KuppingerCole Report

LEADERSHIP COMPASS

By Alejandro Leal
October 04, 2022

Leadership Compass on Passwordless Authentication

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

By **Alejandro Leal**

Content

1 Introduction / Executive Summary

The password is remnant of an era before hacking and credential-based attacks became a widespread problem. Although the internet has changed significantly since the early days, passwords have practically remained the same. In parallel, cybercriminals have targeted operating systems with increasing sophistication and frequency as computers have become more accessible worldwide.

For years, IT professionals have discussed the idea of passwords becoming obsolete. The issue with passwords is that they can easily be stolen and compromised. In addition, passwords can be costly, time-consuming, difficult to manage, and result in poor user experience. Furthermore, the fact that password reuse is a common practice among customers and employees only exacerbates the problem.

To make matters worse, credential-based attacks and account takeover fraud cases have been on the rise, which have disrupted businesses and organizations already affected by the COVID-19 pandemic, the global supply chain crisis, and the 2022 Russian invasion of Ukraine. The security risks and inconvenience of passwords has led to a trend in which organizations are replacing and eliminating passwords altogether.

Keeping passwords secure is a top priority for organizations because once one is compromised, it is very difficult to prevent or detect a security breach since attackers are in possession of a legitimate password. By getting rid of the risk associated with passwords, however, organizations will add a significant layer to the overall security of their IT infrastructure.

As a result, Passwordless Authentication has become a popular and catchy term. It is used to describe a set of identity verification solutions that remove the password from all aspects of the authentication flow and from the recovery process as well. Therefore, by eliminating passwords as a method of authentication, organizations will remain competitive, secure, compliant and have a modern authentication system that does not require users to remember passwords.

Some passwordless options have been around for a while but are starting to be implemented more by enterprises and even consumer-facing businesses. For example, smart cards and hardware tokens have been used as an alternative to usernames and passwords for decades. Nevertheless, some of the distinctive features of passwordless solutions include the ability to support a wide range of authenticators, public key cryptography, biometrics, comprehensive APIs, and support for legacy applications and services, among other things.

Account recovery must also be considered for IAM and especially passwordless authentication solutions: when users forget passwords, lose credentials, or change devices, they need ways to get access to their accounts. To ensure users can regain access to their accounts without compromising their security, a variety of trusted recovery options should be available.

The development of open standards such as FIDO2 and WebAuthn have further generated adoption of passwordless technologies. Moreover, the U.S. government recently published a cybersecurity memorandum emphasizing the need for stronger enterprise identity and access controls, including using phishing-resistant MFA and adopting a Zero Trust model.

Consequently, organizations' systems must cease supporting legacy authentication methods that are prone to phishing attacks, such as mobile SMS codes, voice calls, push notifications or one-time passcodes (OTP). It is therefore imperative that organizations and agencies pursue greater use of passwordless authentication solutions as they modernize their authentication systems.

The need for Passwordless Authentication solutions is increasing, but finding one that is simple, effective, and secure is challenging. Organizations must confront password-based threats and find alternatives without disrupting their users or business practices. If implemented successfully, a Passwordless Authentication solution will not only increase the security posture of the organization but also deliver a convenient and frictionless user experience.

There are a sizable number of vendors in the Passwordless Authentication market. Many of the vendors have developed specialized risk-based passwordless products and services, which can integrate with customers' on-premises IAM components and support the migration of legacy applications to modern authentication systems. However, we prefer vendors who deliver a solution that can be applied to multiple use cases (workforce, consumer, partners). Therefore, the major players in the Passwordless Authentication segment are covered within this KuppingerCole Leadership Compass.

1.1 Highlights

- The use of the password dates back to an era before hacking and credentials-based attacks became a common and pervasive problem.
- As long as passwords continue to be used, businesses and organizations will remain vulnerable to identity attacks.
- Geopolitical tensions and global disruptions have made organizations more susceptible to account takeover attacks and fraud cases.
- A passwordless MFA solution should be able to provide a frictionless login experience and eliminate the reliance on passwords or other easily phishable factors.
- The creation of open standards such as FIDO2 and WebAuthn have increased adoption of passwordless technologies.
- The Passwordless Authentication market is a dynamic, exciting, and competitive space where different vendors provide similar but unique solutions.
- The Overall Leaders (in alphabetical order) are 1Kosmos, CyberArk, Entrust, ForgeRock, HID

Global, HYPR, IBM, Microsoft, Ping Identity, Thales, and Transmit Security.

- The Product Leaders (in alphabetical order) are 1Kosmos, Beyond Identity, CyberArk, Entrust, ForgeRock, HID Global, HYPR, IBM, IDEE, Microsoft, Nevis Security, Ping Identity, RSA, Thales, and Transmit Security.
- The Innovation Leaders (in alphabetical order) are 1Kosmos, Beyond Identity, CyberArk, Entrust, ForgeRock, Futurae Technologies, HID Global, HYPR, IBM, Identité, Ping Identity, and Transmit Security.
- The Market Leaders (in alphabetical order) are Cisco, CyberArk, Entrust, Exostar, ForgeRock, HID Global, IBM, Microsoft, Ping Identity, RSA, Thales, and Transmit Security.

1.2 Market Segment

The Passwordless Authentication market is growing rapidly, with vendors offering mature solutions that support millions of users across different industries including finance, healthcare, government, insurance, manufacturing, and retail. It is therefore essential for organizations to choose the right passwordless solution that meets their unique requirements and needs around security, user experience, and technology stack.

As will be reflected in this report, it is evident that some vendors provide nearly every feature one would need in a Passwordless Authentication service, while others are more specialized, and thus have different kinds of technical capabilities. For example, some smaller vendors are targeting mobile operators, the government-to-citizen (G2C) market, as well as small and medium-sized enterprises (SME). In other words, this Leadership Compass includes both pure passwordless players as well as those who are able to support passwordless in some form.

KuppingerCole research indicates that the particular market segments that vendors choose to target often has a direct effect on the type of features available in their Passwordless Authentication solutions. This has yielded a dynamic, exciting, and competitive space where different vendors provide similar but unique methods for customers, partners, and employees. Furthermore, this Leadership Compass will examine solutions that are available for both on-premises and cloud-based deployment.

As smartphones and other consumer electronic devices have become increasingly prevalent, requiring login and account access from end users using these devices has proven to be essential. Therefore, enterprises and organizations are using QR codes, fingerprints, and other biometrics to enroll and authenticate their users, thereby propelling the demand for passwordless authentication.

Passwordless solutions are typically used alongside other authentication processes, such as multifactor authentication (MFA) or single sign-on (SSO) and are becoming more popular as an alternative for traditional username and password authentication. Despite improvements in authentication over the past few years, cybercriminals still use a wide range of techniques and procedures to gain unauthorized access.

Traditional MFA solutions were supposed to overcome the issue of passwords; however, the problem is that some MFA solutions still rely on a password as the first factor or backup factor for authentication. By adopting a passwordless MFA, users are protected against phishing and ransomware attacks by using authentication factors that cannot be easily obtained by attackers, thus, increasing security and convenience.

While many passwordless authentication solutions describe themselves as such, they are actually just disguised passwords with extra steps. Various solutions are still password-bound such as password managers, and legacy multi-factor authentication (MFA) solutions, which utilize passwords as a factor in their authentication process.

In essence, Passwordless Authentication solutions should provide a consistent login experience across all devices, introduce a frictionless user experience, include an integrated authentication approach, and ensure that no passwords or password hashes are traveling over the network anymore.

It's important to note that although password databases may be omitted in passwordless authentication systems, users may still have to enter passwords or PINs occasionally. Solutions that use passwords or PINs (locally) as a "last resort" for reset or authentication when other methods fail will be considered in this Leadership Compass, despite a preference for end-to-end passwordless approaches.

Overall, we expect to see further momentum. The continuing and increasing shift to remote and hybrid work will contribute to further adoption of Passwordless Authentication solutions and services by both workforce and customers. Also, the ongoing transformation of legacy IAM solutions into modern architectures with API support and flexible deployment models also plays a crucial role in this process.

What remains to be seen is if Passwordless Authentication customers can overcome old-school mentalities. Despite the promise of new security methods, many people are still reluctant to move away from traditional security methods due to user acceptance, lack of knowledge, security limitations, and deployment costs.

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.

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.

1.3 Delivery Models

Passwordless Authentication solutions are mainly delivered as a cloud hosted Software as a Service

(SaaS), with all participating vendors providing this deployment model. However, support and integration with on-premises environments are also offered by most vendors. Despite the continued relevance of on-premises deployments, organizations are requiring more agile multi-cloud and multi-hybrid deployments that provide a gradual migration to the cloud. On the one hand, for SaaS offerings, the licensing models are often priced per user, per transaction, and per time period. On the other hand, for on-premises deployments, licensing costs can be measured as per-user or per-server.

1.4 Required Capabilities

This Leadership Compass analyzes which of the Passwordless Authentication offerings in the market are best suited to form the foundation for a Zero Trust model, in providing

- An integrated and secure authentication approach
- A strong level of usability (e.g., simple device onboarding; recurring authentication)
- Authentication methods that eliminate passwords and other easily phishable factors
- The ability for organizations to control which users and devices can access sensitive information

Thus, solutions must not only deliver functionality and support for integration, but also meet our requirements regarding the architecture, deployment model, and their interoperability with traditional applications, cloud services, and new digital services.?

The focus is on solutions that cover these capabilities:

- Support for a broad range of authenticators
- Strong Authentication (e.g., 2FA, MFA)
- Risk, context-based, and continuous authentication
- Adaptive and step-up authentication
- Support for legacy applications and services?
- Strong cryptographic approaches (Private/Public Key, Zero Knowledge Encryption)
- Integration with 3rd-party authenticators
- Integration to MDM and UEM solutions
- Integration capabilities to established platforms such as Microsoft Azure AD
- Frictionless user experience
- Device trust on multiple devices

- Support for all major Identity Federation standards, including SAML and OAuth
- Comprehensive set of APIs
- Flexible, modern software architecture
- BYOD support
- Scalability and performance
- Delegated administration

We expect solutions to cover a majority of these capabilities at least at a good baseline level. There is no minimum number of customers or revenue caps that vendors must meet -- both large international companies and small but innovative startups are included in this report. Some vendors did not respond to requests to participate or chose not to participate. Profiles of these vendors, as well as other interesting vendors, can be found in Chapter 6, "Vendors to Watch".

2 Leadership

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

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

- Product
- Innovation
- Market

2.1 Overall Leadership

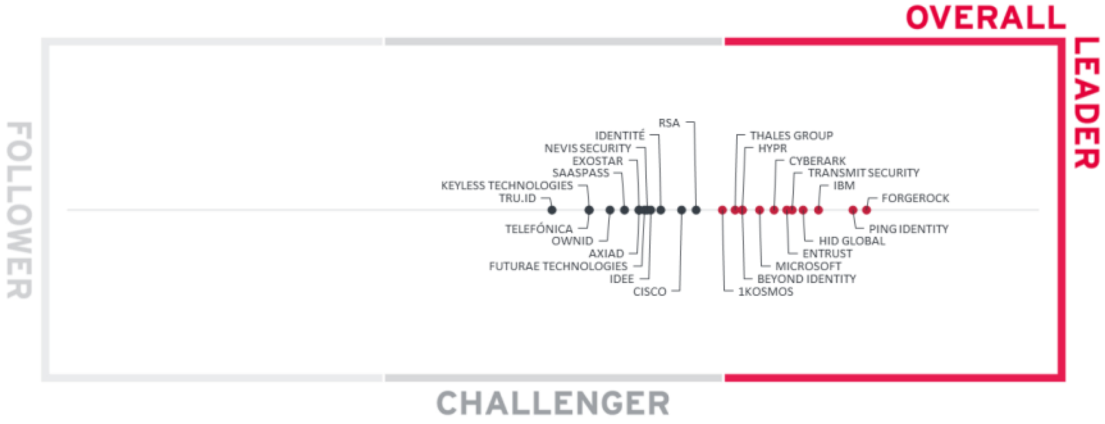


Figure 1: The Overall Leadership rating for the Passwordless Authentication market segment

The Passwordless 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, HID Global, Transmit Security, Entrust, CyberArk, Microsoft, HYPR, Beyond Identity, Thales, and 1Kosmos. The leaders include a mix of leading IAM vendors, innovative start-ups, ID management providers, and authentication specialists.

In the overall rating, we see ForgeRock and Ping Identity in first and second place respectively. The ForgeRock Identity Platform provides good access management features, strong orchestration capabilities, and excellent integration. Ping Identity's solution, on the other hand, is highly scalable and flexible. It also provides strong support for standards as well as OOTB connectors to SaaS/IDaaS. While both differ in their approaches, these solutions provide a strong set of capabilities in a modern architecture and thus can serve well as the foundation for a Passwordless Authentication solution. Next is IBM, followed by HID Global, Transmit Security and Entrust. IBM\'s solution is highly scalable, integrates easily with 3rd parties for MFA, and offers a wide selection of authentication mechanisms. HID Global provides strong credential issuance and management capabilities while Transmit Security offers excellent orchestration capabilities and strong omni-channel features. Last but not least, Entrust's solution delivers strong features in risk based adaptive step-up authentication and proximity- based high assurance passwordless login. These are well-established vendors with a global partner ecosystem, strong market position, and presence in various regions of the world.

Following is a group of vendors that includes CyberArk, Microsoft, HYPR, Beyond Identity, Thales, and 1Kosmos. This group of vendors is a mix of established and emerging players, some being stronger in their market position (Microsoft, Thales, and CyberArk) and others in innovativeness (Beyond Identity, 1Kosmos, and HYPR). Furthermore, some of these vendors provide nearly every feature one would expect in a Passwordless Authentication service, while others are more specialized, and thus have different kinds of technical capabilities and use cases. For example, 1Kosmos, despite being a relatively young vendor, has various innovative features and strong identity proofing and onboarding capabilities. Beyond Identity, also a young and innovative vendor, offers strong device trust and management capabilities while HYPR delivers protection from the desktop authentication to backend applications and support for MacOS, Windows, and Unix systems. Although North America is the primary market for these vendors, they are rapidly expanding in other regions as well. We strongly recommend further detailed analysis of the information provided in this document for choosing the vendors that are the best fit for your requirements.

The Challenger segment is much more populated than the Leaders segment. In the first group of Challengers, closely following the overall leaders, we see RSA and Cisco. On the one hand, RSA's solution provides a fully integrated and scalable service with flexible hybrid deployment options. On the other hand, Cisco delivers strong device trust and risk-based authentication capabilities. Both vendors score well in the market leadership but with some gaps in the innovation category. In the next group, we find Identité, IDEE, Nevis Security, Futurae Technologies, Exostar, Axiad, SAASPASS, OwnID, Keyless Technologies, Telefonica, and tru.ID. Here we see a mix of vendor types: IAM specialists, specialists for biometric authentication, vendors focusing on SIM-card based authentication, and others that are focused on specific areas related to decentralized identity/self-sovereign identity (SSI). They have overall good capabilities and a high degree of flexibility in configuration, while lacking some of the more advanced features other vendors provide, including integration to other platforms or the ability to support multiple use cases. All vendors within the Challenger section have good products with varying levels of device management, orchestration, deployment, and API capabilities. Furthermore, some still have limited global presence, affecting their rating for Overall Leadership.

Overall Leaders are (in alphabetical order):

- 1Kosmos
- Beyond Identity
- CyberArk
- Entrust
- ForgeRock
- HID Global
- HYPR
- IBM
- Microsoft
- Ping Identity
- Thales
- Transmit Security

2.2 Product Leadership

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.

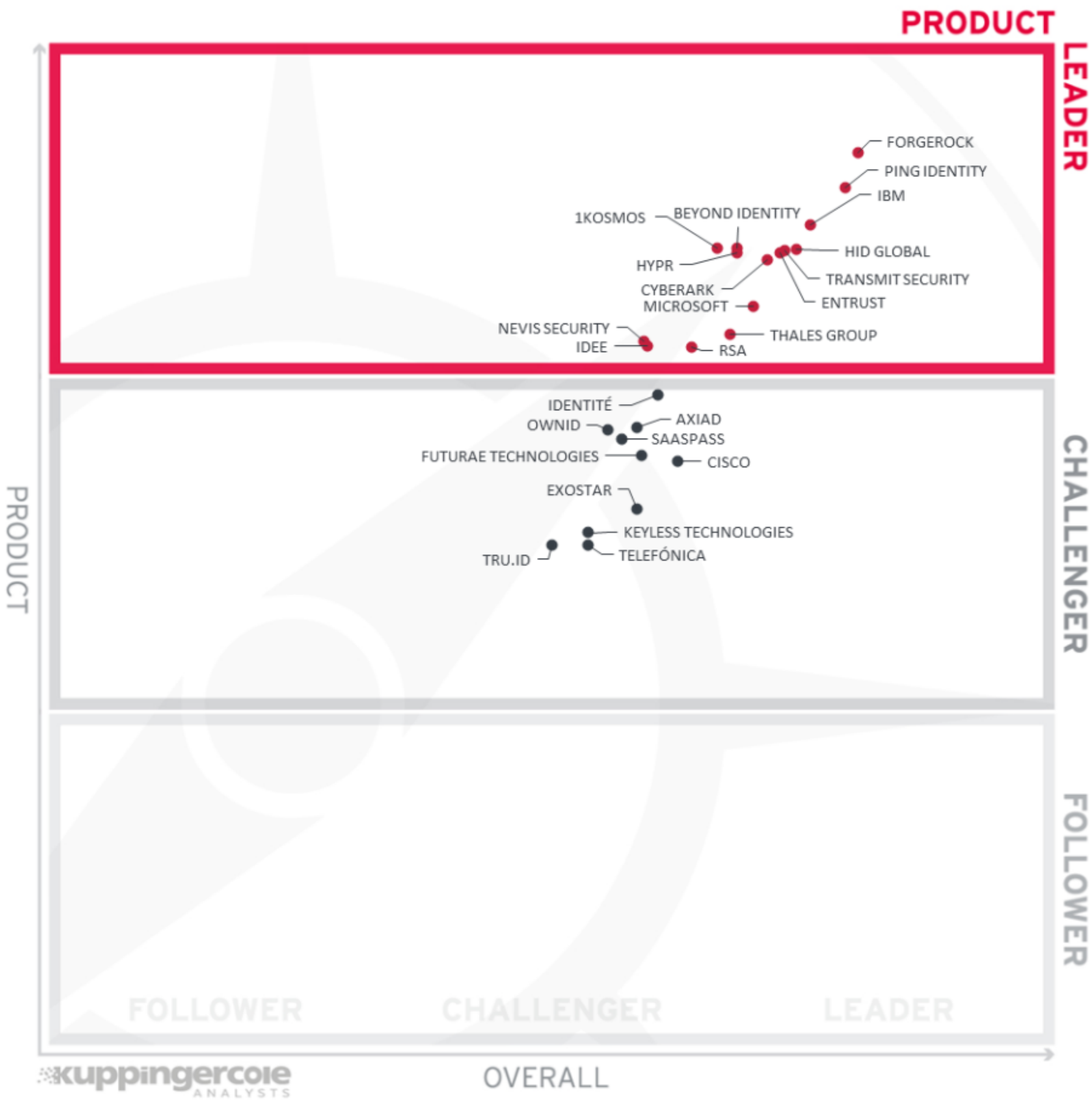


Figure 2: Product Leaders in the Passwordless Authentication market segment

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

The Product Leaders in Passwordless Authentication are ForgeRock, Ping Identity, IBM, 1Kosmos, Beyond Identity, HID Global, Transmit Security, Entrust, HYPR, CyberArk, Microsoft, Thales, Nevis Security, IDEE, and RSA. Each of their products contains a sufficient level of innovation, strong capabilities, and delivered product vision to merit standing at the top of the rating. All vendors in the Product Leadership deliver leading-edge capabilities across the depth and breadth of the Passwordless Authentication capability spectrum evaluated for the purpose of scoring the vendors in this Leadership Compass.

We find that Challengers are clustered mostly in the middle of the chart. At the top we see Identité, Axiad, OwnID, SAASPASS, Futurae Technologies, Cisco, Exostar, Keyless Technologies, tru.ID, and Telefonica. All these vendors have interesting offerings but lack certain advanced capabilities that we expect to see, either in the depth or breadth of functionalities seen in the Leadership segment offerings or in the ability to support multiple use cases.

Product Leaders (in alphabetical order):

- 1Kosmos
- Beyond Identity
- CyberArk
- Entrust
- ForgeRock
- HID Global
- HYPR
- IBM
- IDEE
- Microsoft
- Nevis Security
- Ping Identity
- RSA
- Thales
- Transmit Security

2.3 Innovation Leadership

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.

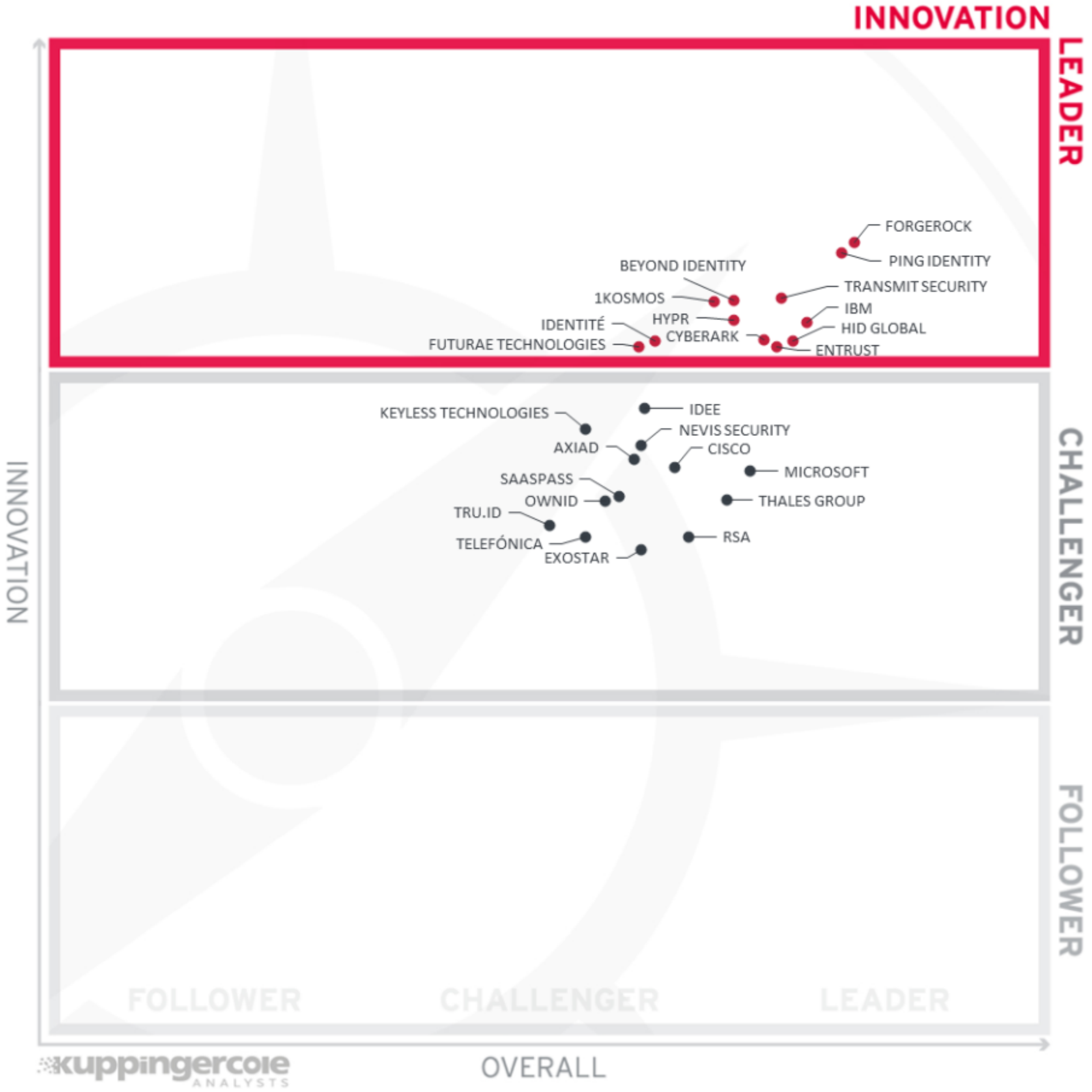


Figure 3: Innovation Leaders in the Enterprise Authentication market segment

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. This Leadership Compass saw a large number of innovative vendors providing unique and exciting technologies. Therefore, this was a very competitive category. Vendors continue to differentiate themselves by innovating in different areas, such as strong adaptive authentication capabilities, device management, orchestration, integrating with legacy systems, providing APIs and API security, fraud detection, automation, decentralized identity & verifiable credentials, or using a more modern containerized and microservices-based product.

The Innovation Leaders in Passwordless Authentication are ForgeRock, Ping Identity, Transmit Security, Beyond Identity, 1Kosmos, HYPR, IBM, CyberArk, HID Global, Identité, Futurae Technologies, and Entrust. 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 IDEE, Keyless Technologies, Nevis Security, Axiad, Cisco, Microsoft, SAASPASS, Thales, OwnID, tru.ID, Telefonica, RSA, and Exostar. These companies also have some specific innovations that make their offerings attractive to their customers, but need to shift their emphasis to deploying newer technologies.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- Beyond Identity
- CyberArk
- Entrust
- ForgeRock
- Futurae Technologies
- HID Global
- HYPR
- IBM
- Identité
- Ping Identity
- Transmit Security

2.4 Market Leadership

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

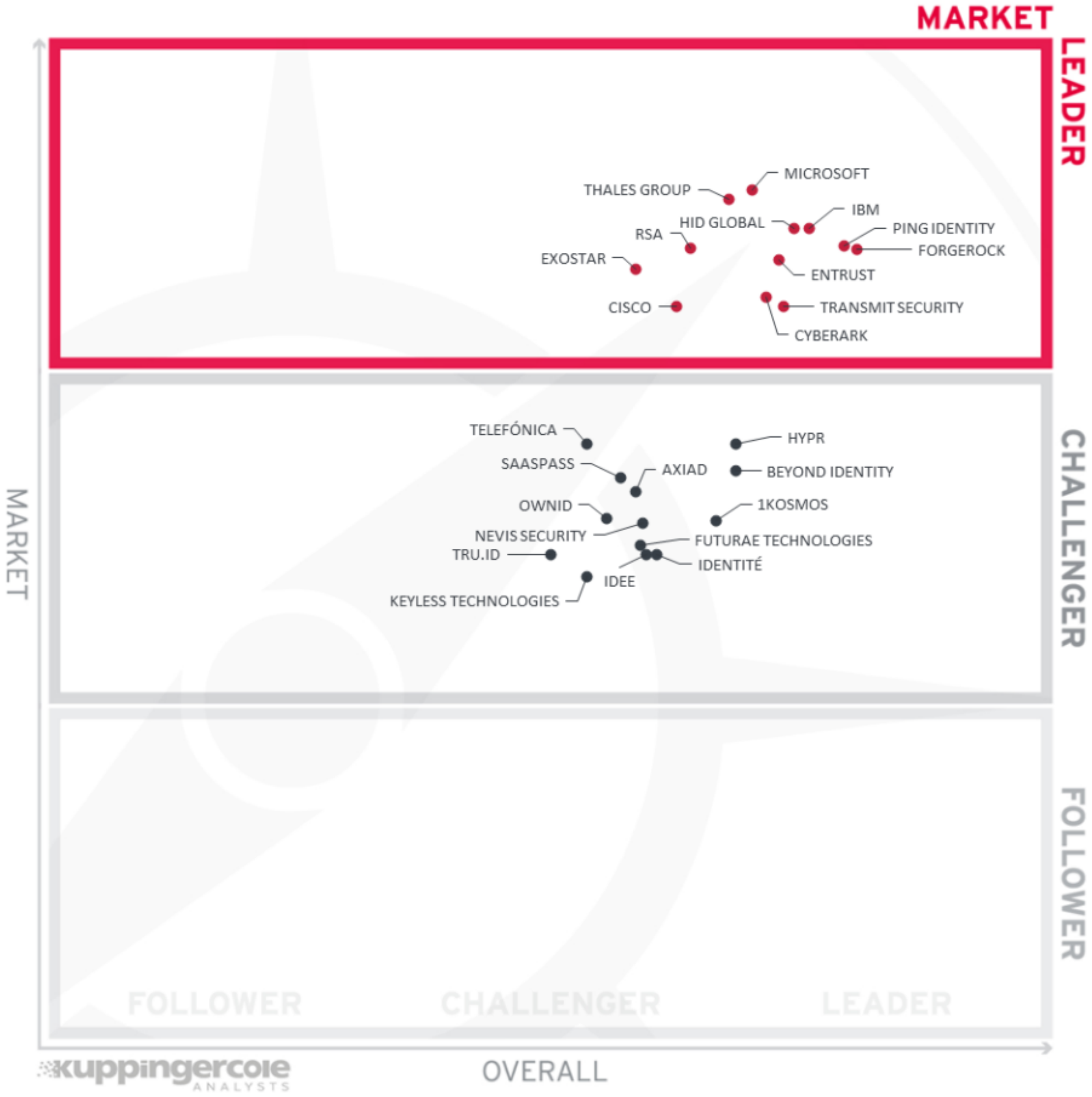


Figure 4: Market Leaders in the Enterprise Authentication market segment

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 Passwordless Authentication are Microsoft, Thales, IBM, HID Global, Ping Identity, RSA, ForgeRock, Entrust, Exostar, CyberArk, Cisco, and Transmit Security. These are well-known names in the IAM space and have size and presence in the Passwordless Authentication segment to justify their leadership ranking.

The top Challengers are Telefonica, HYPR, Beyond Identity, SAASPASS, Axiad, OwnID, 1Kosmos, Nevis Security, Futurae Technologies, tru.ID, IDEE, Identité, and Keyless Technologies. Several of these vendors are relatively young, lack a comprehensive global presence, and focus mainly on a single industry or region.

Market Leaders (in alphabetical order):

- Cisco
- CyberArk
- Entrust
- Exostar
- ForgeRock
- HID Global
- IBM
- Microsoft
- Ping Identity
- RSA
- Thales
- Transmit Security

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.

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

3.1 The Market/Product Matrix

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

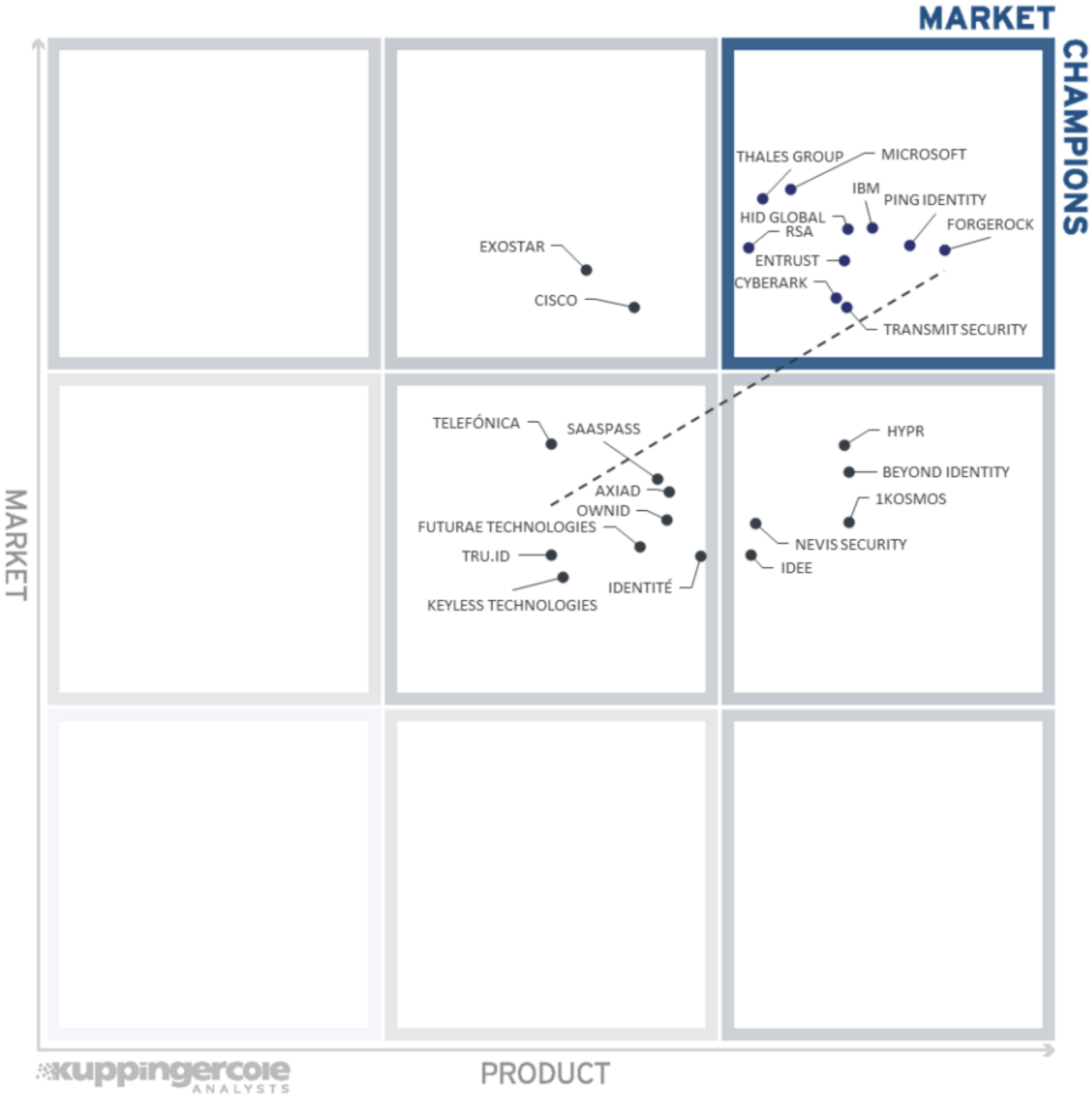


Figure 5: The Market/Product Matrix

Vendors below the line have a weaker market position than expected according to their product maturity. Vendors above the line are sort of "overperformers" when comparing Market Leadership and Product Leadership. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

This comparison shows which vendors are better positioned in our Product Leadership analysis than their position in the Market Leadership analysis. Vendors above the line are somewhat "overperforming" in the market. It comes as no surprise that these are often very large vendors, while vendors below the line may more often be innovative but focused on specific regions as an example.

In the upper right segment, we find "Market Champions". Given that the Passwordless Authentication market is still growing, we see Microsoft and Thales as market champions positioned in the top right-hand box. Close to this group of long-established players in the same box are (in alphabetical order) CyberArk, Entrust, ForgeRock, HID Global, IBM, Ping Identity, RSA, and Transmit Security.

Exostar and Cisco are positioned in the box to the left of market champions, depicting their stronger market success over the product strength. However, based on their market share, global presence, and partner ecosystem, we believe they have good potential for further growth.

In the middle right-hand box, we see a number of vendors that deliver strong product capabilities for Passwordless Authentication but are not yet considered Market Champions. HYPR, Beyond Identity, 1Kosmos, Nevis Security, and IDEE have a strong potential to improve their market position due to the more robust product capabilities they are already delivering.

In the middle of the chart, we see the vendors that provide good but not leading-edge capabilities and therefore are not market leaders. They also have moderate market success as compared to market champions. These vendors include (in alphabetical order) Axiad, Futurae Technologies, Identité, Keyless Technologies, OwnID, SAASPASS, Telefonica and Tru.ID. For example, Identite has a strong market position in the SME market, while OwnID and Futurae Technologies have a significant presence in EMEA markets as well as growing presence in North America. All the vendors below the line are underperforming in terms of market share. However, we believe that each has a chance for significant growth.

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 tightly constrained to the line, with a significant number of established vendors plus some smaller vendors.

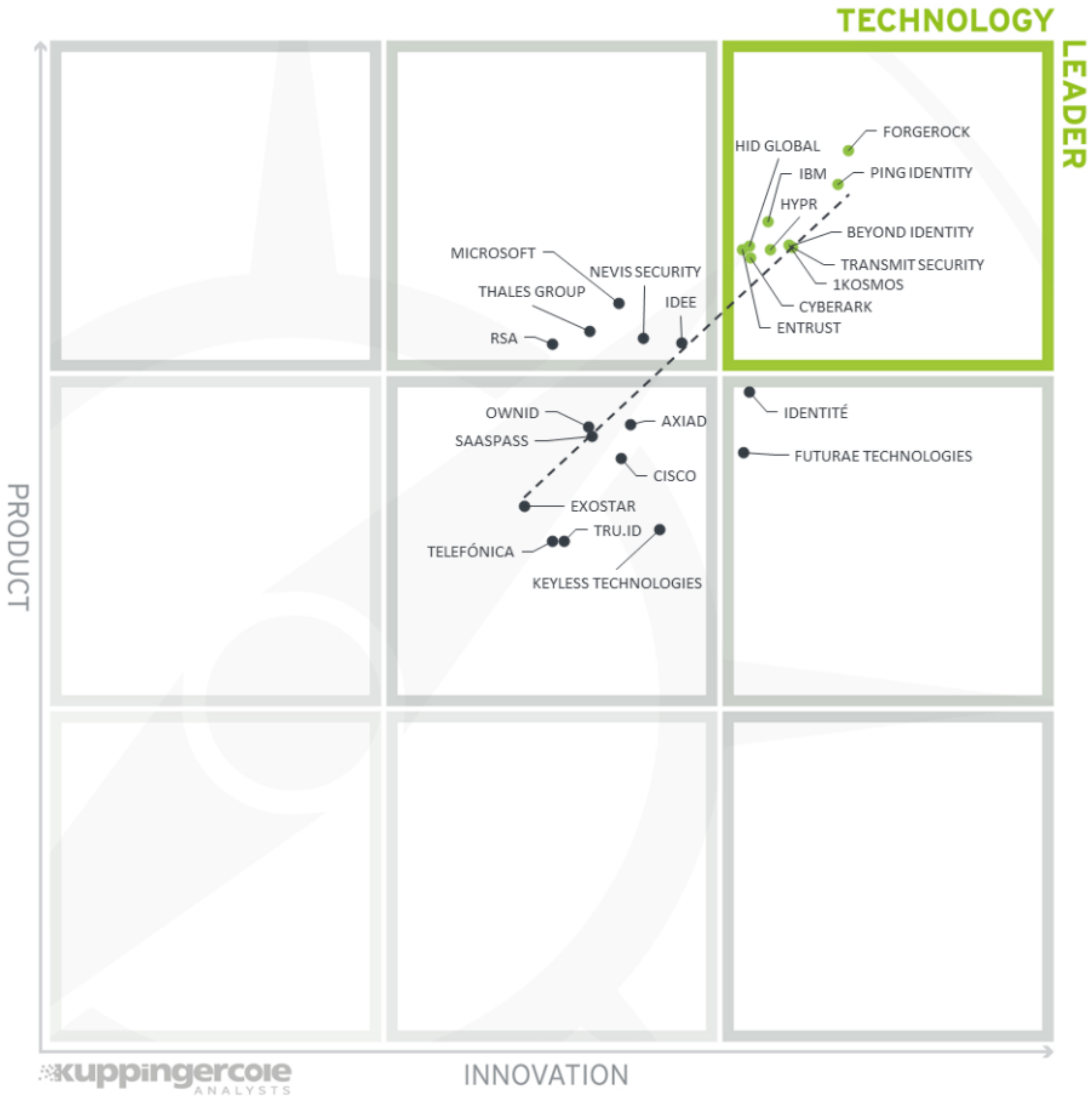


Figure 6: The Product/Innovation Matrix

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

Here, we see a good correlation between the product and innovation rating. Many vendors placed close to the dotted line, indicating a healthy mix of product and innovation leadership in the market. Looking at the Technology Leaders segment, we find most leading vendors scattered throughout the box in the upper right corner. The leading vendors are (in alphabetical order) 1Kosmos, Beyond Identity, CyberArk, Entrust, ForgeRock, HID Global, HYPR, IBM, Ping Identity, and Transmit Security. ForgeRock, Ping Identity, and IBM are placed closest to the axis depicting a good balance of product features and innovation. Entrust, HID

Global, CyberArk, Transmit Security, 1Kosmos, HYPR, and Beyond Identity are following closely behind while Identité and Futurae Technologies are just below the Technology Leaders. While these vendors all take different approaches for delivering a a Passwordless Authentication solution, all perform well in both the current product offering and the innovation they demonstrate.

Five vendors appear in the top middle box with good products but less innovation than the leaders, including Microsoft, Thales, Nevis Security, RSA, and IDEE. However, there is room for improvement. For example, Microsoft has been creating new standards such as multi-device FIDO credentials in conjunction with the FIDO Alliance and other companies, while Thales has been offering a distinctive feature that allows its solution to comply with country-specific regulatory requirements.

Most of the vendors appear in the middle box, showing both innovation and product capabilities. However, they remain at a Challenger level in both product and innovation ratings. These vendors include (in alphabetical order) Axiad, Cisco, Exostar, Keyless Technologies, OwnID, SAASPASS, Telefonica, and tru.ID. Considering their strong technology capabilities, we believe they have a good chance of growing further. For example, Axiad's MyCircle delivers an innovative identity proofing capability that enables co-workers to assist in resetting PINs, renewing a token, or verifying credentials. Moreover, Keyless Technologies provides a solution that combines advanced cryptography with facial biometrics and authentication, while Telefonica and tru.ID leverage the existing cryptographic security of the SIM card to authenticate and secure employees and customers. These vendors have a strong potential in further increasing their position in the Passwordless Authentication market.

3.3 The Innovation/Market Matrix

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

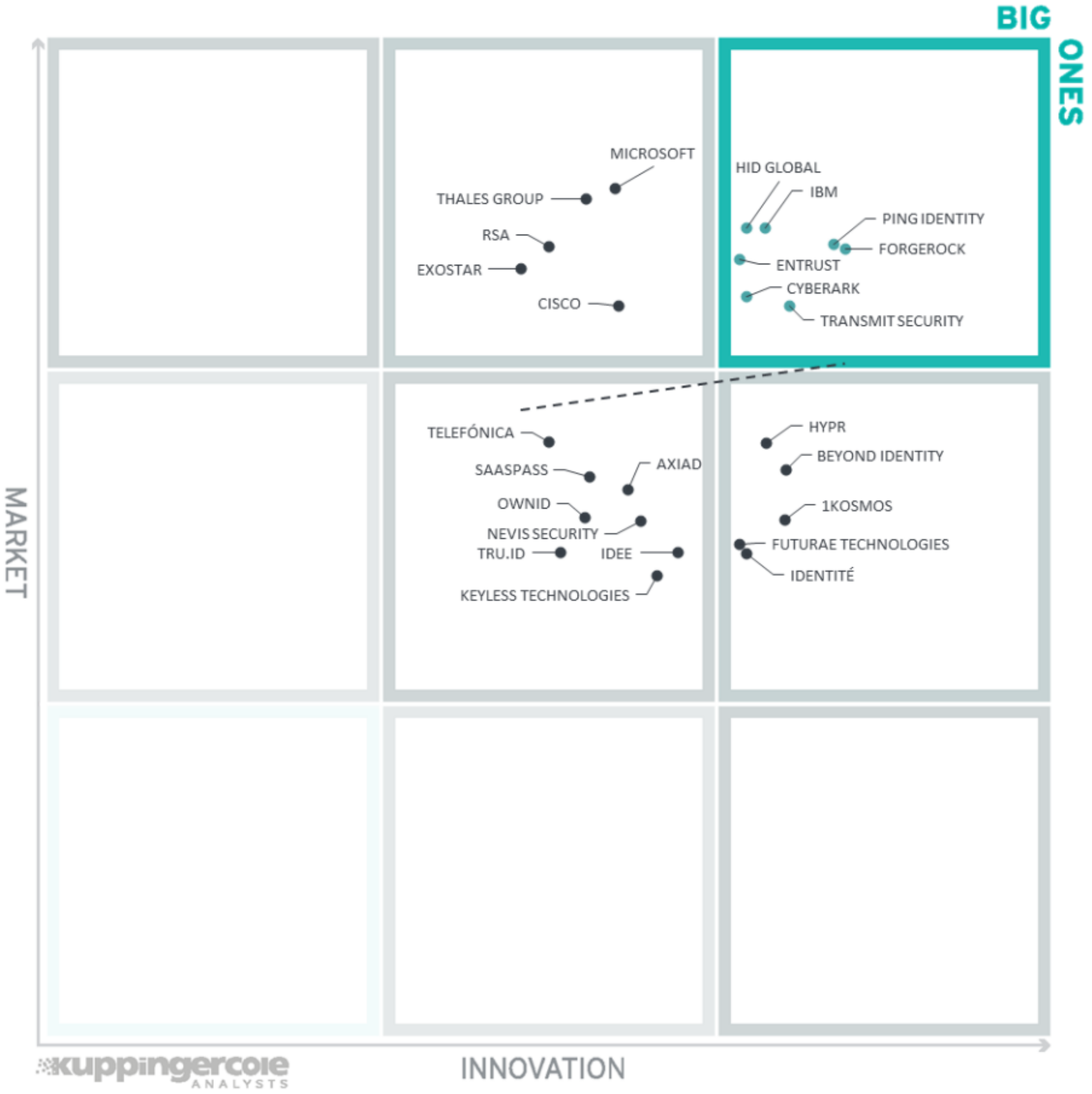


Figure 7: The Innovation/Market Matrix

Vendors above the line are performing well in the market as well as showing Innovation Leadership; while vendors below the line show an ability to innovate though having less market share, and thus the biggest potential for improving their market position.

In the upper right-hand corner box, we find the "Big Ones" in the Passwordless Authentication market. We see (in alphabetical order) CyberArk, ForgeRock, Entrust, HID Global, IBM, Ping Identity, and Transmit Security. These companies are being rewarded by the market for the level of innovation they provide in their products and services.

Microsoft, Thales, RSA, Exostar, and Cisco are shown in the top middle box with a stronger market, although less innovation than the leaders.

Five vendors, 1Komsos, Beyond Identity, HYPR, Futurae Technologies, and Identité, are shown in the middle right box showing good innovation with slightly less market presence than the vendors in the "Big Ones" category.

The segment in the middle of the chart contains a third of the vendors rated as challengers both for market and innovation, which includes (in alphabetical order) Axiad, IDEE, Keyless Technologies, Nevis Security, OwnID, SAASPASS, Telefonica, and tru.ID. Keyless, tru.ID, and Axiad.

4 Products and Vendors at a Glance

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

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	Deployment	Interoperability	Usability
1Kosmos BlockID Workforce and BlockID Customer	🟢	🟢	🟢	🟢	🟢
Axiad Cloud	🟩	🟢	🟩	🟩	🟩
Beyond Identity Secure Workforce and Secure Customers	🟢	🟢	🟩	🟢	🟢
Cisco Duo	🟢	🟩	🟩	🟩	🟩
CyberArk Identity Security Platform	🟢	🟢	🟩	🟢	🟢
Entrust Identity	🟢	🟢	🟢	🟢	🟢
Exostar The Exostar Platform	🟢	🟡	🟩	🟡	🟡
ForgeRock Identity Platform	🟢	🟢	🟢	🟢	🟢
Futurae Technologies	🟢	🟩	🟩	🟡	🟩
HID Global Authentication Platform	🟢	🟢	🟢	🟩	🟢
HYPR Passwordless MFA Platform	🟢	🟢	🟩	🟢	🟢
IBM Security Verify	🟢	🟢	🟢	🟢	🟩
IDEE AuthN	🟢	🟩	🟩	🟩	🟢
Identité NoPass for Employees and NoPass for Consumer	🟩	🟩	🟩	🟡	🟢
Keyless Technologies Workforce and Consumer	🟩	🟡	🟩	🟡	🟩
Microsoft Azure Active Directory	🟢	🟢	🟩	🟩	🟢
NEVIS Security Identity Suite and Authentication Cloud	🟢	🟩	🟩	🟩	🟩
OwnID	🟩	🟡	🟢	🟩	🟢
Ping Identity PingOne Cloud	🟢	🟢	🟢	🟢	🟢
RSA SecurID	🟢	🟩	🟢	🟩	🟢
SAASPASS IAM	🟩	🟩	🟡	🟢	🟢
Telefónica Tech Number Verify	🟡	🟡	🟩	🟠	🟩
Thales SafeNet Trusted Access	🟢	🟢	🟩	🟩	🟩
Transmit Security CIAM Platform	🟢	🟢	🟢	🟩	🟢
tru.ID SIM-based Authentication SDK and SIM-based Authentication App	🟡	🟡	🟩	🟠	🟩

Product	Security	Functionality	Deployment	Interoperability	Usability
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
1Kosmos	🟩	🟡	🟢	🟡
Axiad	🟢	🟡	🟢	🟡
Beyond Identity	🟩	🟢	🟢	🟩
Cisco	🟢	🟩	🟩	🟩
CyberArk	🟩	🟩	🟢	🟩
Entrust	🟩	🟩	🟩	🟩
Exostar	🟡	🟩	🟩	🟢
ForgeRock	🟩	🟩	🟩	🟩
Futurae Technologies	🟩	🟡	🟡	🟡
HID Global	🟩	🟩	🟩	🟩
HYPR	🟩	🟢	🟢	🟢
IBM	🟩	🟩	🟩	🟩
IDEE	🟢	🟡	🟡	🟡
Identité	🟩	🟡	🟡	🟡
Keyless	🟢	🟡	🟡	🟡
Microsoft	🟢	🟩	🟩	🟩
NEVIS Security AG	🟢	🟡	🟡	🟡
OwnID	🟢	🟢	🟡	🟢
Ping Identity	🟩	🟩	🟩	🟩
RSA Security	🟡	🟩	🟩	🟩
SAASPASS	🟢	🟡	🟡	🟢
Telefónica Tech	🟡	🟢	🟢	🟡
Thales	🟢	🟩	🟩	🟩
Transmit Security	🟩	🟩	🟢	🟩
tru.ID	🟡	🟡	🟠	🟡
Legend	🔴 critical	🟠 weak	🟡 neutral	🟢 positive 🟩 strong positive

Table 2: Comparative overview of the ratings for vendors

5 Product/Vendor evaluation

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

Spider graphs

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

- **Account Recovery**
  This rating is based on how solutions handle account recovery procedures. The solution must make it easy for end users to securely recover access without contacting a call center or visiting a store when they need it.
- **Architecture and Deployment**
  This category represents the combination of the architecture and the deployment options. In architecture, we look at the type of architecture and focus on modern, modular architectures based on microservices. This also affects deployment, given that container-based deployments provide good flexibility.
- **Authenticator support**
  This section looks at the breadth of authentication support, as well as the depth of contextual and risk-adaptive authentication. Advanced support for authentication mechanisms, especially FIDO, mobile, and behavioral biometrics and mobile SDKs are also preferred.
- **APIs**
  This category is related to the architecture but focuses more on the comprehensiveness of APIs and the simplicity of customization. This also evaluates the level of API security and the need for stable APIs. APIs furthermore build the foundation for providing an Identity API Layer to digital services and for orchestration with other services.
- **Device Trust**
  In a passwordless solution, this is an essential component. Device trust is the process of verifying whether a device (or multiple devices) should be trusted and authorized to perform certain tasks. This rating is influenced by factors including support for multiple devices, device health checks, and support for BYOD.
- **IAM support**

This section evaluates the number of IAM capabilities and features. Furthermore, supporting existing applications and integrating the legacy IAM platforms is essential for a migration towards a modern Passwordless Authentication at the pace of the customer. Thus, supporting legacy IAM and legacy applications is an important element in our rating of solutions that deliver a passwordless approach.

- **Scalability**
  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.

5.1 1Kosmos

1Kosmos was founded in 2018 and is headquartered in New Jersey. With its innovative blockchain ID solution, the company offers digital identity and passwordless authentication solutions for enterprises and consumers. The BlockID platform provides a suite of products for enterprise use (BlockID Workforce), private consumer use (BlockID Customer), and identity verification (BlockID Verify). The BlockID platform unifies identity proofing and passwordless authentication, including SIM (subscriber identity module) binding capabilities that prevent online fraud and account takeover. Coverage includes North America, Western Europe, Middle East, India, Singapore, and Australia.

BlockID as SaaS supports public and private cloud and hybrid deployment models. In addition to the rapid deployment and user adoption, the Block ID platform supports legacy systems and multiple authentication channels with a high level of flexibility and scalability. For their workforce offering, BlockID Workforce introduces identity proofing and onboarding features which allow employees to enroll their biometric credentials to login. The solution encrypts each user's biometric data with their own cryptographic key pair, storing the private key in their device's secure enclave. BlockID Customer provides biometric passwordless authentication with optional identity proofing that can adjust to flexible levels of identity assertion to support the evolving needs of customers while maintaining access to multiple accounts via one consistent experience.

The BlockID platform also supports contextual and risk-adaptive authentication including device, user, network, and geolocation-based attributes that could be used to augment enterprise-grade access policies. Furthermore, the platform provides APIs for its proofing, authentication, and access management mechanisms. Supported API protocols include REST, SOAP, JSON-RPC, GRPC, SCIM, and Webhooks. To strengthen security and support compliance, 1Kosmos has been independently certified with the ISO/IEC 27001 and EIDAS standards, as well as certified by FIDO2, NIST 800-63-3, and is currently undergoing SOC 2 Type II.

1Kosmos positions itself as an interesting alternative to the established offerings supporting mid-market to enterprise organizations. However, being a rather small vendor, 1Kosmos has a still relatively small global partner ecosystem. On the other hand, the company is very innovative and provides a modern solution that fits well to the requirements of a Passwordless Authentication solution. 1Kosmos appears in both the product and innovation leadership categories which should be of interest to organizations in North America and the APAC regions.

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

1KOSMOS

Strengths

- Identity proofing and onboarding capabilities
- Strong and well-documented set of APIs
- Various innovative features, such as the use of a private blockchain to store data
- Risk-adaptive authentication
- Flexible account recovery options
- FIDO 2 certified

Challenges

- Global partner ecosystem is growing, but still not very large
- Customer presence is still primarily focused in North America
- SCIM based provisioning not currently supported
- SOC 2 Type II certification in work

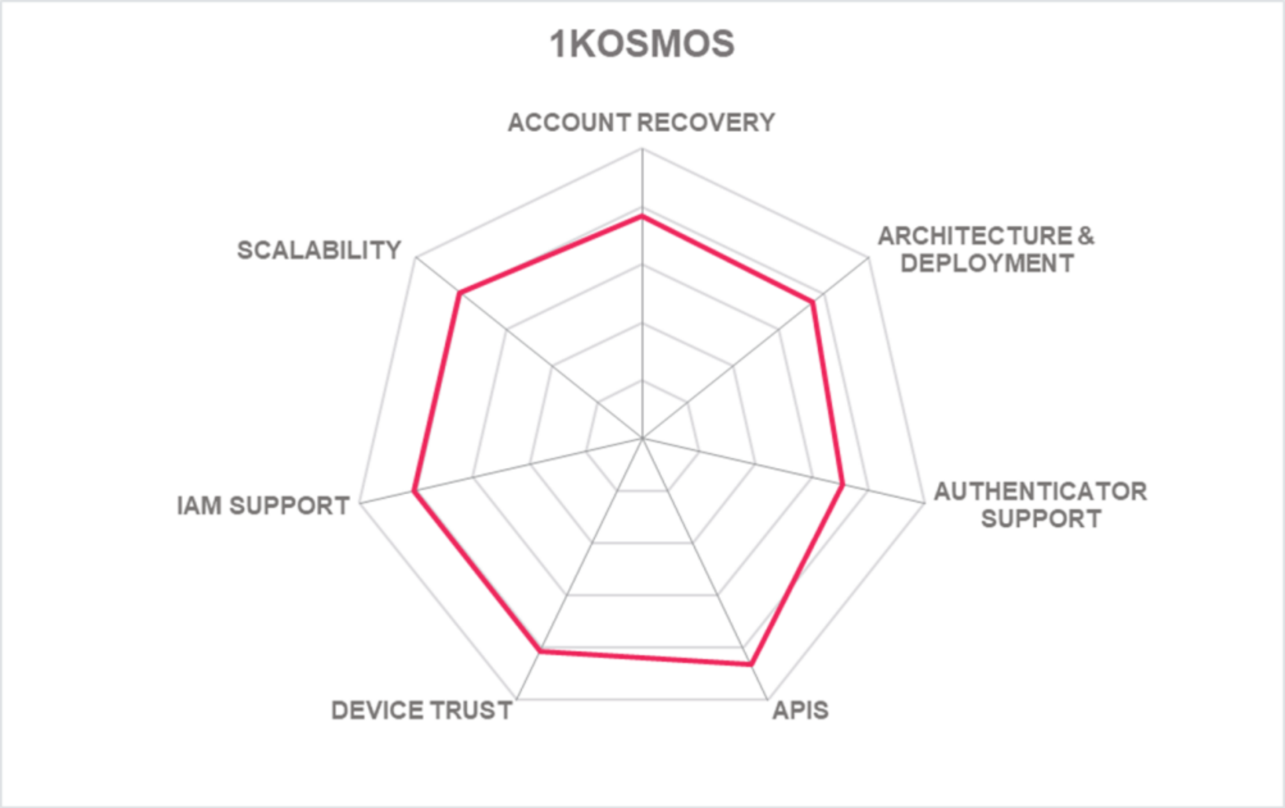
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


1KOSMOS
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.2 Axiad

Axiad, founded in 2010, is an established and trusted player in the passwordless and IAM market. The company is based in Santa Clara, California with additional offices in Canada and India. Axiad's sweet spot is the mid-market and large enterprises in North America and the EMEA region. Their solution Axiad Cloud is an integrated authentication platform that delivers passwordless authentication in a holistic manner for enterprise, government, healthcare, insurance, and financial use cases.

The solution supports a wide range of credentials including YubiKey and smart cards and modules such as authentication, enterprise PKI, Unified Credential Management, and passwordless/MFA. Axiad Cloud provides an interesting offering called Airlock. With Airlock, customers can enforce and control the rollout of passwordless to their end users using an endpoint client. This feature integrates easily with a company's existing IAM infrastructure and can be customized to ensure that users are following the company's security policies.

Furthermore, Axiad Cloud also enables peer-to-peer credential management support with a feature called MyCircle which effectively crowd-sources helpdesk actions to co-workers. In essence, this identity proofing solution allows co-workers to assist in resetting PINs, renewing a token, or verifying credentials. For overburdened IT teams, this offering delivers a cost-effective and secure solution without having to engage with the helpdesk.

As a SaaS solution, Axiad Cloud is low touch and provides a seamless and rich set of self-management tools for end users and administrators. In addition, the platform has interoperability with most large identity providers (IdPs) such as Azure Active Directory and any SCIM 2.0 compliant provider. Common standards and protocols such as SAML, Open ID Connect, and OAuth are also supported. Axiad is ISO 27001/27018 and SSAE SOC 2 Type2 certified.

Axiad Cloud provides a secure and simplified single platform that allows customers to address authentication in a holistic fashion. In sum, any organization that is looking for modular authentication services, credential management, or remote onboarding and integration may want to take a look at Axiad capabilities in this area.

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

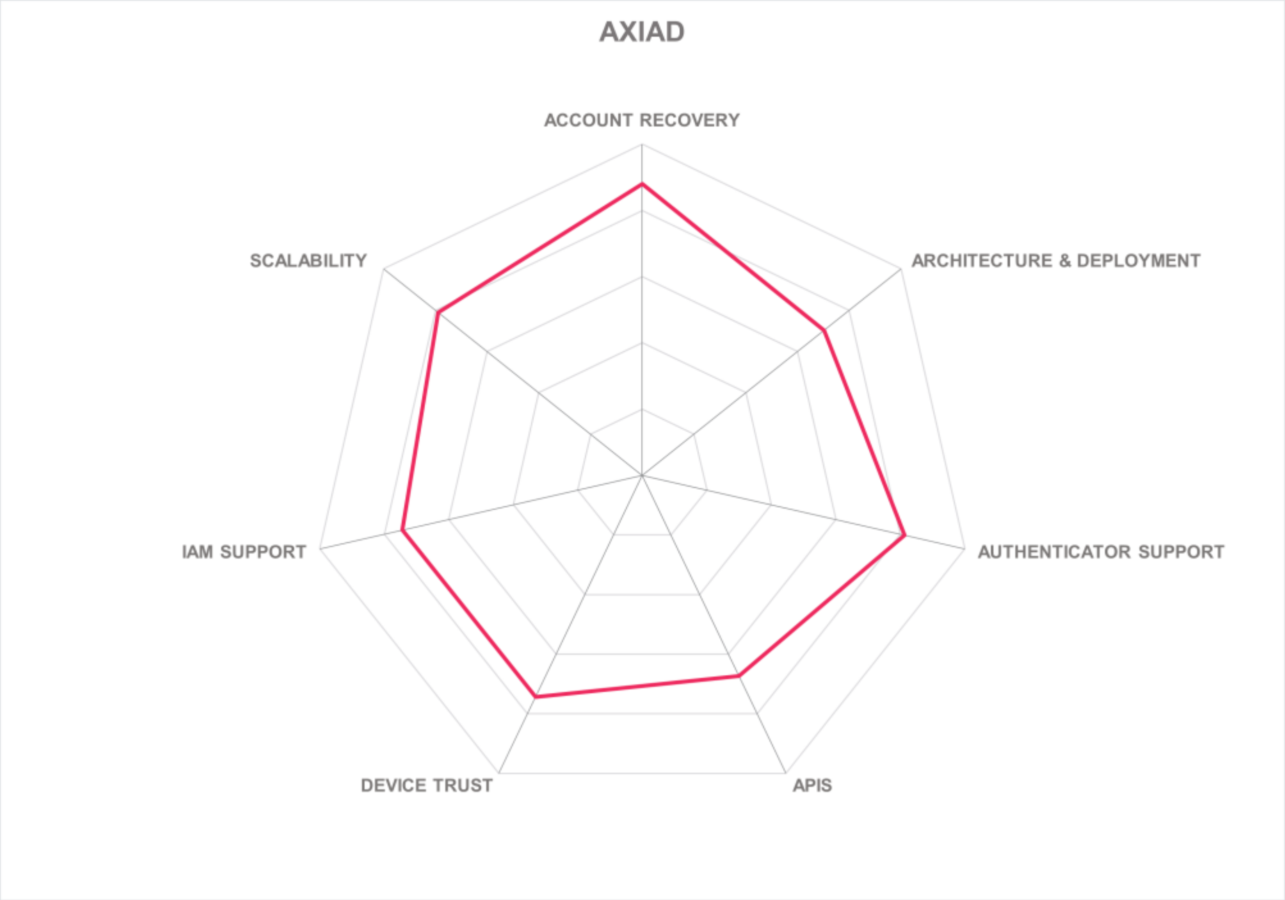
axiad

Strengths

- Good set of capabilities for identity proofing
- Endpoint client that allows customers to enforce the rollout of passwordless MFA
- Friendly solution for Hybrid and BYOD scenarios
- Self-service access through a single portal
- Credential management

Challenges

- Smaller company but rapidly expanding
- No connectors to identity vetting services but improvements are on the roadmap
- Lack of risk-based access controls


AXIAD
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.3 Beyond Identity

Beyond Identity was founded in 2019. They are headquartered in New York and have offices and customers around the world. As an innovator in passwordless MFA solutions, Beyond Identity aims to lay the foundation of a passwordless future by eliminating passwords and other phishable factors. The company offers a broad range of capabilities supporting passwordless MFA, device trust, and risk-based authentication.

Beyond Identity's capacity to deliver a cryptographic method to validate the identity of a person using multiple devices, including unmanaged devices and BYOD, in real time is a key advantage. Their workforce offering, Secure Workforce, enforces device trust by combining an identity device-bound solution together with real-time device checks for secure access. The solution validates that each device is registered to a known and authorized user via validation of private key possession within the device hardware enclave and by assessing whether the device meets the security requirements in real-time and continuously during authenticated sessions. Secure Workforce replaces passwords with secure credentials based on their patent-pending solution that uses self-signed certificates and public-private key pairs.

Secure Customers, their CIAM offering, is a cross-platform passwordless authentication solution that allows businesses and organizations to provide consumers with a frictionless authentication experience without passwords, push notifications, one-time codes, and second devices for native mobile and web applications running on any device and platform. The solution is deployed through embeddable SDKs, which are available for both native mobile and web applications. This allows companies to deliver a branded first-party native experience across all their applications to accelerate conversions throughout the user journey while providing protection from account takeover fraud.

The solution is compliant with PSD2 Strong Customer Authentication. In addition, Beyond Identity uses an API-first and standards-based approach which integrates easily with other Access Management solutions, identity proofing solutions, and endpoint security tools such as Okta, Auth0, Ping Identity, ForgeRock, Microsoft Azure AD, and Microsoft ADFS (for on-prem or hybrid deployments).

By adopting Beyond Identity's passwordless MFA, users are protected against phishing and ransomware attempts by using authentication factors that cannot be easily manipulated by attackers. It is not possible to go passwordless in a single step, however Beyond Identity makes it easier for organizations to connect a passwordless solution to a SSO system. Overall, Beyond Identity appears in both the product and innovation leadership categories.

BEYOND IDENTITY

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

Strengths

- Friendly user experience
- Built to work well for users with multiple devices
- Strong authentication method with public-private key pairs
- Control access based on continuously analyzing device risk signals
- No need for maintaining an own CA or relying on third-party CAs
- A collection of SDKs in popular development languages

Challenges

- ISO/IEC 27001 audit not initiated yet
- No support for transaction signing but enhancements are on the roadmap
- Lack of support for legacy systems that continue to rely on passwords

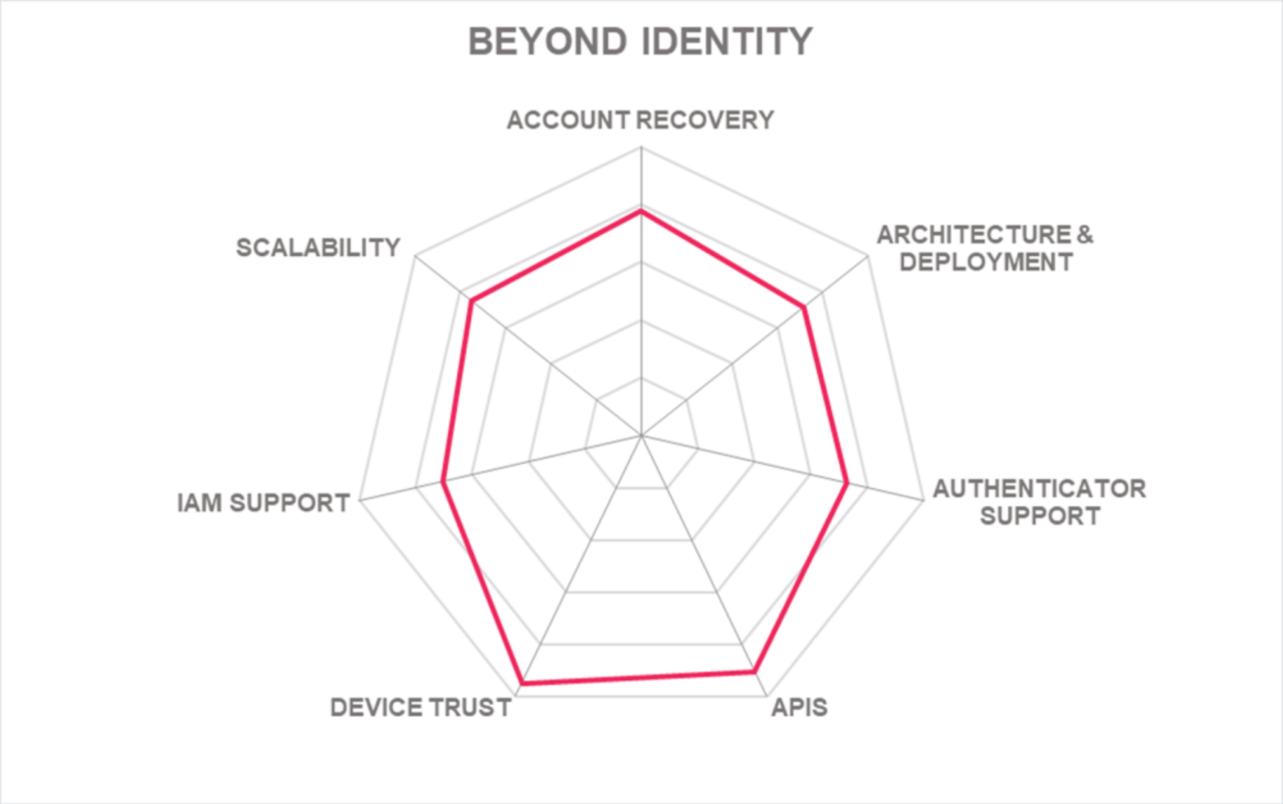
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


BEYOND IDENTITY
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.4 Cisco

Cisco was founded in 1984 and its headquarters are located in San Jose, California. With presence in more than 100 countries, the company has customers in manufacturing, transportation, mining, power utilities, oil & gas, and water utilities sectors. The name of the product is Duo Security, and it is a fully multi-tenant SaaS security solution focused on the workforce. The solution provides secure access to applications and data, no matter where users are -- on any device. Duo's Zero Trust access for the workforce includes: authentication of users (MFA and passwordless), verifies devices (real time posture check on Mac, Windows, iOS, and Android), and enables access (SSO and VPN-less remote access). Licensing options include a per user and per month subscription charge.

For authenticating users, Duo has traditionally been associated with providing MFA in a variety of different ways including wearables, FIDO2 keys, SMS, hardware tokens, biometrics, push via their mobile app, and passwordless. The solution offers customer access policies that evaluate contextual access patterns and leverage anomalies to remediate compromised credentials. Duo also makes sure that each registered device is registered to a known and authorized user by continuously verifying whether or not the device meets the security requirements. The solution assesses the device security posture by checking the operating device, biometric authentication and firewall enablement, encryption status, up to date software, etc.

Furthermore, administrators using Duo get full control in deciding whether or not to enable passwordless on Duo's policies. They have the flexibility to use group-based policy, application-based policy, or global-based policy (all application and users). Admins also have the ability to turn on or off the password option as fallback which provides a convenient escape patch for those use cases. Cisco has been independently certified with the ISO/IEC 27001 and SOC 2 Type II, as well as certified by FIDO2, NIST 800-57 Key Management, and PCI-DSS v 3.2.

Duo's strong, dynamic risk-based authentication ensures that access policies can be consistently enforced for any user and any application to match even the most business-critical security requirements. Overall, Duo's adaptive MFA creates trust in users, devices, and the work applications they access. It integrates easily with any identity provider and reduces reliance on passwords. For organizations that utilize Cisco solutions, the Duo platform is a compelling case for workforce access, remote work, and hybrid scenarios.

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

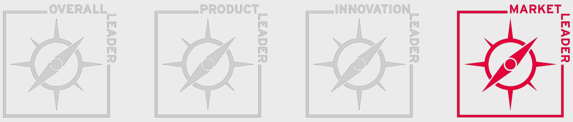
Strengths

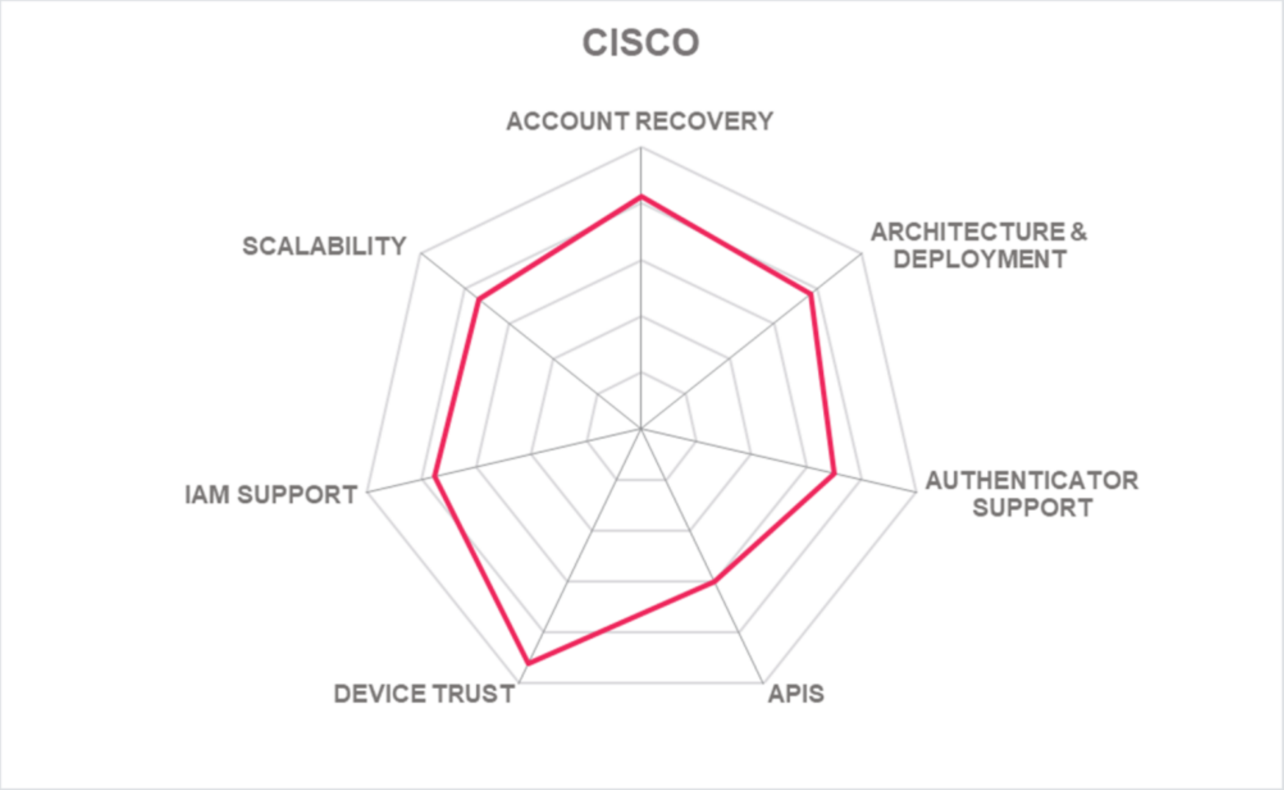
- Strong presence and global partner ecosystem
- Multiple security certifications
- Duo’s integration with Cisco WebEx
- Good protocol support: SAML, OAuth2, and OpenID Connect
- Out-of-the-box integration with Windows Hello and Windows Hello for Business
- Strong device trust and risk-based authentication capabilities

Challenges

- Lack of omni-channel capabilities
- The solution does not provide SDKs
- No connectors to identity vetting services
- SCIM based provisioning not currently supported

Leader in




CISCO
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.5 CyberArk

Having been in the market since 1999, CyberArk has established itself as a leader in Identity Security. CyberArk helps companies protect their highest-value information assets, infrastructure, identities, and applications. Headquartered in Israel and the US, CyberArk has offices in the U.K., France, Germany, the Netherlands, India, and Singapore and serves customers in more than 65 countries. Since the acquisition of Idaptive in May 2020, a spin-off of Centrify, the company has continued to add technical functionalities to its broad suite of products in response to changing market demands.

CyberArk has a compelling solution for passwordless authentication for all types of identities including human (employees, customers, vendors, partners, etc.) and machine (passwordless authentication for machine-to-machine communication) for the workforce and DevOps. CyberArk Identity Security Platform is a fully cloud hosted SaaS-delivered service. However, CyberArk does offer multiple paths to integrate with on-prem environments and even offers the ability to store user secrets in a self-hosted vault. The platform is composed of security services such as Single Sign-on, Adaptive MFA, Analytics & Reporting, User Lifecycle Management, Directory Services, and Endpoint authentication.

CyberArk Identity provides the ability for users to easily register their device via email, SMS, or QR code scan in a completely passwordless fashion for all possible applications. Furthermore, CyberArk supports hardware tokens, CAC/PIV card, Duo, Feitian, Google Titan, Kensington Security Key, OneSpan DigiPass, RSA SecurID, Smartcards, Symantec VIP, Thetis, and Yubikey tokens. In addition, CyberArk supports FIDO2 standards and also integrates with many other vendors through other standards such as OATH HOTP/TOTP, RADIUS, SAML, and OIDC.

Overall, CyberArk Identity offers an advanced and scalable solution for continuous passwordless authentication with minimal interference to the end users. Moreover, the solution has deep integration with CyberArk PAM which allows customers to get the platform offering when they use CyberArk for PAM, IAM, and passwordless authentication. CyberArk appears in the product, market, and innovation leadership categories. This makes CyberArk an interesting option for organizations seeking a comprehensive, feature-rich, and modern passwordless solution.

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

CYBERARK®

Strengths

- Convenient solution for remote access and BYOD scenarios
- Flexible deployments
- Large selection of authenticators accepted
- Integration with CyberArk PAM
- Strong partner ecosystem
- Proven scalability

Challenges

- No support for portable identity
- No support for device roaming
- Limited capabilities for biometric verification but enhancements are on the roadmap

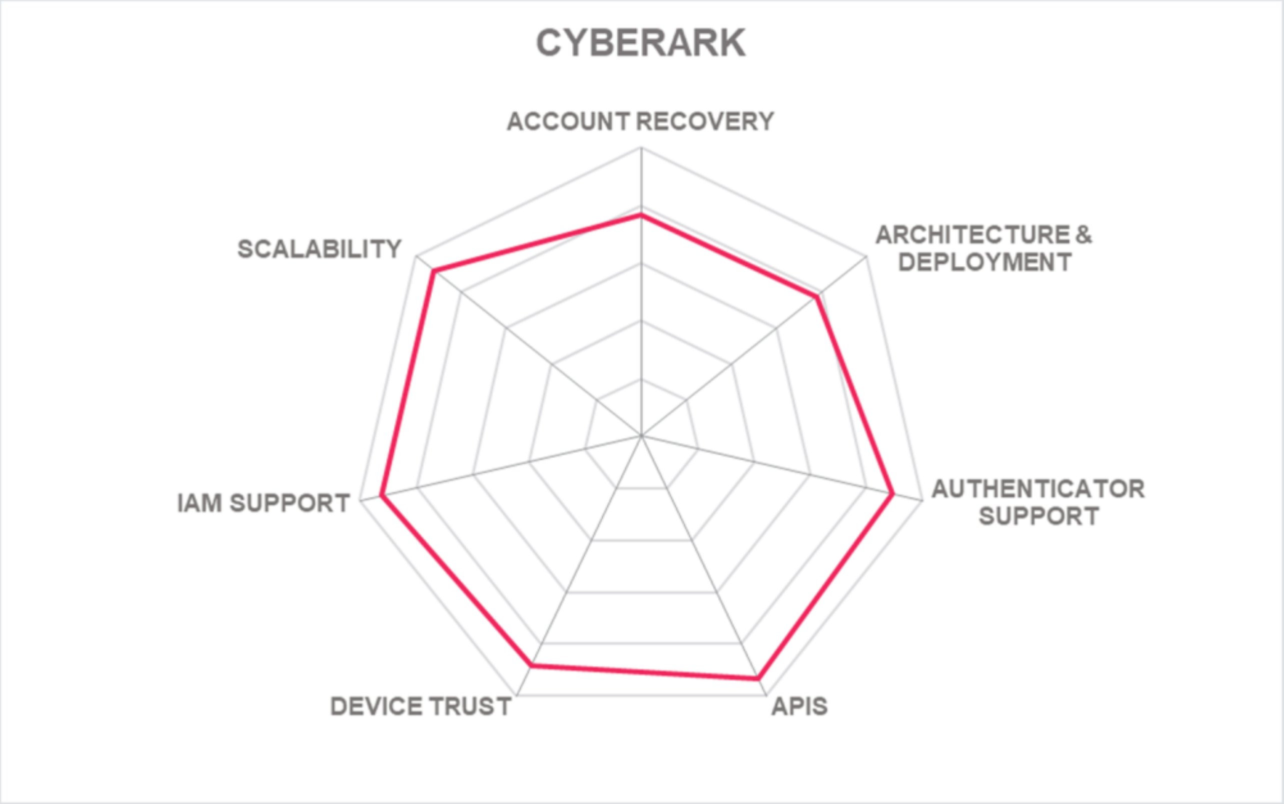
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


CYBERARK
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.6 Entrust

Entrust, formerly known as Entrust Datacard, is a well-established vendor and trusted by leading customers in finance, government, healthcare, insurance, and enterprise use cases. The company provides identity-based security software and services in the areas of public key infrastructure (PKI), multi-factor authentication, and fraud detection for those looking to access secure networks, connected devices, or conduct financial transactions. Headquartered in Minneapolis, MN, Entrust also has offices in London, Tokyo, Washington, D.C., and other cities internationally.

Entrust Identity is the unified authentication portfolio: IDaaS is the Cloud based SaaS IAM offering, the former Identity Guard is now Identity Enterprise, and SMS PASSCODE is now known as Identity Essentials. Entrust Identity is a cloud-based IAM platform that facilitates multi-factor authentication (MFA), FIDO2 and credential-based passwordless access, single sign-on (SSO), and more. The platform has three product lines for workforce, consumer, and citizen use cases. It is an all-in-one user authentication and authorization solution with flexible cloud, hybrid, and on-premises deployment models that helps organizations implement a passwordless approach.

Entrust accepts multiple authentication methods, including Authy, FIDO, their own Entrust app and Derived PIV credentials app. Moreover, the platform supports CAC/PIV card, Duo, Feitian, Google Titan, Kensington Security Keys, Smartcards, Thetis, Yubikey tokens, and any OATH compliant hardware tokens. API protocols include SOAP, REST, SCIM, RADIUS, and LDAP. Other protocols supported include JWT, Kerberos, OAuth, OIDC, and SAML.

With Entrust Identity, credentials can be tailored to meet the needs and preferences of users by issuing credentials that utilize their mobile device, including mobile push authentications, one-time passwords (OTPs), FIDO keys or smart credentials secured by PKI. The platform also includes an innovative proximity-based authentication capability that allows for email signing and encryption. In addition, Entrust Identity adaptive risk engine evaluates device type, IP address, geo-location and velocity, and user attributes to assess whether the security posture of the device meets security and compliance requirements.

Entrust appears in the product, market, and innovation leadership categories. In sum, Entrust has a global partner ecosystem and presence that help in delivering their solutions. Entrust Identity has an innovative set of capabilities for customers who need high security assurance. For organizations that broadly utilize Entrust solutions, the Entrust Identity as a Service is an interesting option for organizations wishing to eliminate the reliance on passwords and the inconvenience of legacy MFA.

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

ENTRUST

Strengths

- Global partner ecosystem
- Good admin interface
- Microservice architecture
- Risk based adaptive step-up authentication
- Derived PIV / Smartcard on mobile app support
- Proximity-based high assurance passwordless login

Challenges

- SOC 2 Type II not obtained yet
- Limited Identity Orchestration capabilities but enhancements are on the roadmap

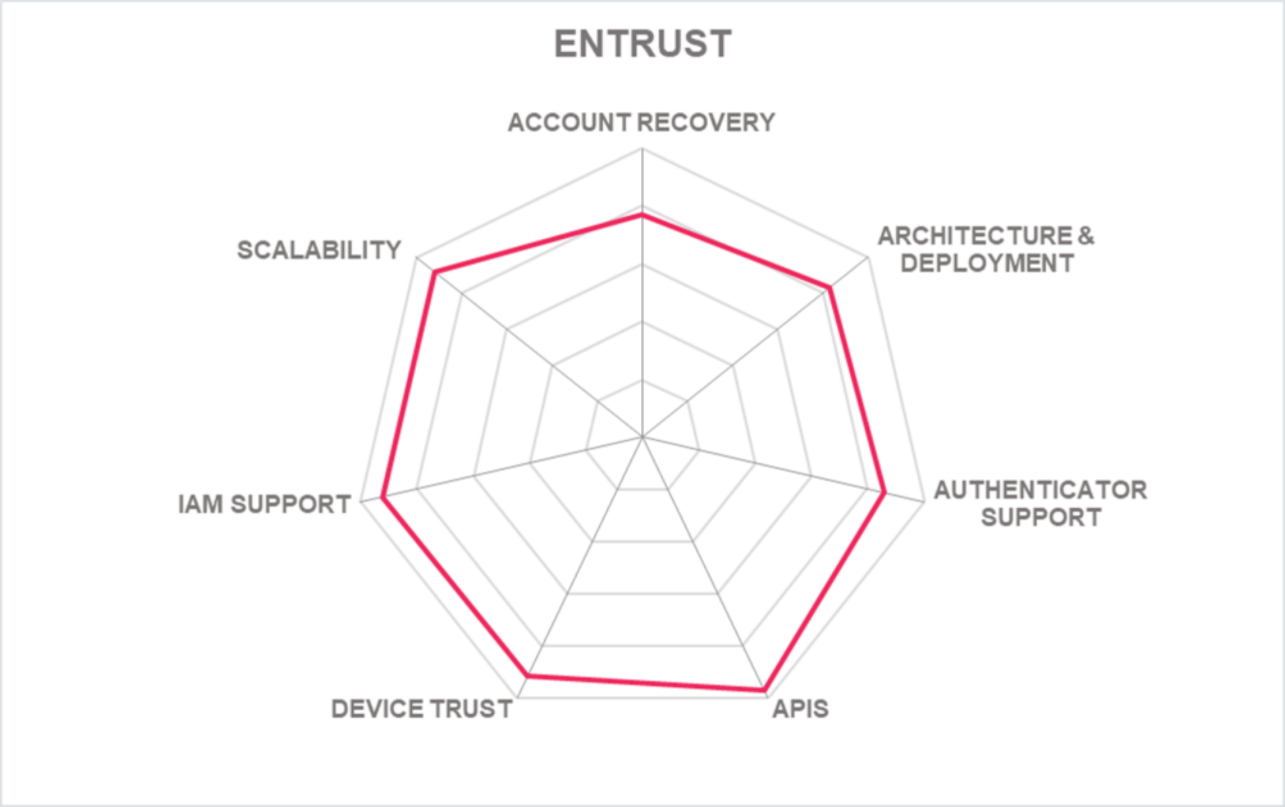
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


ENTRUST
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.7 Exostar

Exostar was founded in 2000. Its headquarters are located in Herndon, Virginia, with additional development centers in the UK and Bangalore, India. The company is a leader in secure, compliant cloud-based solutions that improve collaboration, information sharing, and supply chain management for many organizations in 175 countries. Exostar is a steward of communities in highly regulated industries such as defense, aerospace, life sciences, healthcare, and financial services. The Exostar Platform's Onboarding and Secure Access modules deliver identity and access management, onboarding, identity proofing, credentialing, and lifecycle management into their own, third party, and customer hosted applications or SaaS applications. With The Exostar Platform, Exostar can onboard organizations and individuals very rapidly, delivering a connect-once, single sign-on, passwordless authentication experience for application owners and internal/external app users.

Exostar has provided passwordless capabilities for years, dating back to before passwordless became a market term. A primary example is The Exostar Platform's support for passwordless authentication via hardware tokens for the defense industrial base sector. The Exostar Platform provides access to applications that either Exostar or its customers run and manage. The Exostar Platform's Applications module includes third party applications, portals to customer applications, and Exostar applications that span identity management, secure collaboration, supply chain and supplier management, and governance, risk, and compliance. In addition, Exostar hosts applications in environments such as Microsoft's Government Cloud Computing (GCC) High (supporting cybersecurity requirements mandated by the U.S. Department of Defense that agencies, cleared personnel, and all contractors throughout the DoD supply chain in the U.S., the UK, and worldwide must meet). However, Exostar does not do device management because it does not align with the demands and operating requirements of their customers.

Nevertheless, Exostar provides innovative identity proofing capabilities and validation services for high-assurance environments, supports PKI and two-factor authentication services such as one-time passwords (OTP), mobile-based push authentication, smartcards, and other forms of enterprise identity. Moreover, Exostar is a Certification Authority and has been named a full-service credential service provider by the Kantara Initiative. Exostar also supports JWT, Kerberos, OAuth2, OIDC, and SAML tokens/protocols.

Exostar is different than the other vendors because they are focused on highly regulated industries. They might do fewer things but do them really well and are much more focused. Furthermore, Exostar continues to add innovative features to The Exostar Platform; their roadmap includes items such as Adaptive Step-up, Document Verification, and integration with various applications. Exostar and its identity proofing, passwordless, and credentialing capabilities provide a good alternative for customers in complex and highly regulated industries.

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

EXOSTAR®

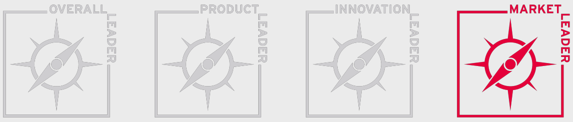
Strengths

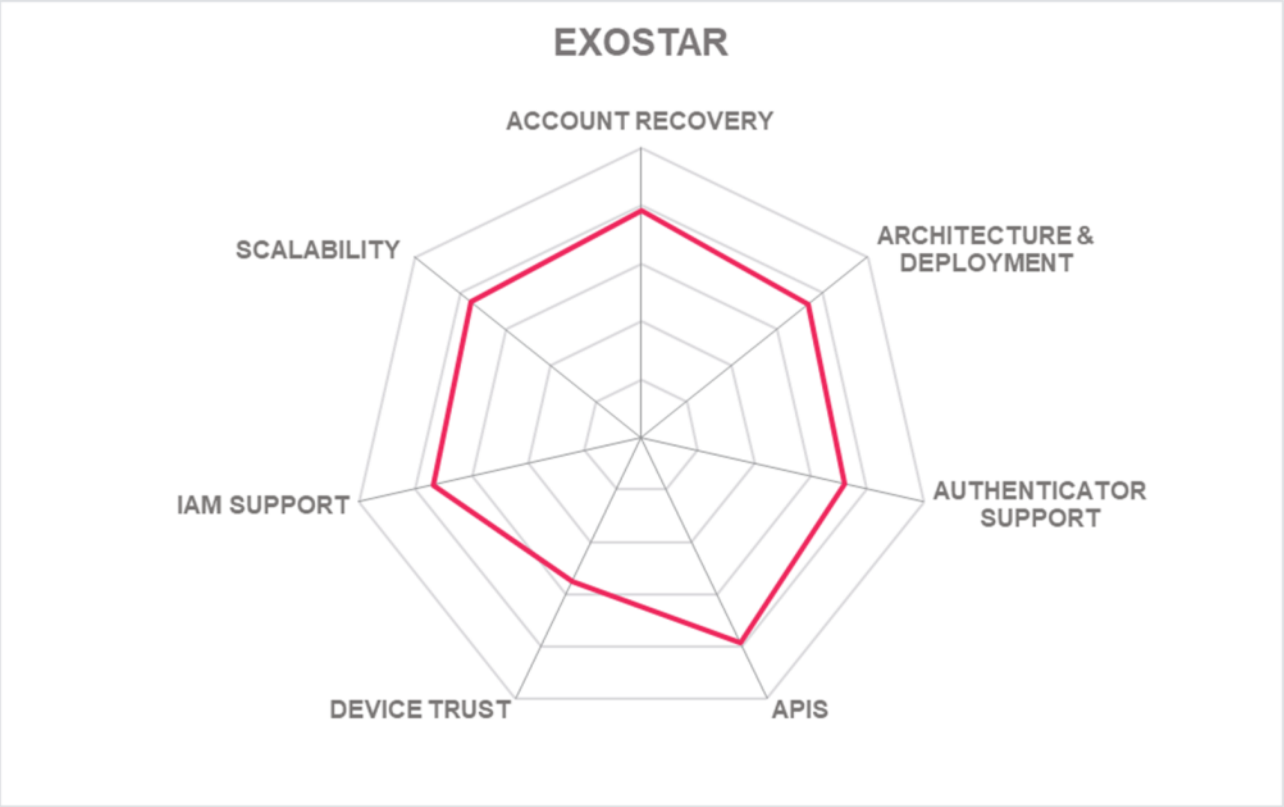
? Strong partner ecosystem and global presence
? Good employee onboarding features
? Flexible deployment models
? Complies with the U.S. DoD DFARS 7012 (NIST 800-171) and the U.K. Official Sensitive & Cyber Essentials
? Extensive experience and well-established vendor in highly-sensitive industries
? Strong Identity Proofing capabilities

Challenges

? Push-back from customers when introducing passwordless in highly regulated industries
? Lack of omni-channel capabilities
? No support for dynamic scaling but enhancements are on the roadmap
? No specific support for device trust on multiple devices

Leader in




EXOSTAR
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.8 ForgeRock

ForgeRock was founded in 2010 and is headquartered in the Bay Area but with many offices around the world. The ForgeRock Identity Platform unifies the various IAM solutions provided by ForgeRock, such as Access Management, Identity Management, IoT/Edge Security, Identity Gateway, Identity Governance, Privacy & Consent Management, and other components including Directory Services. In addition, ForgeRock has a strong expanding partner ecosystem. The ForgeRock Trust Network is a technology alliance program and partner channel that consists of approximately 130 partners who build, test, and integrate various capabilities including Strong Authentication, Biometric ID, Risk and Fraud Mitigation, and Identity Proofing into the ForgeRock Identity Platform.

Their Identity Platform serves both B2E and B2C markets and primarily targets CIAM and Workforce use cases for large enterprise customers. ForgeRock features a highly modular and flexible architecture with multiple plugin points to meet any customer deployment. The platform can be deployed on-premises, in any IaaS environment, or in the cloud (including in as a SaaS) and can co-exist in a hybrid or multi-cloud fashion. All ForgeRock services and capabilities are available via a developer-friendly REST API, but in addition to this, ForgeRock provides SDKs for web applications, mobile applications (iOS and Android) and IoT Devices (Go).

Intelligent User Journeys and Intelligent Access are the services which facilitate passwordless authentication in ForgeRock Identity Platform. These features allow registration flows to be embedded directly into an authentication journey while creating a seamless way for end-users to register and authenticate at the same time. The solution also provides the ability to create a personalized journey based on customer choice and allows admins to register FIDO2 authenticators to a user's account as part of the authentication journey. Three WebAuthn authentication nodes are included in the platform; one for creating credentials, one for using those credentials, and one for adding information about the FIDO2 device to a user's profile for later authentication. WebAuthn nodes support Windows Hello, Touch ID, and any FIDO or U2F security keys such as YubiKeys, Feitian, Titan, etc.

ForgeRock supports CAC/PIV card, Duo, Feitian, Google Titan, OneSpan DigiPass, RSA SecureID, Symantec VIP, Smartcards, Yubikey tokens, and any OATH compliant hardware tokens. API protocols include SOAP, REST, Webhooks, GRPC, and LDAP. Other protocols supported include JWT, RADIUS, Kerberos, OAuth, OIDC, and SAML. With its many innovative features and flexible architecture, ForgeRock Identity Platform should be on the short list for organizations considering deploying passwordless authentication solutions. ForgeRock appears in the product, market, and innovation leadership categories.

ForgeRock

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

Strengths

- Global partner ecosystem
- Strong features for Access Management
- Excellent orchestration capabilities
- Highly scalable microservices architecture
- Broad range of passwordless authenticators accepted
- Comprehensive set of APIs

Challenges

- No integration with UEM solutions
- Risk analysis engine is not addressable via APIs, but improvements are on the roadmap
- FIDO supported but not certified

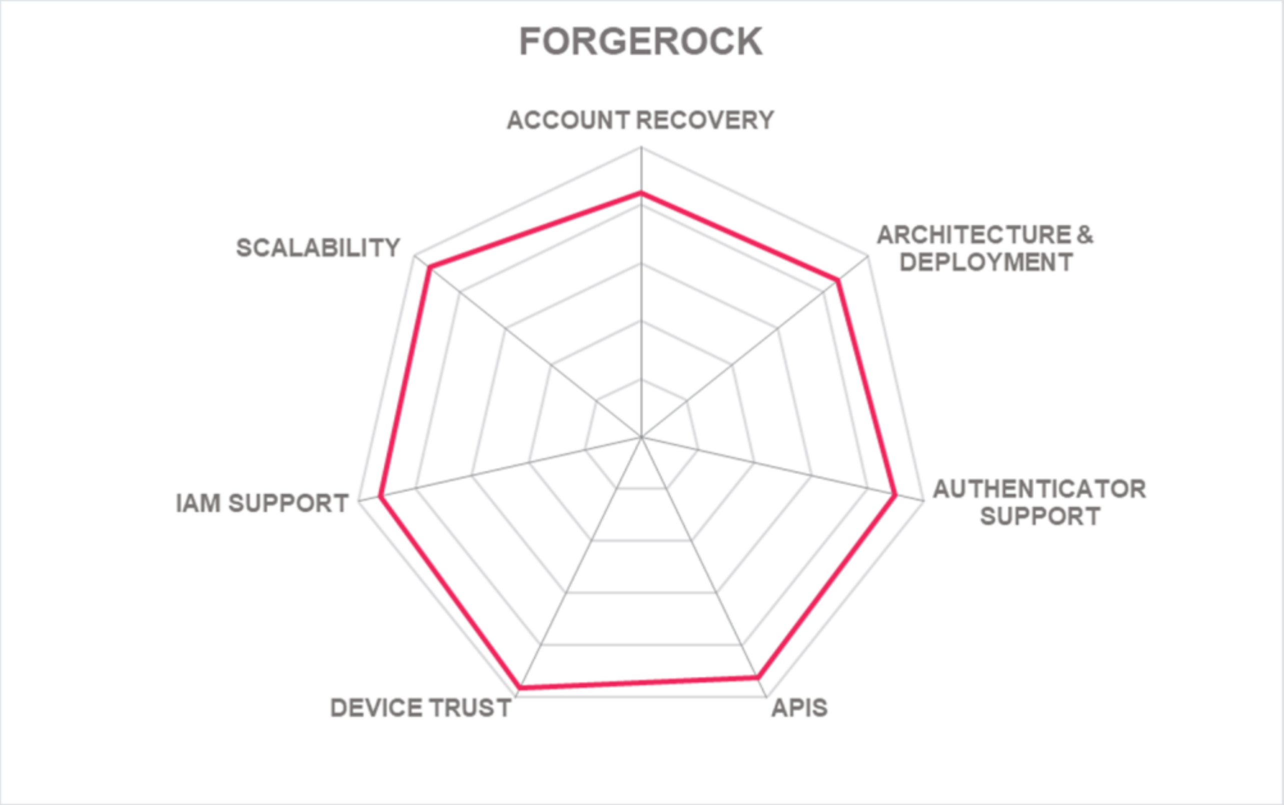
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


FORGEROCK
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.9 Futurae Technologies

Futurae was created in 2016 as an ETH-Zurich spin-off. Futurae's founders have a background in cybersecurity and usability research in academia which sets them apart from most competitors. The company is a provider of MFA and transaction confirmation solutions focused on the global financial industry and expanding to other verticals. The Futurae Authentication Platform delivers a high level of flexibility with a deep focus on user experience for organizations of all sizes, from agile tech companies to established enterprises.

Among its wide range of offers, the company offers a passwordless authentication experience using the authenticator app approach. The user receives a push notification or alternatively, the user scans a QR code which then prompts the user to approve the login. The solution offers easy enrollment and migration of mobile devices. The automatic account recovery feature (also known as account migration) allows users to migrate their security token currently enrolled to a different device or to the same one after deleting and reinstalling the app. This mechanism migrates the account using each platform's (Android/iOS) backup mechanism when the previous app installation had enrolled the account. Hence, it enables the user to recover their accounts in a new app installation automatically by securely storing a recovery token on the device and the Futurae backend, as well as in the device backups. Automatic account recovery solves one of the industry's key drivers for user friction and operational costs.

Moreover, the product allows flexibility with optional security features such as context-based adaptive authentication, PIN (in whitelabel applications, or using the Futurae mobile SDKs), or biometric authentication (e.g., fingerprint or face recognition) whenever such technologies are available on the user's mobile device. The portfolio also offers transaction signing technologies. Futurae's solution for transaction signing follows the "what you see is what you sign" principle and is PSD2 and 3DS2 compliant. In addition, Futurae deployment has been independently certified with the ISO/IEC 27001 and SOC 2 Type II, as well as certified by FIDO2, ISO 9001:2008, and PCI-DSS v 3.2. Futurae offers API-based integration compatible with all modern IAMs and core-banking systems, and also supports FIDO2, RADIUS, OAuth, OIDC, JWT, and SAML.

Further, Futurae offers a comprehensive admin dashboard enabling organization administrators to easily manage services and review user behavior and analytics. Administrators can manage users, devices, the integration, and configure several security and usability settings. The dynamic license management is also fully managed from within the admin dashboard.

Futurae, despite still being a relatively young vendor, has demonstrated its ability to win and serve high-demand customers with a broad set of advanced requirements and needs in different geographies and at different scale. With its comprehensive authentication portfolio, it is an interesting foundation for enabling a passwordless approach specifically for mid-market companies, but also larger organizations looking for an integrated approach with a strong set of capabilities.

FUTURAE

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

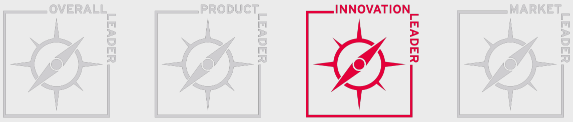
Strengths

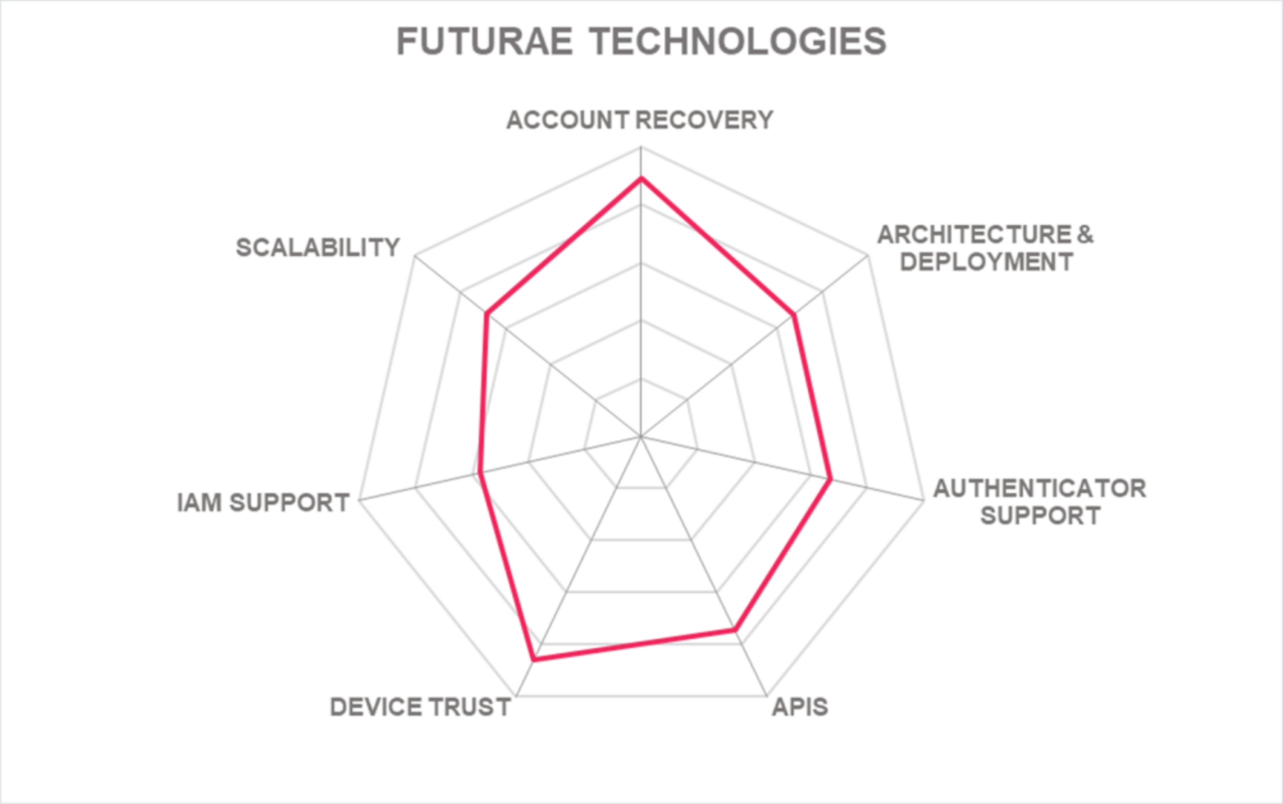
- Good breadth and depth of features, specifically for device management
- Solid capabilities for account migration and automatic account recovery
- Strong support for risk-based analytics
- PSD2 and 3DS2 compliant
- Transaction signing capabilities
- Has obtained multiple relevant security and conformance certifications

Challenges

- Lacks of out-of-the-box support for integrating with Windows Hello for Business
- No interoperability with PAM systems
- Remote access not supported
- Microsoft Azure AD not supported

Leader in




FUTURAE TECHNOLOGIES
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.10 HID Global

HID Global is a subsidiary of ASSA ABLOY Group AB of Stockholm. Assa Abloy AB is a Swedish conglomerate whose offerings include products and services related to locks, doors, gates, and entrance automation. HID Global's US headquarters are located in Austin, TX. With over 4,000 employees worldwide and international offices that support more than 100 countries, the company develops highly secure solutions for identity and access management, including physical access controls, smart identity card manufacturing, credential issuance and management, biometric authentication, and identity proofing.

The HID Global Authentication Platform offering is targeted for workforce, consumers, and partners. It includes on-premises and cloud-based solutions and authenticators like smart card, security key, hardware tokens, biometrics, or mobile authentication solutions to simplify secure identity and access management. The risk and fraud prevention solution paired with the Authentication Platform can evaluate a full range of device intelligence, including device health and history. In addition, HID Global is also in the identity assurance verification, credential issuance and management business. Customers in highly regulated environments can utilize HID Global for authoritative attribute lookups, remote document verification, and electronic credential assignment.

HID Global's cloud-based authentication solutions enable standards-based security by being ISO 27001, ISO 27018, and SOC2 Type 2 certified, and compliant with GDPR and UK-GDPR. For APIs, HID Global supports REST, SOAP, WebAuthn, Webhooks, and SCIM, and CSV/JSON/XML formats. The company also supports the FIDO ecosystem as well as standards such as OAuth, OIDC, RADIUS, and SAML, which can be used to facilitate interoperability with other IAM and IDaaS systems. As a result, HID's authentication services are able to scale to support the specific needs of each go-to-market use case.

Overall, HID Global has been a strong player in government and enterprise workforce IAM for years and is moving more into consumer use cases. HID Global is a solid option for organizations with highly regulated industries, high security requirements, and complex integration. However, even large businesses, in particular outside of the very heavily regulated industries, might benefit from the integrated approach and the flexible deployment options. The company has an excellent reputation for identity and access control products and appears in the product, market, and innovation categories.

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

HID®

Strengths

- Proven scalability
- Modern architecture
- Global partner ecosystem
- Wide range of MFA types
- Secure mobile SDK for device intelligence
- Strong credential issuance and management capabilities

Challenges

- Device roaming not supported but enhancements are being considered
- Lack of compromised credential evaluation capabilities
- Risk and fraud prevention solution lacks interoperability with 3rd party services
- No PAM interoperability

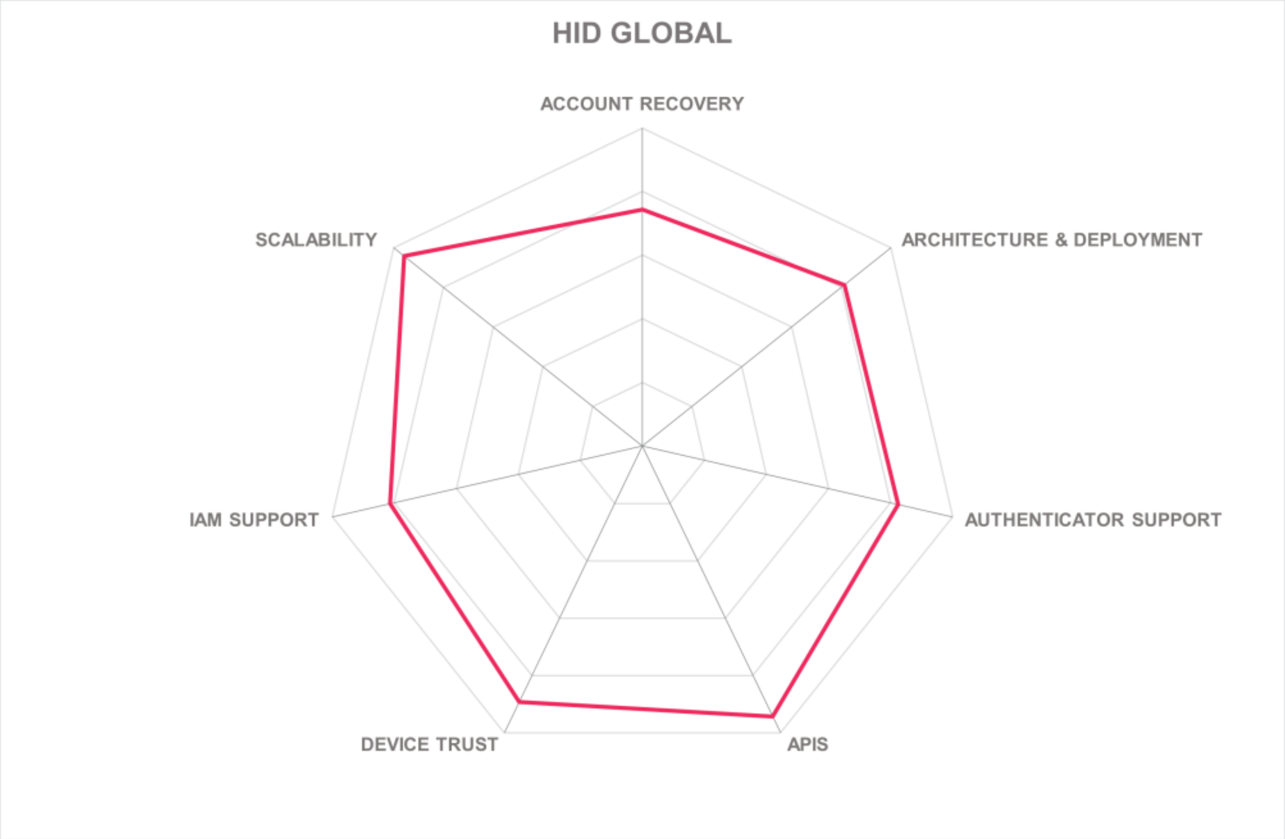
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


HID GLOBAL
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.11 HYPR

Founded in 2014, HYPR is a global company with offices in North America, EMEA, and Asia. With HYPR, secure logins can be performed with its passwordless phishing-resistant MFA solution that identifies users before they even enter the network. In contrast to many other solutions, HYPR integrates with the desktop authentication, securing initial access of users to their systems. Other solutions in this market segment only target access to, e.g., cloud services, but not the authentication event. As a result, the entire path from initial access to a system can be protected at multiple levels. HYPR supports workforce use cases via smartphone app or smart key. For consumers, HYPR offers both mobile app integrations via SDKs, as well as app-less login using the smartphone camera.

The company is also a board member of the FIDO Alliance, helping to drive innovation and adoption of FIDO standards. To eliminate shared secrets and improve security, HYPR's passwordless MFA technology transforms a regular smart device into a secure FIDO authenticator. The HYPR authentication flow is initiated from the smartphone of the user, via the HYPR app. It sends an authentication request to the HYPR cloud, which returns a cryptographic challenge and information about the authentication policy. The solution uses two cryptographic keys: a private key kept secret on the user's mobile device at the hardware-level and a public key stored on the HYPR True Passwordless Server. If this is a verified user, authentication is completed. The HYPR app also provides public key encrypted offline PINs for safe yet simple authentication when there is no internet connection available.

With its support for a wide range of complex use cases and its integration with Microsoft Active Directory and Windows Hello for Business, HYPR also supports a range of common use cases such as kiosk mode (multiple users for one device) or run as administrator mode (one smartphone and device used to authenticate multiple users), as well as support for VDI and RDP (Remote Desktops). HYPR can be integrated / federated with SSO providers: Okta/Auth0, Ping Identity, Microsoft Azure AD, Google Workspace, ForgeRock, and generic OIDC federation with any OAuth / OIDC compliant solution. In addition, the solution also has a Derived PIV Credentials mobile app, and accepts Yubikey, Feitian and any other smart key that is FIDO2 certified.

As part of the partnership with Silverfort and Strata, the solution also supports legacy systems. In sum, HYPR counts amongst the leading-edge solutions for passwordless authentication. The HYPR platform is an excellent choice for customers who need strong desktop authentication or remote authentication for complex use cases. Furthermore, HYPR appears in both the product and innovative leadership categories.

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

HYPR

Strengths

- Full support for FIDO standards
- Good device management features
- Strong portable identity capabilities
- Utilizes strong cryptographic algorithms and secure elements on the smartphone or desktop device
- Secures initial access and delivers protection from the desktop authentication
- Passwordless desktop SSO for both macOS, Windows, and Unix

Challenges

- No support for risk-based access controls but improvements are on the roadmap
- Risk analysis engine not accessible via API
- SCIM based provisioning not currently supported but enhancements are expected later this year

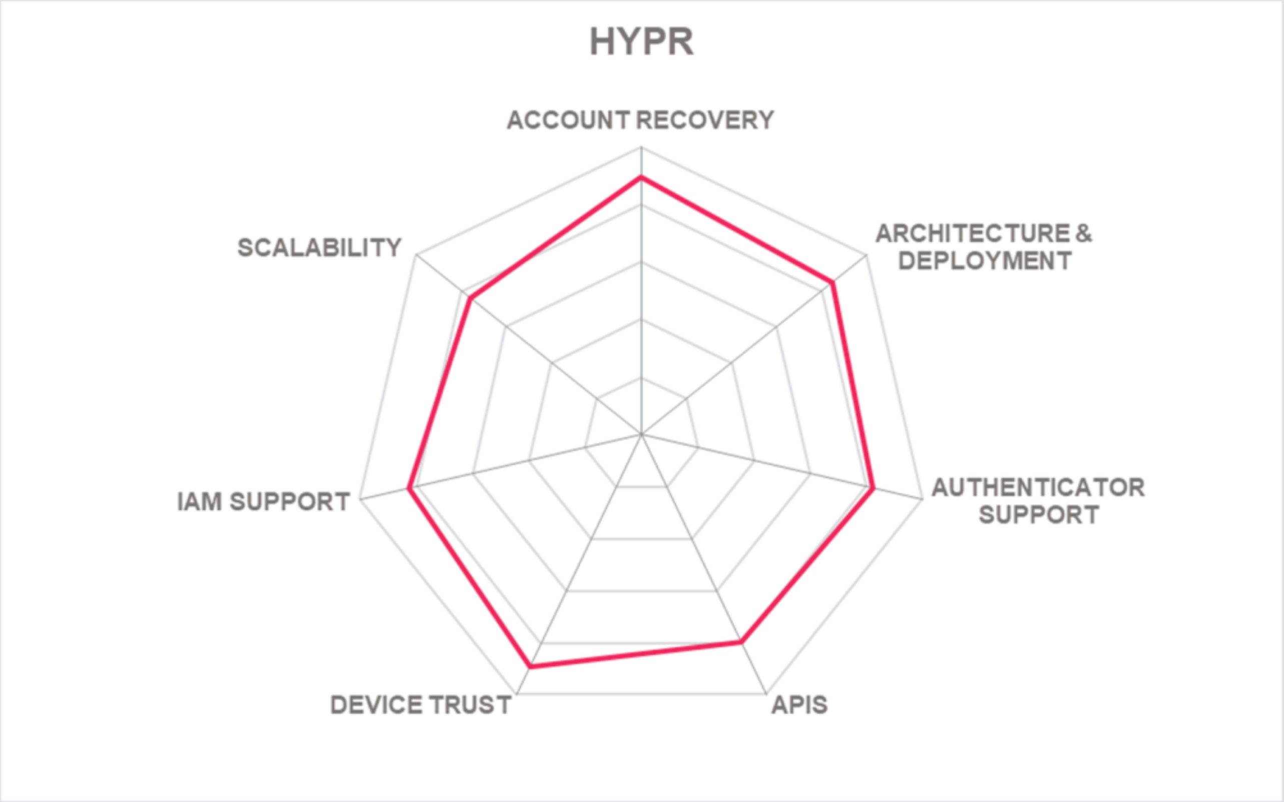
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


HYPR
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.12 IBM

IBM Corporation is a multinational technology and consulting company headquartered in Armonk, New York, USA. Founded in 1911, IBM has evolved from a computing hardware manufacturer into offering a broad range of software solutions, infrastructure hosting, and consulting services in such high-value markets as business intelligence, data analytics, cloud computing, virtualization, information security, and identity and access management. With a strong global presence and customers and partners across the globe, IBM is a major player in the market.

IBM Security Verify provides fully cloud based deployments for SSO, MFA, Adaptive Access, Privileged Access, Lifecycle Management, and Passwordless Authentication. The offering is a multi-tenant containerized and highly scalable solution built on microservices providing Identity use cases as a service. Components can run on-prem in traditional datacenters or private clouds, in cloud-based IaaS services like Azure, AWS, and IBM Cloud, and PaaS by way of Docker-based deployments. Licensing models include monthly active users, monthly/quarterly/annual registered users as well as per-appliance and per-node options.

IBM accepts a long list of authentication mechanisms, including hardware tokens, CAC/PIV card, Duo, Feitian, Google Titan, Kensington Security Key, OneSpan DigiPass, RSA SecurID, Smartcards, Symantec VIP, Thetis, and Yubikey tokens. Protocols supported include JWT, Kerberos, OAuth, OIDC, RADIUS, TACACS, and SAML. It is also ISO 27001/27018 certified, PCI-DSS Level 1, and SSAE 18 SOC 2 Type 2 attested. All major account recovery types are available, and customers can configure others via APIs. For additional application connectivity, REST, SOAP, WebAuthn, and Webhooks and LDAP and SCIM for provisioning are supported.

IBM positions itself as a leader in the IAM space and provides feature-rich and modern solutions for customers that intend to adopt a passwordless approach. IBM also benefits from its integration to other IBM services such as IBM QRadar. 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. IBM appears in the product, market, and innovation leadership categories.

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

IBM

Strengths

- Strong global partner ecosystem
- Proven scalability
- Modern microservice-based architecture
- Well-documented set of APIs
- Integration with 3rd-parties for MFA and identity proofing capabilities (but requires customization)
- FIDO 2 Server certified
- Wide selection of authentication mechanisms supported

Challenges

- No support for transaction signing
- No support for remote access
- PAM component is an OEM product, provided by Delinea

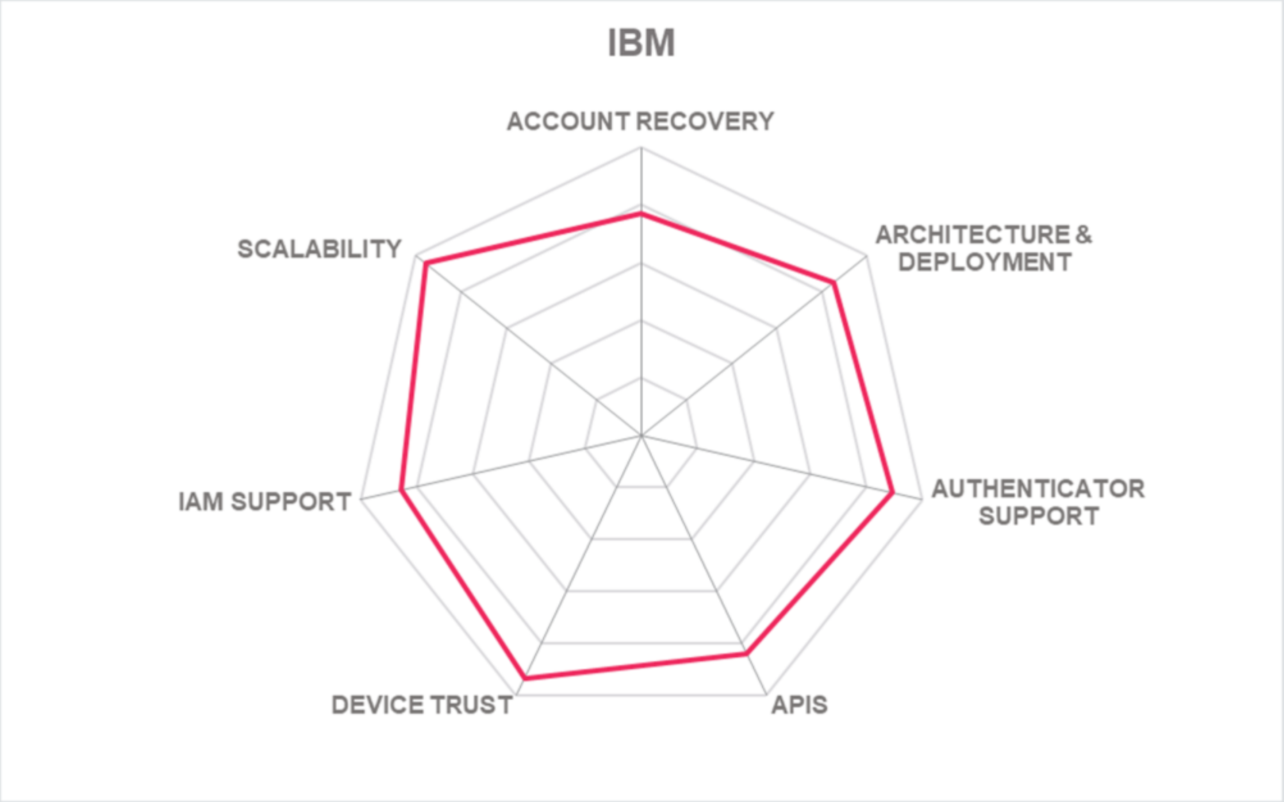
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


IBM
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.13 IDEE

IDEE GmbH was founded in 2015 and headquartered in Munich. IDEE is a small but innovative vendor in the broader IAM market that delivers solutions for phish-proof passwordless authentication and authorization services to SMB and enterprise customers in the insurance, finance, and telecommunications industries. The company is focused on Europe and North America regions with a growing number of customers in Africa and the Middle East.

AuthN is a passwordless and phish-proof MFA solution targeted at workforce, consumers, and partner use cases. The solution aims to prevent credential phishing and account take over, provides a same-device MFA approach which does not require a second device such as a USB key or Smartphone to achieve MFA, and delivers fast integration for standard use cases and APIs for custom integration. Licensing options for workforce use cases are per identity per month while CIAM use cases are per identity per month and per transaction.

The provisioning of credentials (authentication and authorization keys) is done in a hardware-backed cryptographic module such as secure enclave and secure element, in a way that would be very difficult to compromise. In addition, local device authentication such as TouchID is leveraged to ensure the user credential never leaves the user device. IDEE does not have access to any user data -- not in storage or even when a user account is being recovered.

IDEE is in compliance with FIPS 197, NIST 800-57, NIST SP800-63, PCI-DSS v 3.2, HIPAA/HITRUST, GDPR, PSD2 SCA, ISO 29115, AND UK GPG 45 standards. The solution supports hardware tokens such as Feitan, Google Titan, and Kensington security keys. For additional application connectivity, the solution supports REST, JSON, SCIM, LDAP, and RADIUS upon customer requests. Furthermore, AuthN supports cloud or on-premises directories. Some common examples include, AWS, Google, Okta, Keycloak, ForgeRock, Ping Identity, etc.

IDEE, being a rather young vendor, has a still relatively small global presence, compared to many of the other vendors. On the other hand, the company is very innovative and provides a flexible modern solution based on a scalable microservices architecture that fits well to the requirements of a modern passwordless authentication approach. IDEE appears in the innovative leadership category.

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

IDEE

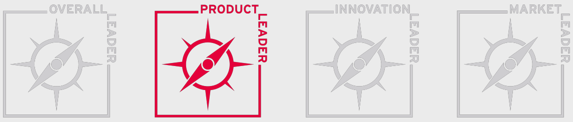
Strengths

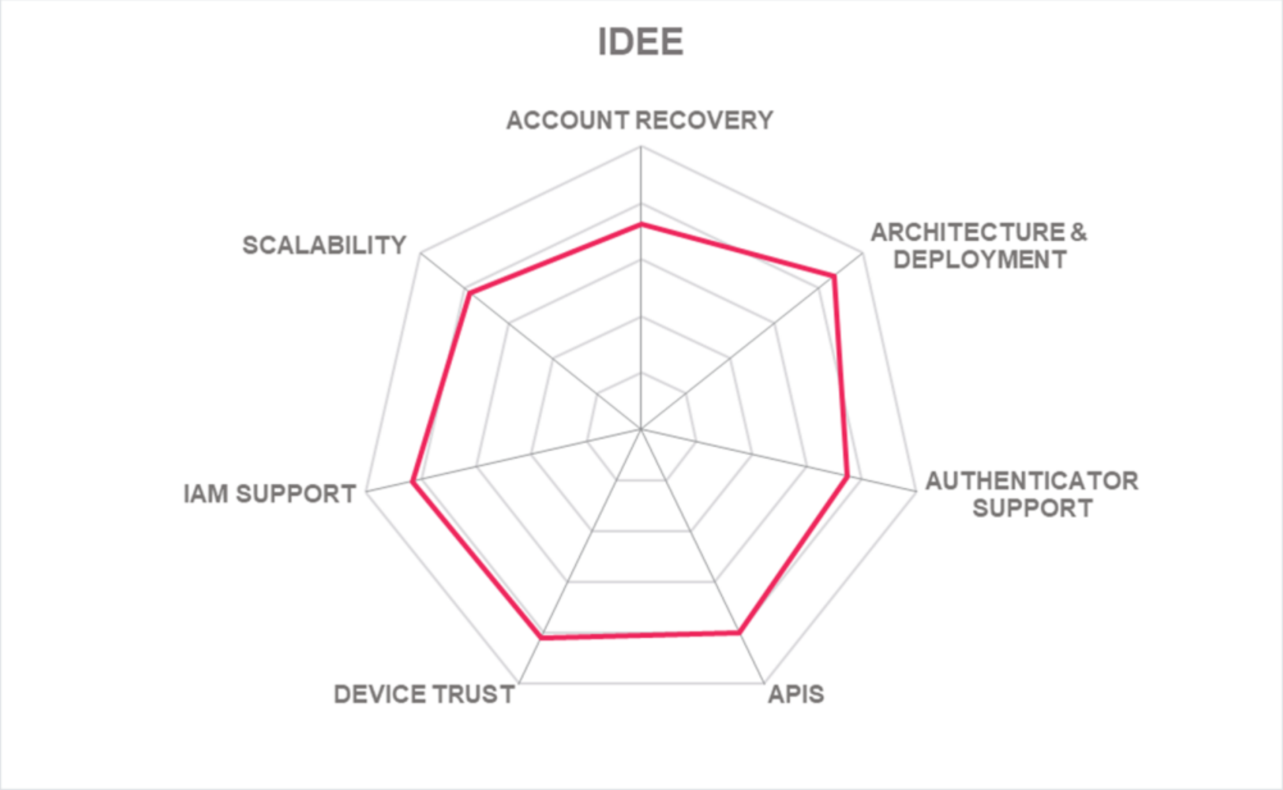
- Many SaaS connectors
- Easy to deploy
- Many authenticator options
- Flexible, modern microservices-based architecture
- Out-of-the-box integration with Windows Hello and Windows Hello for Business
- Same device MFA approach

Challenges

- Still a relatively small vendor, but with some large customers
- SOC 2Type II certification in work

Leader in




IDEE
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.14 Identité

Identité was publicly established in April 2020 and headquartered in Clearwater, Florida. The company was founded by a team of security and enterprise software veterans and its client-base is mainly composed of small and medium enterprises and moving up-market. With sales agents in North America, Latin America, and Europe, Identité's mission is to provide clients with a simple and secure user experience. Identité offers easy-to-use software solutions, cloud services and on-premises deployments.

Identité operates in three domains: access, identity, and privileged. Products include NoPass for Consumer and NoPass for Employees. Their CIAM offering, NoPass for Consumer, includes APIs and an SDK which can be integrated into a company's web portal and mobile app to enable passwordless authentication. NoPass for Employee, the workforce offering, operates as an identity broker linked to existing authentication systems to enable passwordless MFA. The solution focuses on all types of users that are performing MFA by replacing the shared secret password-authentication method with a decentralized token. It does not use passwords, credentials, or hashes on the database because all the credentials are by way of tokens on the user's device (iOS, Android, PC or Mac).

Identité's Full Duplex-Authentication is an innovative feature (patented and registered trademark) that is built into all the client's devices and applications. Essentially, the NoPass server must first authenticate to the user properly before requesting and authenticating the user's token. This drastically reduces the chance of phishing, impersonation, and "Man-in-the-Middle" attacks. The feature also includes a visual confirmation for the user that allows them to confirm login by comparing a simple picture and a number. This is easier than OTP methods that require a user to type a 6--8-character code, but it still requires an action by the user.

Identité supports Kerberos, SAML, OAuth, OIDC, and JWT. For additional application connectivity, the solution supports REST, RESP, RADIUS, and SCIM and LDAP for provisioning. The solution has simple integration tools that connects to Active Directory, Azure, VPN's, RDP Gateways, SSO services and more. Small and medium enterprises looking for a cost-effective, innovative, and secure solution should definitely evaluate Identité NoPass. The company appears in the innovative leadership category.

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

Identité®

Strengths

- Good option for SMBs
- Strong device management capabilities
- Strong federation standards support
- Desktop unlock capabilities
- Fast registration and easy deployment
- Full Duplex-Authentication capability

Challenges

- No support for third-party services but enhancements are on the roadmap
- Risk engine not accessible via API
- Smaller company but with a growing global footprint
- ISO/IEC 27001 and SOC 2 Type II not attained

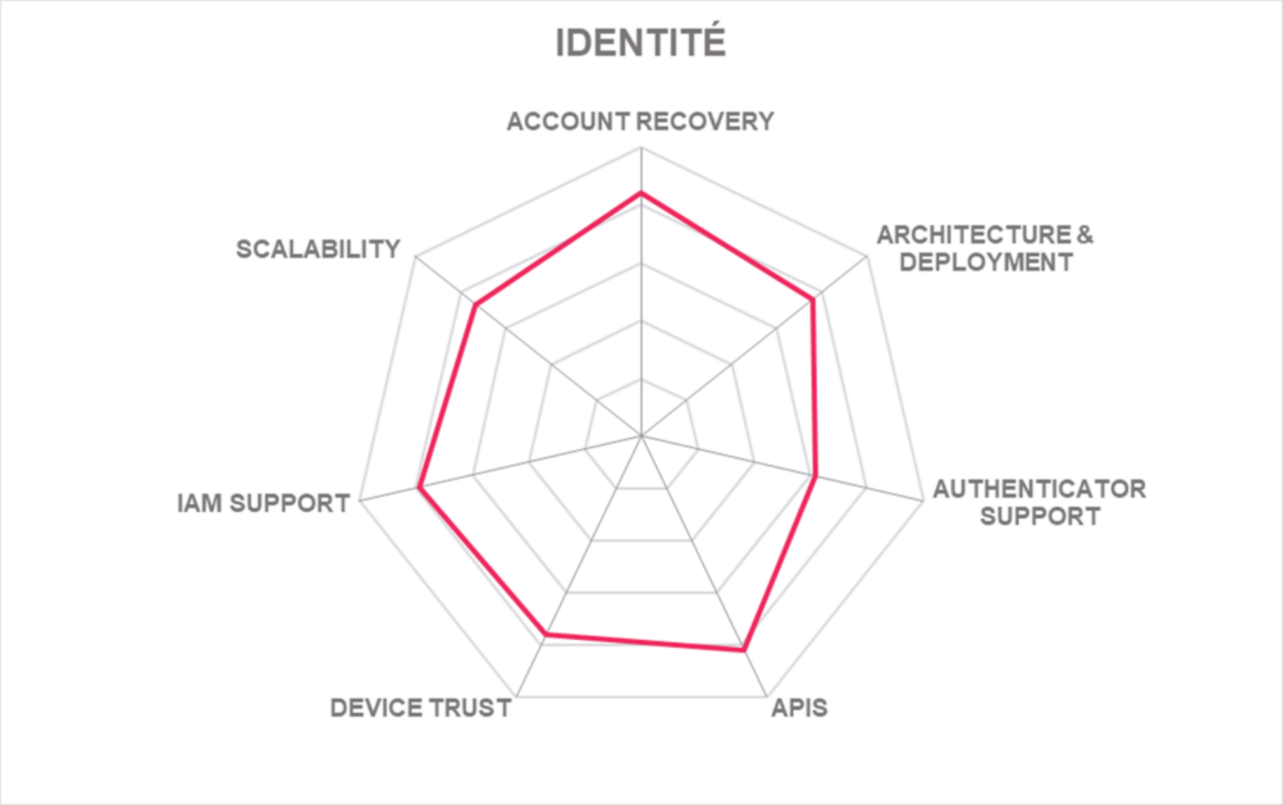
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


IDENTITÉ
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.15 Keyless

Keyless was founded in 2019 and is headquartered in London, UK. It is an innovative deep-tech identity company that develops and provides a privacy-preserving passwordless biometric authentication solution. Keyless\' unique value proposition is derived from combining advanced cryptography with facial biometrics and authentication. The product is based on 10 years of research in academia on technologies such as secure multi-party computation, zero knowledge proofs, and biometrics.

The workforce offering includes passwordless SSO, desktop MFA, and remote login which provides the ability to integrate protocols for VPN, SASE, and other kinds of remote access systems that do not have SSO through a SAML or OpenID connection. The consumer offering has multiple use cases such as customer KYC, account recovery, and SDKs which incorporates all the features and core technologies of Keyless authentication. The Keyless SDK works on Android 7+, iOS 12+ operating systems, and Windows 10 devices. However, Keyless\' facial recognition functions independently from the underlying operating systems and does not rely on Apple FaceID or any Android facial recognition software. Both the Keyless Authenticator and SDK support user registration, user authentication, device identification and authentication, and utilize their API to the Keyless Network.

The Keyless solution is a fully decentralized multi-factor biometric authentication and identity management platform. The solution eliminates the need to store passwords, cryptographic keys, and other authentication data in a central repository without compromising on convenience and user privacy. This is possible through the use of network-based biometric authentication that combines the security profile of a decentralized system with the availability of cloud-like architectures. In addition to biometrics, Keyless incorporates risk-based authentication elements to assess device health and detect whether devices are jailbroken. Keyless is currently undergoing formal ISO27001 certification.

Although Keyless is a relatively young vendor, the Keyless platform is a great option for organizations looking to modularly upgrade their authentication capabilities, utilize advanced cryptography to strengthen their privacy, and go passwordless. While Keyless has a significant number of customers, supporting more certifications will appeal to customers in certain regulated industries and others that have strict security requirements.

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

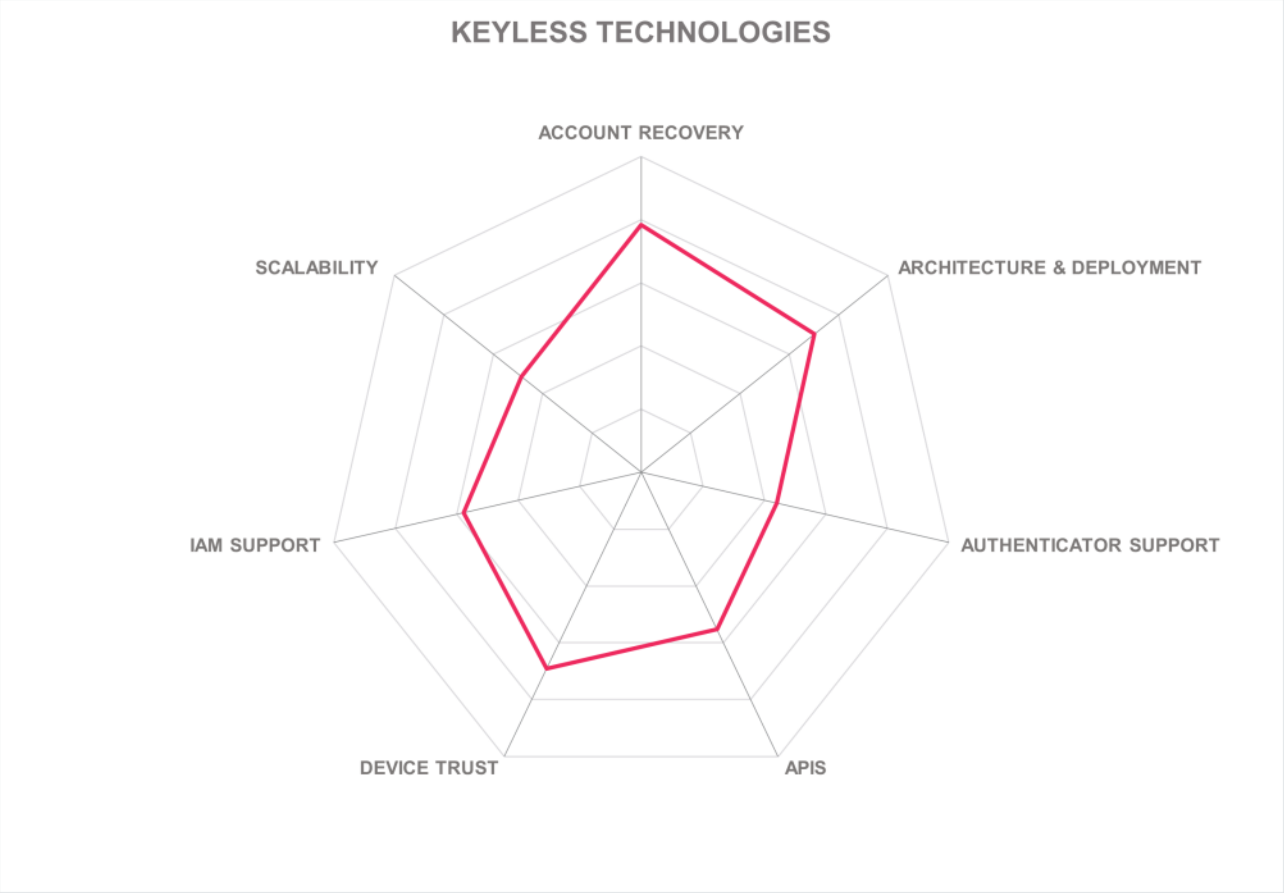
KEYLESS

Strengths

- FIDO 2 certified
- Fully passwordless authentication solution
- Easy integration and maintenance
- Consistent experience across all devices
- Innovative use of biometrics
- Promotes privacy regulation compliance including EU GDPR, PSD2, and CCPA/CPRA

Challenges

- Customer presence is still primarily focused in EMEA
- OAuth, Kerberos, and JWT not supported
- No connectors to identity vetting services
- SCIM and LDAP based provisioning not currently supported


KEYLESS TECHNOLOGIES
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.16 Microsoft

Microsoft Azure Active Directory (Azure AD) is a cloud-based identity and access management service focused on facilitating business to consumer applications and providing enterprise authentication capabilities. Azure AD is one of the global leaders in the cloud infrastructure market and it is delivered via dozens of data centers operating globally. Licensing for Azure AD is according to numbers of monthly active users, or by numbers of registered per month/quarter/year. The solution focuses on workforce, consumer, and partner use cases.

The solution offers three passwordless authentication methods that integrate with Azure AD including Windows Hello for Business, passwordless phone sign-in (Microsoft Authenticator), and FIDO2 security keys (platform and external). These credential types fall into the passwordless category and provide strong authentication methods based on public key infrastructure (PKI). With PKI integration and built-in support for single sign-on (SSO), Windows Hello for Business provides a convenient method for seamlessly accessing resources on-premises and in the cloud. The Microsoft Authenticator app uses the same basic authentication pattern as Windows Hello for Business while the FIDO2 security keys allow users to register and sign into their Azure AD or hybrid Azure AD joined Windows 10 devices. In addition, the platform can be used to add MFA as a strong authentication on top of popular IDPs, so the user can sign in with their LinkedIn or Google account and then do MFA.

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. In addition, hardware authenticators such as CAC/PIV cards, Duo, Feitian, OATH (any), OneSpan DigiPass, Thetis, Smartcards, Symantec VIP, and Yubikey tokens are supported as well. Azure AD also works with JWT, Kerberos, OAuth, OIDC, and SAML. Users can be provisioned by LDAP, SCIM, cloud-specific APIs, and self-registration. All account recovery mechanisms are present.

Each organization has different requirements and needs when it comes to adopting a passwordless approach. However, Microsoft Azure Active Directory has the scalability and performance to provide organizations with three options and feature-rich capabilities. The solution should be on the shortlist for any organization looking for robust enterprise authentication services. Microsoft appears in the product and market leadership categories.

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

Azure

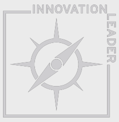
Strengths

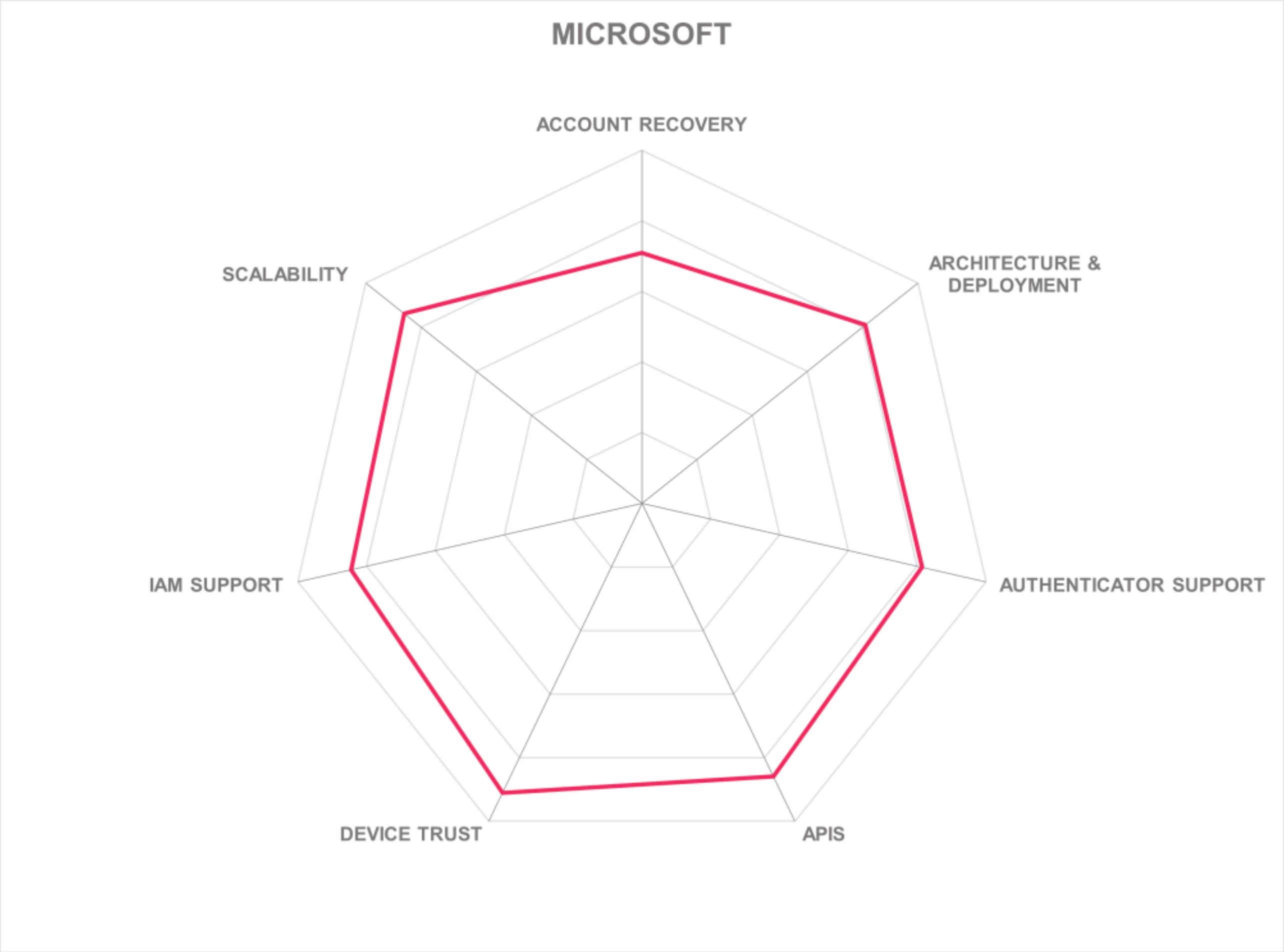
- High scalability
- Flexible deployments
- FIDO2 security key providers
- Board-level position at the FIDO Alliance
- Strong device management capabilities
- Global partner ecosystem and strong geographical presence

Challenges

- No support for transaction signing
- Self-service workflows cannot be customized

Leader in




MICROSOFT
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.17 NEVIS Security AG

Until early 2020, Nevis was a part of AdNovum Informatik AG, but was then spun off as a separate company. Nevis Security protects many banking, insurance, healthcare, and government portals and secures a large percentage of e-banking transactions in Switzerland making it one of the leaders in identity and access management solutions in the country. Nevis recently expanded into the UK market and has a strong presence in Germany and Singapore. In addition to its headquarters in Zurich, Nevis operates offices in Germany and Hungary.

With their solid background and strength in CIAM, their main target audience is passwordless authentication for consumers. The solution is available as a standalone SaaS subscription service, or as integrated part of the Nevis Identity Suite. Thus, providing customers with the choice they require to find the best possible deployment option. The solution is FIDO UAF and FIDO2 certified and supports the following use cases: passwordless MFA backed by device biometrics, cryptographically secured transaction confirmations with the "What you see is what you sign" principle, username-less authentication, and multi-account support. For onboarding and recovery, Nevis supports out-of-the-box integration using fully automated document-based identity verification. This allows users to easily register a new device 24x7 after losing a device.

Nevis also provides a fully brandable and hardened Access App that runs on any Android device with a TEE and Android 6+, and on any iOS with support for biometrics. Furthermore, Nevis supports Feitian, Google Titan, Kensington Security Key, OATH, OneSpan DigiPass, RSA SecurID, Smartcards, Thetis, and Yubikey tokens. In addition, Nevis also integrates with many other vendors through other standards such as OAuth, SAML, and OIDC.

Nevis, despite still being a relatively small vendor, has demonstrated its ability to serve customers in different geographies and at different scales. Their CIAM offering provides core account recovery and device management capabilities with strengths in omni-channel experience and transaction confirmation. Nevis Security continues to improve its set of passwordless capabilities and should be of interest to organizations within the EMEA region and Southeast Asia.

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

NEVIS

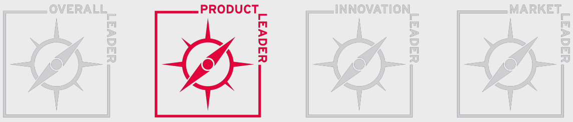
Strengths

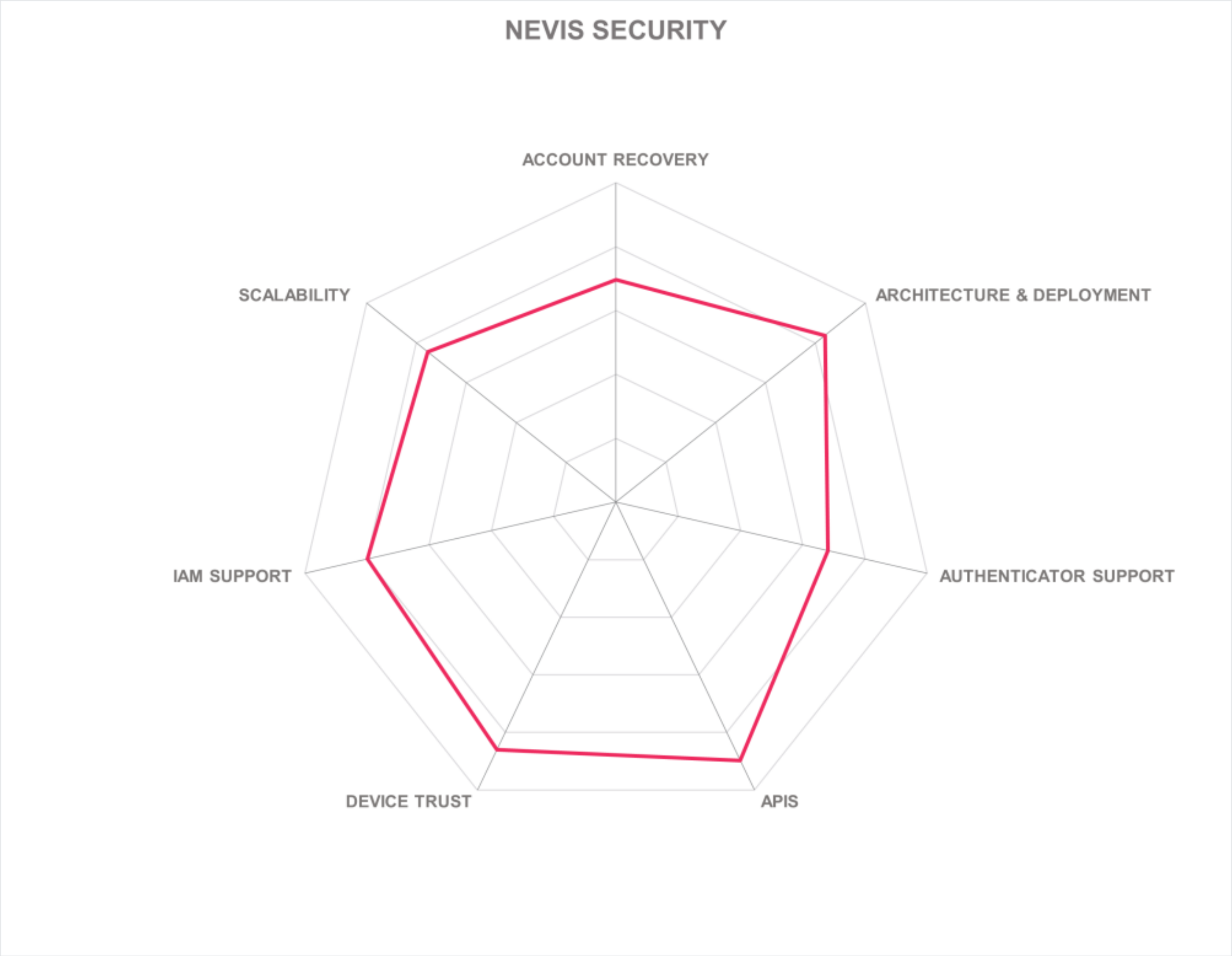
- Strong API security
- Strong transaction confirmation capabilities
- Out-of-the-box integration with automated document-based identity verification
- Hardened mobile app and SDK
- Flexible deployment options
- High security authentication and identity solutions for finance, government, and insurance industries
- FIDO UAF and 2.0 certified

Challenges

- Limited market reach outside the EU, but continuously expanding
- ISO/IEC 27001 and SOC 2 Type II not attained
- Some limitations on third-party integration options
- No support for portable/decentralized identity

Leader in




NEVIS SECURITY
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.18 OwnID

Started by Gigya co-founder and long-time executives, OwnID was founded in 2021 and has offices and team members in Tel Aviv, San Francisco, Kyiv, and Mallorca. OwnID adds cross-device native passwordless capabilities to any website authentication flows to improve the user experience and security. It can be used for B2B2C use cases. Customers range from small to large enterprises in EMEA and North America.

The solution is a fully multi-tenant SaaS solution and allows end-users to instantly sign-in with their phone biometrics instead of using a password on any platform, without installing an app. OwnID aims to increase conversion and security while supporting different edge cases such as cross device, non-FIDO support, and account recovery. It includes self-service onboarding and integration which allows the user to create an account and choose the identity platform they are using.

OwnID does not have any database to store users, keys, or any personal information. The solution leverages the identity management systems of their clients to store the public part of the encryption keys that are in the device. Once the user does the initial login with OwnID, the phone creates the public-private key pair. On a desktop computer, users register and log in by scanning a QR code with their mobile device's camera. The authentication flow is web-based and does not require the installation of an app. Users only need their phone device to authenticate.

The solution follows a biometrics-first approach. However, if a user is logging in on desktop and their phone is not available, the user can still log in via magic link as a fallback. Protocols understood include JWT, Kerberos, OAuth, OIDC, RADIUS, SAML, and TACACS. Out of the box integration supports the identity management platform providers such as SAP, CVC, Amazon Cognito, Firebase, and others.

Despite being a young and small vendor, OwnID has demonstrated its ability to serve large customers from broad range of industries. With its decentralized features, it is an interesting foundation for implementing a passwordless approach.

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

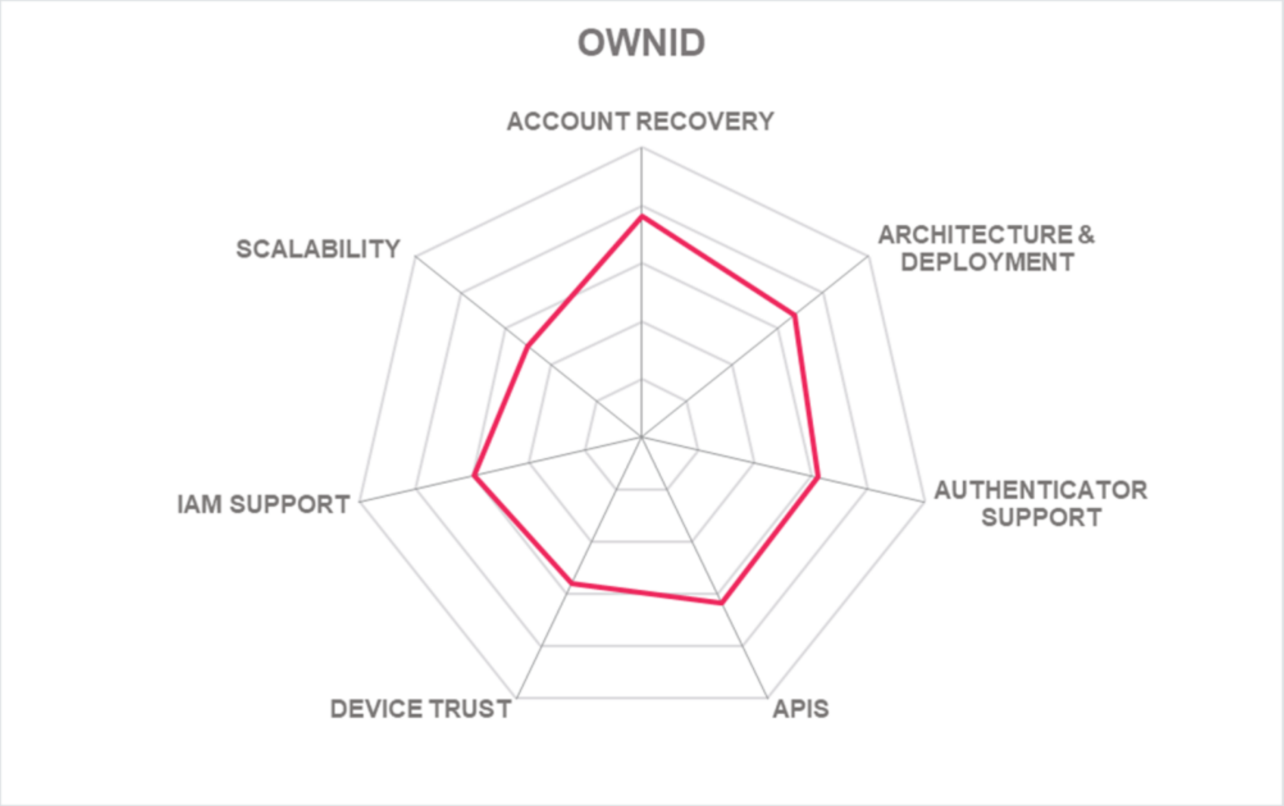
OwnID

Strengths

- Friendly user experience
- No app is needed
- Whitelabel and web-based solution
- Microservices approach
- Strong support for different edge cases
- Strong self-service onboarding and integration features
- Keys are not stored on servers

Challenges

- Small customer base but expanding
- No support for device trust on multiple devices
- ISO/IEC 27001 and SOC 2 Type II not supported
- Additional IDaaS platform support would be useful, but enhancements are on the roadmap


OWNID
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.19 Ping Identity

Ping Identity was founded in 2002 and based in Denver, Colorado. Ping Identity was among the first of the enterprise IAM vendors to adapt to consumer-facing requirements. Ping Identity products can be licensed standalone, as well as through solution packages. SaaS delivered products include PingOne SSO (cloud authentication and directory), PingOne MFA (cloud MFA for customers), PingID (cloud MFA for workforce), PingOne Risk (cloud risk management), PingOne Verify (identity verification for customers), PingOne Fraud (customer fraud detection), and more.

However, Ping recently acquired an orchestration service called Singular Key which is now known as PingOne DaVinci and is available to all Ping customers. By providing the ability to create user journeys across the entire identity lifecycle, orchestration has become an enabling foundation of the PingOne Cloud Platform. DaVinci can orchestrate journeys that include any third party, including Ping competitors. It includes connectors to both Ping and third-party services to build flows that contain ID verification, fraud detection, authentication, account recovery, authorization capabilities, and much more. The tool is built on a microservices-based architecture and is an IAM independent identity experience platform. PingOne DaVinci works across many different passwordless scenarios while incorporating risk signals capabilities and allowing users to create flows with different identity companies. The solution has connectors to Ping and third-party dynamic authorization and policy-based authentication features.

PingOne Cloud Platform supports Feitian, Google Titan, Kensington, OneSpan DigiPass, RSA SecurID, Symantec VIP, Thetis, Yubikey and any OATH compatible hardware authenticators. JWT, OAuth, OIDC, RADIUS, and SAML are supported. Furthermore, 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 Identity is also self-certified with CSA and certifies/attests with ISO 27001 and SSAE SOC 2 Type 2.

Ping Identity's cloud-ready software 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. Organizations looking to get started on a passwordless journey should consider Ping Identity's products and services. Ping appears on the product, market, and innovation leadership categories.

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

Ping Identity.

Strengths

- Proven scalability
- Many OOTB connectors to SaaS/IDaaS
- Lots of authentication options
- Excellent orchestration capabilities
- Strong dynamic authorization features
- Breadth and depth of standards protocol support for legacy and modern access management use cases

Challenges

- Main presence in North America, but continuously expanding
- Dashboards are not customizable
- Limited support for accessible authentication per the W3C's Web Content Accessibility Guidelines, but improvements are on the roadmap

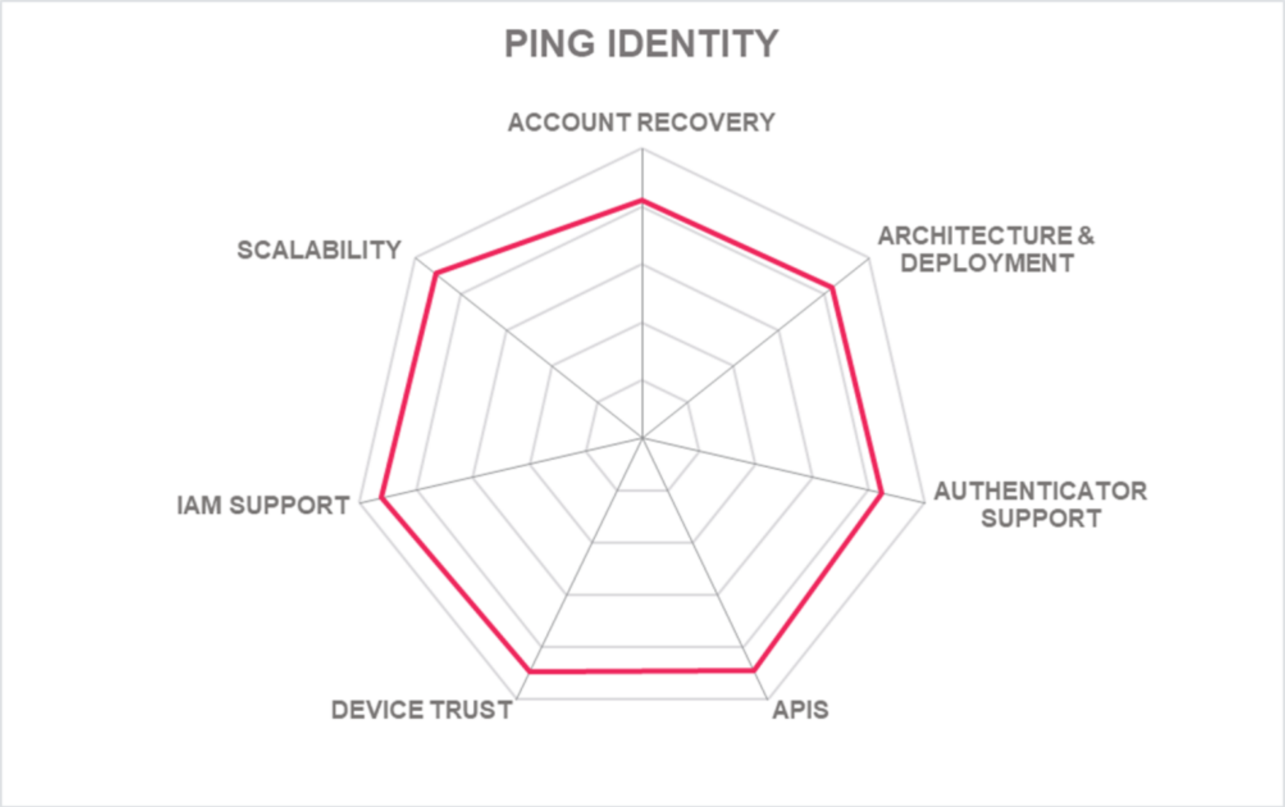
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


PING IDENTITY
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.20 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 again operates independently and has a focus on identity. The company offers industry-leading solutions in identity assurance, access control, encryption, key management, compliance, security information management, and fraud protection. RSA is also a board member of the FIDO Alliance.

RSA provides a fully integrated service available on-premises with SecurID or hybrid cloud with the newly available ID Plus, consisting of a Cloud Authentication Service, RSA Authentication Manager and Single Sign-On portal. RSA offers passwordless MFA, machine learning enhanced risk analytics, and hardware and software tokens that can be purchased separately or as part of the ID Plus solution subscription plan. The cloud service can stand on its own, but it can also be deployed as an additional layer of services and protection on top of the traditional on-prem authentication services. This enables their customers to adopt cloud services and migrate at their own pace.

RSA supports a broad range of authentication methods. These include a variety of ways for mobile authentication, including push to approve, OTP, SMS voice, and support for a range of biometric authenticators including Apple FaceID and TouchID, and Samsung Fingerprint. In addition to their own well-known authenticators, RSA accepts Feitian, Google Titan, Kensington, Thetis, and Yubikey hardware tokens. RSA also provides a native mobile application and native SDK which is available to build customer applications or integrate functionality into an existing application. Furthermore, RSA recently completed milestones for FIPS 197, FIPS 140-2 and NIST 800-57 to demonstrate compliance as part of FedRAMP.

With the breadth and depth of functionality, RSA solutions are scalable and provide good hardware-based authentication methods. Backed by a global ecosystem, the company can readily deploy such solutions. For organizations that broadly utilize RSA products, SecurID and ID Plus are good options for organizations wishing to commence a passwordless journey.

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

RSA®

Strengths

- Good option for remote access
- Large selection of PAM integrations
- Broad range of authentication methods
- FIDO U2F & 2.0 certified server
- Scales well for large enterprises with many users, entitlements, and policies
- Flexible integration to full suite of RSA security products
- Hybrid deployment addresses on-premises and cloud models

Challenges

- Lack of device health checks features but improvements are on the roadmap
- No connectors to identity vetting services
- No specific support for dynamic scaling

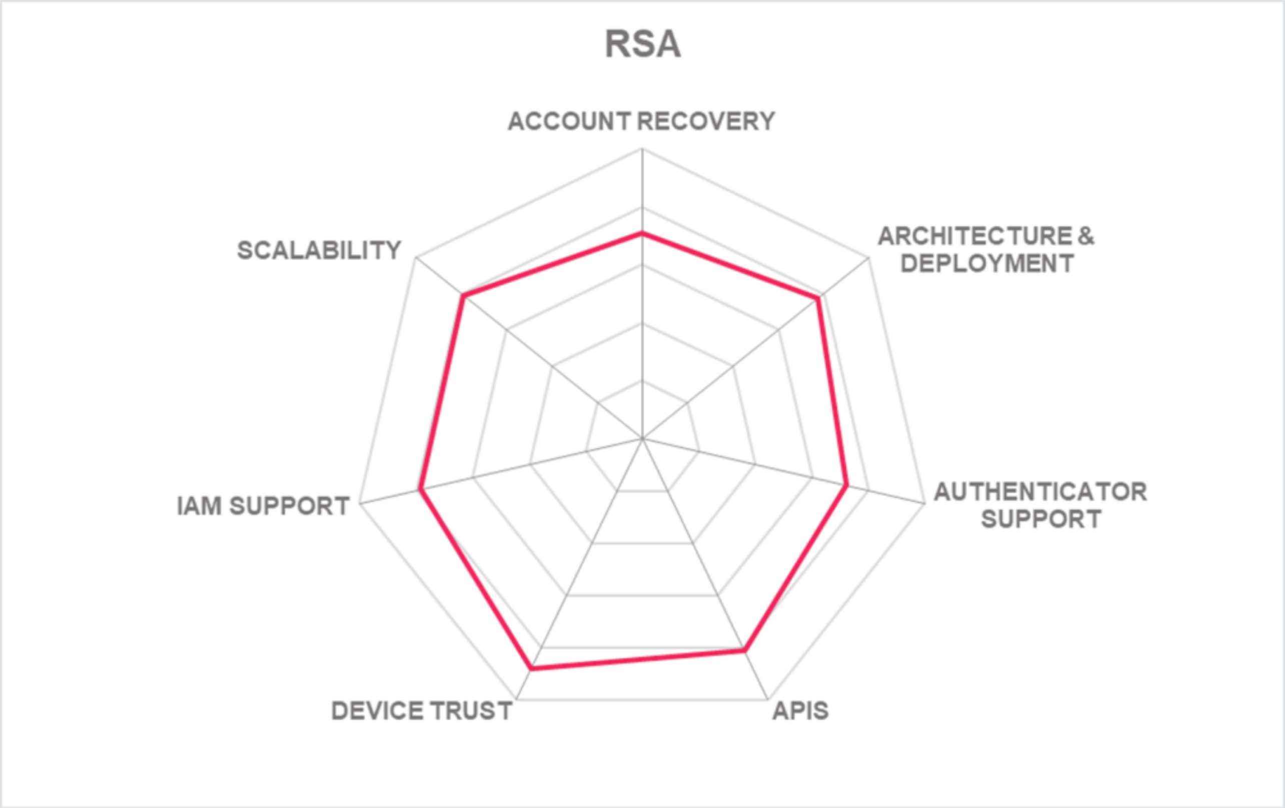
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


RSA
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.21 SAASPASS

SAASPASS was formed in 2013 and is headquartered in San Francisco. Their product, SAASPASS IAM, is centered on providing passwordless authentication services to small and large customers in the government, defense, finance, and insurance industries. The solution is built on a passwordless architecture and zero trust security model. It's available on both as SaaS and on-premises. The platform delivers capabilities such as MFA, SSO, shared access management, directory services, access control policies, endpoint protection, PAM, reporting and auditing, and delegated admin types.

SAASPASS IAM is available for workforce, consumer, and partner use cases. It provides MFA and phishing resistant methods such as remote log in and mobile URL callback. It supports third party tokens and standards like FIDO U2F, FIDO2, HOTP, and TOTP (non-FIDO devices). 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.

The use of APIs is granular and allows the possibility of building applications by just scanning the encrypted bar code. API support includes REST, SOAP, and Websockets, and CSV/JSON/XML formats. SAASPASS also offers a mobile SDK that companies can incorporate that functionality into their own mobile app, with multiple MFA methods supported, or launch their own branded authenticator app for their web apps. The solution also supports LDAP and SCIM for provisioning. SAASPASS IAM has many pre-built MFA integrations ranging from VPNs, Radius, RDP, and legacy protocols like Microsoft Exchange Server, Outlook for desktop, MAPI, and ActiveSync for mobile. In addition, the platform includes a self-service bulk email registration tool that allows registration for FIDO2 tokens to be able to be done at scale. It is also compliant with PSD2 Strong Customer Authentication requirements.

The SAASPASS product supports a good variety of authenticators, and it offers good scalability which makes it attractive for environments where high security and authentication assurance is needed. 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	● ● ● ● ○
Deployment	● ● ● ○ ○
Interoperability	● ● ● ● ●
Usability	● ● ● ● ●

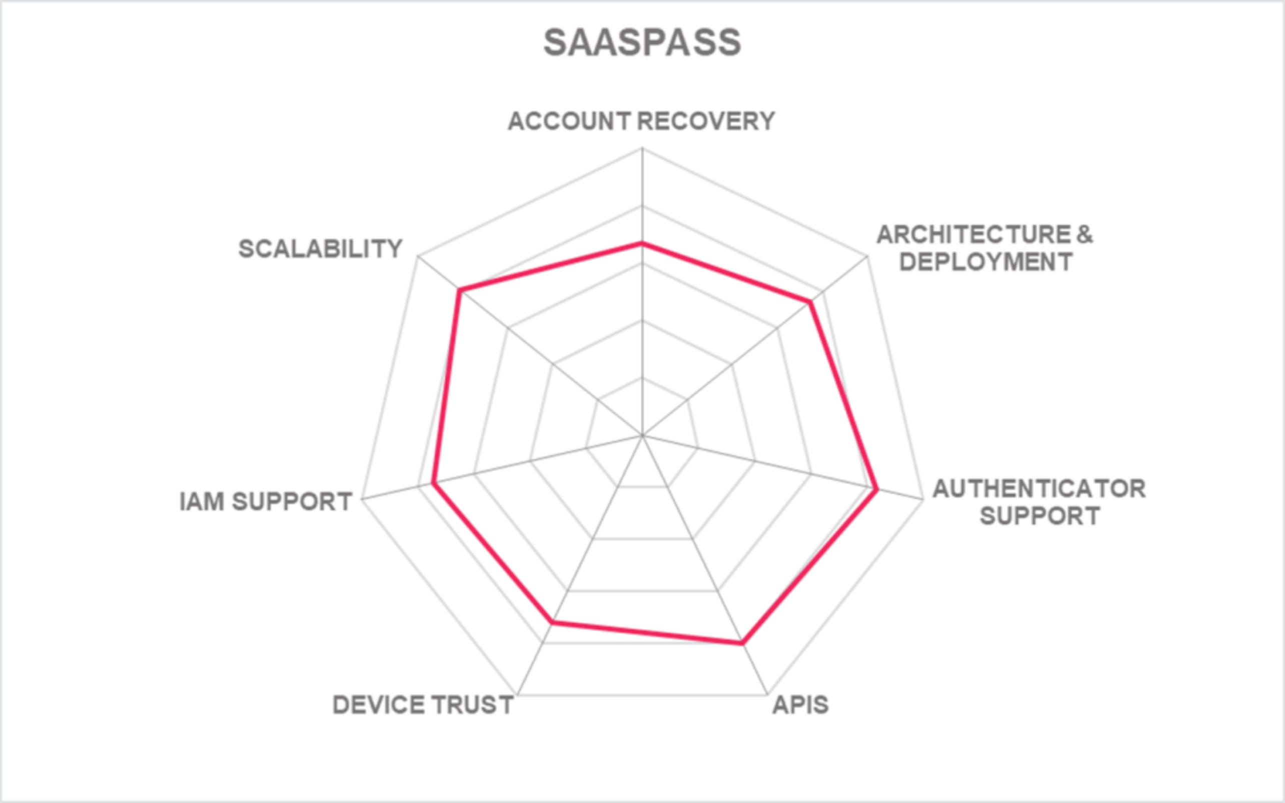
SAASPASS

Strengths

- Comprehensive set of APIs
- Good support for relevant standards
- Friendly user experience
- Flexible deployment options
- Large range of MFA types supported
- Good selection of SaaS app connectors

Challenges

- Mainly focused on North America, but growing rapidly in the EMEA and APAC regions.
- Lack of out-of-the-box support for integrating with Windows Hello for Business


SAASPASS
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.22 Telefónica Tech

Telefónica Tech, part of Telefónica, is a leading company in digital transformation. The company offers a wide range of integrated technological services and solutions in Cyber Security, Cloud, IoT, Big Data, AI, and Blockchain.

Telefónica is one of the largest telecommunications service providers in the world. The company offers fixed and mobile connectivity as well as a wide range of digital services for customers. Telefónica Tech has presence and strategic hubs in Spain, Brazil, the UK, Germany, and Latin America, and offers B2B API solutions around digital identity and the use of mobile phone/SIM card as trust anchor for digital identities solutions for APIs.

Number Verify is a SIM-based authentication solution that provides a frictionless, phishing-resistant, cryptographically-secure (because of the SIM card), possession factor authentication method. It is integrated directly into the mobile network and can perform a real-time verification of the mobile number and SIM card which provides a strong device binding. The solution is targeted to workforce, consumer, and partner use cases. Normally, it is sold through channel partners such as Twilio, TruID, and Prove. The licensing model is per transaction; however, other licensing models are in development.

Number Verify is a new passwordless authentication product available from leading Mobile Network Operators in Europe. While SIM-based authentication is not a new technology, it is relatively new in Europe. It is already very well proven in other markets such as China (1.3 billion transactions per day). The solution delivers fast, simple, and friendly authentication while providing security at the same time. Moreover, in the event of device change/replacement, users will be required to get a new SIM card and re-enroll it in an existing or new device.

The product has the potential to shape and create new opportunities in the passwordless authentication market. However, it lacks some capabilities in terms of authentication options and device management compared to most vendors. They may want to consider pursuing more security certifications to increase adoption and market share. Their presence in South America, both in terms of strategic hubs and sales target, is a plus for that region and for their own growth potential. Therefore, Numbery Verify should be on the short list for organizations considering deploying phishing resistant and device-based possession features.

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

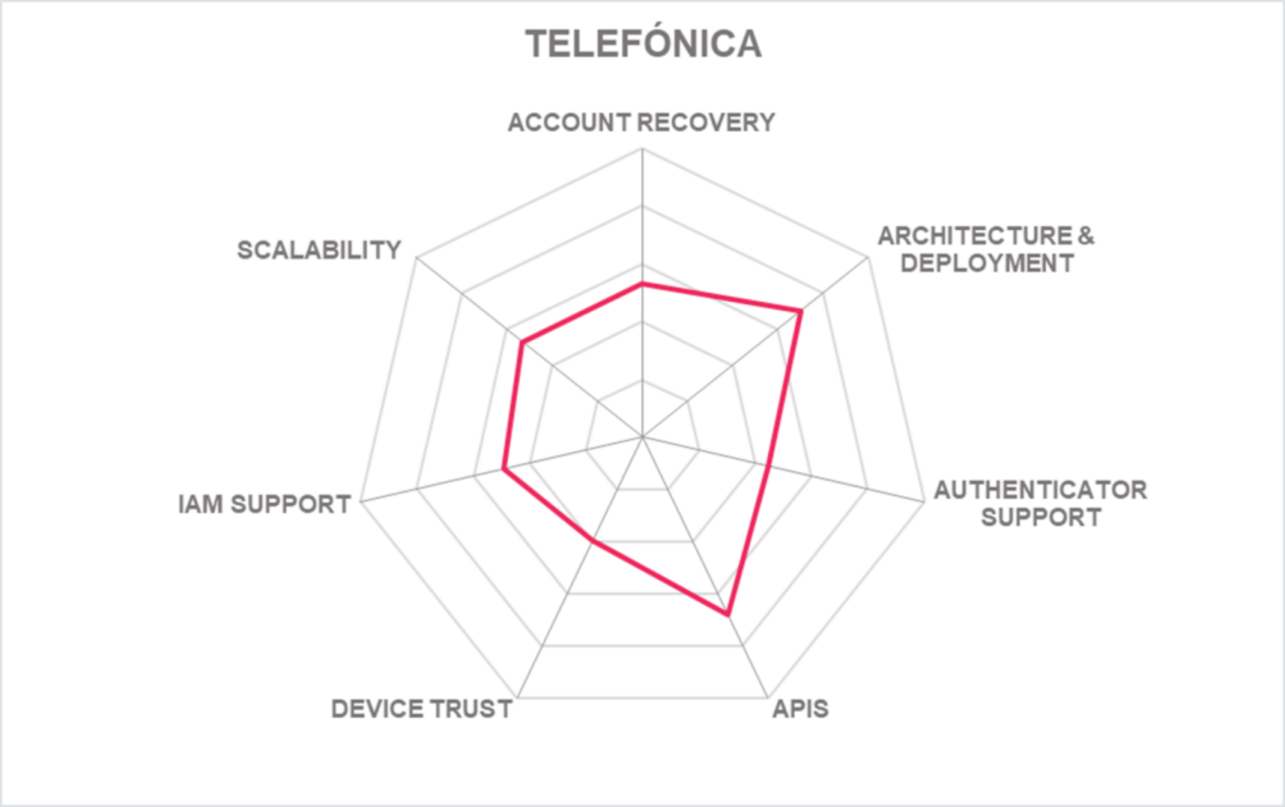
Telefónica Tech

Strengths

- Easy to use
- Innovative features
- Strong SIM-based authentication
- Frictionless logins and friendly user experience
- Phishing resistant and cryptographically secure
- Large global partner network and geographical presence

Challenges

- SAML not supported
- More security certifications needed
- Additional out-of-box integrations for major IAM platforms needed, but developments are on the roadmap
- No device health checks since the solution has no reliance on the integrity of the device


TELEFÓNICA
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.23 Thales

Thales is a French multinational company and leader in the aerospace, transportation, and defense and security markets. With its presence and through a large network of distributors and sellers, Thales has a unique capability to design, develop and deploy equipment, systems and services that meet the most complex security requirements. Furthermore, the company recently acquired Dutch CIAM company OneWelcome, one of the leading European providers of CIAM (Consumer IAM).

SafeNet Trusted Access is a fully cloud-based access management and authentication service delivered as SaaS and mainly focused for enterprise use cases. However, the solution provides hybrid deployment (specifically for large organizations with a multinational presence). This platform allows all authentication events to take place on-premises which enables customers to comply with country-specific regulatory requirements. Furthermore, SafeNet Trusted Access provides a wide range of modules for policy management, application management, authentication, logs, and dashboards.

The risk engine can process the following factors: IP address, geo-location, impossible travel, device fingerprint/ID/type, device health and history, software signatures, and input from user behavioral analysis services. Thales attests to CSA Star Level 1, and has certifications for ISO 27001/27018, SSAE SOC 2 Type 2, UK G-Cloud as well as eIDAS, ANSSI, and FIDO2. The solution accepts CAC/PIV, Feitian, Google Titan, any OATH-based, RSA SecurID, Smart Cards, Thetis, and Yubikey hardware authenticators. Thales supports Kerberos, OAuth, OIDC, RADIUS, and SAML protocols and LDAP and SCIM for bulk provisioning.

As the threat landscape becomes more sophisticated, organizations understand that they need to expand MFA to a much broader range of users and applications. The value of the platform is that Thales can offer a broader range of authentication methods. Organizations in highly regulated industries and organizations that place a premium on security, in both the public and private sectors, that need high strength MFA options may want to consider Thales' SafeNet Trusted Access.

THALES

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

Strengths

- Strong identity proofing capabilities
- Flexible deployments
- Ability to comply with country-specific regulatory requirements
- Good OOTB selection of connectors
- Excellent anti-tampering security mechanisms
- Broad range of authenticator types supported

Challenges

- Risk engine not accessible via API
- No integration with UEM solutions

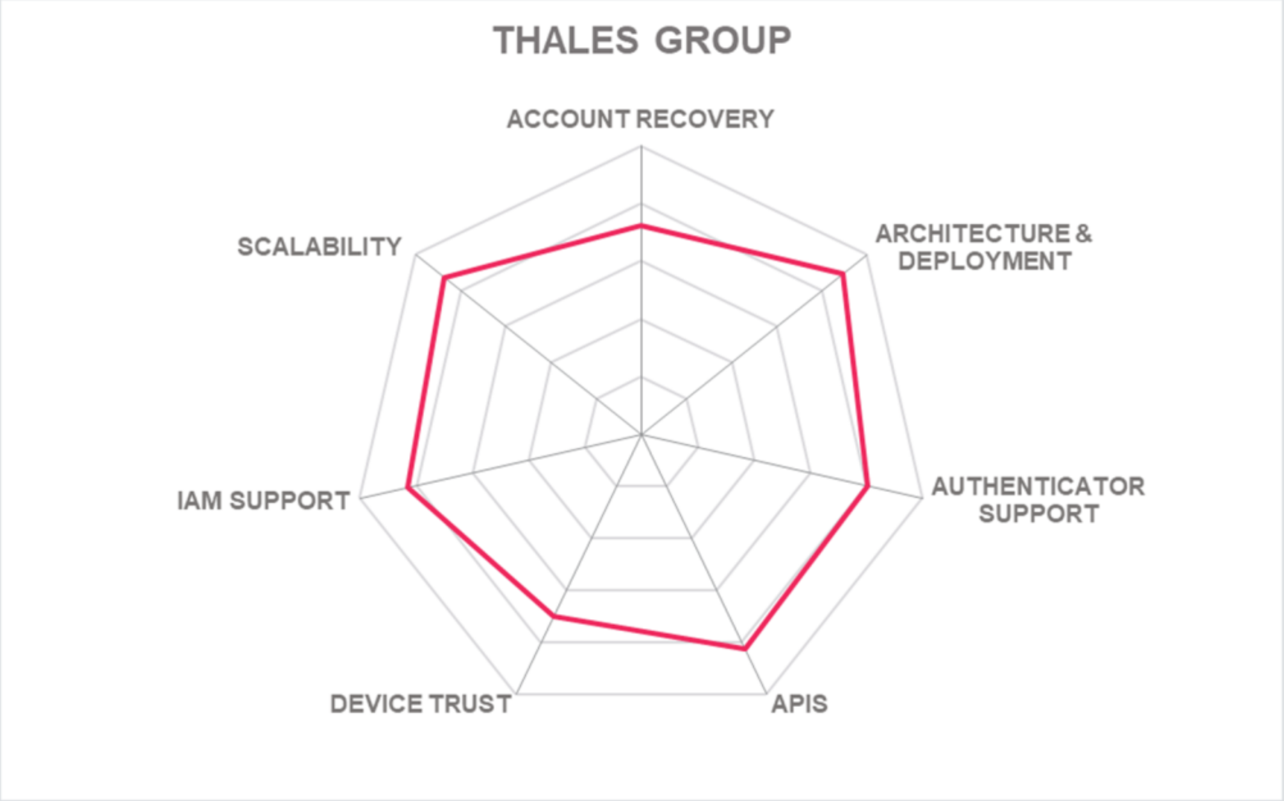
Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER


THALES GROUP
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.24 Transmit Security

Transmit Security was founded in 2014 and is headquartered in Tel Aviv and Boston. The company provides innovative authentication and risk management solutions to small and large companies worldwide. Its portfolio is built to address B2C, B2B, and B2B2C IAM needs. Transmit Security offers a comprehensive passwordless authentication solution for customer and workforce authentication. The platform includes several modules such as app-less web authentication, workstation authentication, advanced decisioning engine, integration engine and more. However, the specific architecture deployed depends on the specific customer use cases.

Transmit Security's platform has strong omni-channel capabilities and covers cross-channel use cases in a simple and seamless manner. In addition, its platform and identity orchestration capabilities allow organizations to configure and build flexible identities-related customer journeys. Also, it is not necessary for users to use a mobile app for authentication, only their native devices are needed. Furthermore, customers can embed the functionality of their passwordless into the customer's own mobile app.

Transmit Security supports CAC/PIV cards, Duo, Feitian, Google Titan, Kensington Security Key, OneSpan DigiPass, RSA SecurID, Smartcards, Symantec VIP, Thetis, and Yubikey tokens. In addition, Transmit supports FIDO2 standards and also integrates with many other vendors through other protocols such as Kerberos, RADIUS, JWT, OATH, SAML and OIDC. Transmit also offers a secure mobile SDK that gathers the full range of device intelligence. All the normal account recovery mechanisms are present.

Transmit Security's platform processes over a billion transactions daily for their customers worldwide. The platform has one of the most feature-rich offerings in the passwordless authentication market and would likely be suitable for any type of organization looking to adopt a passwordless solution. Transmit Security appears in the product, market, and innovation leadership categories.

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

transmit security

Strengths

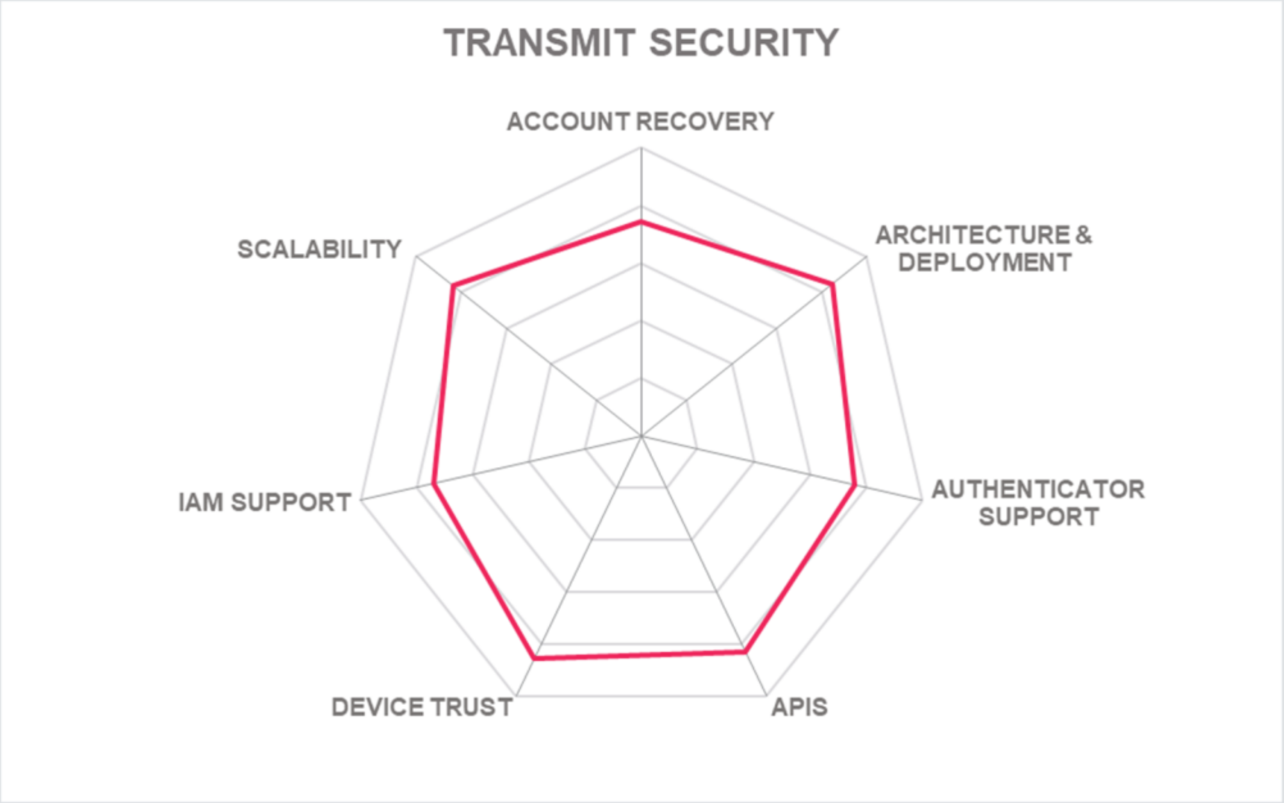
- User friendly platform
- Global partner ecosystem
- Flexible deployment options
- Good selection of authenticators
- Strong omni-channel features
- Excellent orchestration capabilities

Challenges

- Device health checks mechanisms are limited
- Lack of OOTB connectors for SaaS apps

Leader in

OVERALL LEADER · PRODUCT LEADER · INNOVATION LEADER · MARKET LEADER


TRANSMIT SECURITY
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

5.25 tru.ID

Tru.ID is headquartered in London and was founded in 2020 by serial entrepreneurs who previously built cloud communications and payments platforms mBlox, Nexmo, and Boku. Despite being a young and small vendor, tru.ID is innovative and provides a distinctive passwordless and phishing resistant solution. Tru.ID uses the cryptographic security of the SIM card that resides in every phone to deliver a binary response that confirms a verified identity (with the mobile number), a verified credential (with the SIM card), and a verified digital presence (with the active session). The product is targeted to workforce, consumer, and partner use cases.

tru.ID provides an enterprise-friendly single point of integration for businesses looking to deploy SIM-based authentication. tru.ID\'s APIs provide an abstraction layer on top of the disparate, individual APIs provided by Mobile Network Operators (MNOs). By connecting to tru.ID, businesses avoid the need to contact and connect with technically to multiple MNOs in every market. The company connects mobile operators and carriers in Germany, Italy, UK, Spain, France, Netherlands, India, Canada and recently in the US. The solution is a multi-tenant cloud service hosted by tru.ID on AWS, distributed across multiple geographical sites. To ensure compliance with local data-privacy laws, each of these clouds is completely geo-sovereign.

The solution is designed to replace passwords, SMS codes, and Bank Card Readers with a secure Digital Identity based on the SIM card in the user's mobile phone. In this approach, cloning is prevented based on modern SIM card algorithms, as well as tampering, since the encryption key is stored within the SIM card. To authenticate a device and user, the solution passes the phone number from the mobile handset of the customer to the mobile operator. The Mobile Network Operator then provides a Y/N response to evaluate whether or not the phone number corresponds to the SIM card in the active mobile data session. Apart from the phone number, the solution does not store any personal information, and once processed, it is encrypted with a one-way hash that cannot be further accessed.

Since the solution is mobile-first, tru.ID also offers a first-party authenticator app, which can be useful for enterprise authenticator usage. tru.ID also provides an OpenID Connect service that makes it easy for customers to add tru.ID as a passwordless authentication option with any existing IAM platform that supports OIDC. Tru.ID provides a possession-factor solution that is low-code, data privacy compliant, cryptographically secure, and easy to use. However, the number of OOTB connectors for SaaS applications and device management capabilities need to be addressed. Organizations that prefer a cost-effective and user-friendly phishing resistant solution for their enterprise authentication and Identity API security needs should consider tru.ID.

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

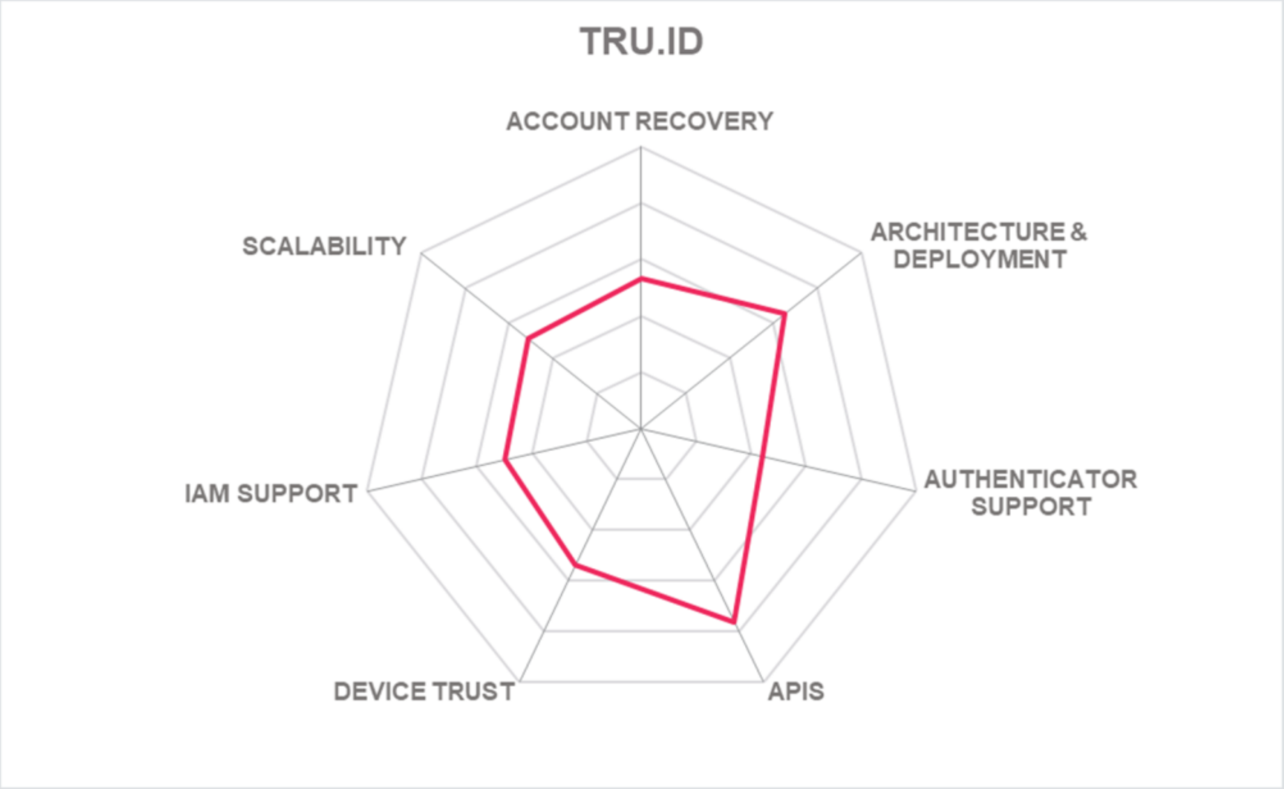
tru.id

Strengths

- Cost-efficient
- Easy to deploy and user friendly
- SIM-based authentication via API
- Low code OIDC implementation
- Available for iOS and Android
- Phishing resistant and cryptographically secure
- Comprehensive set of APIs and rich developer tools

Challenges

- SAML not supported
- Smaller company but rapidly expanding
- Limited device management capabilities
- Security certifications and standards in progress
- Additional out-of-box integrations for major IAM platforms needed, but developments are on the roadmap


TRU.ID
ACCOUNT RECOVERY
ARCHITECTURE & DEPLOYMENT
AUTHENTICATOR SUPPORT
APIS
DEVICE TRUST
IAM SUPPORT
SCALABILITY

6 Related Research

Leadership Compass CIAM Platforms
Leadership Compass Enterprise Authentication
Leadership Compass Consumer Authentication
Leadership Compass Identity Fabrics
Leadership Compass Fraud Reduction Intelligence Platforms
Leadership Compass Providers of Verified Identity
Whitepaper Customer Authentication with Zero-Friction Passwordless Authentication
Whitepaper Serving the Customer in the Digital Age
Whitepaper Technical Approaches to Consent Management and Dynamic Access Management: Ping Identity
Whitepaper Simplifying and Strengthening Authentication with Passwordless Desktop MFA
Whitepaper A Passwordless Future Begins with Credential Management
Whitepaper The Future is Passwordless. If you do it right
Whitepaper Planning for a \"Passwordless\" future
Executive View Beyond Identity Secure Customers
Executive View OneWelcome Customer Identity and B2B Identity
Executive View IBM Security Verify for CIAM
Executive View HYPR Passwordless and Phishing-resistant Authentication

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 within that market segment. It is the compass which assists you in identifying the vendors and products/services in that market which you should consider for product decisions. It should be noted that it is inadequate to pick vendors based only on the information provided within this report.

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

Types of Leadership

We look at four types of leaders:

- **Product Leaders:** Product Leaders identify the leading-edge products in the particular market. These products deliver most of the capabilities 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 they become Overall Leaders by being above average in all areas.

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

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

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

Product rating

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

KuppingerCole uses the following categories to rate products:

- **Security
- Functionality
- Deployment
- Interoperability
- Usability**

Security is a measure of the degree of security within the product / service. This is a key requirement and evidence of a well-defined approach to internal security as well as capabilities to enable its secure use by the customer are key factors we look for. The rating includes our assessment of security vulnerabilities and the way the vendor deals with them.

Functionality is a measure of three factors: what the vendor promises to deliver, the state of the art and what KuppingerCole expects vendors to deliver to meet customer requirements. To score well there must be evidence that the product / service delivers on all of these.

Deployment is measured by how easy or difficult it is to deploy and operate the product or service. This considers the degree in which the vendor has integrated the relevant individual technologies or products. It also looks at what is needed to deploy, operate, manage, and discontinue the product / service.

Interoperability refers to the ability of the product / service to work with other vendors' products, standards, or technologies. It considers the extent to which the product / service supports industry standards as well as widely deployed technologies. We also expect the product to support programmatic access through a well-documented and secure set of APIs.

Usability is a measure of how easy the product / service is to use and to administer. We look for user interfaces that are logically and intuitive as well as a high degree of consistency across user interfaces across the different products / services from the vendor.

We focus on security, functionality, ease of delivery, 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 the highest potential for failure of IT projects.
- Lack of excellence in Security, Functionality, Ease of Delivery, Interoperability, and Usability results in the need for increased human participation in the deployment and maintenance of IT services.
- Increased need for manual intervention and lack of Security, Functionality, Ease of Delivery, Interoperability, and Usability not only significantly increase costs, but inevitably lead to mistakes that can create opportunities for attack to succeed and services to fail.

KuppingerCole's evaluation of products / services from a given vendor considers the degree of product Security, Functionality, Ease of Delivery, Interoperability, and Usability which to be of the highest importance. This is because lack of excellence in any of these areas can result in weak, costly and ineffective IT infrastructure.

Vendor rating

We also rate vendors on the following characteristics

- Innovativeness
- Market position

- Financial strength
- Ecosystem

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

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

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

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

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

Rating scale for products and vendors

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

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

Positive
Strong support for a feature area or strong position of the company, but with some minor gaps or shortcomings. Using Security as an example, this can indicate some gaps in fine-grained access controls of administrative entitlements. For market reach, it can indicate the global reach of a partner network, but a rather small number of partners.

Neutral

Acceptable support for feature areas or acceptable position of the company, but with several requirements we set for these areas not being met. Using functionality as an example, this can indicate that some of the major feature areas we are looking for aren't met, while others are well served. For Market Position, it could indicate a regional-only presence.

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

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

Inclusion and exclusion of vendors

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

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

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

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

We provide a quick overview about vendors not covered and their 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 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.