, RADIUS, and SAML protocol support is present. LDAP and SCIM can be used for bulk provisioning. Self-registration is also possible. Email/SMS OTP, help desk, and customized API driven account recovery mechanisms can be used.

SafeNet's risk engine can process device intel though not visible to customers. It also can evaluate user history but does not perform attribute lookups. Behavioral biometrics are not included. Identity vetting and external compromised credential intelligence services are not integrated. Anonymous network and TOR detection are provided by Neustar. ML-enhanced detection algorithms inform the risk engine. Policies cannot be imported. The admin interface for policy writing is hierarchical and uses drop-down lists.

REST (with versioning), SOAP, and WebAuthn APIs and JSON/XML formats are supported. However, the risk engine itself is not accessible over APIs, nor is the output available for downstream application consumption. Thales offers OOTB connectors to various on-premises, SaaS, and network applications in their application catalog. Connectors are also available for Azure AD, CA, IBM, Oracle, Ping Identity, SailPoint, and Saviynt IAM and IDaaS systems; and BeyondTrust, CyberArk, Thycotic, and Wallix PAM systems. RBAC and delegated access control models are supported. SafeNet can transmit event data to SIEMs using syslog or JSON.

Thales attests to CSA Star Level 1, and has certifications for ISO 27001/27018, SSAE SOC 2 Type 2, and UK G-Cloud. Crypto components meet FIPS 140-2. Customers are typically drawn by the high-security options SafeNet provides. Organizations, in both the public and private sectors, that need high strength MFA options but do not need complex API access to the risk engine may want to consider Thales' SafeNet Suite.

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

THALES

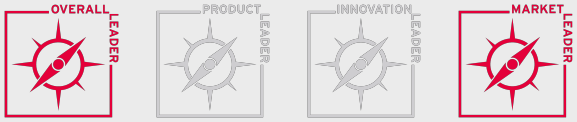
Strengths

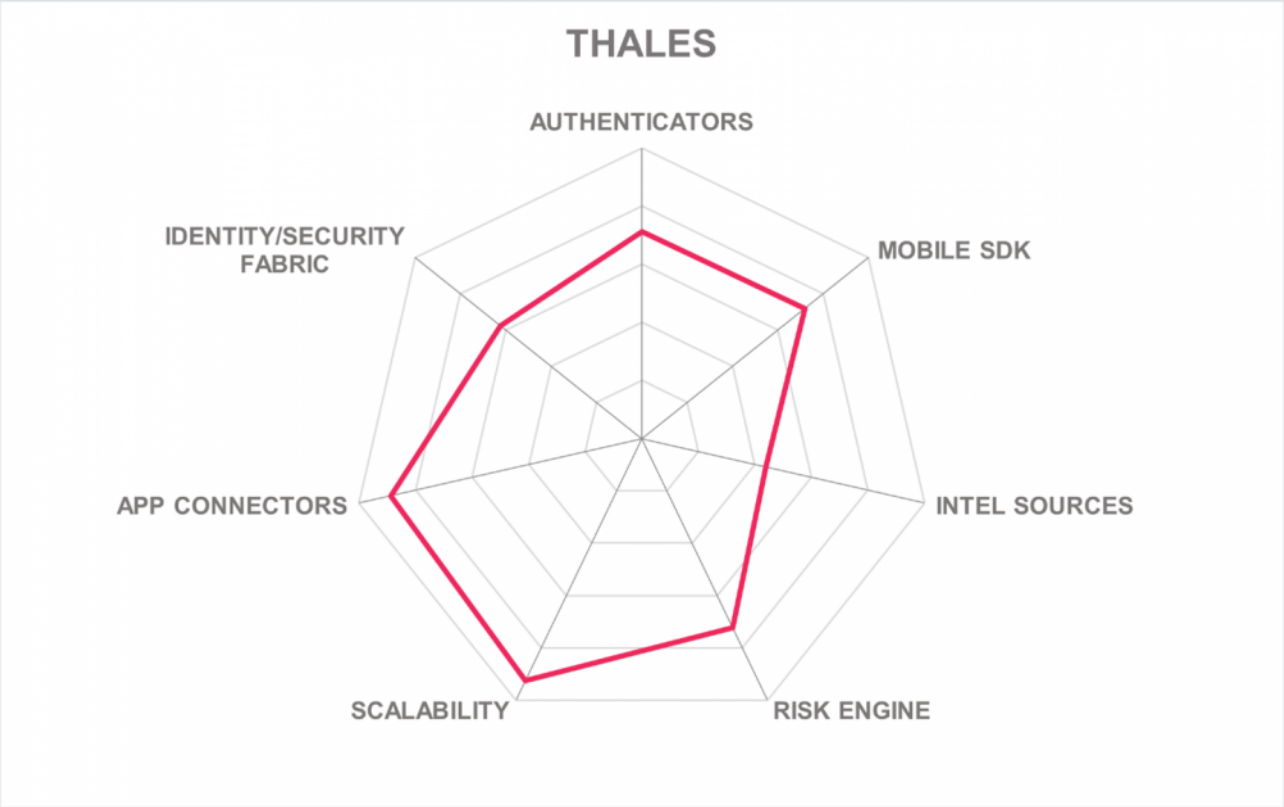
- IDPrime and SafeNet eTokens are FIDO 2.0 certified (preview but not GA yet)
- Good OOTB selection of connectors for a variety of applications, including some uncommon apps
- Integrations with most IAM and IDaaS products
- Strong anti-tampering security mechanisms
- ML risk detection models

Challenges

- Narrower list of authenticator apps and tokens supported than some
- Risk engine not accessible via API
- No behavioral biometrics
- Additional threat intelligence sources may be beneficial for some customers

Leader in




THALES
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.17 Transmit Security

Transmit Security was founded in 2013 and is headquartered in Tel Aviv, Israel, and has US headquarters in Boston, Massachusetts. The company is self-funded. In addition to IAM, Transmit Security offers an industry-leading Fraud Reduction Intelligence Platform. The company's Enterprise IAM platform can be installed on-premises on RHEL or Windows; packaged as a Docker container; deployed in AWS, Azure, or GCP IaaS. They also operate a multi-cloud SaaS across Alibaba, AWS, Azure, and GCP, running in data centers on five continents. Licensing options include active/registered users per variable time period and/or per-login/session charges.

Transmit accepts an impressive array of authenticators: Aegis, Authy, DeepNet, Derived PIV, Duo, Google, LastPass, Microsoft, Okta, OneSpan, SAASPASS, and SafeNet apps; mobile push notifications, Android and iOS biometrics; FIDO UAF/U2F/2.0; and Duo, Feitian, Google Titan, Kensington, OATH (any), OneSpan DigiPass, RSA SecurID, Symantec VIP, Thetis, and Yubikey hardware tokens. Transmit offers a secure mobile SDK that gathers the full range of device intelligence. JWT, OAuth, OIDC, RADIUS, and SAML standards are supported. LDAP, SCIM, and self-registration methods can be used for provisioning. All the normal account recovery mechanisms are present.

Transmit can evaluate a plethora of device intelligence signals and user attributes/history/behavioral analysis in its risk engine. Identity vetting service and compromised credential integrations can be configured. Behavioral biometrics are supported. Transmit allows policy import, and its admin interface features easy-to-use drag-and-drop input and flow-chart editing for policy authoring.

For APIs, REST, SOAP, Webhooks, and WebAuthn protocols (with versioning) and CSV, JSON, and XML formats are supported. Connections can be configured for Atlassian, AWS, Azure, Box, DocuSign, Dropbox, GCP, Intuit, Oracle, Salesforce, SAP, ServiceNow, Slack, VMware, and Workday. Transmit interoperates with Azure AD, ForgeRock, IBM, Ping Identity, and Okta IAM/IDaaS solutions; and CyberArk for PAM. Additional PAM integrations are configurable. Transmit can communicate with SIEMS using syslog and CEF. ABAC/RBAC and delegated access models are supported.

Transmit Security is ISO 27001/27018 and SSAE SOC 2 Type2 certified. Though the service is relatively young, it has the ability to scale to meet the demands of global enterprises. Transmit has one of the most feature-rich offerings in the enterprise authentication market and would likely be suitable for any type of organization looking to modernize its IAM with state-of-the-art authentication services.

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

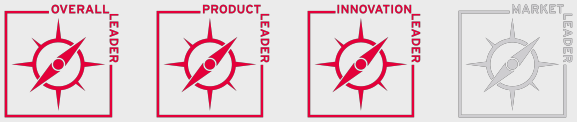
Strengths

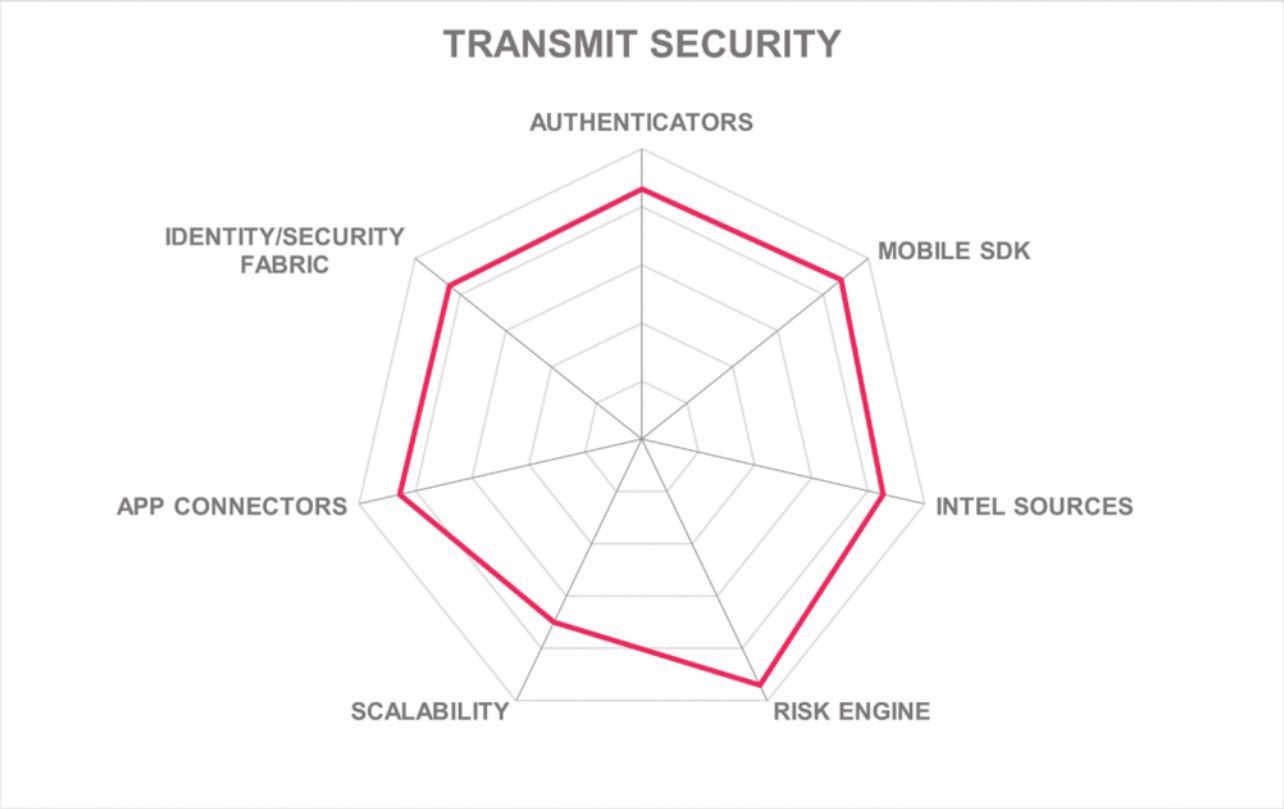
- FIDO UAF 1.1 & 2.0 certified
- Excellent selection of authenticators
- Behavioral biometrics included
- Risk engine processes comprehensive list of signals and risk factors
- Good support for relevant standards
- Easy-to-use admin interface

Challenges

- Smaller company but rapidly expanding
- Additional OOTB connectors for SaaS apps may benefit customers
- Additional connectors for VPNs and network device could be advantageous

Leader in




TRANSMIT SECURITY
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

5.18 WSO2

WSO2 was founded in 2005. They are an open-source IAM solution provider. Their target market is identity architects and developers who can take advantage of their API-driven and highly customizable product. Related products include Enterprise Integrator and API Manager. The solution requires a JVM, so it can be run on-premises on any supporting OS or in any IaaS. WSO2 also offers a managed service capability. They are launching as SaaS on AWS in two US regions. The product is licensed per-server under the Apache 2.0 License and is supported through annual subscriptions.

WSO2 accepts Aegis, Authy, Duo, Google, LastPass, Microsoft, and SAASPASS apps; mobile push notifications are possible via integration with Duo, InWebo, and MePin.; FIDO U2F/2.0, OATH token-based and Duo, Feitian, Google Titan, Kensington, OneSpan DigiPass, RSA SecurID, Smart Cards, Symantec VIP, Thetis, and Yubikey hardware tokens. WSO2 has connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, but Android/iOS biometrics are not supported. The SDK does not currently collect device attributes, but an update with more functionality is expected. Protocol support includes JWT, Kerberos, OAuth, OIDC, SAML, WS-Fed, and WS-Trust. Users can be on-boarded via CSV import, LDAP, SCIM, and self-registration. KBA, email links, and SMS OTP are the primary account recovery methods, although customers can configure other options as needed.

The risk engine can process device intelligence from Entgra's open-source MDM/UEM solution, which requires a separate deployment. Behavioral biometrics, compromised credential intelligence, and identity proofing services are not included, but with customization, Identity Server can integrate with 3rd-party vendors for these functions. WSO2 allows policy import over JSON or XACML. The policy editor interface is list-driven. The output can be made as granular as necessary and the engine itself is accessible through API, which allows integration with authorization systems.

WSO2 has excellent API support: OData, REST (versioned), RPC, SOAP, Webhooks, Websockets, WebAuthn; and CSV/JSON/XML formats. Customers can extend this to include AMQP, JMS, and MQTT. Connectors to collaboration apps, CRM, IaaS, office productivity, etc. can be found in the **WSO2 Store**. There are no dedicated connectors to other IAM, IGA, or PAM solutions, although customers can configure them using standards. ABAC/RBAC and delegated admin models are supported.

WSO2's crypto functions use FIPS 140-2 components; and Identity Server is ISO/IEC 15408 EAL2+ certified. The product does have some areas where they are missing functionality, such as mobile SDK, behavioral biometrics, compromised credential intelligence, and some of these are due to be addressed in the months ahead while others can be augmented currently with 3rd-party integrations. WSO2 is a global company with an extensive support and partner network. Organizations that prefer open-source integration solutions should consider WSO2 for their enterprise authentication and Identity API security needs.

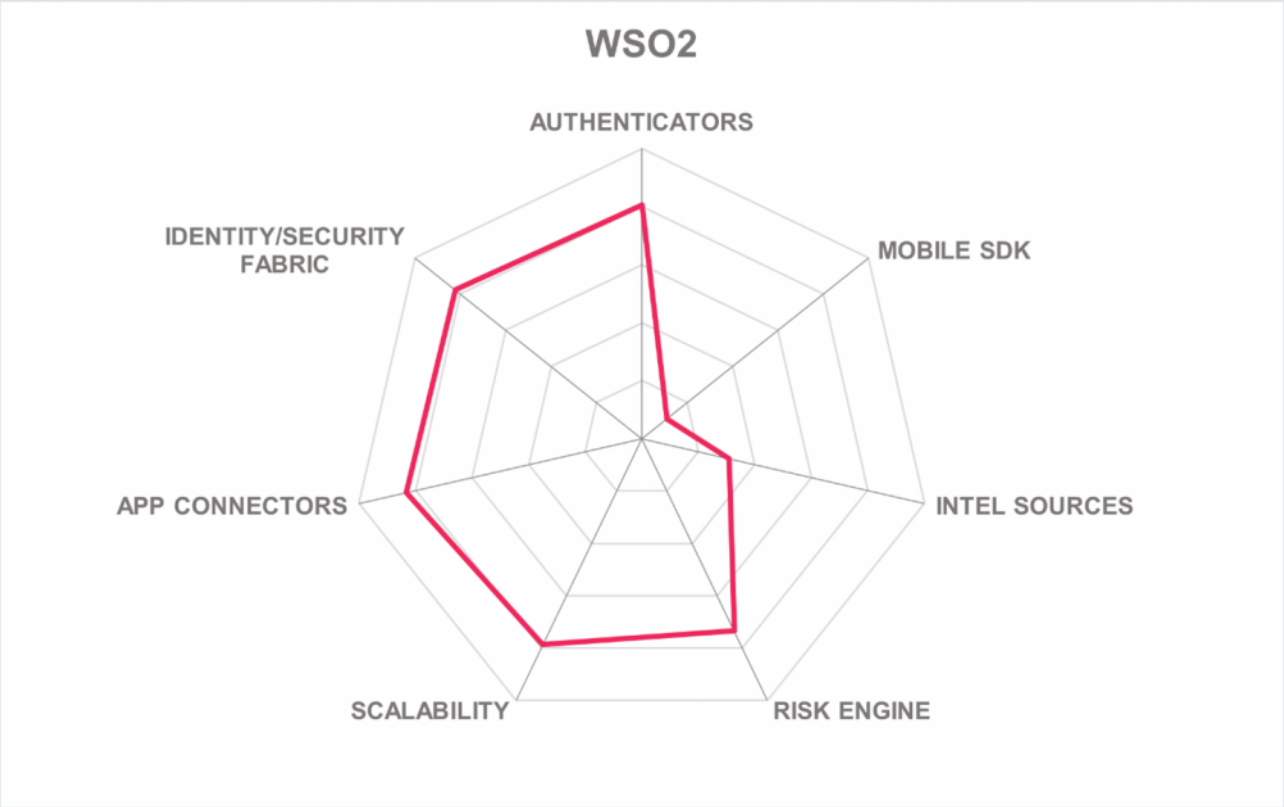
Security	●●●●●
Functionality	●●●●○
Interoperability	●●●●●
Usability	●●●●○
Deployment	●●●●○

Strengths

- Great support for IAM standards
- API first strategy allows customers to decentralize IAM services
- Highly extensible product
- Good selection of authenticators
- Large global partner network

Challenges

- No built-in behavioral biometrics or credential intel but can be configured
- Mobile SDK in work
- Collecting device attributes requires the use of Entgra MDM/UEM
- Late entrant to SaaS deployment
- More connectors for IAM/IGA/PAM and SaaS apps needed


WSO2
AUTHENTICATORS
MOBILE SDK
INTEL SOURCES
RISK ENGINE
SCALABILITY
APP CONNECTORS
IDENTITY/SECURITY FABRIC

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 Enterprise Authentication or are not yet mature enough to be considered in this evaluation. We provide short abstracts below on these vendors.

6.1 Amazon Cognito

Amazon offers enterprise authentication functionality with Cognito. Cognito supports OAuth, OIDC, and SAML for federation. Cognito was originally built for controlling access to Amazon resources. All services are exposed via APIs, meaning it is also categorized as an Identity API Platform and a component of an Identity Fabric. Amazon's computing environment is PCI-DSS, SOC 2 Type 2, ISO/EIC 27001, ISO/EIC 27017, ISO/EIC 27018, and ISO 9001 compliant. Amazon Cognito has adaptive authentication based on device recognition and IP address. Amazon Cognito supports multiple authentication methods including password, OTP over SMS, and authenticator applications out of the box, and can be configured to support hardware tokens and WebAuthn. Amazon Cognito also has alerting capabilities through Amazon Cloudwatch Alarms and traffic visualization through Cloudwatch Dashboards. KuppingerCole will follow developments in Amazon Cognito.

Why worth watching: As the largest IaaS provider in the world, Amazon's identity services will be increasingly used to deliver IDaaS for workforce use cases and CIAM.

6.2 Callsign

Callsign is a mid-stage venture-backed company that was founded in London in 2012. Their solution, Intelligence Driven Authentication, is a multi-faceted authentication service that is used for B2E and B2C use cases, and also has fraud reduction capabilities. The product can be installed on-premises on Linux or Windows, in IaaS as Docker containers, and they host a SaaS version in multiple regions on AWS. Callsign supports many authenticator types, provides a rich mobile SDK, and leverages behavioral biometrics from its SDK and JavaScript on browsers. Third-party intelligence sources are also ingested and examined. ML detection algorithms allow for continuous authentication and reduce the need to interrupt users with explicit authentication events.

Why worth watching: Callsign has a highly innovative product with broad support for authenticators and a good risk engine. They are focused on consumer authentication but their solution would also work well for enterprise workforce use cases.

6.3 Cisco Secure Access by Duo

Cisco acquired Duo Security in 2018, a veteran multi-factor authentication vendor and one of the leading providers of access security solutions. Cisco Secure Access by Duo is a fully multi-tenant SaaS security solution focused on verifying users and devices while protecting applications. It provides a scalable MFA platform that can accommodate an enterprise of any size, focusing on reducing the complexity of user identity verification while monitoring the health of their devices before connecting them to the applications they use. The platform provides a range of risk-based capabilities, like detecting 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, and so on.

Why worth watching: Duo not only protects users from numerous cyber threats like phishing, credential hijacking, or other identity-based attacks; but also, from the Zero Trust perspective, it establishes user identities and maintains device trust before any access request to an application, effectively eliminating any implicit trust of traditional network architectures.

6.4 ESET Secure Authentication

ESET is a well-respected vendor of cybersecurity solutions, headquartered in Bratislava, Slovakia and with offices around the world. ESET Secure Authentication supports mobile apps and push notifications, FIDO, and some hardware tokens. They also offer an SDK so that customers can extend the MFA options as needed. ESET provides connectors to popular SaaS applications such as Dropbox, Google G-Suite, and Microsoft O365; and many VPNs including Barracuda, Cisco, Citrix, Checkpoint, Fortinet, Juniper, Palo Alto, and SonicWall.

Why worth watching: ESET's global customer base for endpoint security products could easily add-on their Secure Authentication solutions and increase their market share in the enterprise authentication space.

6.5 Optimal IdM

Optimal IdM was founded in 2005 and is headquartered in Florida. Optimal IDM offers OptimalCloud which provides SSO, MFA, Federation capabilities for Federation IAM, CIAM, and IDaaS use cases. OptimalCloud

also provides APIs for WAM solutions. In terms of authenticators, the platform accepts several hardware and software tokens, FIDO U2F devices, and Android/iOS biometrics. Optimal IdM also allows evaluation of multiple risk factors.

Why worth watching: Optimal IdM has good support for federated SSO and could expand its authenticator selection and compete directly in the authentication service market.

6.6 TransUnion (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.

Why worth watching: iovation's intelligence services are used by many CIAM and IDaaS vendors as well as IAM operators. We have evaluated TransUnion's products in prior reports and will continue to follow them and include them in future reports.

6.7 United Security Partners

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-premises 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.

Why worth watching: 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.

6.8 Veridium

Veridium was founded in London in 2017. They're a series B startup specializing in passwordless authentication. Their solutions serve both consumer and workforce applications. Supported authentication technologies include mobile biometrics, behavioral biometrics, and geo-fencing. Veridium has partnerships with ForgeRock and Okta and provides SSO to on-premises apps and VPN as well as SaaS apps. Their

services offer strong and user-friendly MFA to help customers comply with GDPR and PSD2 SCA.

Why worth watching: Veridium focuses on leading-edge but dependable authentication methods and includes certified support for FIDO 2.0.

7 Related Research

Leadership Compass: Cloud-based MFA Solutions – 70967
Leadership Compass: Adaptive Authentication - 79011
Leadership Compass: Consumer Authentication - 80061
Leadership Brief: Why Adaptive Authentication Is A Must – 72008
Leadership Brief: Mobile Connect – 71518

Methodology

About KuppingerCole's Leadership Compass

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

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

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

Types of Leadership

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

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

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

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

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

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

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

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

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

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

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

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

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

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

Vendor rating

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

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

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

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

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

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

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

Rating scale for products and vendors

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

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

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

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

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

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

Inclusion and exclusion of vendors

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

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

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

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

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

Content of Figures

Copyright

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

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

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