KuppingerCole ANALYSTS

Passwordless Authentication for Enterprises

Alejandro Leal

September 3, 2024



LEADERSHIP COMPASS 2024

This report provides a detailed examination of passwordless authentication technologies designed for enterprise use cases. As organizations increasingly prioritize robust and streamlined security protocols, the demand for sophisticated passwordless solutions has grown significantly. This report explores the current landscape of enterprise-focused passwordless authentication technologies and guides businesses in selecting the most effective solution to meet their security needs. By analyzing the market segment, vendor product and service functionality, relative market share, and innovative approaches, organizations can make informed decisions about their authentication strategies for their employees and systems.

Contents

Executive Summary 4
Key Findings 6
Market Analysis 7
Market size 8
Delivery Models 9
Required Capabilities 9
Leadership 13
Overall Leadership 13
Product Leadership 15
Innovation Leadership 17
Market Leadership 19
Products and Vendors at a Glance 21
Product/Vendor evaluation 24
Spider graphs 24
1Kosmos – BlockID Workforce 26
Axiad – Axiad Cloud 29
Beyond Identity – Secure Workforce 32
cidaas – cidaas 35
Cisco – Duo 38
CyberArk – Identity Security Platform 41
Entrust – Identity as a Service (IDaaS) 44
Exostar – The Exostar Platform 47
GSMA – Number Verify 50
HID – Authentication Platform 53
HYPR – Identity Assurance Platform 56

© 2024 KUPPINGERCOLE ANALYSTS AG

IBM – IBM Security Verify 59
Idee – AuthN 62
Infinipoint – Zero Trust Workforce Access Platform 65
Microsoft – Microsoft Entra 68
Nok Nok – Nok Nok S3 Suite and Nok Nok Authentication Cloud 71
Okta – Okta Identity Cloud 74
One Identity – OneLogin Platform 77
OneSpan – OneSpan Authentication 80
Ping Identity – The Ping Identity Platform 83
Pointsharp – Pointsharp Platform 86
RSA – ID Plus 89
SAASPASS – SAASPASS IAM 92
Secfense – User Access Security Broker 94
SecureAuth – SecureAuth Workforce 96
Systola – SystoLOCK 99
Thales – OneWelcome 101
Vendors to Watch 104
Identité 104
IDlayr 104
Keyless Technologies 104
Micro Focus 105
Yubico 105

Executive Summary

In this Leadership Compass, we assess solutions that lay the groundwork for enterprises in adopting passwordless authentication. To better understand the fundamental principles this report is based on, please refer to KuppingerCole's Research Methodology.

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. To minimize the dependence on passwords, the industry has been working for a long time on different technical solutions and standards. As the industry continues to embrace innovative solutions, the era of passwordless is gradually evolving into more secure, user-friendly, and efficient authentication methods, marking a new stage in the evolution of digital security.

Given the security risks and inconvenience associated with passwords, there is a trend for organizations to replace and eliminate passwords altogether. Although the Internet has changed significantly since its inception, password authentication has remained virtually the same. The issue with passwords is that they can easily be stolen and compromised—without the knowledge of the user or the service provider. 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.

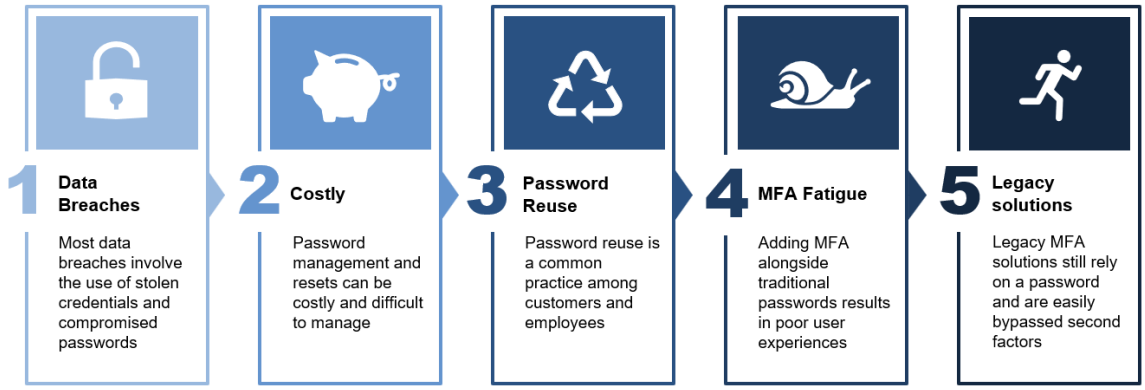


Figure 1: The problem with passwords

As a result, enterprises across various sectors are seeking more advanced security solutions to protect sensitive data and maintain high levels of operational integrity. In addition, as enterprises grow and their workforces become more mobile and distributed, particularly with the rise of remote work, the limitations of traditional passwords become even more pronounced. Large enterprises may have half a dozen or more different authentication systems, each potentially configured for different segments of the organization or for specific applications and services. This fragmentation may be due to historical acquisitions of other companies, departmental preferences, or the implementation of specialized solutions for certain types of data access.

©2024 KUPPINGERCOLE ANALYSTS AG

Ensuring secure access across different devices and locations demands a more robust and flexible authentication method. Passwordless authentication systems have emerged as a compelling alternative, offering enhanced security features and improved user convenience compared to traditional methods. Adopting passwordless authentication can lead to significant cost savings for enterprises. It reduces the burden on IT support related to password issues and decreases the potential financial losses from data breaches linked to compromised passwords. By investing in passwordless technologies, enterprises not only strengthen their security measures, but also position themselves as forward-thinking, prioritizing both user experience and protection against future threats.

Although passwordless options have been around for a while, some recent solutions are gaining traction with 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, frictionless user experience, and support for legacy applications and services.

It is important to note that passwordless authentication solutions tailored for enterprise use cases and those designed for consumer use cases exhibit distinct differences in response to varied expectations. Enterprise-focused solutions are typically designed to enhance security and control, integrating with existing corporate IT systems and aligning with internal security protocols and compliance requirements. These solutions often incorporate multifactor authentication (MFA) mechanisms that might include biometric data, security tokens, or mobile device verification to ensure robust protection against unauthorized access, particularly for sensitive corporate data and systems.

On the other hand, consumer-focused solutions must prioritize additional functionalities such as omnichannel experiences, self-service options, robust privacy management, a consistent and user-friendly interface, and the flexibility to operate on any device. These heightened expectations stem from the diverse preferences and demands of consumers who prioritize a personalized and adaptable authentication experience. The drive for convenience is paramount in consumer settings, where users expect to transition seamlessly between devices and platforms without noticeable security procedures hindering their interaction with digital services. For more information, read our Leadership Compass on Passwordless Authentication for Consumers.

Notably, user experience expectations diverge significantly between employees and consumers. Employees may tolerate more friction in the authentication process, aligning with organizational IAM policies, whereas consumers, driven by convenience, are prone to disengage if faced with complexity or delays. Additionally, consumer solutions must navigate the challenges of unmanaged IT environments, requiring adaptability to authenticate users securely on any device while prioritizing privacy and compliance with stringent regulations like GDPR. In essence, while both enterprise and consumer solutions aim for secure authentication, their emphasis on security measures, user experience, and scalability varies to meet the unique needs of each user category.

© 2024 KUPPINGERCOLE ANALYSTS AG

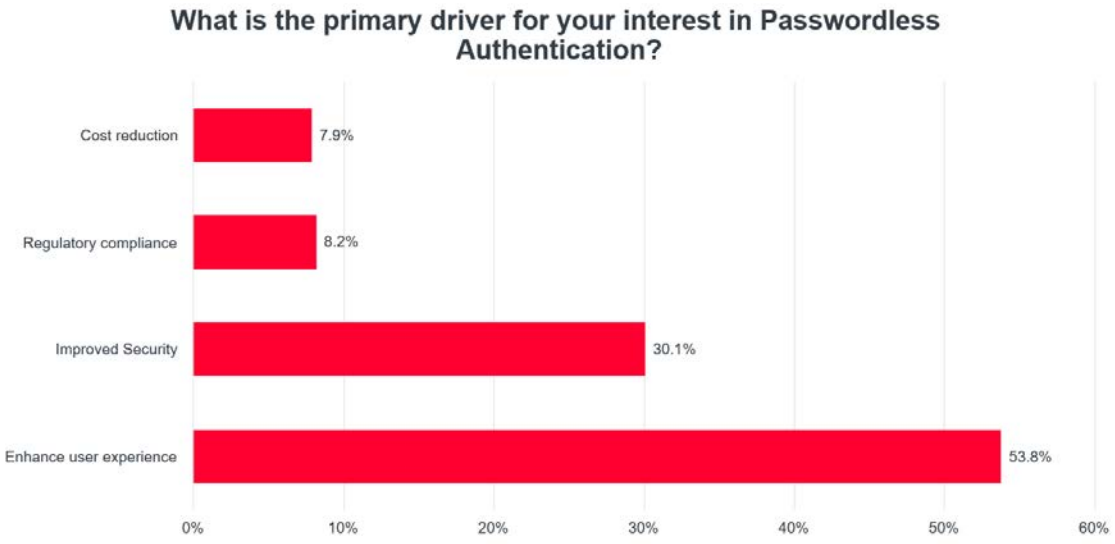


Figure 2: Main drivers of passwordless authentication adoption

However, organizations seeking passwordless authentication solutions must consider various factors, including security, ease of implementation, interoperability, and cost-effectiveness. The importance of user experience cannot be overstated, as seamless authentication processes are essential for further adoption. By understanding these considerations and evaluating the offerings from different vendors, enterprises can identify the solution that best meets their specific needs and preferences.

Key Findings

What are the top considerations buyers should know about?

- The passwordless authentication market is dynamic, vibrant, and competitive, with different vendors offering similar but distinct solutions.
- Despite the presence of major players, the evolving nature of the market allows smaller companies to enter and establish a niche by leveraging technical innovation or catering to specific use cases.
- User experience expectations diverge significantly between employees and consumers. While both groups benefit from the security and efficiency of passwordless systems, their divergent contexts and priorities necessitate tailored approaches.
- Enterprise-focused solutions are typically designed to enhance security and control, integrating with existing corporate IT systems and aligning with internal security protocols and compliance requirements.
- The creation of open standards such as FIDO2 and WebAuthn has increased the adoption of passwordless technologies. In addition, the use of passkeys is likely to be a catalyst for widespread adoption.

© 2024 KUPPINGERCOLE ANALYSTS AG

- The future promises a landscape where fewer passwords are needed, and their presence is largely obscured by passwordless solutions. However, passwords will still lurk in the shadows, along with the risks they impose, as lingering relics of an older era of digital authentication.
- The Overall Leaders (in alphabetical order) are 1Kosmos, Beyond Identity, Cisco, CyberArk, Entrust, HID, HYPR, IBM, Microsoft, Okta, OneSpan, Ping Identity, and Thales.

Market Analysis

The market for passwordless authentication products and services has witnessed exponential growth recently, driven by the increasing demand for secure and user-friendly authentication methods. This surge in demand has resulted in the emergence of a diverse set of vendors vying for prominence within the passwordless landscape. While the market is not yet considered mature, it remains highly dynamic and rife with opportunities for both established players and newcomers alike.

Despite the presence of major players, the evolving nature of the market allows smaller companies to enter and establish a niche by leveraging technical innovation or catering to specific use cases. This approach diversifies the market and drives competition and innovation, enriching the range of solutions available and pushing the boundaries of what passwordless technologies can achieve. Therefore, this KuppingerCole Leadership Compass deals with the most important players in the field of passwordless authentication for enterprises.

The accelerating adoption of passwordless solutions is closely tied to the evolving regulatory landscape and the establishment of industry standards. For example, 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. Furthermore, the development of open standards such as Fast Identity Online (FIDO) 2 has further generated adoption of passwordless technologies.

FIDO2 uses public key cryptography and strong authentication to enable passwordless authentication while reducing the risk of password-related attacks, such as phishing and credential stuffing. FIDO has also worked with companies such as Microsoft, Google, and Apple to integrate and adopt FIDO standards across their operating systems. More recently, these companies have announced plans to support passkeys on their platforms. For example, Apple's latest update, iOS 16 for iPhones as well as macOS Ventura for Macs, now supports passkeys, while Google introduced support for passkeys in December 2022.

Although the advantages are clear, several challenges hinder the widespread adoption of FIDO-based passwordless solutions in enterprises. First, there is the issue of interoperability; enterprises often use a complex mix of systems and technologies, and FIDO's protocols must integrate across all of them without compromising security or user experience. Additionally, while FIDO offers robust security features, enterprises must still manage the account recovery process effectively — a critical aspect that FIDO does not directly address, potentially leaving room for security gaps if not properly handled. These

challenges require careful consideration and strategic planning to ensure that the transition to passwordless authentication aligns with the enterprise's security needs and business goals.

Nevertheless, the transition to passwordless forms of authentication will continue to gain momentum. Organizations must evaluate the assurance level they seek for their applications and, if appropriate, leverage the benefits of passwordless technology. Therefore, 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). These techniques, once standard practices, are increasingly considered less secure and are no longer trusted by security professionals.

Market size

KuppingerCole predicts that the Compound Annual Growth Rate (CAGR) goes up to 31.1%, leading the passwordless authentication market to reach 6.6 billion USD by 2025. This expected growth can also be attributed to the user-friendliness of this method and to the possibility of the easy integration of those systems within a company framework, as well as the rising cases of data theft and the constant search of the companies to protect their sensitive information. North America and EMEA are the regions where this service is experiencing the strongest growth.

If implemented successfully, a passwordless solution will not only increase the security posture of the organization, but also deliver a convenient and frictionless user experience. While these solutions promise enhanced security and convenience, enterprises are faced with a myriad of options in the market. This report aims to demystify the landscape of passwordless authentication, offering organizations guidance in navigating the diverse array of products and services available.

What remains to be seen in the market is whether customers can overcome old-school mentalities. Despite the promise of new authentication methods, many people are still reluctant to move away from traditional security methods due to user acceptance, lack of education, security limitations, and deployment costs. In addition, there's also an interoperability issue that needs to be addressed in websites, ledgers, and wallets. This challenge arises from the diverse range of authentication protocols and standards used across different platforms and services, leading to compatibility issues and fragmentation in the authentication ecosystem.

For instance, if a password is still required by a third-party and the website does not support WebAuthn or similar technologies, users are forced to revert to traditional passwords, complicating what should be a streamlined process. This often results in an inconvenient and frustrating experience, as it contradicts the ease and security promised by passwordless solutions. For a more detailed exploration of these scenarios, take a look at The Second Law of AuthN Dynamics.

Additionally, some vendors continue to offer username/password authentication as an option for account recovery, available at the customer’s choice and not as a mandatory feature.

However, to truly advance toward a passwordless future, vendors must prioritize educating users on the vulnerabilities associated with traditional password systems and actively develop innovative or more secure alternatives. This approach enhances security and aligns with evolving expectations for more convenient and robust authentication solutions.

The declaration that "the password is dead" has echoed throughout the tech community for well over two decades, yet the reality is starkly different; passwords remain pervasive and stubbornly entrenched in digital authentication processes. Despite the significant shift towards passwordless authentication, the widespread and rapid disappearance of passwords seems unlikely. As a result, passwordless is destined to become yet another form of strong authentication, with its ability to fill specific use cases such as enterprise authentication.

The future promises a landscape where fewer passwords are needed, and their presence is largely obscured by passwordless solutions. However, passwords will still lurk in the shadows, a lingering relic of an older era of digital authentication. Although the need for passwordless authentication is growing, finding a solution that is simple, effective, and secure is challenging. For this reason, selecting the right passwordless solution that meets the unique challenges and needs of each organization is essential. The passwordless journey must consider the expectations of each of your organization's segments as well as the appropriate level of security and user experience.

Delivery Models

Passwordless authentication solutions are mainly delivered as a cloud hosted software-as-a-service (SaaS) solution, 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 period. On the other hand, for on-premises deployments, licensing costs can be measured as per-user or per-server.

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.

© 2024 KUPPINGERCOLE ANALYSTS AG

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 is essential for accommodating diverse user preferences and needs. This includes various methods such as physical (e.g., fingerprint, facial recognition) and behavioral (e.g., keystroke or mouse movement) biometrics, hardware tokens, mobile push notifications, and knowledge-based authentication.

Strong authentication, encompassing Two-Factor Authentication (2FA) and Multi-Factor Authentication (MFA), provides an added layer of security by requiring users to provide multiple forms of verification before gaining access. 2FA and MFA mechanisms are typically constructed from two or more authentication elements taken from three categories (something the user knows, like a password or PIN; something the user has, like a hardware device or mobile phone; and something the user is, like a biometric feature).

Risk, context-based, and continuous authentication leverages contextual information such as device location, user behavior patterns, and transaction history to dynamically assess the risk level associated with each authentication attempt. This approach enables organizations to adapt authentication requirements based on real-time risk assessments.

Adaptive and step-up authentication further enhance security by dynamically adjusting authentication requirements based on risk levels. Adaptive authentication automatically selects the appropriate authentication method based on contextual factors, while step-up authentication prompts users for additional verification when the risk level is elevated.

Support for legacy applications and services is crucial for ensuring seamless integration with existing infrastructure, allowing organizations to modernize their authentication processes without disrupting legacy systems.

Strong cryptographic approaches, such as Private/Public Key and Zero Knowledge Encryption enhance data confidentiality and integrity during authentication. Private/Public Key encryption uses asymmetric cryptography, where data is encrypted with a public key and decrypted with a private key. Zero Knowledge Encryption verifies credentials without exposing sensitive data.

Integration with third-party authenticators enables organizations to leverage additional authentication methods provided by external providers, expanding the range of options available to users.

Integration to MDM and UEM solutions involves connecting identity management systems with platforms that oversee and secure corporate devices. This integration ensures that device management policies align with user authentication and access controls, bolstering security across all organizational endpoints.

© 2024 KUPPINGERCOLE ANALYSTS AG

Integration capabilities to established platforms enable seamless integration with existing identity and access management (IAM) solutions, ensuring interoperability and ease of deployment.

Frictionless user experience refers to the design and implementation of systems and interfaces that minimize or eliminate obstacles and complexities that hinder user interaction. This approach is essential for promoting user adoption and satisfaction. Solutions should prioritize simplicity and ease of use while maintaining strong security measures.

Device trust across multiple devices allows organizations to establish trust levels for different devices based on factors such as device health, compliance status, and user behavior, enabling secure authentication across various endpoints.

Support for all major identity federation standards, including SAML (Security Assertion Markup Language) and OAuth, facilitates seamless single sign-on (SSO) experiences across different applications and services.

Comprehensive set of APIs refers to a robust and extensive collection of APIs that allow for deep customization and integration of software systems. These APIs facilitate interaction between different software components and third-party applications, enabling developers to build rich, interoperable, and scalable applications tailored to specific organizational needs.

Flexible, modern software architecture ensures scalability, resilience, and adaptability to evolving security threats and technological advancements. Such architectures are typically modular, making it easier to update, extend, or replace components without affecting the overall system.

BYOD support refers to the capability of identity management systems to accommodate personal devices used for work purposes. This feature ensures that personal smartphones, tablets, or laptops used to access corporate resources comply with security protocols while preserving user convenience and privacy.

Scalability and performance are critical for supporting large-scale deployments and ensuring responsive authentication processes, particularly in high-demand environments with millions of users. This involves ensuring that the system can expand to support an increased number of users, transactions, or data volume without degradation of performance.

Delegated administration allows for the distribution of administrative responsibilities among selected users or groups within an organization. This approach facilitates the efficient management of user access and security settings by enabling designated personnel to handle specific administrative duties under overarching IT security guidelines.

We expect solutions to cover most of these capabilities, at least at a 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."

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify 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 various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

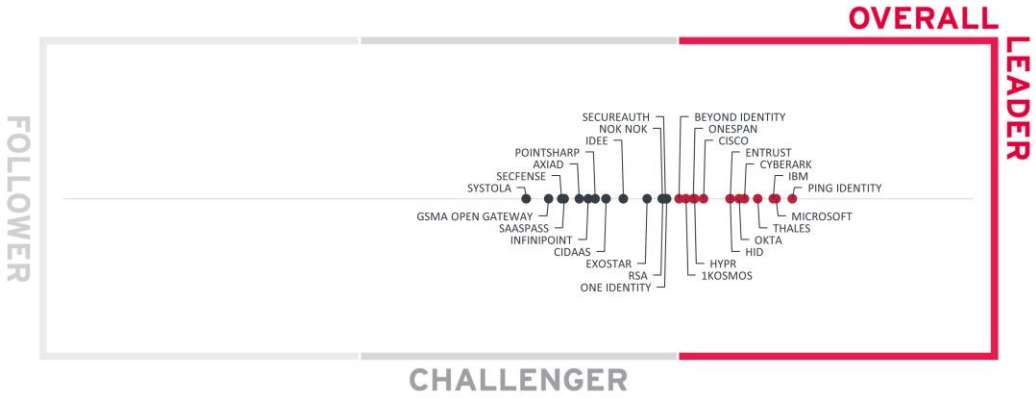


Figure 3: Overall Leadership in the passwordless authentication for enterprises market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

Ping Identity is in front in the Overall Leaders. The Ping Identity Platform stands out with its comprehensive approach, combining the strengths of ForgeRock and Ping Identity to offer a set of identity services addressing various challenges. Next is IBM, followed by Microsoft, Thales, CyberArk, Okta, HID, and Entrust. IBM's solution benefits from its integration to other IBM services and offers a wide selection of authentication mechanisms. Microsoft has the scalability and performance to provide organizations with several passwordless options

and feature-rich capabilities while Thales offers a versatile set of features designed to facilitate passwordless experiences for all user groups. CyberArk's solution is suitable for WFH and BYOD scenarios, as well as for organizations seeking a unified, passwordless approach. Okta delivers native user experiences for administrators and end-users, including an admin console, end-user dashboard, and native mobile/desktop apps. HID stands out for its identity verification services and strong credential issuance and management capabilities. Finally, 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 Cisco, HYPR, OneSpan, 1Kosmos, and Beyond Identity. This group of vendors is a mix of established and emerging players, some being stronger in their market position (Cisco and OneSpan) and others in innovativeness (HYPR, 1Kosmos, and Beyond Identity). 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.

The Challenger segment is more populated than the Leaders segment. Here, we see One Identity, SecureAuth, Nok Nok, RSA, Exostar, IDEE, cidaas, Infinipoint, Pointsharp, Axiad, SAASPASS, Secfense, GSMA, and Systola. 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 device posture features or compliance with major standards. All vendors within the Challenger section have good products with varying levels of scalability, orchestration, deployment, and API capabilities. Furthermore, some still have limited global presence, affecting their rating for Overall Leadership.

The Overall Leaders are (in alphabetical order):

- 1Kosmos
- Beyond Identity
- Cisco
- CyberArk
- Entrust
- HID
- HYPR
- IBM
- Microsoft
- Okta
- OneSpan
- Ping Identity
- Thales

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 4: Product Leadership in the passwordless authentication for enterprises market

In this 2024 edition, Ping Identity and IBM top the list for Product Leadership. CyberArk, Microsoft, Thales, HID, Entrust, and Okta are in close proximity far above the Leadership threshold. HYPR, Beyond Identity, 1Kosmos, Cisco, OneSpan, One Identity, IDEE, SecureAuth, RSA, Nok Nok, and cidaas are all north of the dividing line between challengers

and leaders here. These solutions are the most complete in terms of functionality, internal product security, deployment options, interoperability, usability, and integrations available.

Infinipoint, Exostar, and Axiad are at the top of the challengers for Product Leadership. SAASPASS, Secfense, Systola, Pointsharp, and GSMA are in the middle of the Challenger pack. The challengers need to add features and functions as will be elaborated upon in this report.

Product Leaders (in alphabetical order):

- 1Kosmos
- Beyond Identity
- cidaas
- Cisco
- CyberArk
- Entrust
- HID
- HYPR
- IBM
- IDEE
- Microsoft
- Nok Nok
- Okta
- One Identity
- OneSpan
- Ping Identity
- RSA
- SecureAuth
- Thales

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.

This view is mainly based on the evaluation of innovative features, services, and technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

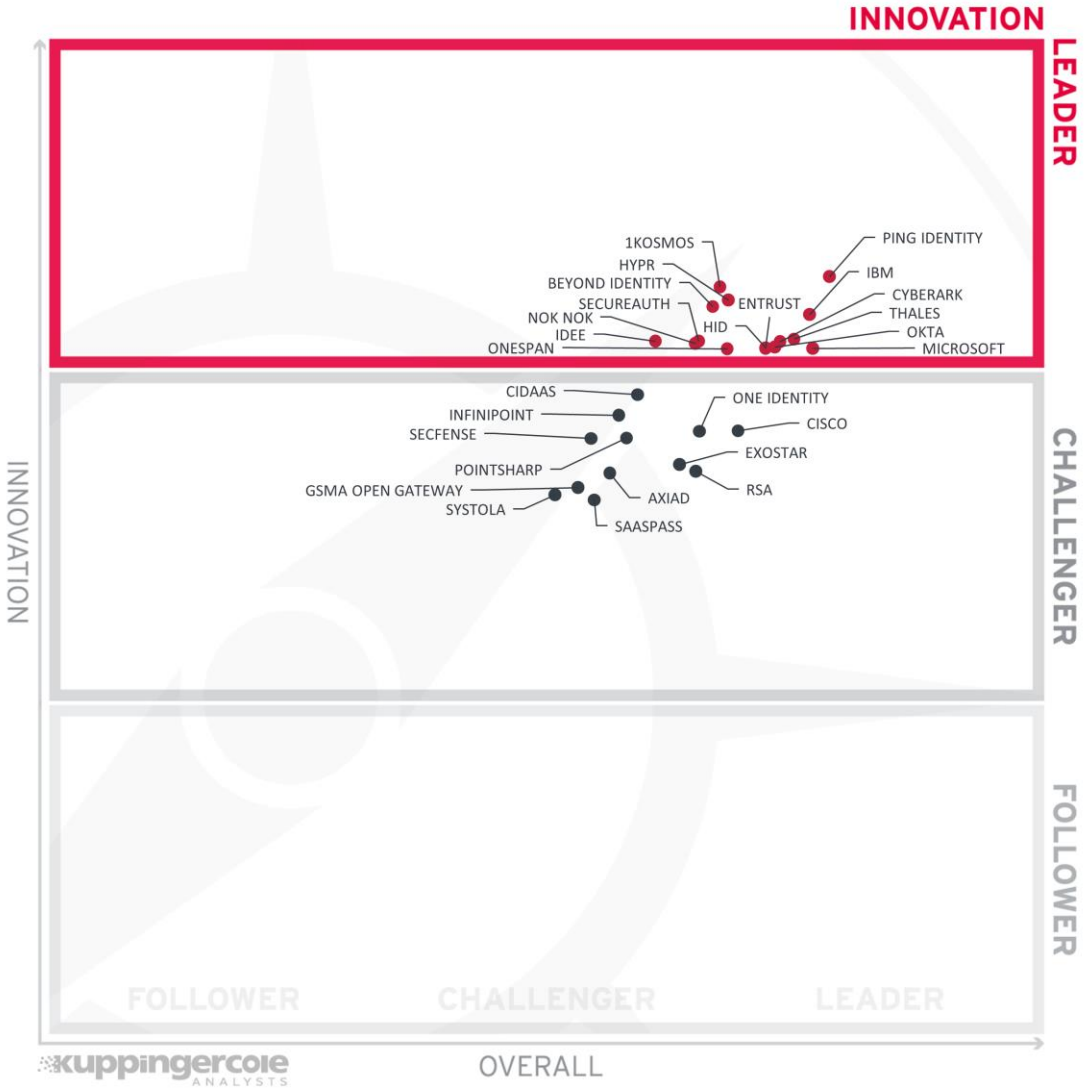


Figure 5: Innovation Leadership in the passwordless authentication for enterprises market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests, but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a 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.

Ping Identity, 1Kosmos, HYPR, Beyond Identity, and IBM form the uppermost tier of Innovation Leaders in Passwordless for Enterprises. Thales, CyberArk, SecureAuth, Nok Nok, Okta, HID, Entrust, OneSpan, Microsoft, and IDEE are also in the Innovation Leader area, each offering advanced capabilities that appeal to deploying organizations.

Cidaas and Infinipoint are the top Challengers in Innovation, exhibiting significant advancements but slightly behind those above. Next, we find Cisco, Secfense, Pointsharp, One Identity, Exostar, Axiad, GSMA, RSA, Systola, and SAASPASS. Each of these vendors have specific innovations, likely targeted at their existing customer base.

Innovation Leaders (in alphabetical order):

- 1Kosmos
- Beyond Identity
- CyberArk
- Entrust
- HID
- HYPR
- IBM
- IDEE
- Microsoft
- Nok Nok
- Okta
- OneSpan
- Ping Identity
- SecureAuth
- Thales

© 2024 KUPPINGERCOLE ANALYSTS AG

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the number of transactions evaluated, the 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 the financial health of the participating companies. Market Leadership, from our perspective, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.



Figure 6: Market Leaders in the passwordless authentication for enterprises market

Microsoft is leading the market, being a dominant player in the IAM space. Following them are large IT vendors with a considerable footprint in the IAM market; these are Thales, Ping Identity, IBM, Okta, CyberArk, Entrust, Cisco, HID, RSA, Exostar, One Identity, and OneSpan.

The rest of the vendors are rated as Challengers. These are smaller vendors with mostly small partner ecosystems and limited market presence on a global scale. Several of these vendors are relatively young and focus mainly on a single industry or region.

Market Leaders (in alphabetical order):

- Cisco
- CyberArk
- Entrust
- Exostar
- HID
- IBM
- Microsoft
- Okta
- One Identity
- OneSpan
- Ping Identity
- RSA
- Thales

Products and Vendors at a Glance

This section provides an overview of the various products we have analyzed within this Leadership Compass. 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. Since some vendors may have multiple products, these are listed according to the vendor's name.

Vendor	Security	Functionality	Deployment	Interoperability	Usability
1Kosmos	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Axiad	Positive	Strong Positive	Strong Positive	Positive	Positive
Beyond Identity	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
cidaas	Positive	Strong Positive	Strong Positive	Strong Positive	Positive
Cisco	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
CyberArk	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Entrust	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Exostar	Strong Positive	Positive	Positive	Positive	Positive
GSMA	Positive	Neutral	Positive	Weak	Positive
HID	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
HYPR	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
IDEE	Strong Positive	Positive	Strong Positive	Strong Positive	Strong Positive
Infinipoint	Strong Positive	Positive	Positive	Strong Positive	Positive
Microsoft	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Nok Nok	Strong Positive	Strong Positive	Strong Positive	Positive	Strong Positive
Okta	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive
One Identity	Strong Positive	Strong Positive	Positive	Strong Positive	Strong Positive
OneSpan	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Positive
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive	Strong Positive

© 2024 KUPPINGERCOLE ANALYSTS AG

Pointsharp	Positive	Strong Positive	Positive	Positive	Strong Positive
RSA	Strong Positive	Positive	Strong Positive	Strong Positive	Strong Positive
SAASPASS	Positive	Positive	Neutral	Strong Positive	Strong Positive
Secfense	Neutral	Positive	Strong Positive	Positive	Positive
SecureAuth	Strong Positive	Positive	Strong Positive	Positive	Strong Positive
Systola	Positive	Positive	Positive	Weak	Positive
Thales	Strong Positive	Strong Positive	Strong Positive	Strong 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	Strong Positive	Positive	Positive	Positive
Axiad	Neutral	Neutral	Positive	Neutral
Beyond Identity	Strong Positive	Positive	Positive	Strong Positive
cidaas	Positive	Neutral	Neutral	Weak
Cisco	Positive	Strong Positive	Strong Positive	Strong Positive
CyberArk	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Entrust	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Exostar	Neutral	Strong Positive	Strong Positive	Strong Positive
GSMA	Neutral	Neutral	Positive	Neutral
HID	Strong Positive	Strong Positive	Strong Positive	Strong Positive
HYPR	Strong Positive	Positive	Positive	Positive
IBM	Strong Positive	Strong Positive	Strong Positive	Strong Positive
IDEE	Strong Positive	Neutral	Neutral	Neutral
Infinipoint	Positive	Neutral	Neutral	Neutral
Microsoft	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Nok Nok	Strong Positive	Positive	Neutral	Positive
Okta	Strong Positive	Strong Positive	Strong Positive	Strong Positive
One Identity	Positive	Strong Positive	Strong Positive	Strong Positive

© 2024 KUPPINGERCOLE ANALYSTS AG

OneSpan	Strong Positive	Strong Positive	Positive	Positive
Ping Identity	Strong Positive	Strong Positive	Strong Positive	Strong Positive
Pointsharp	Positive	Neutral	Positive	Neutral
RSA	Neutral	Strong Positive	Strong Positive	Strong Positive
SAASPASS	Neutral	Neutral	Neutral	Positive
Secfense	Positive	Neutral	Weak	Neutral
SecureAuth	Strong Positive	Positive	Positive	Positive
Systola	Neutral	Weak	Weak	Neutral
Thales	Strong Positive	Strong Positive	Strong Positive	Strong Positive

Table 2: Comparative overview of the ratings for vendors

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 this market segment, we look at the following categories:

Architecture – 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.

Authentication – here, we measure the variety and usefulness of authentication methods present within each solution. Almost all solutions support username/password and various OTP methods. Therefore, advanced support for authentication mechanisms, especially FIDO, mobile, behavioral biometrics and mobile SDKs are preferred.

Device Posture – this looks at how the vendor's solution can enforce corporate security policies across devices, ensuring compliance with internal and external standards. It evaluates 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, device trust, and support for BYOD.

IAM Support – here, we evaluate 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 solution 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.

Identity APIs – this category is related to architecture but focuses more on the extensive range and adaptability of APIs beyond basic REST support. This category assesses not only the variety of API protocols available, but also emphasizes the ease with which these APIs can be customized to fit specific business needs. They ensure reliable integration and consistent performance across various digital services. Identity APIs are pivotal in supporting scalable, secure, and flexible identity services that can adapt to the evolving demands of modern digital ecosystems.

Scalability – this rating is influenced by many factors including the architecture of the vendor solution, the number of customers supported and deployment models available. For SaaS-delivered solutions, multi-cloud utilization, geographic distribution, SLAs, and maximum supported number of transactions per second are considered.

© 2024 KUPPINGERCOLE ANALYSTS AG

Compliance – here, we assess the robustness of the security measures implemented, including encryption standards, data protection, compliance with regulatory requirements, and the ability to resist various threats, including phishing, ransomware, fraud, and other password-based threats. This category also looks at whether the vendor has obtained relevant security certifications and accreditations, such as ISO/IEC 27001, SOC 2 Type II, or others.

© 2024 KUPPINGERCOLE ANALYSTS AG

1Kosmos – BlockID Workforce

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 1Kosmos platform provides a suite of products for enterprise use (BlockID Workforce), private consumer use (BlockID Customer), and identity verification (BlockID Verify). The 1Kosmos 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. They have simplified their licensing options to just per-user.

1Kosmos improves workforce identity verification by optimizing the speed and accuracy of onboarding processes, crucial for organizations adopting remote or hybrid work models. It provides a self-service identity verification system that recognizes government-issued credentials from 205 countries. This automation reduces administrative tasks and accelerates the onboarding of new employees by streamlining document verification and minimizing manual overhead. With BlockID Workforce, users authenticate using various methods, depending on their needs, the risk profile of the activity, and the security requirements of each access request.

The solution addresses the unique challenges of shared workstation environments common in sectors like call centers, travel, hospitality, and manufacturing. 1Kosmos provides a biometric key, capable of withstanding 200,000 uses and registering up to 10 fingerprints per user. It connects to a central authentication server—available as both cloud-based or on-premises—allowing numerous users to securely log in from a single device without personal hardware tokens. The biometric key is easily replaceable if damaged, ensuring no need for user re-registration and maintaining secure, continuous access across various settings.

In addition, 1Kosmos offers a biometric capability known as LiveID, which uses a proprietary 3D modelling technique for face detection. It is patent pending and captures the live motion, emotion, as well as 3D map of a user’s face while enrolling the user. This is immediately followed by asking the user to provide a government-issued document such as a driver's license or a passport to ensure that the user enrolling the LiveID is the same user who has enrolled into the platform. Through the feature, account recovery relies on a user's facial biometrics, captured during registration, thus ensuring identity verification, and eliminating the risk of unauthorized account access.

The solution supports industry authentication standards such as OAuth, OIDC, SAML, WS-Fed, WS-Trust, and FIDO. It also provides legacy support for RADIUS and offers interoperability across a wide range of operating systems, including Windows, MacOS, iOS, Android, Linux, and Unix. To strengthen security compliance, 1Kosmos has been independently certified with the ISO/IEC 27001 and EIDAS standards, as well as certified by FIDO2, AICPA SOC 2 Type II, and DEA EPCS and ISO/IEC 30107-3 by iBeta. The company is also certified to the NIST 800-63-3 standard by Kantara. Furthermore, 1Kosmos provides its own authenticator, which is FIDO2 certified, and it also supports Yubico, Trust Key,

Feitian, OneSpan, Thetis, Google Titan, and others. The platform has also enabled authentication using the FIDO key on the 1Kosmos mobile app itself.

In addition to the rapid deployment, the 1Kosmos platform supports legacy systems and multiple authentication channels with a high level of flexibility and scalability. Overall, 1Kosmos offers a robust and innovative approach to passwordless authentication that combines advanced biometric authentication, strong fraud detection features, support for verifiable credentials, and seamless integration capabilities. 1Kosmos appears in the overall, product, and innovation leadership categories, which should be of interest to organizations in North America and the APAC.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 3: 1Kosmos' rating

Strengths

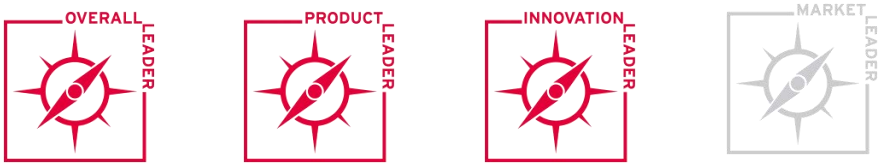
- Flexible account recovery options.
- Many out-of-the-box integrations.
- Mature platform with significant customer base.
- Identity proofing and onboarding capabilities.
- Strong set of APIs for integration.
- Integrates identity verification and passwordless authentication into a single platform.
- Support for a variety of use cases, including shared workstation environments.

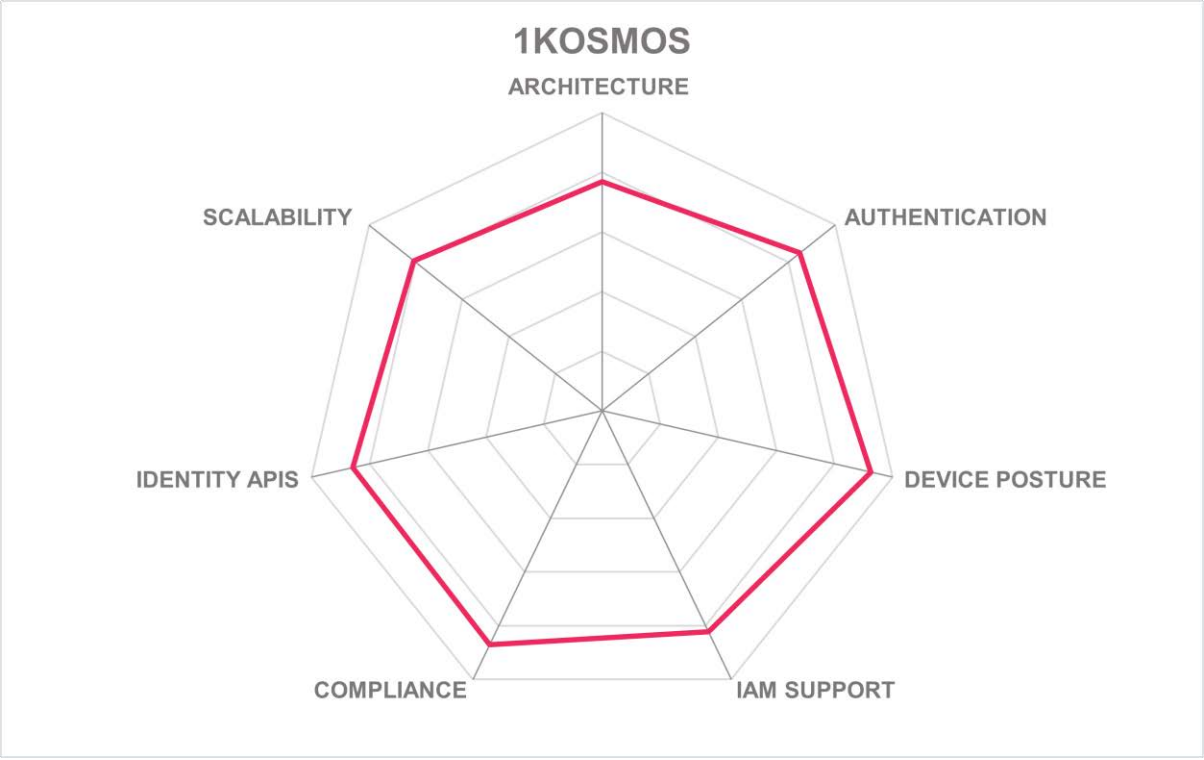
Challenges

- Does not use compromised credential intelligence.
- Little market visibility outside of North America and the APAC regions.
- Limited reporting capabilities but enhancements are on the roadmap.
- Rapid evolution of standards requires continuous, high technology investments.

©2024 KUPPINGERCOLE ANALYSTS AG

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


1KOSMOS
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Axiad – Axiad Cloud

Axiad, founded in 2010, is an established 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. Axiad offers a holistic passwordless orchestration platform, Axiad Cloud, that can augment authentication systems across an organization or act as its standalone MFA solution while addressing the complexities of a typically heterogeneous IT infrastructure. Licensing models supported include per-transaction and per-time-period options.

Axiad Cloud includes advanced self-service capabilities that increase efficiency and security within an organization. The Axiad AirLock feature automates help desk operations and credential enrollment, enabling organizations to enforce and control the rollout of passwordless authentication through an endpoint client that integrates with existing IAM infrastructure. This customization ensures compliance with organizational security policies. Axiad MyCircle offers peer-to-peer credential management, allowing co-workers to assist each other with tasks like resetting PINs, renewing tokens, or verifying credentials, effectively decentralizing helpdesk responsibilities. This approach alleviates the burden on IT teams and provides a cost-effective and secure alternative to traditional helpdesk interactions, enhancing operational efficiencies across the board.

Additionally, the solution is specifically crafted for either cloud-based scenarios or integration into on-premises setups within air-gapped and critical environments, providing robust, government-grade, phishing-resistant authentication without relying on passwords. The solution addresses a wide range of user needs, including employees, contractors, vendors and suppliers, by offering various authentication methods, including physical devices such as YubiKeys, smart cards, PIV cards and USB keys, as well as virtual platform options such as virtual smart cards. The solution supports FIDO U2F, FIDO2, mobile push, and mobile apps. Axiad expects to achieve FIDO2 certification in 2025 on the strength of a Q3 2024 update that supports provisioning of FIDO2 security keys as well as an “on-behalf” function that allows IAM administrators to manage passkeys for extended enterprise workforces.

In addition to FIDO support, Axiad Cloud also provides two enterprise-class PKI-as-a-Service capabilities. The first allows admins to deploy x.509 certificates to endpoint devices, hardware-based authenticators, and machines like Linux servers and Apple endpoints that don’t support a full range of FIDO functionality. The second works in conjunction with MFA methods to support phishing-resistant user authentication. In addition, the PKIaaS capabilities support WFH, BYOD, and partner devices, the workloads found in VMs and containers, and encrypted interactions for emails and attached documents across the entire environment. In any of these use cases, customization of certificate authorities, certificates and advanced workflows like renewal and revocation are enabled through a broad range of included protocols.

As a SaaS solution, Axiad Cloud is low-touch and provides a rich set of self-management tools for end users and administrators. High-scale deployment is eased through the AirLock feature described above, which brings issuance prompts directly to the user’ login screen without having to redirect them to additional applications or portals. Importantly, this feature

works for new issuance and renewal in a consistent workflow that is manageable and accessible for non-IT endpoint users. 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 Type II certified.

Axiad Cloud provides a secure and simplified single platform that allows customers to address authentication in a holistic fashion. As an augmentation focused on enterprise-class credential management, it allows customers to enhance their existing MFA solutions to make them phishing-resistant and robust enough to meet NIST, CISA and FedRAMP standards. Axiad Cloud's flexibility and robust security features make it an attractive choice for enterprises looking to enhance their cybersecurity posture without complicating their existing IT infrastructure.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

Table 4: Axiad's rating

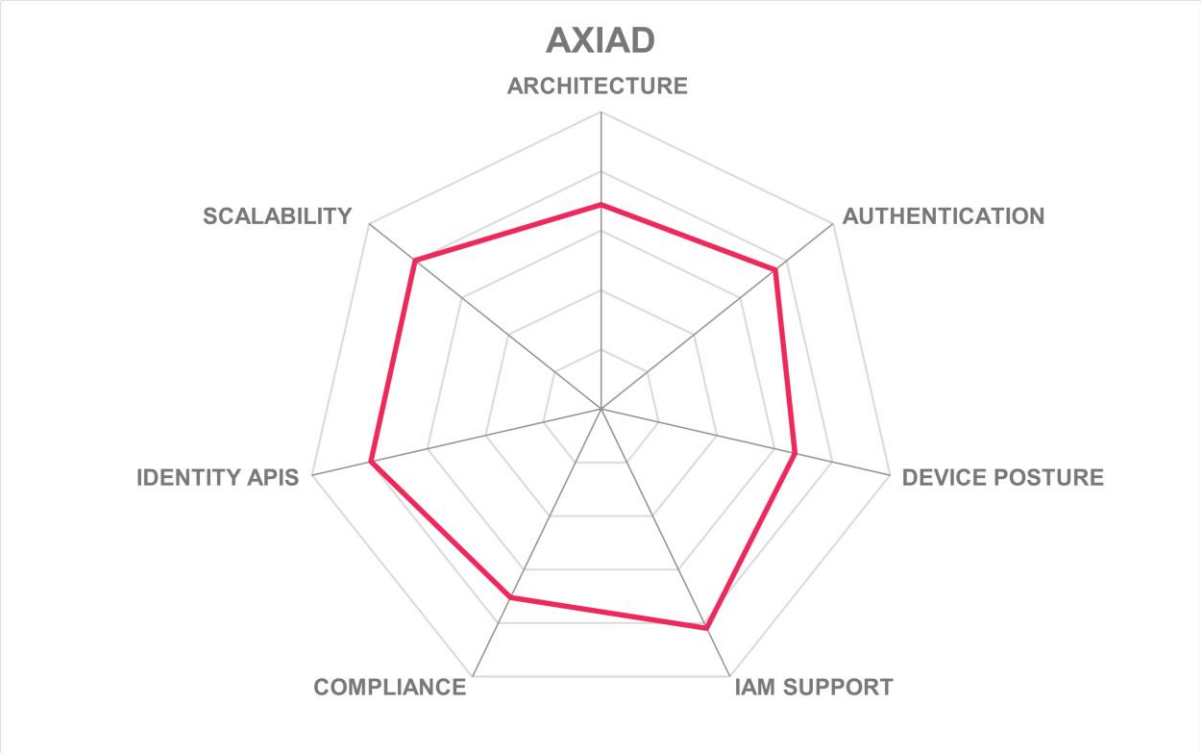
Strengths

- Specialist in workforce authentication.
- Wide range of authenticators.
- Extensive support for certificate-based device security.
- Built-in, cloud-based, customizable PKI.
- Integrates easily with a company's existing IAM infrastructure.
- Self-service capabilities such as AirLock and MyCircle.
- Good solution for hybrid and BYOD scenarios.
- Unique peer-to-peer credential management scheme increases usability and decreases support costs.
- Endpoint client that allows customers to enforce the rollout of passwordless MFA.

Challenges

- Missing FIDO2 certification.
- Customer presence is still primarily in North America.
- Dashboards are not customizable, but improvements are on the roadmap.

©2024 KUPPINGERCOLE ANALYSTS AG


AXIAD
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Beyond Identity – Secure Workforce

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, risk-based authentication, and Zero Trust approaches. The company is primarily focused on North America but has a growing number of customers in EMEA. Secure Workforce products offer per user licensing on a monthly basis.

Secure Workforce is a passwordless MFA solution aimed at organizations looking to eliminate passwords as an authentication method. The platform replaces passwords with secure credentials based on their solution that uses self-signed certificates and public-private key pairs. Using the self-signed x.509 certificate and the public-private key pairs ensures that users are in possession of only two attributes: "something you are" from the device biometric and "something you own" from the possession of a private key. The private key is securely stored in the device's enclave, ensuring it remains fixed and unexposed, which is critical for maintaining its integrity and confidentiality. This private key is cryptographically tied to the user's identity during registration, enhancing security by ensuring that the key is unique and distinctly associated with that user only. Biometric verification acts as proof of possession, confirming the user's identity by demonstrating control over the private key through a biometric challenge.

The prevalence of remote work and the use of cloud-based applications has made device trust an essential part of the security architecture of an organization. Beyond Identity's capacity to deliver a cryptographic method to validate the identity of a person using multiple devices, including unmanaged devices and Bring Your Own Device (BYOD), in real time is a key advantage. To further enforce device trust and security, the solution verifies that the user behind the device (or multiple) is authorized to use the device and detects if the device is secure enough for accessing the application or service being requested. It improves security by extracting over 100 different data points on device security posture to make informed, policy-based authentication decisions. This approach integrates risk signals from advanced EDR tools like CrowdStrike and SentinelOne, providing a dynamic security assessment that adjusts to real-time risks. Additionally, the solution incorporates continuous authentication mechanisms.

Beyond Identity uses OAuth and OIDC protocols with downstream support for SAML to integrate with single sign-on solutions (SSOs) as a delegate identity provider. Moreover, Beyond Identity uses an API-first and standards-based approach which integrates with other access management solutions, identity proofing solutions, and endpoint security tools for on-premises or hybrid deployments. API protocols supported include REST, JSON-RPC, gRPC, GraphQL, Webhooks, SCIM, LDAP, and more. SAML, OIDC, OAuth2, and JWT are supported as well. The solution has achieved FIDO2 certification.

In conclusion, Beyond Identity not only simplifies and secures workforce use cases, but also empowers organizations on their passwordless journey by providing innovative solutions that enhance user experience, bolster security, and drive digital transformation. The platform

aims to enforce device trust and lay the groundwork for the foundation of a Zero Trust architecture. By leveraging Beyond Identity's passwordless MFA, users are fortified against phishing and ransomware threats, leading to an improved overall passwordless journey. Beyond Identity appears in the overall, product, and innovation leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 5: Beyond Identity's rating

Strengths

- 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 own CA or relying on third-party CAs.
- Broad set of integration to access management platforms, based on support for common standards.
- Device agnostic application ensures good fit for today's WFH and remote working trends.

Challenges

- Little market visibility outside of North America.
- ISO/IEC 27001 audit not yet initiated.
- Lack of support for legacy systems that continue to rely on passwords.
- Limited selection of authenticators.

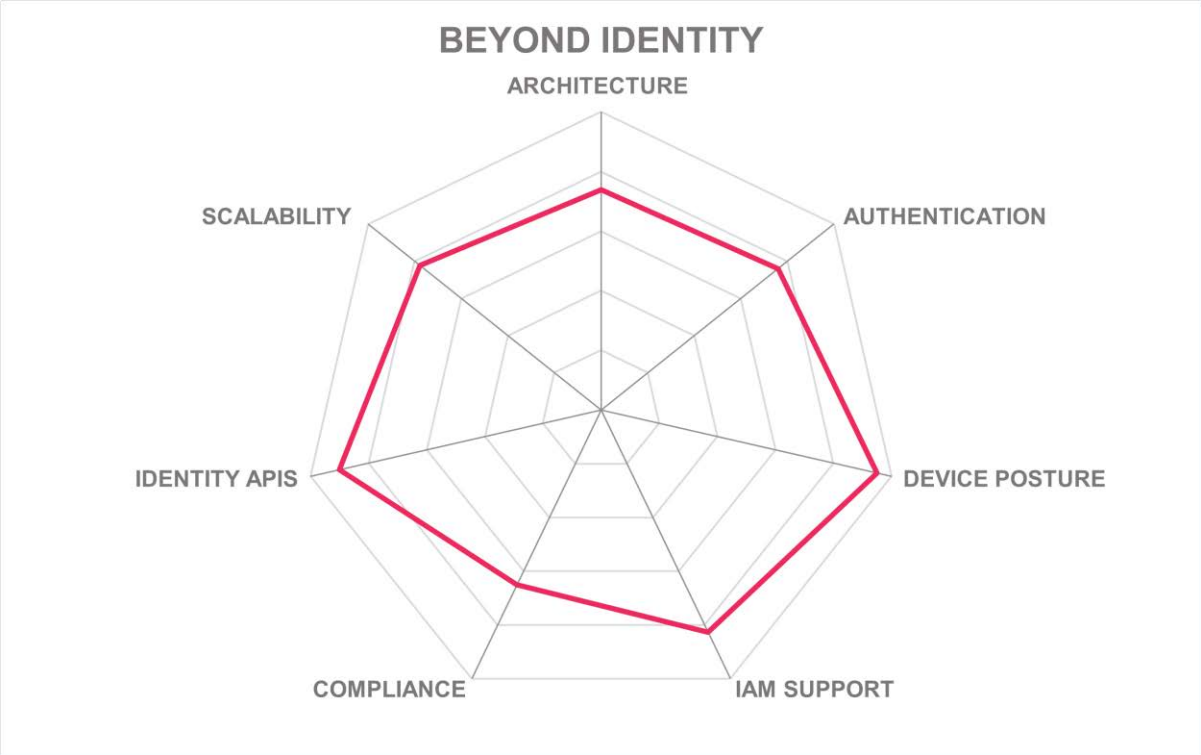
Leader in










BEYOND IDENTITY
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

cidaas – cidaas

cidaas was launched as a brand in 2018. It is the Identity-as-a-Service offering of Widas ID GmbH. The Widas Group is a globally active IT service and innovative software company, founded in 1997 and headquartered in Germany. cidaas is hosted primarily as SaaS in multiple public IaaS providers and their own facilities. Their service is globally distributed for high availability and scalability, utilizing multiple data centers in the EU, Asia, and North America. The company is mainly focused on Europe, but with a growing number of customers in North America and the APAC region. Licensing/subscription options are based on feature packages and include pricing by either monthly active or registered users.

cidaas delivers a turnkey solution for federated identities, SSO, MFA, and passwordless authentication. It is a flexible and scalable solution based on microservices, making it easy to integrate with various systems. For workforce use cases, the solution streamlines user authorization and access management through a dynamic, role-based approach. Leveraging delegated administration capabilities, cidaas enables efficient oversight of user groups and roles, allowing team leads and administrators to manage access to applications and resources.

Additionally, cidaas' fine-grained rights and role management ensures secure access. Users can belong to multiple groups, such as project managers or departmental teams, with specific rights and roles bundled together for delegation and control. This flexibility extends to partners and customers, who can manage their own users, business partners, and, in B2C scenarios, even family and friends. In addition, the platform supports a wide range of authentication options. Some of the most common methods of authentication include magic links, push notifications, and FIDO2.

cidaas has integrated WebAuthn and passkeys so that organizations can incorporate passwordless authentication. The platform's Suggest Verification feature supports a smooth transition from traditional passwords, encouraging users to adopt additional methods such as passkeys during the login process. Furthermore, it enhances its authentication capabilities with the cidaas ID Validator, offering a robust digital identity check to ensure strong authentication across the system.

Moreover, their mobile authenticator app offers facial and voice recognition biometric methods developed by them and is compatible with built-in Android fingerprint and facial recognition and Apple’s FaceID and TouchID. All biometric options include liveness detection. The solution also accepts various authentication methods, including email, phone, SMS OTP and other app-based authenticators such as Google or Microsoft. It supports all federated authentication protocols, including JWT, OAuth2, OIDC, and SAML. cidaas is eIDAS certified and ISO 27001 audited and has a strong focus on secure development practices. However, cidaas is not yet FIDO2 or SOC 2 Type II certified.

Overall, cidaas has a relatively small global presence compared to many of the other vendors. On the other hand, the company is innovative and provides a flexible modern solution based on a scalable microservices architecture that fits to the requirements of a

modern passwordless authentication approach. cidaas should be of interest to organizations within the EMEA region. The company appears in the product leadership category.

Security	Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

Table 6: cidaas' rating

Strengths

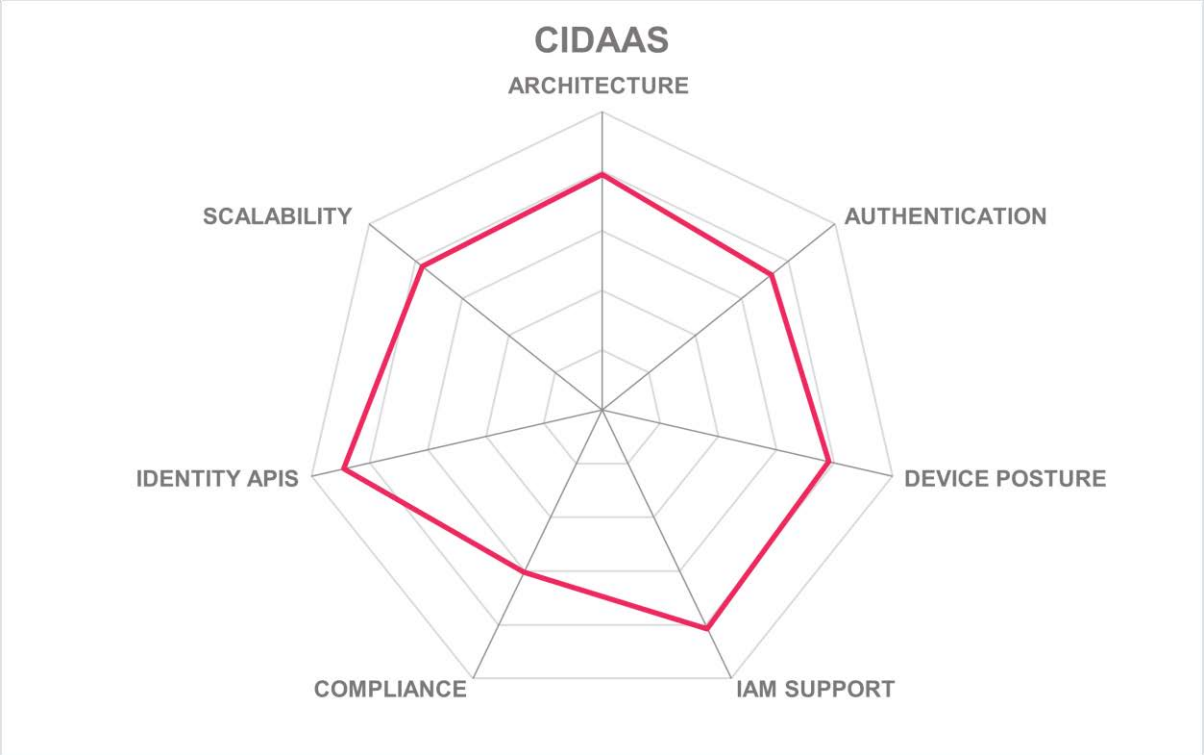
- Based on a microservices architecture.
- Customizable registration workflows.
- Wide range of authentication options.
- Family user relationships are easily managed.
- Good range of MFA options available including FIDO passkeys.
- Suggest Verification feature supports a smooth transition from traditional passwords.

Challenges

- FIDO supported but not certified.
- No support for remote access.
- SOC 2 Type II certification not yet initiated.
- Small global partner ecosystem compared to many of the other vendors.

Leader in




CIDAAS
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Cisco – Duo

Cisco is a multinational technology company based in San Jose, California. Founded in 1984 by the pioneers of the multiprotocol network router concept, the company quickly grew to become one of the world's largest manufacturers of networking hardware and telecommunications equipment. With a presence in more than 100 countries, the company serves customers in a wide range of industries. Cisco Duo is the company's solution in advanced security solutions, designed to protect access to corporate networks and applications across various environments. The solution provides secure access to applications and data, regardless of where users are – on any device. Licensing options include a per user and per month subscription charge.

Cisco Duo has traditionally been associated with providing MFA in various ways including wearables, FIDO2 keys, SMS, hardware tokens, biometrics, push via their mobile app, passkeys, and passwordless. Duo Passwordless minimizes the risk associated with traditional passwords and reduces the administrative burden of managing them. Users benefit from a simplified login process, no longer needing to remember or enter complex passwords and instead using a single biometric gesture for strong, phishing-resistant authentication. Duo Passwordless integrates with Duo Single Sign-On, enabling authentication against an organization's Active Directory or an existing SSO identity provider. This makes it a good choice for enterprises seeking a frictionless transition to a passwordless environment while maintaining strict security and compliance standards.

By verifying devices through trusted endpoints, the solution enables organizations to control which devices can interact with corporate applications and resources. This approach helps verify endpoint trust and effectively blocks access from unmanaged and unknown devices, protecting sensitive data and systems from potential threats of unauthorized access. Duo also makes sure that each registered device is registered to a known and authorized user by continuously verifying whether 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, and so on. 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. Cisco Duo has been independently certified as ISO/IEC 27001, ISO27017, ISO 27018 and SOC 2 Type II compliant, as well as FIDO2 certified, and in alignment with NIST SP 800-63 Digital Identity Guidelines, NIST SP 800-53 Key Management and NIST SP 800-171 and meets the MFA requirements outlined in PCI-DSS v 4.0.

For organizations already invested in Cisco's ecosystem, the Duo platform presents a particularly strong option. It effectively supports workforce access management, remote work setups, and hybrid work environments, offering robust security without compromising on flexibility or user experience. This makes Duo an ideal choice for businesses looking to enhance their cybersecurity measures while accommodating the evolving needs of their workforce in various operating scenarios. Cisco appears in the product, market, and overall leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 7: Cisco's rating

Strengths

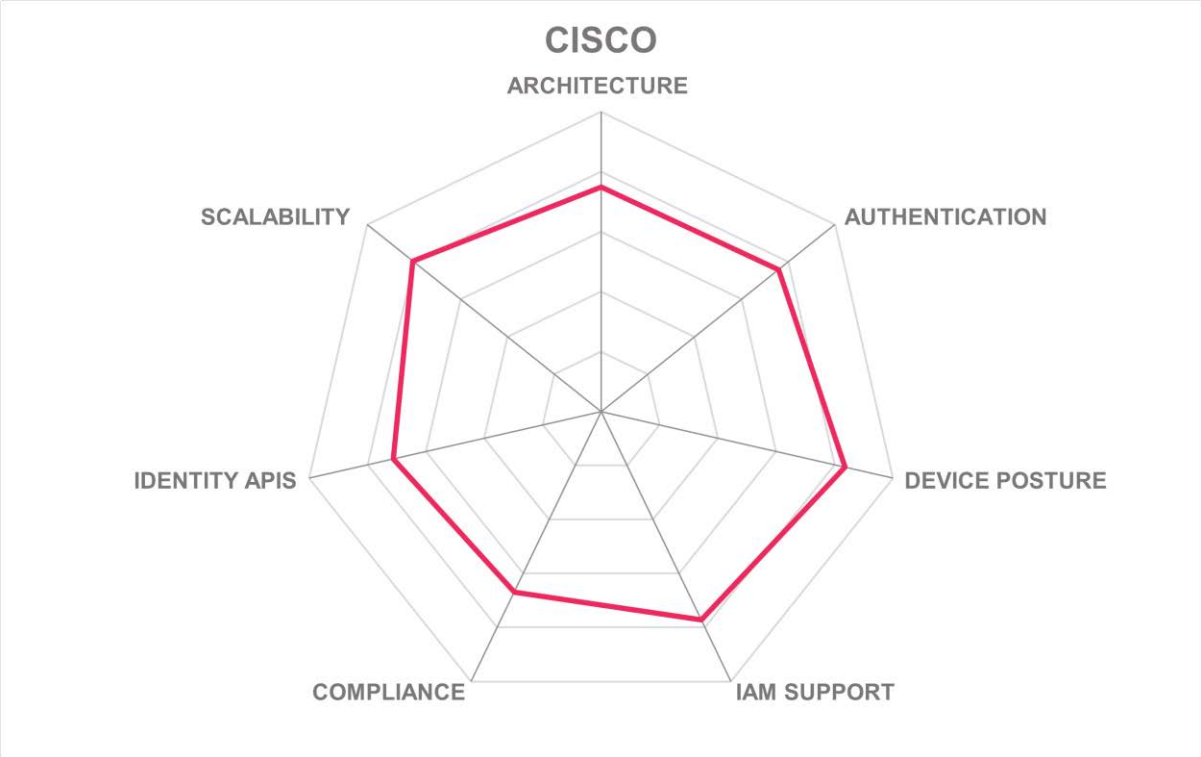
- Global partner ecosystem.
- Multiple security certifications.
- Duo's integration with Cisco Webex.
- Policy customization and enforcement.
- Suitable option for remote and hybrid workflows.
- Wide range of authenticators, including Duo Mobile app Passwordless Push.
- Out-of-the-box integration with Windows Hello and Windows Hello for Business.
- Strong device trust and risk-based authentication capabilities.

Challenges

- SCIM based provisioning is not currently supported.

Leader in




CISCO
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

CyberArk – Identity Security Platform

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

The CyberArk Identity Security Platform is a fully cloud-hosted SaaS service. However, CyberArk provides multiple ways to integrate with on-premises environments and even offers the ability to store user secrets in a self-hosted vault. It supports public cloud and hybrid deployment models with its App Gateway service, enabling VPN-less, Zero Trust access, SSO, and access management capabilities back to on-premises applications and services. The CyberArk Identity Security Platform stands out because it goes beyond just a collection of products. It offers a cohesive set of solutions that work together and share key components, creating a unified platform for various use cases.

The platform provides passwordless authentication for all types of identities including human (employees, customers, vendors, partners, and so on) and machine (passwordless authentication for machine-to-machine communication). In addition, CyberArk recently enhanced its passwordless authentication capabilities by introducing support for passkeys. By leveraging CyberArk's passkeys, users can access applications and websites with phishing-resistant, FIDO2-compliant, and NIST Authenticator Assurance Level (AAL3) authentication that replace passwords and work across different user devices.

Furthermore, the platform improves organizational efficiency and security through its Standard/Advanced Lifecycle Management features, which include pre-integrated application provisioning and deprovisioning, synchronization with Active Directory (AD), and licensing management for Office 365. It also supports self-service application requests and automated approval workflows, as well as inbound provisioning from Human Capital Management (HCM) applications like Workday and SuccessFactors. The CyberArk Identity Security Platform offers flexible integration options, compatible with existing Active Directory, LDAP infrastructures, or CyberArk's own cloud-based directory—or a combination thereof—ensuring integration into diverse IT environments. Additionally, the Access Management solution set extends to endpoint security, with deployable agents for Windows workstations and MacBook devices, and a mobile application available for iOS and Android devices.

CyberArk supports all relevant FIDO2 standards and has integrated with most MFA vendors on the market that support FIDO2. However, CyberArk Identity also integrates with many other vendors using other standards such as OATH HOTP/TOTP, RADIUS, and SAML, and OIDC. Overall, CyberArk Identity offers a holistic and scalable solution for continuous passwordless authentication with minimal interference to the end users. The company's primary focus is on North America, but it has also experienced significant growth in the EMEA, APAC, and Latin America markets, which is bolstered by a robust partner ecosystem. CyberArk appears in the overall, product, market, and innovation leadership

categories. This makes CyberArk a strong option for organizations seeking a unified and feature-rich passwordless solution.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 8: CyberArk's rating

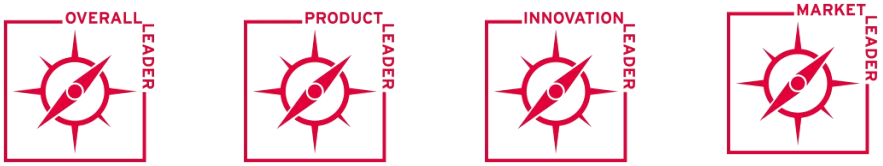
Strengths

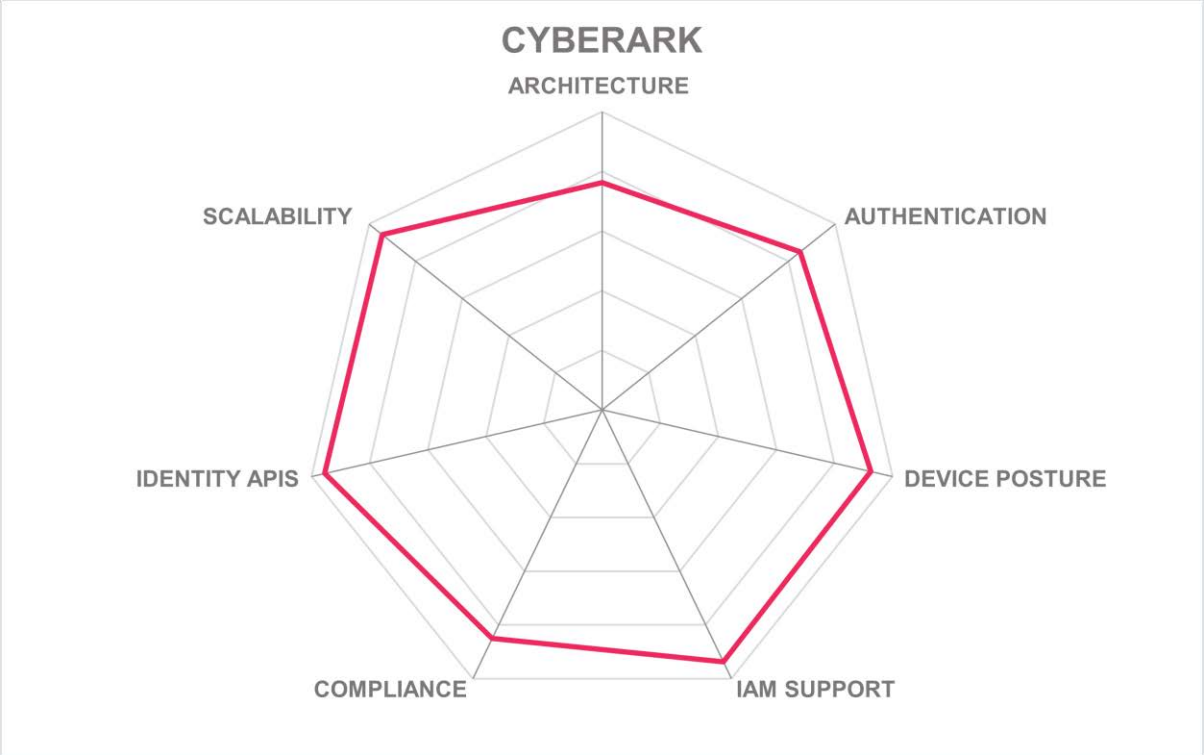
- Large selection of authenticators accepted.
- Strong partner ecosystem.
- Integration with CyberArk PAM.
- Many security certifications.
- Integrated platform, cloud-ready and offers flexible deployment options.
- Shared service approach for analytics, auditing, and administration.
- Convenient solution for remote access and BYOD scenarios.

Challenges

- Integrated, but relying on several products with different origin.
- High modularity of solution could be unfavorable for certain deployments.
- Limited third-party integrations to fraud detection & protection solutions OOB.
- Strong focus on the US as the primary market with growth in EMEA and APAC markets.

Leader in




CYBERARK
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Entrust – Identity as a Service (IDaaS)

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. Headquartered in Minneapolis, MN, Entrust also has offices in London, Tokyo, Washington, D.C., and other international cities. The company provides identity-based security software and services in the areas of public key infrastructure (PKI), multifactor authentication, and fraud detection for those looking to access secure networks, connected devices, or conduct financial transactions. In 2024, Entrust announced the completion of its acquisition of Onfido, a global leader in identity verification and no-code orchestration capabilities. Licensing is available on a per-user basis.

Entrust Identity as a Service (IDaaS) is a cloud-based IAM platform that facilitates a broad range of MFA authenticators, certificate-based passwordless access, SSO, and more. For the workforce, the solution improves digital onboarding with integrated global identity verification, account creation, identity workflow and orchestration, and digital signing capabilities. The platform has three product lines for workforce, consumer, and citizen use cases. It is an all-in-one user authentication and authorization solution in the cloud that helps organizations realize a Zero Trust framework with an identity first approach. The solution provides passwordless authentication with x.509 certificate-based authentication for both users and devices, as well as support for FIDO2 keys and passkeys. It supports unique 2FA such as grid cards for frontline and field employees.

In addition, Entrust's adaptive risk-based access capabilities ensure that stringent security measures are applied only when necessary, such as when a user logs in for the first time from a new device. It also considers a user's risk level and inputs from external fraud and analytics sources. Moreover, the solution identifies fraudulent behavior across all web-enabled devices—including desktops, mobiles, and tablets.

Recently, the solution has focused on improving the process of pairing devices, making it more automatic and intuitive for users. Their risk engine evaluates device type, IP address, geolocation, velocity, and user attributes to assess whether the security posture of the device meets security and compliance requirements. API protocols include SOAP, REST, SCIM, RADIUS, and LDAP. Other protocols supported include JWT, Kerberos, OAuth, OIDC, and SAML. Entrust is not SOC 2 Type II certified. However, Entrust is hosted in SOC 2 Type II data centers through AWS. Furthermore, the company’s role as a public Certificate Authority received some scrutiny in 2024, however Entrust released a plan to provide uninterrupted service to its customers and is working to regain its status as a trusted vendor in that market.

In conclusion, Entrust's approach to passwordless authentication offers a flexible and feature-rich solution that enhances user experience while maintaining security measures. The solution has a strong set of capabilities for employees who need high security assurance. Entrust has a global partner ecosystem and presence that help in delivering their solutions. Organizations of all sizes and in all industries should consider Entrust for their passwordless journey. Entrust appears in the overall, product, market, and innovation leadership categories.

© 2024 KUPPINGERCOLE ANALYSTS AG

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 9: Entrust's rating

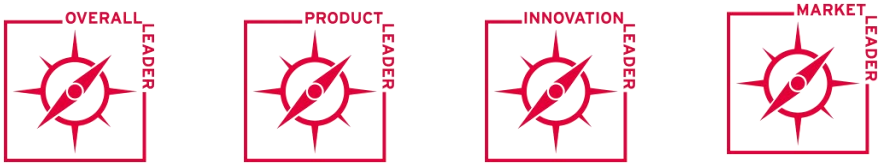
Strengths

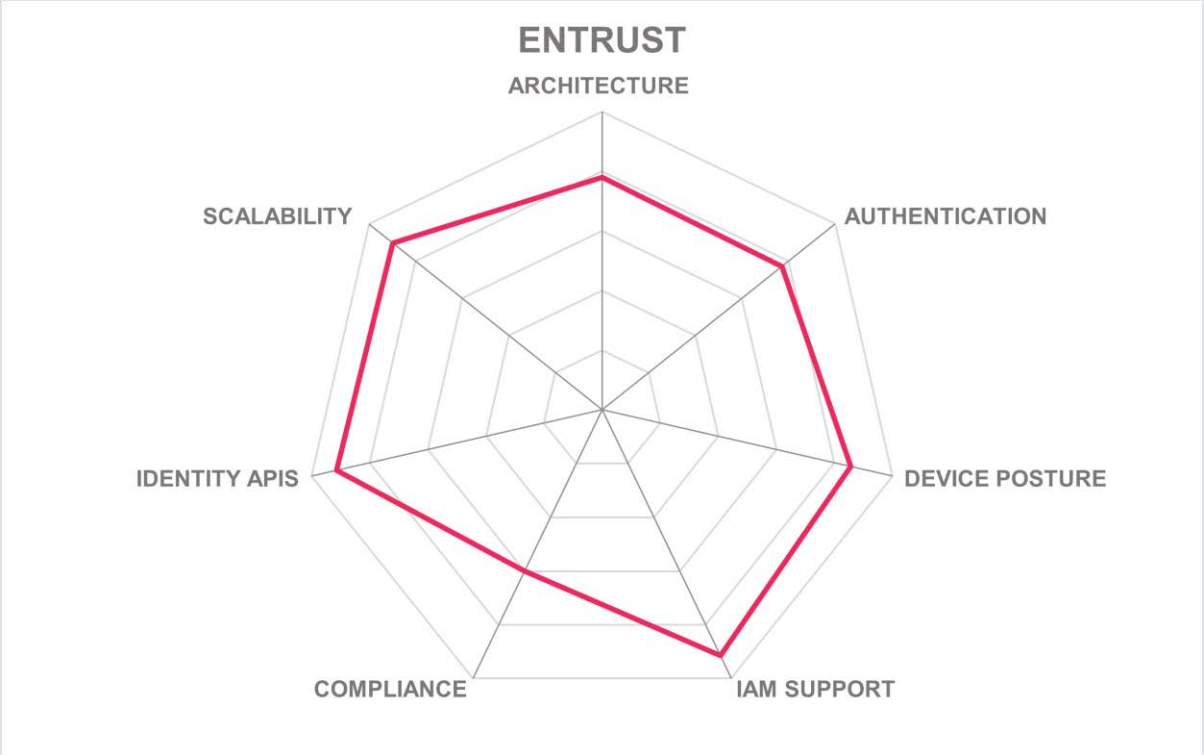
- Global partner ecosystem.
- Broad range of MFA authenticators.
- x.509 certificate-based authentication.
- Risk-based, adaptive step-up authentication.
- Support for 2FA such as grid cards for frontline and field employees.
- Derived Personal Identity Verification (PIV)/Smart card on mobile app support.
- Proximity-based high assurance passwordless login.

Challenges

- Workflow for device registration cannot be customized.
- SOC 2 Type II certification not yet initiated.
- Username/password is supported for account recovery only if chosen by the customer, not as a mandated feature by Entrust.

Leader in




ENTRUST
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Exostar – The Exostar Platform

Exostar was founded in 2000. Its headquarters are in Herndon, Virginia, with additional development centers in the UK and Bangalore, India. The company significantly expanded its portfolio through the acquisition of Pirean in 2018. Exostar is a steward of communities in highly regulated industries such as defense, aerospace, life sciences, healthcare, energy, telecommunications, and financial services. It focuses on providing specialized solutions tailored to specific industries rather than attempting to cater to a broad range of customers. In 2023, Exostar was acquired by Arlington Capital Partners. Coverage includes North America, Europe, Latin America, and the APAC regions. Licensing is available on a per-time period basis.

The Exostar Platform supports both SaaS and on-premises deployments. It offers a set of packaged services (consumer and enterprise access management) as well as the ability to easily build, integrate, and publish custom IAM services and user journeys (built using no-code workflow and the platform's secure plug-in integration service). The platform has been designed in line with the concepts commonly considered for Identity Fabrics—in particular, speed of integration, no-code workflow and orchestration, ease of reuse, and microservices to support the use of specific capabilities in isolation. Additionally, Exostar offers ease of integration through packaged APIs and tenant onboarding via an Authenticator as a Service offering.

Exostar offers a robust identity management suite within the "IDM" layer of The Exostar Platform's Access: One product framework, designed to enable the creation, update, and deletion of user accounts. This layer provides a unified set of identity management services, encompassing access requests, approvals, certifications, and self-service functionalities. Additionally, the solution incorporates an access governance module that features a certification engine. This engine delivers a comprehensive access certification service, essential for maintaining compliance and ensuring that access rights are granted appropriately within the organization. By integrating with third-party identity providers and external systems of record, such as document verification services and eIDAS, the solution facilitates a unified approach to digital customer onboarding, identity proofing, and provisioning passwordless authentication.

The passwordless capabilities described in this report are provided via The Exostar Platform's Access: One product. Exostar provides a comprehensive suite of passwordless authentication features, including support for phishing-resistant multifactor authentication using FIDO2 and third-party authenticators, such as OAuth and QR codes. The platform offers a wide range of passwordless methods, including FIDO2 passkeys, Windows Hello, Apple Local Authentication (Face ID, Touch ID, Optic ID), QR-based login, email, SMS, and knowledge-based authentication.

Exostar's approach prioritizes delivering highly trustworthy user credentials via secure onboarding and identity proofing services the company performs, ensuring alignment with stringent standards such as NIST 800-63. In addition, Exostar is a Certificate Authority (CA) 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 continues to add innovative features to its roadmap. The company is a well-known provider of IAM solutions, and its identity proofing and passwordless capabilities provide a strong offering for organizations in complex and highly regulated industries. With a focus on user experience and high security standards for its trusted communities, Exostar provides organizations with the tools they need to deliver streamlined services while ensuring compliance. Exostar appears in the market leadership category.

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Positive
Usability	Positive

Table 10: Exostar's rating

Strengths

- Good employee onboarding features.
- Strong partner/customer ecosystem and global presence.
- Certified compliant with multiple standards.
- Breadth of authentication options.
- Flexible deployment models.
- Strong identity proofing capabilities.
- Extensive experience and well-established vendor in highly regulated and sensitive industries.

Challenges

- Limited omni-channel capabilities.
- Fraud detection features only available with third-party tools.
- Lack of interoperability with other IDaaS platforms.

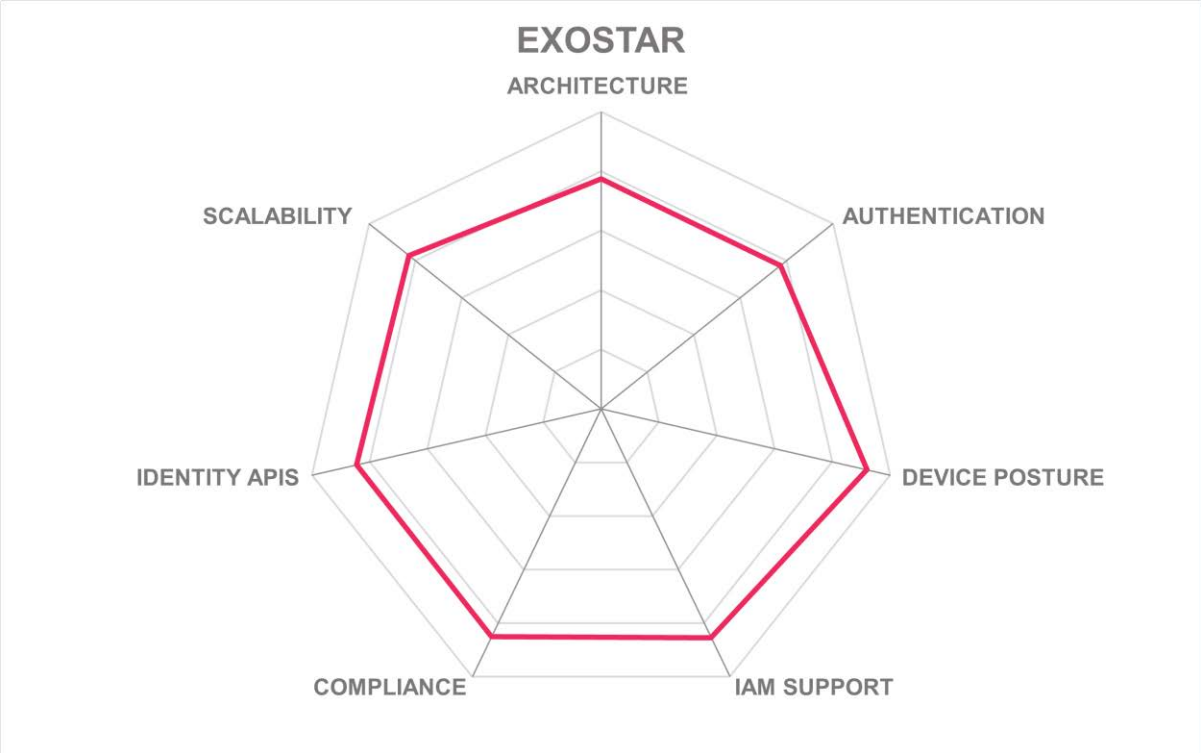
Leader in










EXOSTAR
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

GSMA – Number Verify

Founded in 1995, GSMA is a global organization representing mobile operators and organizations across the mobile ecosystem and adjacent industries. GSMA Open Gateway is a framework of common network API designed to provide universal access to operator networks for developers. The GSMA Open Gateway Memorandum of Understanding (MoU) is supported by some of the world's largest and most innovative mobile network operators (MNOs), currently representing over 65% of mobile connections and over 3 billion users. Mobile Network Operators support has steadily increased since the launch of the initiative in February 2023.

Number Verify is part of the Open Gateway initiative as part of the anti-fraud and identity service suite. 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. Integrated directly into mobile networks, this solution offers real-time verification of an employee's mobile number and SIM card, providing a robust method of confirming the employee's identity through their device.

This system of authentication is not only more secure, but also significantly easier for employees to use compared to traditional methods such as token-based systems or complex password protocols. Employees benefit from a smoother login experience without the need to remember and enter complex passwords, which often leads to increased productivity and reduced downtime.

The solution is targeted to workforce, consumer, and partner use cases. It is offered as a cloud-based, developer first, REST-based API service that allows partners and relying parties to verify possession of a claimed mobile digital identity. The solution is already used by over six thousand trusted parties as part of their mobile app registration flows, with strong improvements in reducing fraud and improving customer satisfaction and experience. 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. It can be considered an evolution of SMS OTP and is complimentary to other 2FA/MFA factors, for example biometrics. It can offer passwordless login for users on its own or combined with other factors, such as device biometrics and FIDO passkeys.

The product has the potential to shape and create new opportunities in the passwordless authentication market. While the GSMA's Number Verify solution may lack certain features compared to most passwordless vendors, such as device posture capabilities, flexible account recovery options, or support for major standards, it is intentionally focused on addressing specific niche areas within the authentication landscape. 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, Number Verify should be on the short list for organizations considering deploying phishing resistant and device-based possession

features. However, it probably wouldn't be suitable for organizations needing more advanced features and integrations.

Security	Positive
Functionality	Neutral
Deployment	Positive
Interoperability	Weak
Usability	Positive

Table 11: GSMA's rating

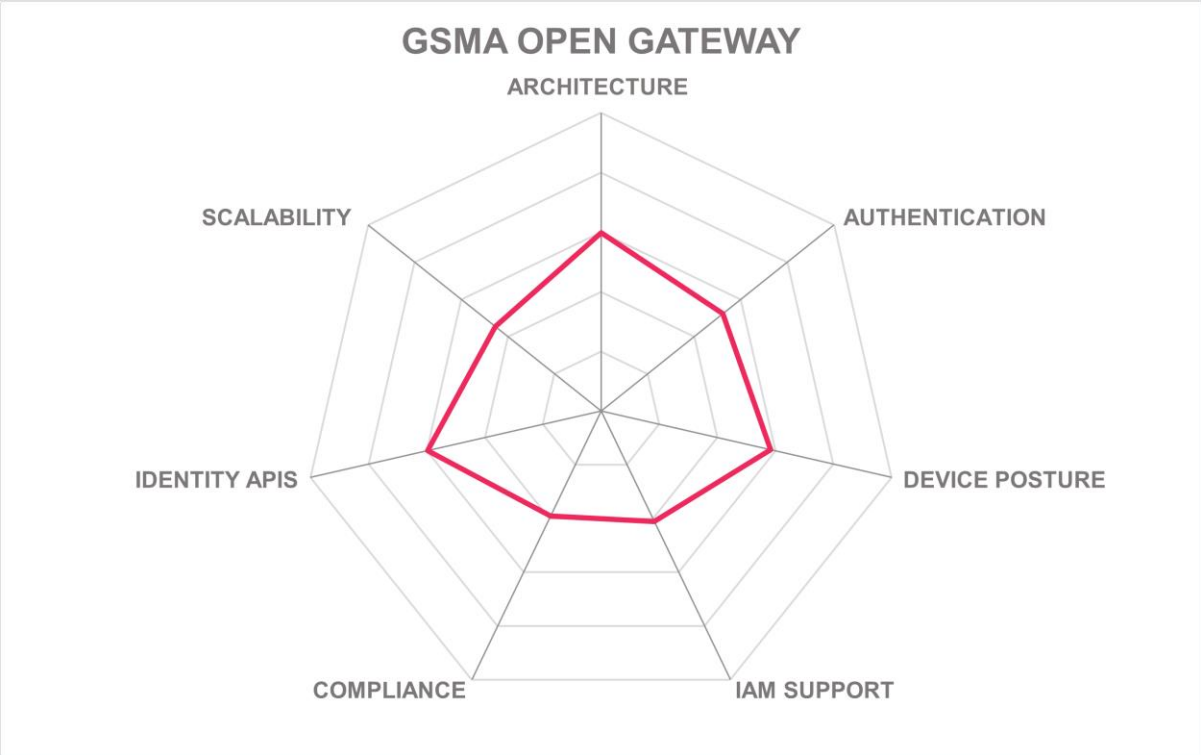
Strengths

- Smooth login experience.
- Strong SIM-based authentication.
- Frictionless logins and friendly user experience.
- Phishing resistant and cryptographically secure.
- Large global partner network and geographical presence.
- Real-time verification of an employee's identity through their device.
- Focused on addressing specific niche areas within the authentication landscape.

Challenges

- No support for major security certifications.
- Lacks certain capabilities compared to most passwordless vendors.
- For account recovery, end users will follow standard MNO procedures for replacing SIM/eSIM cards.
- Increase awareness and educate its customers about the advantages of SIM-based authentication to better establish its offerings in the market.

©2024 KUPPINGERCOLE ANALYSTS AG


GSMA OPEN GATEWAY
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

HID – Authentication Platform

HID is a subsidiary of Assa Abloy Group AB of Stockholm. Assa Abloy AB is a Swedish conglomerate whose solutions include products and services related to locks, doors, gates, and entrance automation. HID's headquarters are in Austin, TX. With over 4,500 employees worldwide and international offices that support more than 100 countries, the company develops highly secure solutions for identity and access management. These include physical access controls, government identities, smart identity card manufacturing, credential issuance and management, biometric authentication, and identity proofing. Licensing models supported include per-transaction, per-user, per-node, per-appliance, and per-server options.

HID's Authentication Platform stands as a flexible solution designed for both consumer and workforce scenarios, offering a blend of strong identity assurance and user-friendly experience. The platform, deployable either on-premises or as a SaaS solution, integrates with various authenticators such as HID Approve, synced passkeys or device-bound passkeys either provided through the Crescendo portfolio or by a third party, catering to diverse authentication needs. HID also manufactures one-time-password hardware tokens.

The HID Approve solution uses mobile devices as authenticators, enabling easy and secure access to VPNs and enterprise applications through push notifications and one-time password (OTP) generation, while the HID Crescendo series, which includes both Crescendo Security Key and Crescendo Smart Card solutions, provides multi-factor and passwordless authentication options to enhance remote access security and simplify access to corporate digital resources. The Crescendo Security Key provides strong authentication without the need for a smart card reader, ideal for employees on the go, while the Crescendo Smart Cards serve as universal credentials that not only grant physical access to facilities, but also enable passwordless login to workstations and networks.

A key element of HID’s solution is that it goes beyond authentication to cover the complete user’s digital journey from onboarding to ongoing fraud prevention. The Identity Verification Service provides strong identity vetting and remote document verification, which are valuable features to strengthen and facilitate onboarding and help attain compliance with regulations around eKYC and AML.

Supplementing the platform, HID’s Credential Management System (CMS) enables enterprises to manage the lifecycle of devices (including Crescendo devices), PINs and digital certificates for employee authentication, data encryption and signing. Additionally, HID's cloud-based authentication solutions enable standards-based security by being ISO 27001, ISO 27018, SOC 2 Type II, and FIDO certified. The Authentication Platform (on-premise and cloud-based) enables compliance with GDPR, PSD2, and UK-GDPR. For APIs, HID supports REST, SOAP, WebAuthn, Webhooks, and SCIM, and CSV/JSON/XML formats as well as Open Banking and OpenID Financial.

The company also supports the FIDO ecosystem with passkeys as well as standards such as OAuth, OIDC, RADIUS, and SAML, which can be used to facilitate interoperability with other IAM and IDaaS systems. HID has been a strong player in the government and

enterprise workforce IAM for years and is moving more into consumer use cases. By offering a diverse range of authentication methods and form factors, HID's Authentication Platform enables organizations to tailor their security solutions to meet specific needs and use cases effectively. HID is a solid option for organizations with highly regulated industries, high security requirements, and complex integration. The company appears in the overall, product, market, and innovation leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 12: HID's rating

Strengths

- Flexible deployments.
- Built-in identity verification services.
- Global partner ecosystem.
- Wide range of MFA types.
- HID Approve and the Crescendo portfolio.
- Strong credential issuance and management capabilities, including remote device unlock and PIN reset, trusted by numerous government agencies globally.
- Crescendo Smart Cards enable passwordless login to workstations and networks, with a shared PIN for FIDO and PKI.

Challenges

- Device health checks currently not supported.
- Lack of compromised credential evaluation capabilities.
- No interoperability with PAM systems.
- Username/password is supported for account recovery only if chosen by the customer, not as a mandated feature by HID.

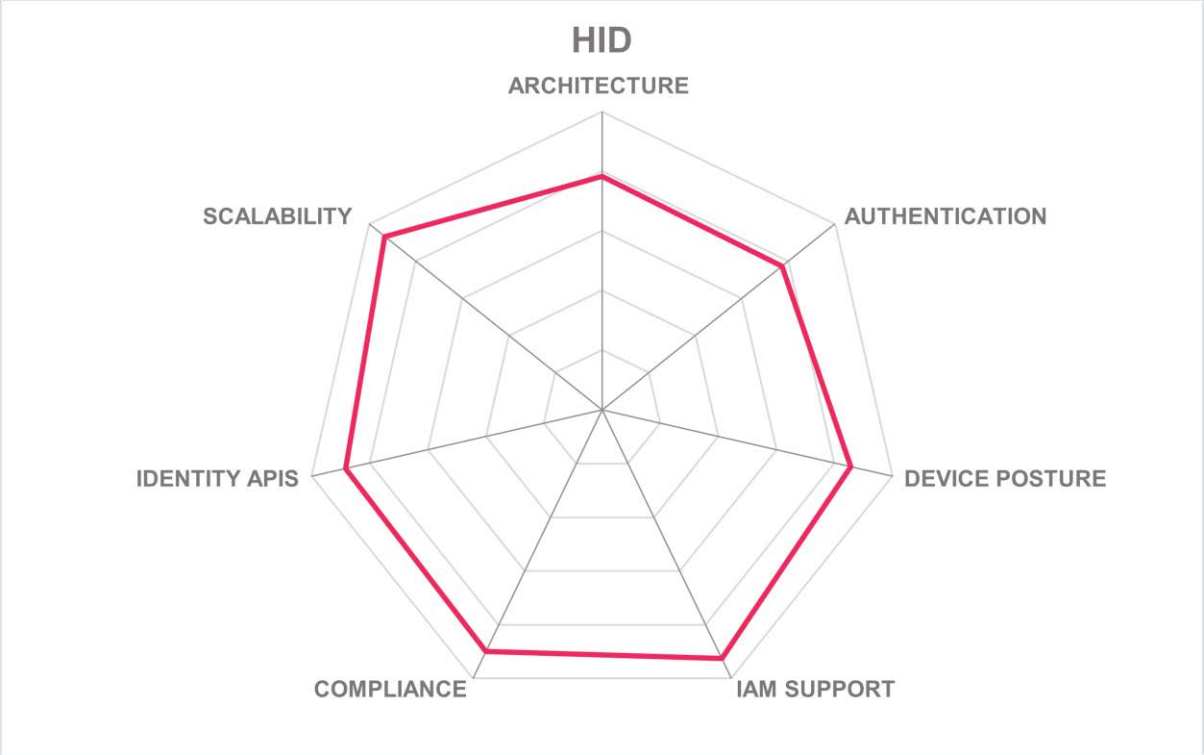
Leader in










HID
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

HYPR – Identity Assurance Platform

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. With HYPR, the entire path from initial access to a system can be protected at multiple levels. Their solutions address both workforce identity and customer identity access management (CIAM), catering to two fundamental enterprise security needs. HYPR is a seat based per user model.

The HYPR Identity Assurance Platform offers a solution to modern authentication challenges with its three core components: HYPR Authenticate, HYPR Adapt, and HYPR Affirm. HYPR Authenticate, powered by FIDO2 certified technology, addresses password-based authentication by replacing passwords and shared secrets with secure passkeys across all user populations, applications, and locations. By eliminating credential-based attacks and offering an intuitive experience, HYPR Authenticate ensures both employees and customers enjoy seamless authentication. HYPR Adapt enables organizations to manage identity-related risks effectively through real-time risk assessment and adaptive security controls. Leveraging a diverse set of data sources including user behavior, mobile, web, and browser signals, HYPR Adapt enforces step-up authentication or re-verification when necessary, minimizing friction while protecting users, systems, and operations. Finally, HYPR Affirm provides identity verification through automated and ongoing processes integrated into identity management workflows. Using AI-powered chat, video, facial recognition, and other cutting-edge technologies, HYPR Affirm helps to mitigate fraud and ensures a user experience and secure method of confirming identities without ever relying on passwords, providing organizations with enhanced security and convenience.

The company is also a board member of the FIDO Alliance, helping to drive innovation and adoption of FIDO standards. To strengthen security and support compliance, HYPR has been independently certified with the ISO/IEC 27001 and SOC 2 Type II. Supported API protocols include REST, RADIUS, and Webhooks. In addition, SAML, OIDC, JWT, and OAuth2 are supported as well. The solution also has a Derived PIV Credentials mobile app, and accepts YubiKey, Feitian, and any other smart key that is FIDO2 certified. The HYPR Mobile App makes it easy for your users to log into their workstations and web accounts with their mobile devices. The app runs on both Android and iOS. Enrollment of the HYPR app commonly is done via an Enterprise Mobility Management/Mobile Device Management (EMM/MDM) solution, or it can simply be downloaded from the app store. The app can be rebranded to the customer's design. 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).

The HYPR Identity Assurance Platform provides valuable support for workforce use cases by enhancing authentication, managing identity-related risks, and streamlining identity verification through its three core components: HYPR Authenticate, HYPR Adapt, and HYPR Affirm. HYPR counts among the leading-edge solutions for passwordless authentication. It

provides a well thought out and secure solution for passwordless and phishing-resistant authentication. Their strength is derived from the support for the entire flow from desktop authentication to backend applications, and the utilization of the established FIDO2 standards. HYPR appears in the overall, product, and innovation leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 13: HYPR's rating

Strengths

- Full support for FIDO standards.
- Strong device posture capabilities.
- Support for both macOS and Windows environments.
- Delivers protection from the desktop authentication on, not just at the application level.
- Strong integration with Microsoft environments, specifically Microsoft Active Directory and Kerberos.
- Utilizes strong cryptographic algorithms and secure elements on the smartphone or desktop device.

Challenges

- No support for non-FIDO devices.
- Dashboards are not customizable.
- Maturing support for delegated administration.
- Limited identity assurance score capabilities but improvements are on the roadmap.

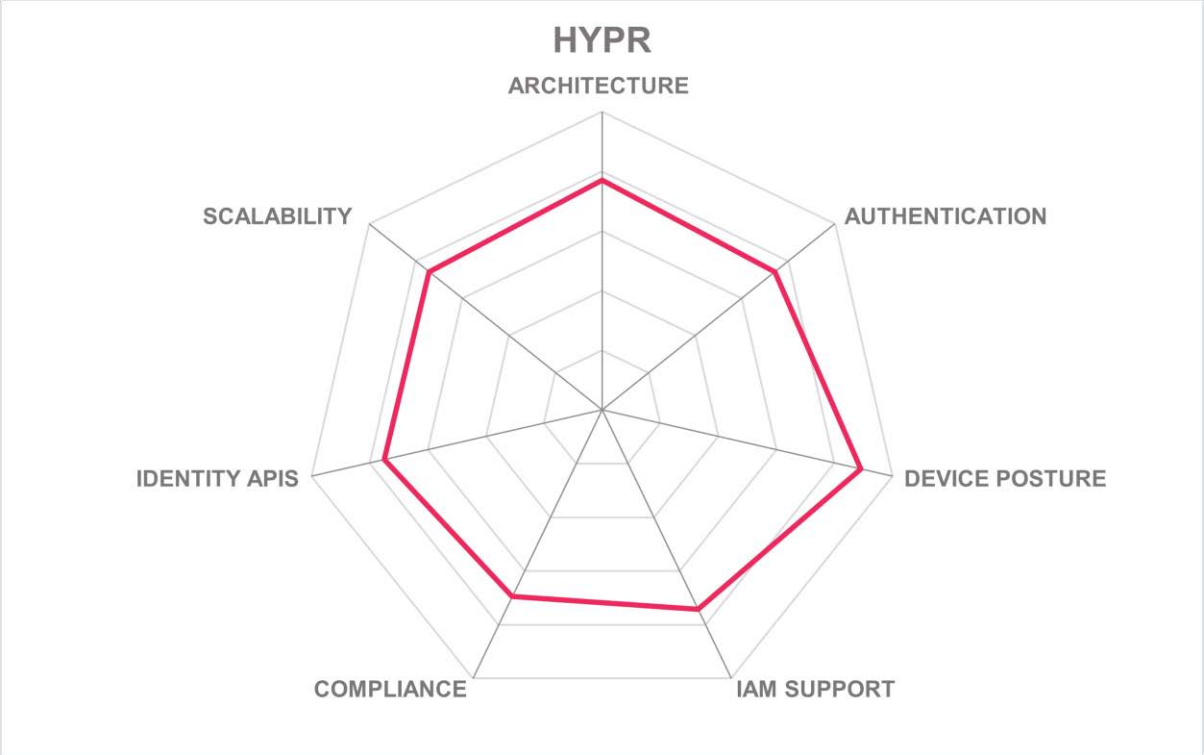
Leader in










HYPR
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

IBM – IBM Security Verify

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. Multiple licensing/subscription options are available.

IBM Security Verify offers a SaaS solution for identity and access management, covering SSO, MFA, adaptive access, privacy and consent management, provisioning, governance, analytics, and passwordless authentication. With a fully cloud-based deployment, administration is conducted through a modern web application, allowing configuration of SSO applications, user records management, access policies, and platform security settings.

Hybrid access management deployments include on-premises repositories and the IBM Application Gateway, ensuring secure access to on-premises web applications. Additionally, IBM Security Verify's on-premises access management and identity governance and administration solutions offer administrative interfaces, policy enforcement points, and governance modules for compliance, lifecycle management, and analytics.

IBM Security Verify can manage large-scale transitions to remote access environments, making it a useful tool for workforce settings. For improved management of remote connections, the IBM Security Secret Server Remote serves as an optional add-on, providing a unified platform to manage multiple remote sessions. Additionally, IBM Security Privileged Manager is designed to thwart malware-based attacks by enforcing least privilege and application control policies and facilitating the discovery of local admin rights.

With a focus on security, scalability, and flexibility, IBM Security Verify caters to the diverse identity management needs of modern organizations. The solution delivers passkeys natively to enable consumers and the workforce at scale. It supports a wide range of passwordless authentication methods, including QR login, passkeys, FIDO2 (TouchID, Windows Hello), and MFA methods such as knowledge questions, SMS OTP, email OTP, voice OTP, and time-based OTP.

In addition, the platform provides granular policy control by application and implements risk-based conditional access, considering factors like new device, IP address, geographic location, device context, and user/group attributes for enhanced security. For additional application connectivity, REST, SOAP, WebAuthn, and Webhooks and LDAP and SCIM for provisioning are supported. It is also ISO 27001/27018 certified, PCI-DSS Level 1, SSAE 18 SOC 2 Type II attested.

IBM has many system integration partners on a global scale and substantial experience in large-scale deployments. IBM positions itself as a leader in the IAM space and provides feature-rich and modern solutions for businesses that intend to adopt a passwordless approach. IBM also benefits from its integration to other IBM services. Organizations that are

looking for mature, highly scalable, and secure enterprise authentication should put IBM on the list of solutions to consider. IBM appears in the overall, product, market, and innovation leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 14: IBM's rating

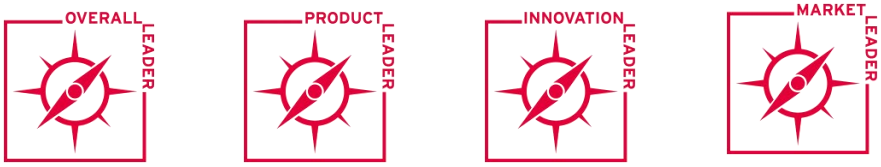
Strengths

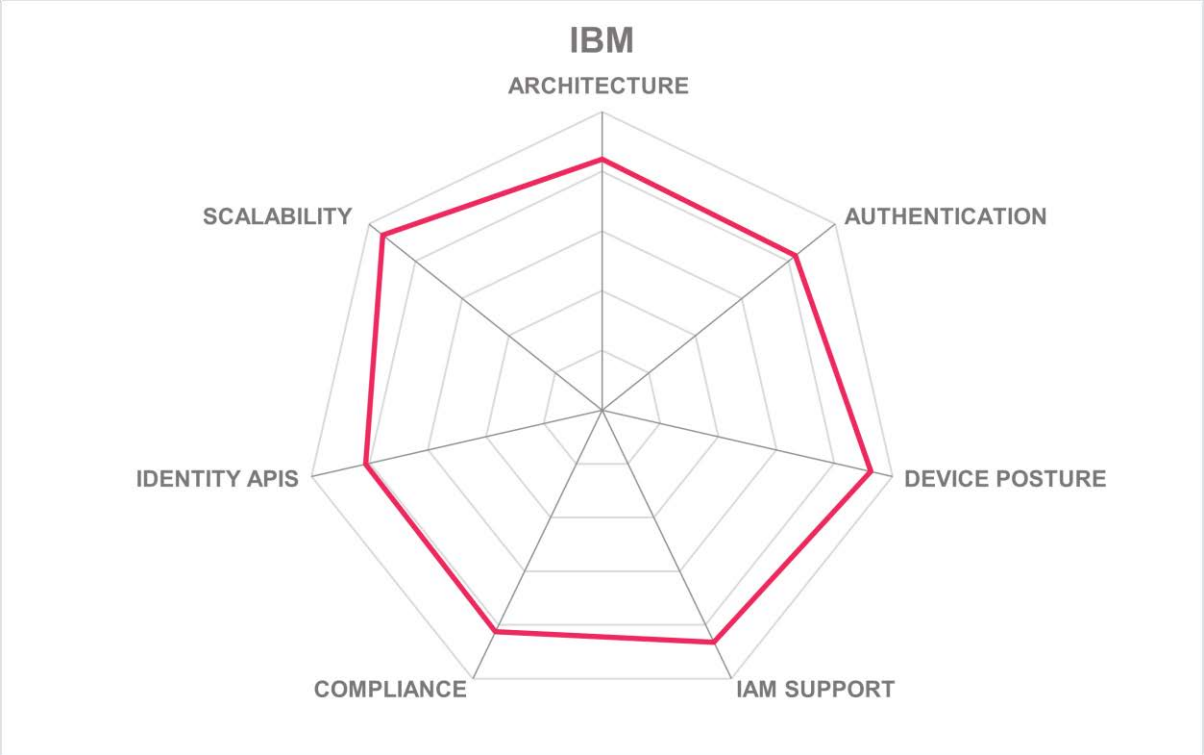
- Strong global partner ecosystem.
- Modern microservice-based architecture.
- Well-documented set of APIs.
- Strong fraud prevention features.
- Support for Verifiable Credentials, DIDs, and wallets.
- Highly scalable containerized, multi-cloud architecture.
- Wide selection of authentication mechanisms supported.

Challenges

- No support for remote access.
- Lack of focus on the mid-market segment.
- Complicated licensing/subscription models.
- Requires integration with other IBM products for some more advanced remote features.

Leader in




IBM
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Idee – AuthN

IDEE GmbH was founded in 2015 and is 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 retail, manufacturing, pharmaceutical, insurance, finance, and telecommunications industries. The company is focused on Europe and North America with a growing number of customers in Africa and the Middle East. Licensing models supported include per-user and per-time-period options.

AuthN by IDEE offers a passwordless, phish-proof MFA solution that can be set up in seconds without requiring users to install any software, agents, or hardware. This advanced MFA not only protects the authentication step but ensures the entire user identity lifecycle—including registration, identity proofing, authenticator establishment, authentication, account recovery, re-identification, and account termination—is immune to phishing attacks. AuthN operates across various platforms, including PCs, macOS, mobile devices, VDIs, remote desktops, and VPNs. It boasts decentralized credentials, explicit transitive trust, and a zero-trust architecture, ensuring no privileged insider threats. Additionally, AuthN supports multi-device usage, remote logout, user self-service, and can be deployed quickly using modern federated authentication standards such as SAML, OIDC, and WS-Fed, alongside automated provisioning via the SCIM protocol and FIDO2 support. Built on a microservices SaaS architecture, AuthN requires no personal identifiable information (PII) or knowledge, making it a secure and versatile option for organizations looking to enhance their cybersecurity infrastructure.

For account recovery, AuthN implements explicit transitive trust to guarantee that account recovery is securely controlled and can only be executed by the authenticated user. Recovery options are limited to authorization through a trusted device or using a recovery key. If neither a trusted device nor a recovery key is available, the account must undergo a reset, treated as a new registration that includes stringent identity proofing to ensure security integrity. Additionally, administrators have the capability to assist users by providing a recovery key, thus maintaining control and security throughout the recovery process.

IDEE is in compliance with FIPS 197, NIST 800-57, NIST SP800-63, PCI-DSS v 3.2, HIPAA/HITRUST, GDPR, ISO 29115, AND UK GPG 45 standards. The company has also been independently certified with the ISO/IEC 27001 and SOC 2 Type II. However, FIDO2 certification is not supported. In addition, the solution supports hardware tokens such as Feitian, Google Titan, and Kensington security keys. For additional application connectivity, the solution supports REST, JSON, SCIM, LDAP, and RADIUS upon customer request. Furthermore, AuthN supports cloud or on-premises directories. The solution can be deployed in multi-tenant or dedicated tenant as per customer's requirement.

IDEE's approach to passwordless authentication is particularly well-suited for enterprise use cases, where the need for both security and ease of use is paramount. Their modern microservices architecture supports scalability across various organizational sizes and ensures that the deployment and management of authentication systems are streamlined and less burdensome. 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. IDEE appears in the product and innovation leadership categories.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 15: Idee's rating

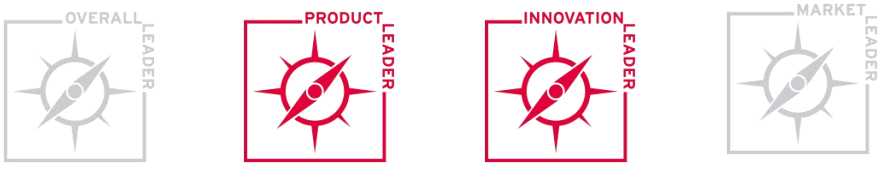
Strengths

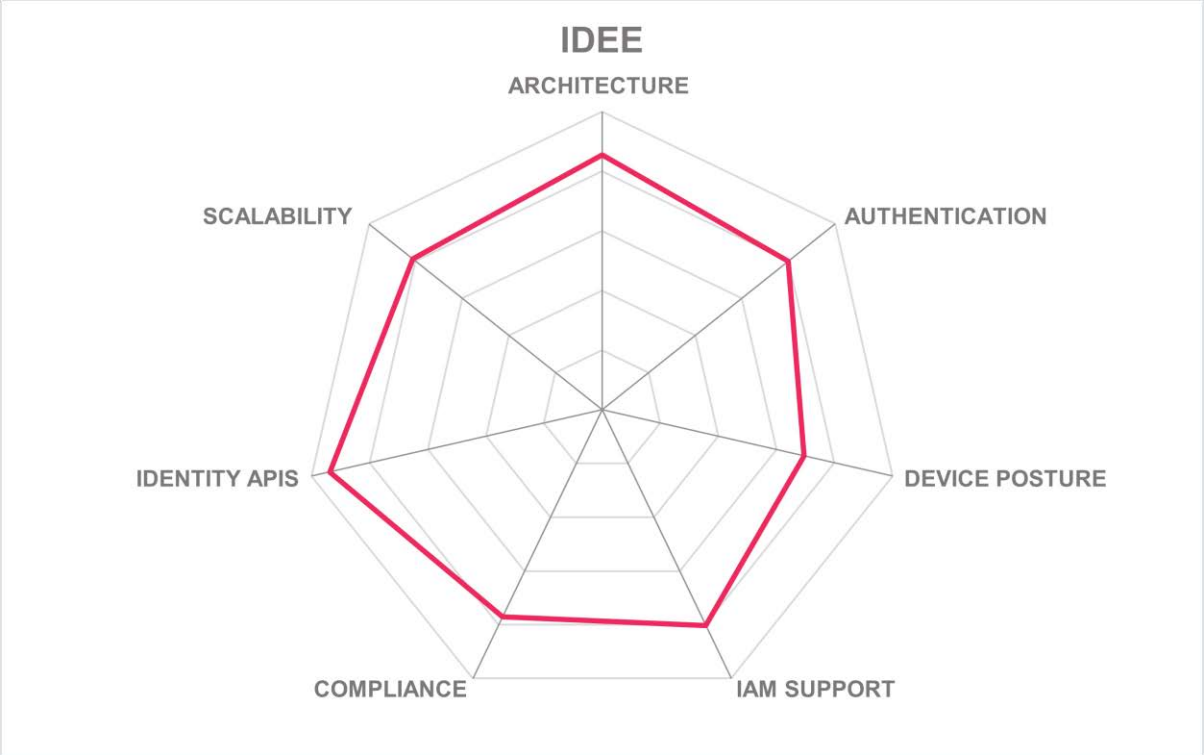
- User-friendly setup that can be quickly deployed.
- Account recovery mechanism.
- Wide range of authenticator options.
- Phish-proof MFA as a default for every access.
- Flexible, modern microservices-based architecture.
- Many security certifications.
- The "same device MFA approach" consolidates all MFA steps onto one device for streamlined and secure user verification.

Challenges

- Missing FIDO2 certification.
- Dashboards are currently not supported.
- Still a relatively small vendor but with some large customers.
- Limited native device posture capabilities; offers integration with existing device management solutions.

Leader in




IDEE
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Infinipoint – Zero Trust Workforce Access Platform

Founded in 2019 and headquartered in Tel Aviv, Infinipoint delivers phishing-resistant passwordless or MFA authentication combined with zero device trust posture verification. The Zero Trust Workforce Access Platform was developed by a team with a background in cybersecurity, motivated by the realization that traditional access systems were often vulnerable and inadequately secured against breaches.

The SaaS platform integrates passkeys with device authentication, conducting posture checks and providing simple one-click remediation for any detected device vulnerabilities upon access. This comprehensive approach allows companies to effectively prevent account takeovers while ensuring uninterrupted user access.

Infinipoint's solution integrates user and device authentication to adhere to zero-trust principles, ensuring secure access within a modern IT environment. It strengthens workforce security by ensuring rigorous authentication of both users and devices, coupled with immediate on-spot remediation for any detected issues. Infinipoint addresses these vulnerabilities by enhancing security at every access point and managing device trust through real-time posture checks and compliance enforcement.

Infinipoint utilizes advanced device classification to differentiate between corporate and non-corporate, as well as computers and mobile devices, allowing for customized access profiles for different user groups. This system enables automatic registration for approved devices and offers manual IT approval for personal devices, ensuring robust security by preventing access from vulnerable devices to sensitive company resources.

Furthermore, the platform's ability to integrate with existing identity providers and its support for passwordless authentication further underline its capacity to provide a secure, user-friendly experience that does not compromise on either accessibility or security. The solution also integrates with CrowdStrike for additional risk assessments. Authentication methods supported include passkeys, mobile push notifications, hardware tokens, security keys, and FIDO2. Common standards and protocols such as SAML, OIDC, JWT, and OAuth2 are also supported. Infinipoint adheres to NIST 800-57 Key Management and is SOC 2 Type II certified.

Despite being a relatively young vendor, Infinipoint has demonstrated prowess and innovation in the passwordless space. The platform's foundation is built on Zero Trust principles, ensuring that each device is thoroughly verified and that detailed posture policies are strictly enforced. This approach effectively prevents weak device configurations and halts potential account takeovers, while maintaining uninterrupted workflow operations. As a result, Infinipoint has become a suitable alternative for enterprises across North America and the EMEA region that prioritize top-tier device security and Zero Trust principles.

© 2024 KUPPINGERCOLE ANALYSTS AG

Security	Strong Positive
Functionality	Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Positive

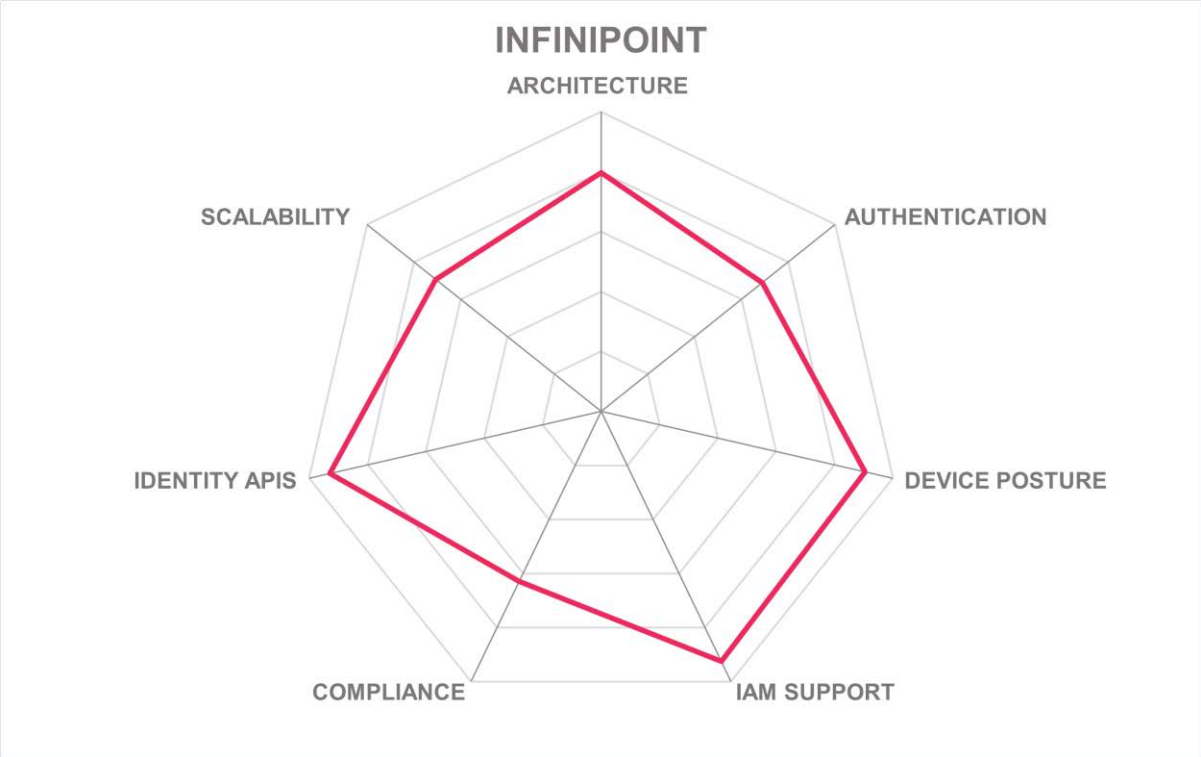
Table 16: Infinipoint's rating

Strengths

- Good option for BYOD scenarios.
- Suitable for medium to mid-market enterprises.
- Strong device health checks features.
- Good mix of authenticators available.
- Built to work well for users with multiple devices.
- Integration with UEM solutions.

Challenges

- Dashboards are not customizable.
- Smaller company but with a growing global footprint.
- ISO/IEC 27001 audit not initiated yet. However, the company is SOC 2 Type II certified.


INFINIPOINT
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Microsoft – Microsoft Entra

Headquartered in Redmond, WA, and founded in 1975, Microsoft is known for operating systems, office automation, and cloud infrastructure. Microsoft Entra has evolved over the years from a cloud directory and access management solution for the Microsoft environment to a comprehensive IAM solution, providing a broad set of capabilities. Microsoft Entra supports applications, hosted in any public or private cloud. Licensing 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.

Microsoft Entra offers five passwordless authentication methods tailored to meet diverse user needs and security requirements. First, Windows Hello for Business provides a seamless experience for information workers with designated Windows PCs, utilizing biometric and PIN credentials tied directly to the user's device. This method offers PKI integration and single sign-on (SSO) support, facilitating access to corporate resources on-premises and in the cloud. Second, the Authenticator App transforms iOS or Android phones into passwordless credentials, allowing users to sign in across platforms and browsers through biometric authentication or PIN confirmation. Third, Entra supports FIDO2, which allows the use of FIDO2 security keys to offer robust authentication. These keys, available in various form factors including USB, Bluetooth, or NFC, provide authentication for Microsoft Entra and hybrid joined Windows 10 devices, as well as supported browsers.

In addition, Entra supports certificate-based authentication (CBA) which enables users to authenticate directly with x.509 certificates against their Microsoft Entra, bolstering security against phishing attacks and ensuring secure sign-in with PKI/CAC cards. Unlike traditional systems, CBA doesn't rely on on-premises federation infrastructure such as Active Directory Federated Services (AD FS), making it a good solution for modern, distributed work environments. Last but not least, Microsoft provides the Temporary Access Pass (TAP) as a bootstrapping method for passwordless authentication. TAP is a time-bound passcode, configurable for single or multiple uses, that allows users to onboard other passwordless methods such as Microsoft Authenticator, FIDO2, and Windows Hello for Business. TAP proves especially beneficial in account recovery situations, allowing users who have lost their primary authentication factors to securely regain access and establish new credentials.

More recently, Entra released the Face Check feature, a facial matching tool that verifies identities by comparing a live selfie with the photo on a user's official document. Powered by Azure AI, it enhances security while ensuring privacy by only sharing match results, not sensitive data. It is effective in preventing fraud by detecting spoofing techniques, including deepfakes. Additionally, Microsoft Entra has obtained an impressive list of security certifications, such as CSA Star, ISO 27001/27018, SSAE 18 SOC 2 Type I/II, and many country-specific security certifications. FIDO2 and OpenID profiles are certified as well. It offers strong support for Access Management capabilities, including hardware authenticators such as CAC/PIV cards, Duo, Feitian, OATH (any), OneSpan Digipass, Thetis, Smart cards, Symantec VIP, and YubiKey tokens. CBAC, RBAC, ABAC, PBAC, RAdAC, and ReBAC principles are supported, and Microsoft Entra ID roles can be assigned to users, groups, and service principals. Microsoft Entra also works with JWT, Kerberos, OAuth, OIDC, and SAML.

Microsoft Entra functionality is available via REST, JSON-RPC, XML-RPCSCIM, LDAP, RADIUS, Java, AMQP, and UDP Socket API.

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

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 17: Microsoft's rating

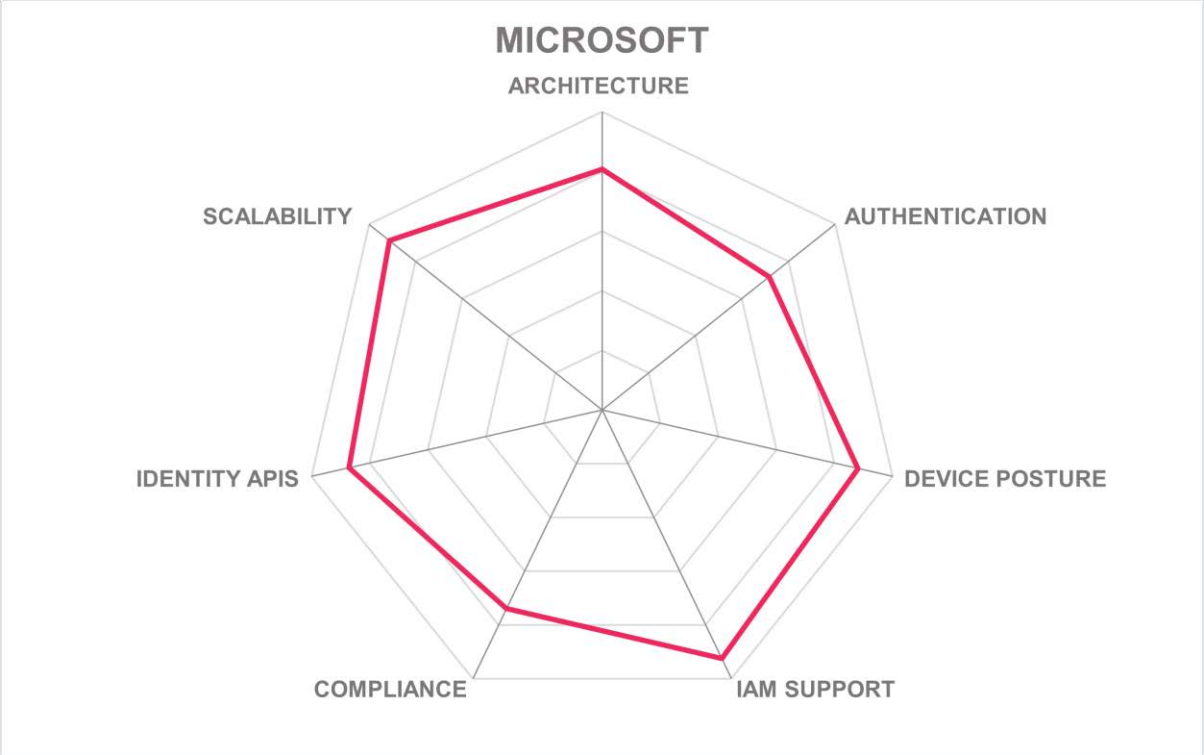
Strengths

- High scalability.
- Support for verifiable credentials (Entra Verified ID).
- Good overall authentication support.
- FIDO2 and app-based passwordless MFA options.
- Coverage of all major areas of IAM in an integrated solution.
- Global partner ecosystem and strong geographical presence.

Challenges

- Only available as multi-tenant, public cloud service.
- No support for voice recognition and iris scan biometrics.

Leader in


MICROSOFT
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Nok Nok – Nok Nok S3 Suite and Nok Nok Authentication Cloud

Founded in 2011, Nok Nok, based in San Jose, California, was founded to replace legacy password-based authentication with next-level passwordless MFA. The company's founders have always understood that a lack of standards was one of the primary inhibitors to broader adoption of strong authentication technologies. This is why Nok Nok was one of the six founding members of the FIDO Alliance. Mid-market and large enterprise customers in North America, EMEA, and APAC are the company's main focus. Licensing is available on a per-user basis.

Nok Nok's S3 Authentication Suite (S3 Suite) is a next-generation authentication platform tailored for regulated and high-security sectors, including financial institutions, mobile network operators, and governments. With the ability to scale to millions of users, the Nok Nok platform is ideally suited for use by enterprises with a large customer base. The S3 Suite encompasses an Authentication Server alongside App SDKs tailored for mobile, web, and smartwatch applications, ensuring wide-reaching accessibility.

With its App SDKs, Nok Nok facilitates deployment of modern FIDO/passkey-based authentication. It provides support for a range of risk signals (additional factors influencing authentication decisions), which include geolocation and travel speed, device health status, jailbreak detection and so on. The solution has native integration with third-party ID verification solutions which can also be leveraged for account recovery purposes.

The Nok Nok solution provides comprehensive attestation support to verify the security characteristics of authentication in BYOD scenarios, including FIDO attestation, Apple App Attest, and Google Play Integrity, which can be configured and evaluated through FIDO policies and a rules engine. By leveraging the existing security features of users' devices and hardware tokens, Nok Nok offers robust, convenient authentication across various applications.

Its adaptive policy engine enables context-based strong authentication, catering to the needs of regulated market verticals. The solution supports the notion of "known"/"trusted" devices. Additional authentication can be triggered when new devices are used for the first time. This is also supported with synced passkeys. Nok Nok offers support for JWT, OIDC, and SAML. However, functionality is available only via REST. The company has not yet attained ISO/IEC 27001 for its Authentication Cloud service. SOC 2 Type II certification work is in progress. Additionally, the S3 Suite is available as a containerized solution and can be operated in the preferred cloud environment of enterprises.

Nok Nok's S3 Authentication Suite effectively supports a broad range of workforce use cases, particularly in high-security and regulated sectors. Nok Nok provides a fully integrated and extensible strong authentication platform based on the FIDO Alliance specifications. It provides a flexible and future-proof solution suitable for the needs of large enterprises. Webhooks and other integrations can easily be implemented using server-side plugins. Plugins for integration with common IAM platforms, such as Ping Federate, ForgeRock AM, Keycloak and others are available. The platform is designed to handle authentication for millions of users, which is essential for large enterprises with extensive employee bases.

© 2024 KUPPINGERCOLE ANALYSTS AG

Nok Nok should be on the short list for organizations considering deploying passwordless authentication solutions. The company appears in the product and innovation leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 18: Nok Nok's rating

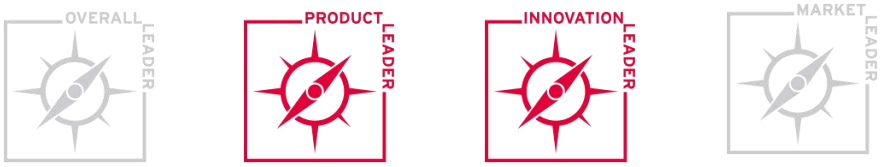
Strengths

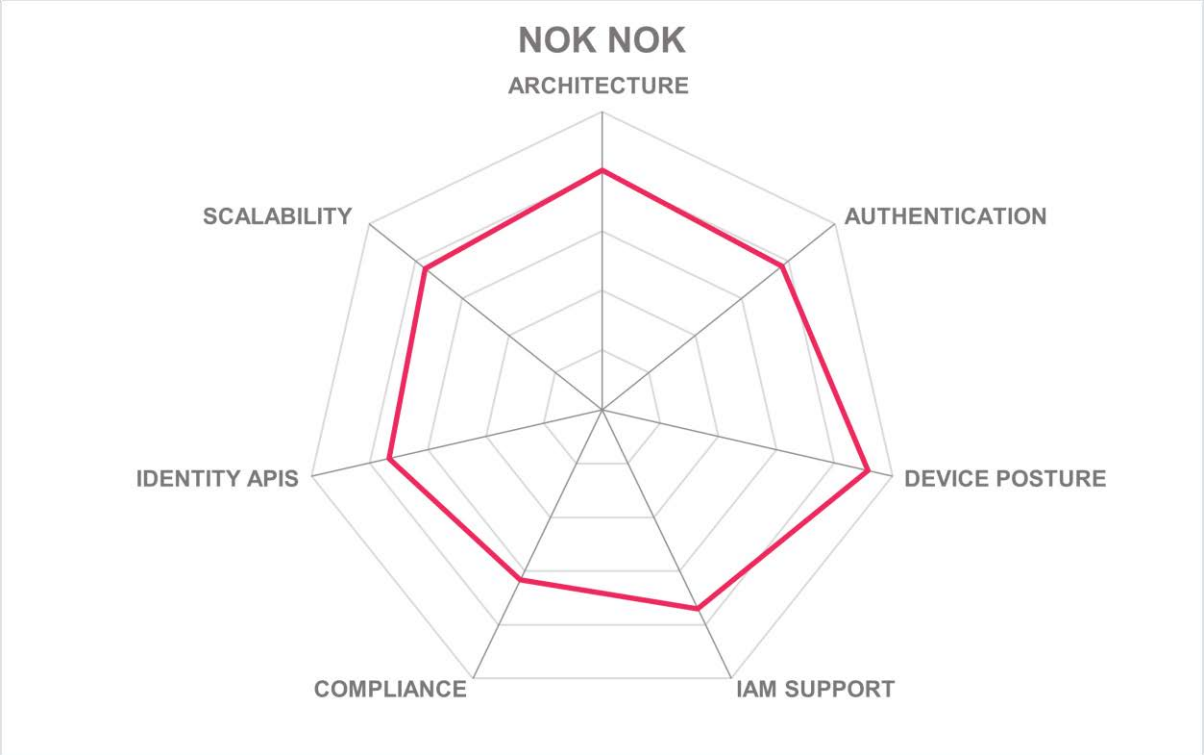
- Founder member of FIDO.
- Good device management capabilities.
- Strong global partner ecosystem.
- Support for a wide range of risk signals.
- OOTB integration with third-party ID verification solutions.
- SDKs tailored for mobile, web, and smartwatch applications.

Challenges

- Limited API protocol support outside of REST.
- ISO/IEC 27001 not attained yet.

Leader in




NOK NOK
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Okta – Okta Identity Cloud

Based in San Francisco, California (US), Okta's cloud identity platform is targeted at both workforce and customer identity management. The company's acquisitions of Auth0 (CIAM, developers) and atSpoke (IGA) broadened Okta's portfolio in 2021. Okta's Identity Cloud is a cloud-based identity platform that provides organizations with a scalable solution for managing user identities, controlling access to devices, applications, and data, and enabling seamless user experiences across various devices and platforms. Moreover, on-premises agents called identity bridges are available for connecting to systems behind the firewall. Okta Access Gateway serves as a reverse proxy for on-premises app SSO and authorization. Pricing is by number of monthly active users.

The platform is used by customers, developers, and businesses to address complex identity problems. Notable features include SSO, context-based Adaptive MFA, Workflows, user provisioning, lifecycle management, API access management, device access, adaptive security policies, and passwordless, phishing-resistant authentication, Device Trust, and integration with a broad range of MDM and endpoint security products including custom built device posture providers. Okta Identity Cloud provides a wide range of capabilities to secure access to applications, devices, and data, while maintaining a user-friendly experience. The company offers native user experiences for administrators and end-users, including an admin console, end-user dashboard, and native mobile/desktop apps.

Additionally, Okta supports application-specific sign-on policies that cater to unique time and device session assurance requirements, along with step-up re-authentication. Administrators have the capability to terminate all sessions for a user through the Admin UI or API and can also selectively end specific sessions via API, enhancing security and control over user access.

Okta Verify is Okta's authenticator app, which can be deployed on mobile and desktop platforms. Among several features, Okta Verify supports Okta FastPass, which enables phishing-resistant, passwordless authentication and device posture checks to help ensure secure access to corporate resources while minimizing end-user friction. FastPass provides a user-friendly, consistent experience across all major platforms and devices, managed or unmanaged. For an even higher level of security assurance, admins can enable device biometrics in combination with FastPass for the end user to provide proof of possession and inherence. If biometrics is not an option or preferred, users can provide a passcode or PIN with FastPass to satisfy 2FA. FastPass can be used to satisfy NIST SP 800-63-3 AAL2 and AAL3 and the draft guidance around NIST SP 800-63-4.

Okta also provides end-to-end phishing resistant flows throughout the entire user lifecycle. Through its partnership with Yubico, admins can pre-enroll a new employee with Okta and ship a pre-registered hardware key, which enables phishing resistant onboarding. Similarly, Okta admins can extend phishing resistant sign-on policies to authentication and recovery flows and enable factor sequencing. For example, admins can configure that a phishing resistant factor is recovered using another phishing resistant factor such as FastPass and with YubiKeys, Smart Cards, and others.

Okta supports many mobile authenticator apps in addition to their own Okta Verify app, as well as passwordless options that include Android/iOS biometrics, Windows Hello for Business, OTP, FIDO U2F/2.0 authenticators, and more. Okta supports REST, Webhooks, WebSockets, and WebAuthn APIs. Okta/Auth0 have many connectors for BI, CRM, marketing analytics and automation, other IAM systems, and popular SaaS apps. Okta also supports OAuth2 Device Flow and machine-to-machine authorization. Customers are using their IoT device identity management features for use cases such as connected cars, home automation, smart speakers, etc. Lastly, Okta has achieved ISO 27001, SOC 2 Type II, OpenID FAPI, CSA Star Level 2, US FedRAMP Moderate and High compliance.

Whether for CIAM or workforce use cases, Okta's cloud-based platform with extensive support for DevOps, strong policy management, and a wide range of API integrations, positions it as a leader in access management solutions. The Okta Identity Cloud's passwordless authentication capabilities allow organizations to embrace modern authentication methods while maintaining a user-friendly experience. Okta has been the target of high-profile cyber-attacks recently from which it continues to recover. In response, the Okta Secure Identity Commitment (OSIC) was conceived, setting a framework to empower our customers and the industry in the fight against Identity attacks. Okta appears in all leadership segments of this Leadership Compass. Organizations contemplating a move to the cloud for their access management services should consider Okta. Organizations that need scalable and flexible passwordless solutions will want to consider Okta Identity Cloud.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 19: Okta's rating

Strengths

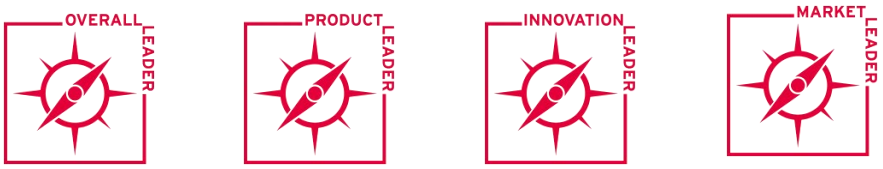
- No code/low code workflow editor.
- Wide range of authentication options.
- Good admin and DevOps support.
- Connectors for over 7,000 apps.
- Highly scalable cloud-delivered services.
- Support for passwordless login to Windows devices.
- Support for phishing authenticator options including FIDO2, WebAuthn, Passkeys, Smart Cards (PIV/CAC).

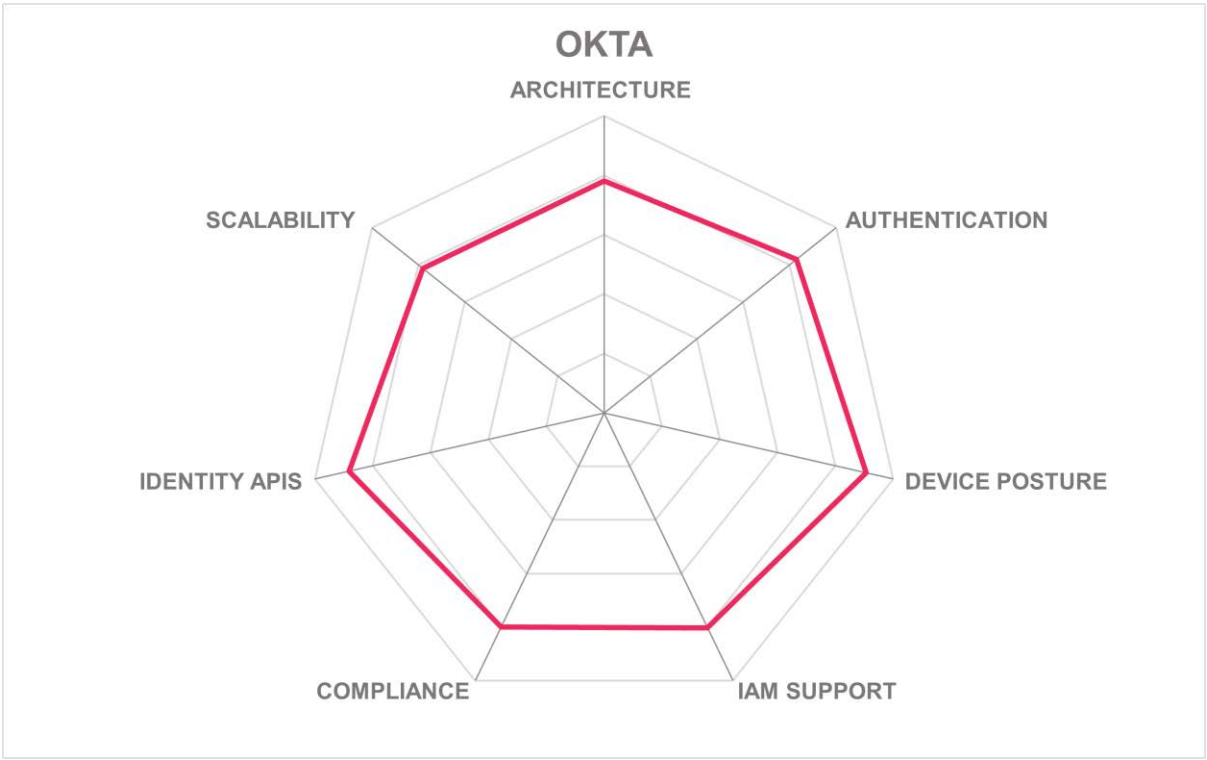
Challenges

- No behavioral biometrics.

- Need to integrate with on-premises appliances, containers, or software delivery options from partners or third parties.
- Okta should raise awareness of its complete identity offering beyond SSO and MFA.

Leader in





One Identity – OneLogin Platform

Founded in 1987 and headquartered in Aliso Viejo, California, One Identity brings together IGA, IAM, PAM, and active directory management capabilities. OneLogin by One Identity offers workforce and customer identity and access management solutions with real-time actionable intelligence and automated configurations. OneLogin has a modern multi-tenant SaaS micro-services architecture based on immutable infrastructure and infrastructure as code, with an on-premises reverse proxy available as a Docker container. On-premises components of the platform are IaaS agnostic, supporting a wide range of IaaS platforms. One Identity has a strong presence across all geographical regions. The company offers a wide range of licensing models.

OneLogin offers passwordless capabilities designed to enhance security across various access points within an organization. It provides application-level authentication policies that can enforce MFA challenges, even if the user is already in a SSO session. This feature is crucial for users with high-level permissions accessing sensitive resources such as finance and HR applications. Additionally, its integration with One Identity's suite—including PAM, IGA, and Active Directory/Entra ID Management—enables the use of OneLogin's passwordless factors for both initial logins and step-up authentication challenges. Passwordless factors primarily include WebAuthn, FIDO2 hardware tokens, and push notifications with number matching. While other options like OTPs, magic links, and SMS codes are available to support specific user communities where enforcing stronger factors may not be feasible. In addition, the OneLogin Protect app provides a tap-and-approve mechanism that incorporates device posture checks. However, the platform has limited support for native device health checks, but these are offered through third-party integrations.

OneLogin's adaptive authentication feature, SmartFactor Authentication, uses machine learning to assess risk based on variables such as location, device, and user behaviour, and dynamically adjusts the required authentication factors during login attempts. The platform provides a BYOD MFA/Trusted IDP feature which allows organizations to enhance their MFA by integrating any third-party authentication which supports OIDC, e.g. a trusted identity provider (TIdP) with OneLogin's Advanced Directory capabilities. This setup enables businesses to bring their own MFA solutions, integrating external MFA mechanisms that aren't necessarily part of OneLogin's third-party partnerships. Organizations can choose a TIdP for authentication, which must use OIDC and cannot rely on JIT provisioning. OneLogin's platform includes robust session management capabilities, an extensive app catalog, APIs for integration, comprehensive logging and reporting, and customizable branding options. OneLogin provides a modern, easy-to-navigate administrative UI and user self-service. Dashboards and reporting options are provided with some native support for some significant compliance frameworks such as GDPR, PDS2, and PCI-DSS. OneLogin's federation-related capabilities include support for SAML 2.0, OAuth 2, OIDC, JWT, and SCIM. The company certifies/attests with ISO 27001 and SSAE SOC 2 Type II. However, FIDO2 certification has not been achieved.

OneLogin presents a feature-rich IAM solution that is well-suited for organizations of any size and type, seeking a scalable platform to address their identity needs. The solution offers

a comprehensive suite of IAM functionalities tailored for both workforce and customer identity needs, ensuring secure and seamless access to resources across various platforms and applications. The inclusion of OneLogin in the product leadership category underscores its effectiveness in the IAM field, highlighting its capability to lead and adapt in a rapidly evolving technology landscape.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 20: One Identity's rating

Strengths

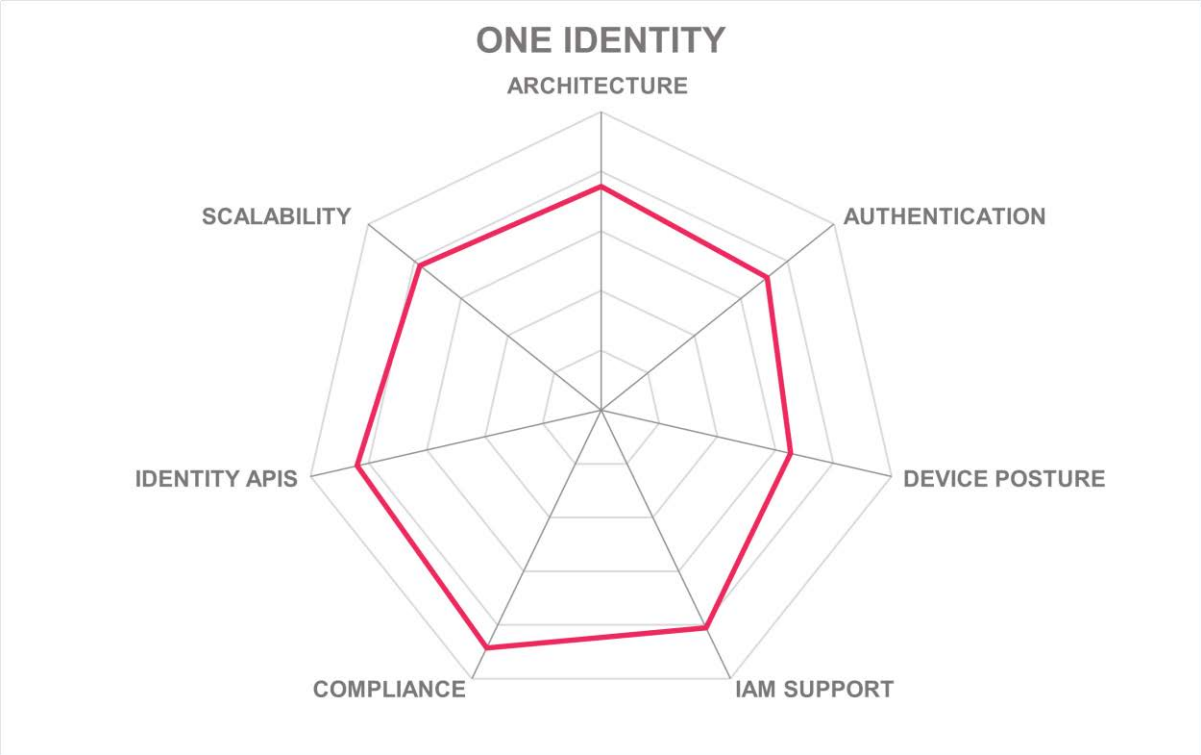
- Strong global partner ecosystem.
- Easy-to-navigate administrative UI and user self-service.
- Support for major compliance frameworks.
- Integration with One Identity's suite—including PAM, IGA, and Active Directory /Entra ID Management.
- BYOD MFA/Trusted IDP feature which allows organizations to enhance their MFA experience.

Challenges

- Missing native FIDO2 certification.
- Workflow for device registration cannot be customized.
- Deep integration with legacy on-premises systems can be a challenge.
- Limited device health checks capabilities. However, it offers integration with third-party tools.

Leader in




ONE IDENTITY
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

OneSpan – OneSpan Authentication

OneSpan, formerly VASCO, is headquartered in Boston, MA, US, and has offices in US, Europe, Canada, Singapore, UAE, Japan, and Sydney. VASCO was founded in 1991 and has a long history of providing highly effective security solutions, including token-based authenticators, e-signature, and fraud prevention to financial services and enterprise customers. VASCO was well-known for its Digipass® products and has acquired several security companies over the years. In May 2018, the new brand, OneSpan, was launched to reflect the strength of a single, integrated solution platform that secures users, devices, and transactions across the digital experience. The company has a presence in North America, EMEA, APAC, and Latin America. It offers a per-user annual term license for their on-premises server and client software. For their cloud software (SaaS), OneSpan supports a per-user model and a per-transaction model based on monthly transaction commitments.

OneSpan delivers security solutions across multiple environments, including cloud, on-premises, and hybrid setups. This adaptability meets diverse business needs and allows organizations to implement security measures tailored to their specific needs. The OneSpan Authentication Suite serves as a state-of-the-art API-based platform, facilitating login requests and e-signature validation to protect online transactions from malicious attacks. It also validates authentication requests to offer secure and seamless access to various corporate resources and applications. On the backend, OneSpan provides solutions such as the OneSpan Cloud Authentication (OCA), a cloud-based MFA solution for online applications, and the OneSpan Authentication Server (OAS), which validates authentication requests for secure access to corporate resources and applications. On the frontend, the solution offers hardware and mobile authenticators, including Digipass hardware authenticators with MFA and transaction signing capabilities, as well as the OneSpan Mobile Authenticator app for secure login via mobile devices using biometrics or PIN with OTP. The Mobile Authenticator Studio provides built-in security and a frictionless authentication experience for mobile applications, while the Mobile Security Suite offers a toolkit for developers, integrating various authentication technologies and improving authentication UX.

Furthermore, the OneSpan Intelligent Adaptive Authentication solution analyzes various data points—including user, device, biometric, historical, behavioral, navigation, and event data—to score each user event, such as registration, login, or transaction, in real-time. This allows the system to dynamically determine and enforce the precise authentication requirements needed for each specific event. By combining software authentication methods with hardware-based security, such as hardware tokens, FIDO2 authenticators and biometric devices, the company delivers a strong level of protection against unauthorized access. In addition, utilizing patented visual transaction signing technology, OneSpan's cross-platform CRONTO technology ensures secure channel support, enabling programmable confirmation of sensitive operations and transactions across various platforms. OneSpan is ISO/IEC 27001, 27017, 27018, SOC 2 Type II, and CSA STAR certified. The company is also certified under the FIDO2 standards.

OneSpan offers a suite of authentication solutions designed to deliver strong security and seamless user experiences across various platforms. The solution excels in providing

tailored project delivery, white-glove treatment support/customer success management, and a commitment to understanding and meeting the unique security challenges faced by each client. Organizations of all sizes and in all industries looking for a feature-rich and flexible solution should consider OneSpan. The company appears in the overall, product, innovation, and market leadership categories.

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Positive

Table 21: OneSpan's rating

Strengths

- Flexible deployments across multiple environments.
- Strong suite of security solutions, covering both software and hardware components.
- Own hardware authenticator platform with native integration.
- ISO/IEC 27001, 27017, 2708 SOC2 Type 2, and CSA STAR certified.
- Scales well for large enterprises and large consumer and business applications with many users.
- Strong transaction signing capabilities through CRONTO.

Challenges

- No support for OAuth2 and OIDC.
- No support for Windows Hello.
- Username/password is supported for account recovery only if chosen by the customer, not as a mandated feature by OneSpan.

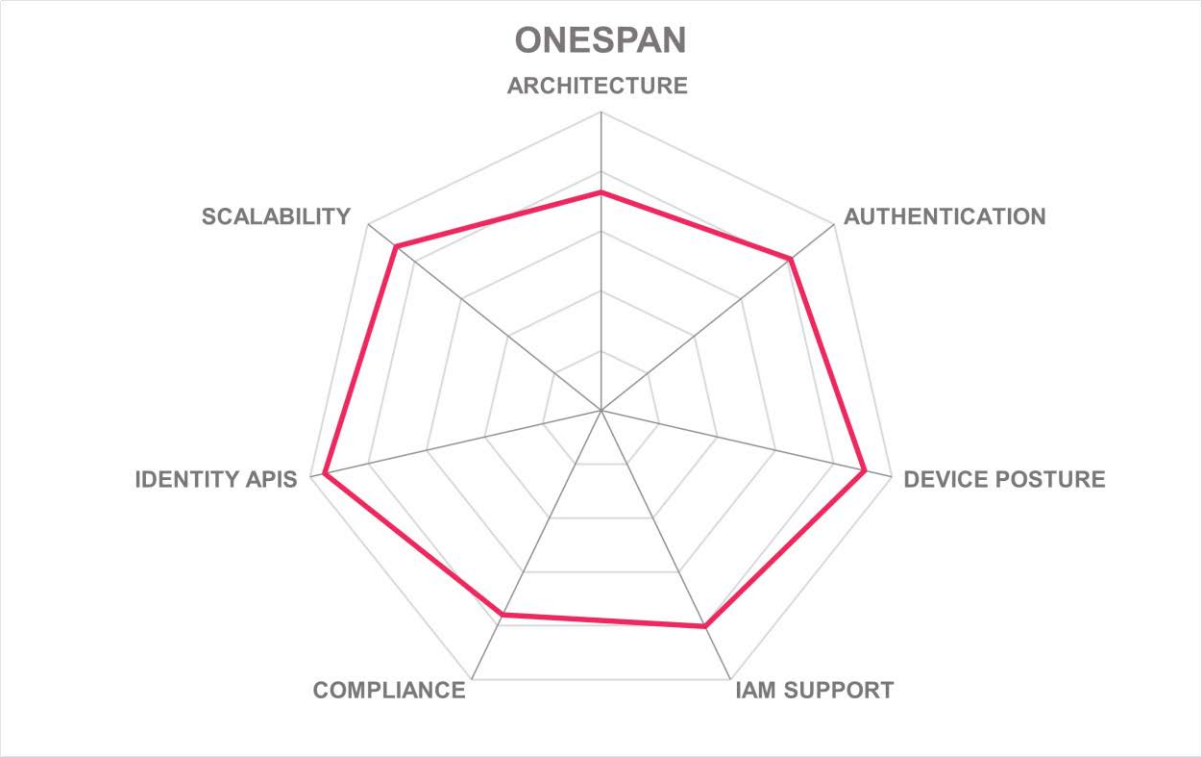
Leader in










ONESPAN
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Ping Identity – The Ping Identity Platform

Ping Identity was founded in 2002 and is based in Denver, Colorado. Ping Identity was among the first of the enterprise IAM vendors to adapt to consumer-facing requirements. With the acquisition of Ping Identity and ForgeRock by Thoma Bravo and the recent merger of the two companies, two strong, established vendors in the IAM field are joining forces. These acquisitions augment the other areas of their identity portfolio. Coverage includes North America, EMEA, APAC, and Latin America. Ping Identity products can be licensed standalone, as well as through solution packages.

The Ping Identity Platform stands out with its comprehensive approach, combining the strengths of ForgeRock and Ping Identity to offer a set of identity services addressing various challenges. It supports a wide range of use cases that include employees, consumers, devices, and partners. The solution extends its capabilities to manage complex partner interactions, including B2B, B2B2C, and B2B2E scenarios. This includes business partners, suppliers, and other external entities that need access to a customer's environment. With a broad focus that includes access management, rich identity management, cloud-native identity governance, and decentralized identity, this platform delivers strong orchestration capabilities at scale. Their approach addresses both modern and legacy systems, ensuring compatibility across a wide range of environments including Mac, Windows, and various legacy protocols.

The platform recognizes that passwordless authentication must cater to diverse user needs and application requirements, supporting various types of authenticators such as authentication apps, hardware tokens, email/phone/SMS OTP, and all flavors of FIDO including passkeys. Moreover, the solution ensures a smooth and self-serve process for recovering access in case of lost or stolen authenticators, offering multiple options for users. Advanced orchestration capabilities within the platform enable the enrollment, usage, recovery, and updating of passwordless authenticators, while also integrating MFA, passwords, and federated SSO paths as required. The solution's functionality is available via APIs and supports SOAP, REST, Webhooks, SCIM, LDAP, and RADIUS. All platform functionality is also available via CLIs. SDKs are provided for a wide range of popular programming languages. Third-party integrations are well-supported, which includes integration to popular ITSM, threat intelligence, EPDR, and UEM solutions. Ping Identity is also self-certified with CSA and certifies/attests with ISO 27001 and SSAE SOC 2 Type II.

With the broad set of capabilities across the increasingly converged platform and the investment into innovation, Ping Identity is well-positioned as a supplier for the modern IT and digital identity landscape. 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. Ping Identity has a strong presence in North America and good representation in EMEA and APAC regions with a suitable partner ecosystem. They appear in all leadership categories in this Leadership Compass.

© 2024 KUPPINGERCOLE ANALYSTS AG

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 22: Ping Identity's rating

Strengths

- Support for decentralized identities.
- Strong global partner network.
- Multiple security certifications.
- Lots of authentication options, including FIDO2, passkeys, hardware tokens and authentication apps.
- Excellent orchestration capabilities.
- Breadth and depth of standards protocol support for legacy and modern access management use cases.

Challenges

- Dashboards are not yet customizable.
- No support for device trust on multiple devices.
- Main presence in North America with rapid growth in the EMEA and APJ regions.
- Wide range of solution components requiring careful evaluation and planning.

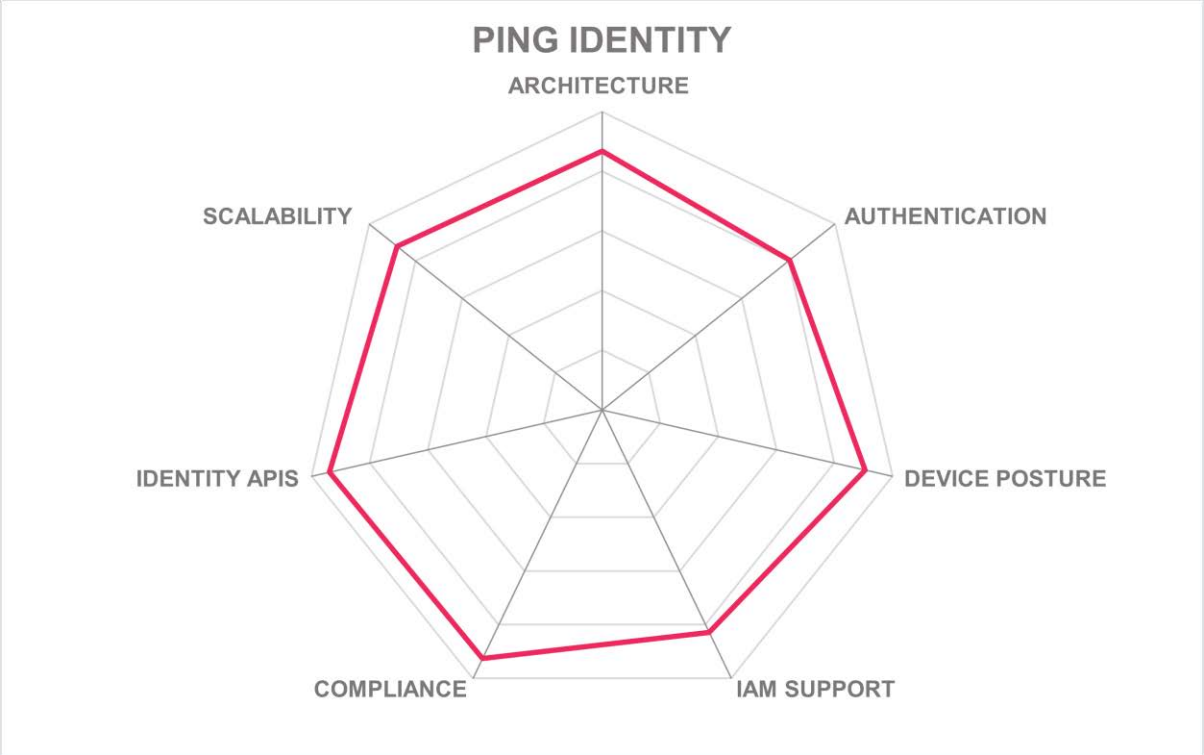
Leader in










PING IDENTITY
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Pointsharp – Pointsharp Platform

Founded in 2006 and headquartered in Stockholm, Pointsharp delivers software and services that help organizations secure data, identities, and access in a user-friendly way. Supported by Main Capital, Pointsharp has expanded its capabilities through strategic acquisitions, including SecMaker, a certificate-based security firm in 2021; Cryptshare, a secure communication expert in 2022; and SIVIS, a specialist in role management in 2023. These acquisitions position Pointsharp as a prominent provider of cybersecurity solutions crafted in Europe, reinforcing European data sovereignty and expanding its technological breadth. The company's focus is on medium, mid-market, and large enterprises in Europe, but with a growing number of customers in North America and Latin America. Licensing is available on a per-user basis.

A significant aspect of Pointsharp's offerings is its adaptability to both cloud-based and on-premises environments, which makes it a versatile choice for organizations transitioning to the cloud or operating in a hybrid IT environment. This flexibility is crucial for sectors like government, healthcare, and defense. Pointsharp's platform ensures that these organizations can maintain control over their data and authentication processes without compromising on security or compliance.

Pointsharp's commitment to supporting complex client environments is evident in its capability to integrate with a myriad of legacy and modern systems. This includes providing solutions that accommodate specific client demands such as maintaining legacy systems while adopting new technologies. The ability to offer tailored solutions extends to detailed policy enforcement, where Pointsharp can implement granular access controls based on various criteria including user role, location, and device compliance, further enhancing the security and customization of its offerings.

The company's platform offers a wide range of authentication methods and passwordless options, including FIDO2, certificates, passkeys, biometrics, smart cards and mobile authenticators, integrated into a cohesive system that efficiently manages and authenticates user access. In addition, the solution offers PKI solutions for both on-premises and cloud-based applications. Moreover, Pointsharp facilitates user identification by integrating with a variety of directories, including Active Directory, Microsoft Entra ID, LDAP, and more. This integration ensures that their suite of authentication, identity, and access management solutions provides modern, user-friendly security customized to meet the unique needs of each organization. Common standards and protocols such as SAML, OIDC, JWT, and OAuth2 are also supported. Pointsharp is ISO/IEC 27001 certified.

Overall, Pointsharp provides a secure, highly customizable and easy-to-use solution that addresses the market's need for user authentication, access and IAM. Through recent acquisitions, the company has significantly expanded its technological capabilities and market reach. Pointsharp is highly adaptable to various deployment environments, supporting everything from on-premises setups to cloud-based infrastructures. It excels in facilitating the transition of legacy systems to modern passwordless solutions, ensuring integration and continuity of operations across diverse technological landscapes.

© 2024 KUPPINGERCOLE ANALYSTS AG

Security	Positive
Functionality	Strong Positive
Deployment	Positive
Interoperability	Positive
Usability	Strong Positive

Table 23: Pointsharp's rating

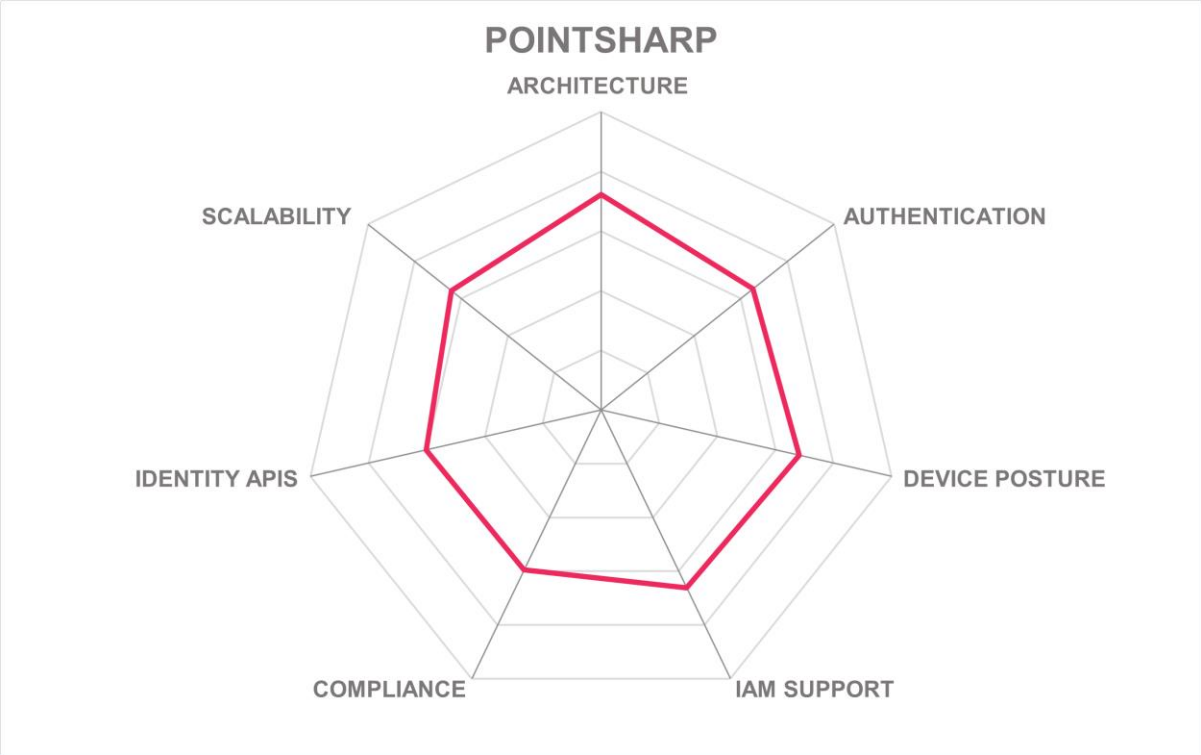
Strengths

- Strong legacy support.
- Possible to run fully on-premises.
- Highly customizable and easy-to-use solution.
- Continuously expanding its capabilities through acquisitions.
- Wide range of authentication methods and passwordless options, including FIDO2, certificates, passkeys, biometrics.
- Versatile choice for organizations transitioning to the cloud or operating in a hybrid IT environment.

Challenges

- A small but well-selected partner ecosystem.
- SCIM based provisioning is not currently supported.
- SOC 2 Type II certification has not been achieved, but on their roadmap.
- Primarily focused on Europe with a growing presence in other regions.

©2024 KUPPINGERCOLE ANALYSTS AG


POINTSHARP
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

RSA – ID Plus

Founded in 1982 and headquartered in Burlington, Massachusetts, RSA offers a range of IAM solutions for both IGA and access management. The company 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 security. It offers industry-leading solutions in identity assurance, access control, encryption, key management, compliance, security information management, and fraud protection. This user-centric approach has led to the development of the RSA Unified Identity Platform (UIP), which brings together RSA Security's three product suites – ID Plus, SecurID, and Governance & Lifecycle. RSA is also a board member of the FIDO Alliance, a co-chair of the Enterprise working group, a member of the UX working group, a member of the FIDO2 technical working group, and a member of the Metadata service technical working group on the FIDO Alliance.

Designed to meet the demands of a dynamic workforce, RSA supports a wide array of authentication methods, including FIDO passkeys, push to approve, OTP, SMS voice, and support for a range of biometric authenticators including Apple FaceID and TouchID, and Samsung Fingerprint. RSA offers passwordless MFA, machine learning enhanced adaptive risk analytics, and hardware and software tokens that can be purchased separately or as part of the ID Plus solution subscription plan. In addition to their own well-known authenticators, RSA supports any FIDO2 or FIDO U2F authenticators, such as HID, Google Titan, Kensington, Thetis, and YubiKey. Smart cards and other third-party authenticators can be supported via third-party IdP integration.

The RSA ID Plus platform can be deployed in cloud, on-premises, or hybrid environments. ID Plus includes several unique access and authentication capabilities, such as high availability enabled via a hybrid deployment that allows for automatic failover to on-premises systems during network disruptions. It also offers a single, unified authenticator application across mobile and desktop OS environments, including macOS, eliminating the need for separate apps for on-premises and cloud authentication. Additionally, ID Plus supports smooth migration from on-premises authentication to cloud without the need for system replacement, avoiding disruptive "rip-and-replace" methods.

RSA Risk AI uses advanced identity intelligence to analyze real-time user access activities for anomalous behavior through advanced machine learning. It then reports the results of the analysis as Identity Confidence scores. The higher the Identity Confidence scores, the more likely it is that this is the same user who is accessing a protected resource. Admins can add Identity Confidence to conditional access policies and assign them to protect access to resources. Risk AI streamlines IT operations by automating complex policy management, reducing unforeseen risks, and strengthening security measures. Furthermore, RSA recently introduced the DS100 authenticator, a cutting-edge, multi-functional hardware authenticator that marries the cryptographic advantages of FIDO protocols with the security benefits of a disconnected one-time passcode (OTP) solution, enabling organizations to meet the diverse authentication needs without the hassle of managing multiple devices.

© 2024 KUPPINGERCOLE ANALYSTS AG

The DS100's firmware is user-updatable, allowing customers to securely update their authenticators with new features and bug fixes without needing hardware replacement. In addition, RSA Mobile Lock is a comprehensive threat and secure access management for iOS and Android devices. Mobile Lock, embedded within the RSA Authenticator mobile application, proactively safeguards organizations from over 60 threats, like jailbroken devices, malware, and suspicious apps, that could compromise managed and unmanaged (BYOD) mobile devices. In case of a threat, it prevents a user from authenticating until the threats are resolved. Unlike MDM solutions, users can still use other mobile device features, ensuring minimal disruption.

Overall, RSA's offerings are well-suited for organizations aiming to modernize their authentication practices while maintaining high security and operational efficiency. RSA's solutions are distinguished by their comprehensive functionality, scalability, and hardware and software-based authentication methods. Backed by a global ecosystem, the company can readily deploy such solutions across various industries and geographic locations. For organizations that broadly utilize RSA products, ID Plus is a viable option for organizations that want to begin a passwordless journey. RSA appears in the product and market leadership categories.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 24: RSA's rating

Strengths

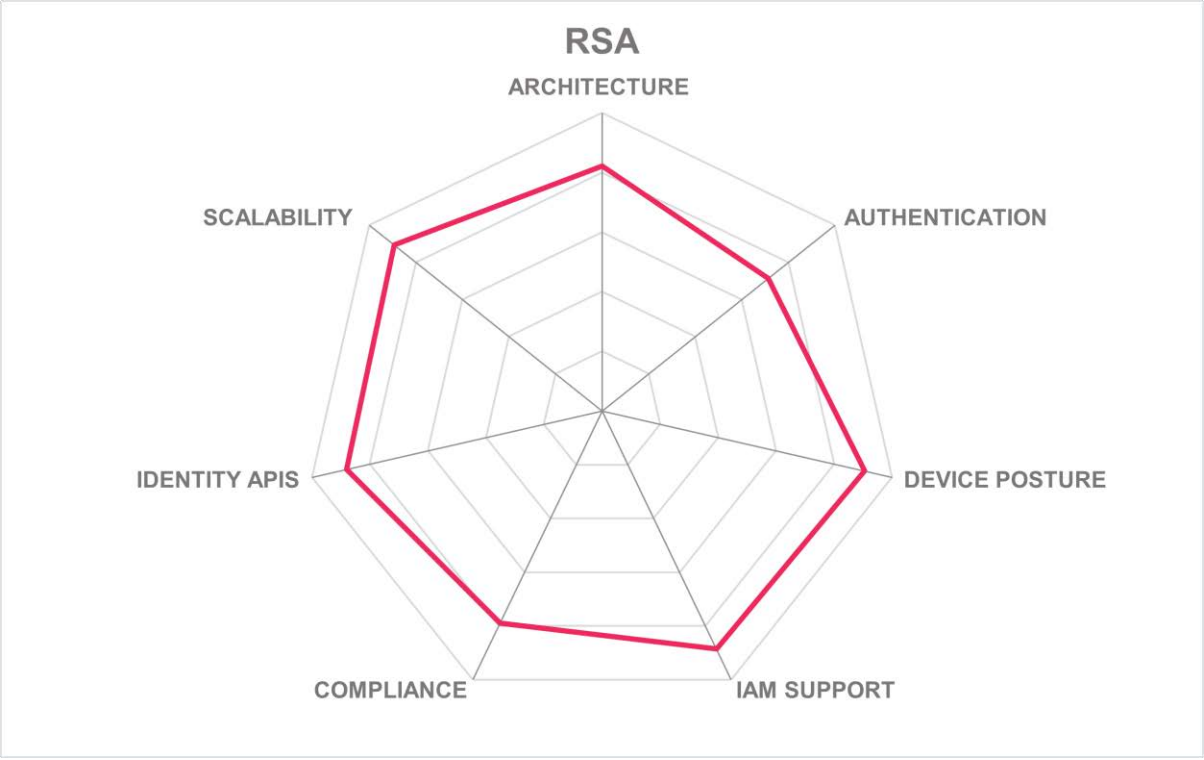
- DS100 hardware authenticator product line.
- Broad range of authentication methods.
- Supports Bring-Your-Own-Authenticator (BYOA) for additional flexibility and control.
- FIDO2 & FIDO U2F certified.
- Large partner ecosystem at global scale.
- Scales well for large enterprises with many users, entitlements, and policies.
- Flexible integration to full suite of RSA security products.
- Hybrid deployment addresses on-premises and cloud models.

Challenges

- No native PAM support, but out-of-the-box integrations.
- Risk engine has limited interoperability with third-party services.

Leader in


OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER


RSA
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

SAASPASS – SAASPASS IAM

SAASPASS was formed in 2013 and is headquartered in San Francisco. Their product, SAASPASS IAM, is centered on providing passwordless authentication services to both 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 is available as both 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 offers a per-fixed cost and per-server model for its on-premises server and client software. For its cloud software (SaaS), it supports a per-user model and a per-period model.

SAASPASS offers a user-friendly solution for IAM needs, providing customers with a single, centralized platform to manage their authentication and security requirements. Unlike other providers that offer separate point solutions requiring multiple purchases and dashboards, SAASPASS consolidates various IAM functionalities into a unified interface, serving as a single pane of glass for all IAM needs. The platform supports various protocols such as JWT, Kerberos, OAuth, OIDC, RADIUS, TACACS, and SAML. However, FIDO2 certification has not yet been attained.

Notably, the platform extends its security coverage to social media, SaaS apps, and on-premises applications, ensuring protection across various digital assets. Furthermore, SAASPASS distinguishes itself with its intuitive UI and user experience (UX) for administrators. SAASPASS also offers a mobile SDK that allows companies to incorporate this functionality into their own mobile app, supporting multiple MFA methods such as mobile authenticators, U2F, UAF, FIDO2, TOTP, and HOTP physical tokens. Their mobile application also supports encrypted barcode scanning, mobile URL callback, and mobile on-device login to prevent MITM attacks. In addition, the solution includes self-service bulk enrollment capabilities. API support includes REST, SOAP, WebSockets, and CSV/JSON/XML formats. The solution also supports LDAP and SCIM for provisioning. However, the company is not ISO 27001 and SOC 2 Type II certified.

The SAASPASS product supports a good variety of authenticators, and it offers reasonable scalability, which makes it attractive for environments where high security and authentication assurance is needed. Organizations looking for modular authentication services or needing to add-on passwordless capabilities to an existing IAM infrastructure may want to look at SAASPASS capabilities in these areas.

Security	Positive
Functionality	Positive
Deployment	Neutral
Interoperability	Strong Positive
Usability	Strong Positive



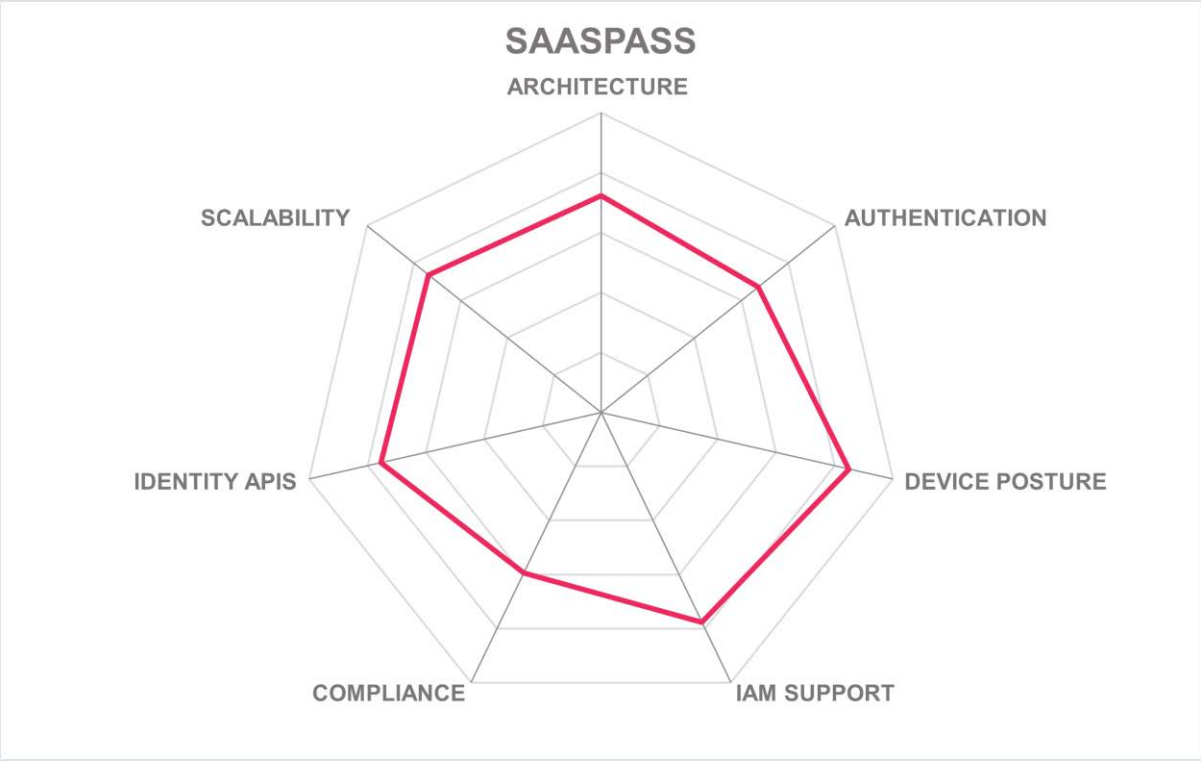
Table 25: SAASPASS' rating

Strengths

- Wide range of MFA types supported.
- Strong device posture capabilities, including support for wearables.
- Good selection of SaaS app connectors.
- Intuitive UI and user experience (UX) for administrators.
- Supports various protocols such as OAuth, OIDC, and SAML.
- Consolidates various IAM functionalities into a unified interface, serving as a single pane of glass.

Challenges

- Missing FIDO2 certification.
- 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.
- SOC 2 Type II and ISO/IEC 27001 certifications not yet initiated.



Secfense – User Access Security Broker

Founded in 2018 and headquartered in Krakow, Poland, Secfense focuses on enhancing user access security for large organizations. The company positions itself as a broker, mediating between users and their applications, especially addressing the challenges posed by legacy systems. The company's focus is on the EMEA and North America regions. Supported licensing models include per-user and per-node options.

Secfense User Access Security Broker is a network traffic broker that learns the traffic patterns related to authentication and builds an additional security layer between users and their applications. It is deployed as a reverse proxy. In addition, Secfense supports passkeys, FIDO2, TOTP, U2F tokens, and multiple hardware tokens such as Duo, Feitian, Google Titan, Kensington, OATH, YubiKey, and more. Username/password for authentication or account recovery is not supported.

The Secfense Authenticator enhances MFA by enabling the implementation of the FIDO2 standard across an organization's systems. Complementing this, Secfense’s micro authorizations increase security by necessitating additional verification at crucial interaction points during user activities. This feature adheres to Zero Trust security principles, thus amplifying defense mechanisms against unauthorized access.

The solution's flexibility allows it to adapt to both web-based and cloud-hosted applications, enhancing its scope as a security layer that can be tailored to a variety of IT environments. Notably, Secfense's solution does not require modification to existing applications, making it a suitable option for enterprises with a complex catalog of applications.

The Full Site Protection capability elevates security by distinguishing between trusted and untrusted networks. Collectively, these features seamlessly integrate to provide comprehensive, scalable, and robust cybersecurity solutions for organizations.

Secfense supports REST and Webhooks. Common standards and protocols such as RADIUS, TACACS, SAML, OIDC, JWT are also supported. However, the company does not yet have certifications for ISO 27001 and SOC 2 Type II. On Secfense's roadmap is the development of the Passwordless Broker, a novel approach in the market that enables passwordless authentication across different applications without the need for software integration or code changes. Secfense provides a good solution that acts as a security broker, helping organizations transition from legacy systems to secure, modern environments.

© 2024 KUPPINGERCOLE ANALYSTS AG

Security	Neutral
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Positive

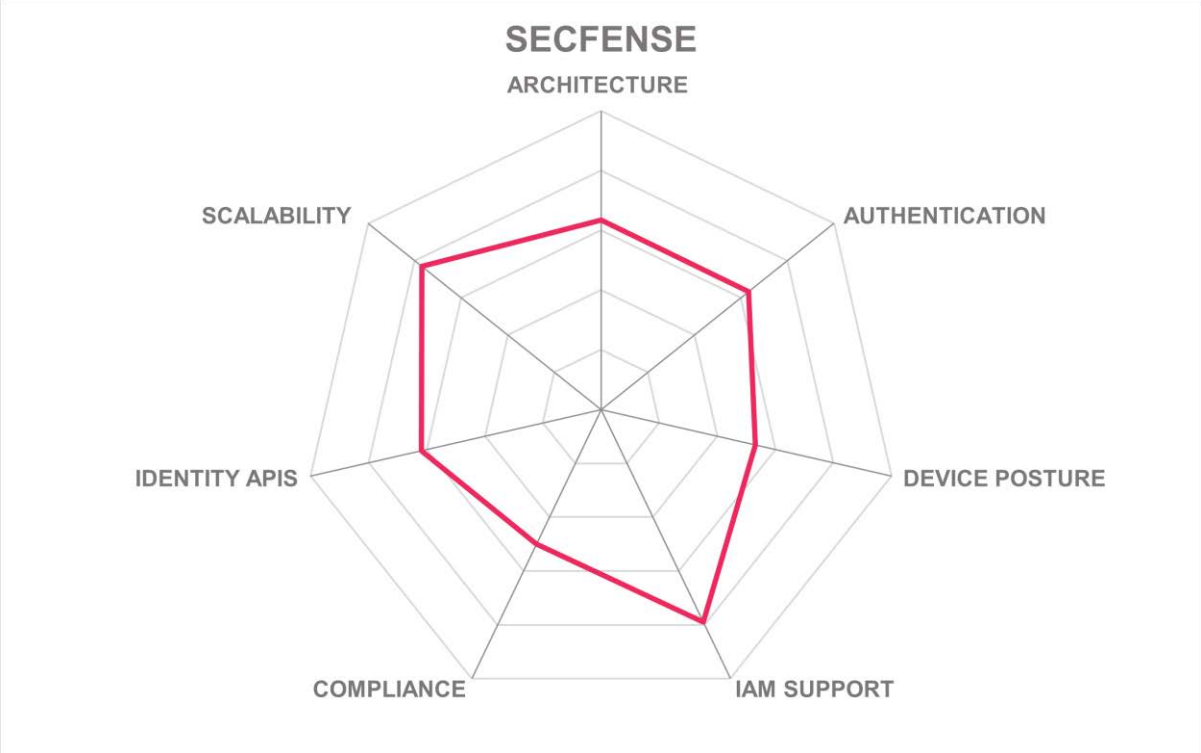
Table 26: Secfense's rating

Strengths

- Micro authorization functionalities.
- Supports various authentication methods, such as FIDO2.
- Enables smooth transition from legacy systems to modern security.

Challenges

- No support for OAuth2.
- Limited device health checks features.
- Small partner ecosystem and limited global reach.
- More security certifications would be helpful.



SecureAuth – SecureAuth Workforce

SecureAuth has been in the market since 2005 and is headquartered in Irvine, CA. The company is dedicated to staying ahead through continuous modernization and innovation. SecureAuth has a large customer base in medium to enterprise organizations, predominantly in North America, with some growth in the EMEA and APAC regions. The company serves organizations in the financial, manufacturing, government, healthcare, insurance, retail, and energy industries. SecureAuth's subscription pricing is based on monthly authorization grant volume, with a tiered model incentivizing higher volumes and performing specific authorizations for each sensitive transaction rather than only once per authenticated session.

In late 2021, SecureAuth's acquired Acceptto and added contextual behavior threat intelligence to its list of capabilities. In 2022, the company launched Arculix, a next generation platform that combines orchestration, passwordless, and continuous authentication capabilities. This solution delivers MFA, risk-based adaptive authentication, SSO, authorization and policy management, and user self-service capabilities. And in late 2023, SecureAuth acquired Cloudentity adding innovations across authorization, end-user consent, and Open Finance as well as further enhancements to SecureAuth's passwordless authentication capabilities, making it a versatile and advanced solution for IAM needs.

SecureAuth offers two solutions: One for Workforce IAM which is based on the core SecureAuth IDP platform and is focused on use-cases where the business owns and/or controls the devices from which users are trying to gain access. The second offering for Customer IAM, based on the Cloudentity platform and focused on use cases where the end user is a customer outside of the company's control (i.e. a B2C scenario) and potentially gaining access through a complex business ecosystem (i.e. a B2B2C or B2P2C scenario). Both solutions now include the orchestration, passwordless and continuous authentication capabilities previously offered and marketed as the Arculix product. The union and realignment of this broad set of technology enables SecureAuth to provide modern frictionless experiences across the entire spectrum of IAM use cases.

SecureAuth solutions provide an innovative approach with its Universal Authentication Fabric (UAF) that encompasses device trust (for root of trust) and an AI/ML driven risk engine that tracks over 200 variables and integrates third-party intelligence. This approach enables continuous authentication that allows users to log-in one time with biometric or other passwordless methods and after that they can log-in passwordlessly into other apps, VPN, VDI, etc. By continuously authenticating users every few minutes with Invisible MFA, the solution provides an easy-to-use experience while securing access. In addition to SecureAuth's risk-driven continuous passwordless technology authentication, email/phone/SMS OTP, most major authenticator apps, Android and iOS biometrics, and all flavors of FIDO (including passkeys) are accepted.

SecureAuth also uses its risk engine to establish a level of assurance (LOA) that begins before the first login and continuously adjusts the LOA score post-authentication throughout the user journey. In addition, the MFA feature enhances security by evaluating access post-authorization using push notifications or verification codes, even offline. SecureAuth's

solutions are implemented in a cloud-native microservice architecture that can support on-premises, cloud, and hybrid deployment models as well as air-gapped environments. SDKs are given that support Java, .NET, Python, Go, Ruby, and JavaScript programming languages and SDKs for Android and iOS platforms. API protocols supported include REST, Webhooks, SCIM, LDAP, and RADIUS. Third-party integrations are well supported, which includes integration to popular ITSM, threat intelligence, EPDR, and UEM solutions.

SecureAuth's solution tackles workforce challenges such as secure remote access, streamlined user authentication processes, and reduced administrative overhead by automating identity management tasks. The company has notably evolved its solution architecture, embracing a modern, microservices-based approach that aligns with contemporary enterprise needs. SecureAuth's advancements have positioned it favorably in this Leadership Compass' product and innovation leadership categories. This acknowledgment underscores its commitment to continuous improvement and innovation in the IAM space.

Security	Strong Positive
Functionality	Positive
Deployment	Strong Positive
Interoperability	Positive
Usability	Strong Positive

Table 27: SecureAuth’s rating

Strengths

- Support for many authentication types.
- Contextual and risk-based authentication.
- Expanding its capabilities through acquisitions.
- Continuously adjusts the LOA score post-authentication throughout the user journey.
- Risk engine authentication secures remote work by pre-emptively identifying and addressing security vulnerabilities.
- Third-party integrations are well supported, which includes integration to popular ITSM, threat intelligence, EPDR, and UEM solutions.

Challenges

- Primarily focused on the North American market.
- Does not use internal compromised credential intelligence.
- Promote the adoption of continuous authentication among customers.
- Username/password is supported for account recovery only if chosen by the customer, not as a mandated feature by SecureAuth.

© 2024 KUPPINGERCOLE ANALYSTS AG

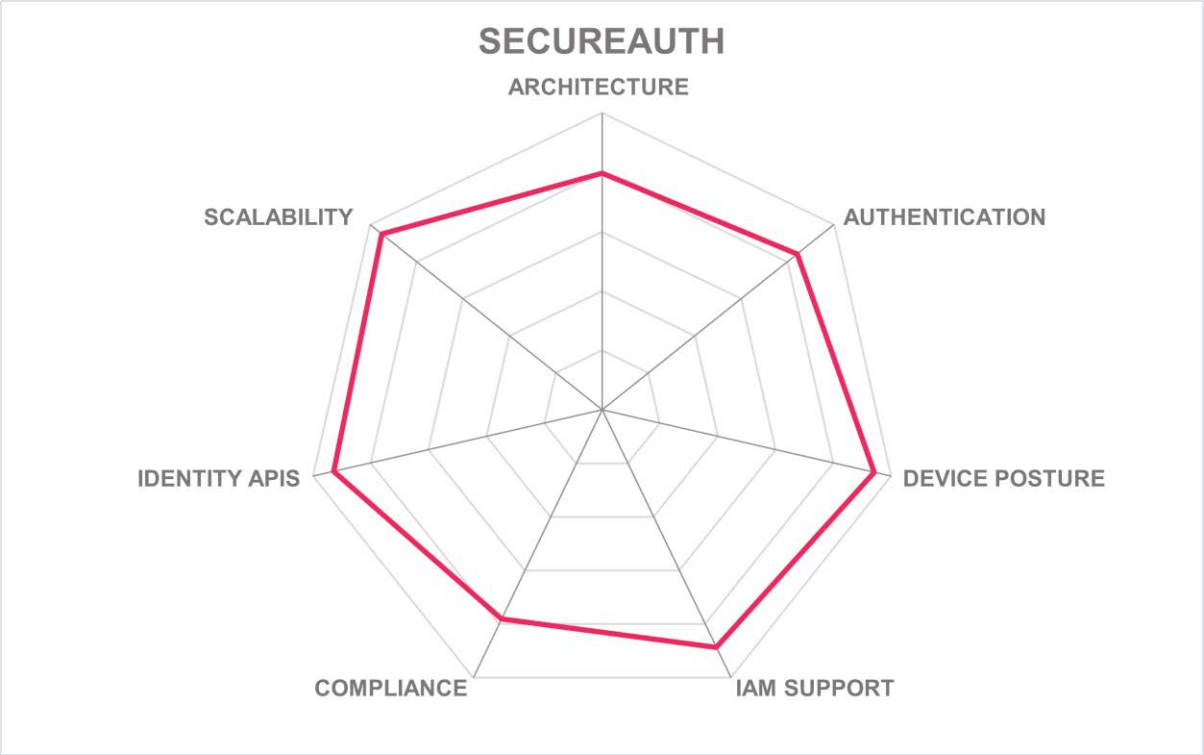
Leader in


OVERALL
LEADER


PRODUCT
LEADER


INNOVATION
LEADER


MARKET
LEADER


SECUREAUTH
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Systola – SystoLOCK

Founded in 2003 and based in Hamburg, Systola specializes in Microsoft Windows enterprise environments and IT security. Systola's target customer is small and medium enterprises in the DACH region. It is particularly effective in sectors such as utilities, manufacturing, healthcare, and finance, where robust security practices are critical. The solution is based on a per-user licensing model, making it a cost-effective solution for enhancing enterprise security.

Systola's passwordless solution focuses on on-premises identity management of employees within Microsoft Windows domains and provides MFA capabilities. In addition, Systola provides diverse authenticators through its SystoLOCK App, NFC cards, and passkeys. This suite ensures that enterprises can secure access across various levels of user permissions and device types, increasing security without compromising on convenience. SystoLOCK's technology hinges on native Windows functionalities, such as PKIs, to manage authentication processes. Moreover, SystoLOCK manages all certificate-related functionalities server-side, which eliminates the risks associated with storing sensitive information on client devices.

For companies with mobile or remote employees, SystoLOCK offers robust offline authentication capabilities. This is especially beneficial for users who need to access corporate resources, including Microsoft 365, through Active Directory Federation Services (ADFS). However, the sole account recovery option available is through the help desk, which might be perceived as inconvenient for users. Systola supports Kerberos, RADIUS, SAML, OIDC, and OAuth2. However, the company does not yet have certifications for ISO 27001 and SOC 2 Type II.

The solution lacks some capabilities in terms of device health checks and account recovery compared to most vendors. They should pursue more security certifications to increase adoption and market share. Their presence in the DACH region, both in terms of strategic hubs and sales target, is a plus for that region and for their own growth potential. Organizations in the DACH region seeking a cost-effective solution and relying on Windows enterprise environments may want to consider Systola.

Security	Positive
Functionality	Positive
Deployment	Positive
Interoperability	Weak
Usability	Positive

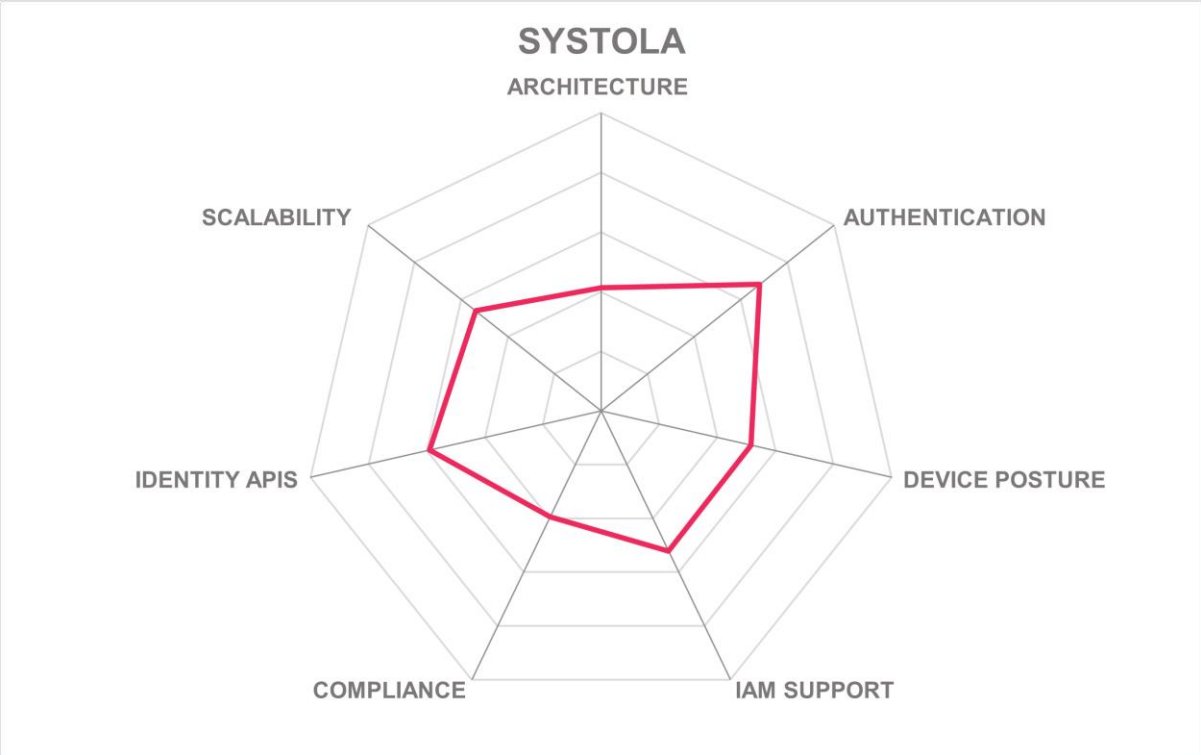
Table 28: Systola's rating

Strengths

- Support for device trust on multiple devices.
- Integrates with UEM solutions.
- Support SAML, OIDC, and OAuth2.
- Accepts most authenticator types.

Challenges

- Missing certifications for ISO 27001 and SOC 2 Type II.
- FIDO2 not supported but it's on their roadmap.
- Only account recovery option available is through the help desk.
- Solution limited to Microsoft Windows environments.



Thales – OneWelcome

Thales is a French global company and leader in the aerospace, transportation, defense, and security markets. Its Digital Identity & Security division sells through a large network of distributors and resellers. In 2022, the company acquired Dutch CIAM company OneWelcome, one of the leading European providers of CIAM. As a result, Thales offers a comprehensive suite of integrated IAM products and services designed to address various identity use cases for customers, partners, and external identities for different verticals like insurance, banking, government, and telecommunications. Multiple pricing schemes are available, including by monthly registered users, fixed cost models for enterprises and MSPs, per-module costs, and per identity verification request.

Recently, Thales introduced the Passwordless 360° strategy, designed to address the widespread challenges organizations encounter when scaling passwordless authentication, which frequently leads to fragmented solutions. This initiative complements the Thales OneWelcome Identity Platform, a flagship SaaS solution that provides organizations with a versatile set of identity applications suitable for various use cases, including customer, partner, and supplier identities. Additionally, OneWelcome Authenticators deliver phishing-resistant, passwordless authentication options, including FIDO and OTP hardware tokens, to safeguard user interactions. Lastly, SafeNet Trusted Access focuses on critical enterprise use cases such as remote and cloud application access, providing strong identity assurance and streamlined access management. It features an extensive administrative interface for policy management, modules for application management, user data handling, access and audit logs, and a dashboard for viewing statistics and alerts.

The solution offers extensive support for passkeys and the ability to synchronize passkeys for use across various devices and low-assurance scenarios. Verifiable credentials support is offered through the User Journey Orchestration module, to connect to national identity schemes for identity validation or natively verify the identity via various methods including liveness detection, ID photo to selfie matching, NFC eID capture, AML checks, manual verification. The Thales Digital ID Wallet can also be used for in-person verification. With Thales, organizations can deploy robust authentication mechanisms, including hardware tokens, wearables, smart cards, and software-based authenticators, ensuring secure access across diverse environments and devices. Support for IaaS installation is not available. Depending on the product component, on-premises and private cloud components are delivered as software deployed to a server or a Docker container.

The product has been independently certified to support compliance with a wide range of standards, including FIPS, ISO 27001, SOC 2 Type II, and eIDAS, to name a few. Overall, Thales offers a comprehensive solution that enables organizations to improve their identity management practices, adapt to evolving technologies, and effectively secure their systems and data. Organizations in highly regulated industries and security-conscious organizations in both the public and private sectors that require strong authentication should consider the OneWelcome Identity Platform. Thales appears in the overall, product, innovation, and market leadership categories.

© 2024 KUPPINGERCOLE ANALYSTS AG

Security	Strong Positive
Functionality	Strong Positive
Deployment	Strong Positive
Interoperability	Strong Positive
Usability	Strong Positive

Table 29: Thales' rating

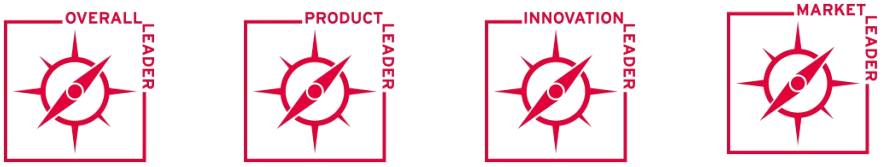
Strengths

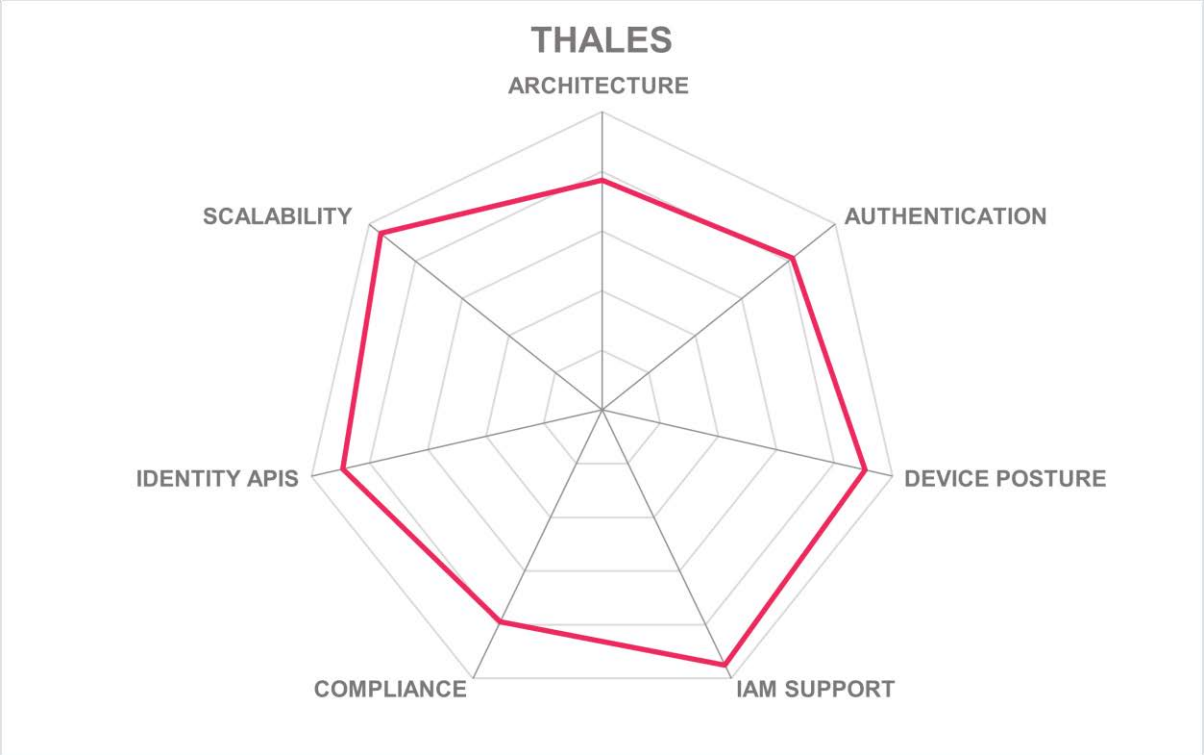
- Strong partner ecosystem.
- Modern UIs and dashboards.
- Support for verifiable credentials.
- Multiple security certifications, including FIDO and biometrics.
- Ability to comply with country-specific regulatory requirements.
- Wide range of authentication mechanisms, including hardware tokens, wearables, smart cards, and software-based authenticators.

Challenges

- Comparatively expensive.
- Push-back from customers when introducing passwordless in highly regulated industries.
- Username/password is supported for account recovery only if chosen by the customer, not as a mandated feature by Thales.

Leader in




THALES
ARCHITECTURE
AUTHENTICATION
DEVICE POSTURE
IAM SUPPORT
COMPLIANCE
IDENTITY APIS
SCALABILITY

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons, but nevertheless offer a significant contribution to the market space.

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.

Why worth watching: Identité operates in three domains: access, identity, and privileged. Products include NoPass for Consumer and NoPass for Employees. The solution focuses on all types of users that are performing MFA by replacing the shared secret password-authentication method with a decentralized token.

IDlayr

IDlayr is headquartered in London and was founded in 2020 by serial entrepreneurs who previously built cloud communications and payments platforms Mblox, Nexmo, and Boku. IDlayr 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.

Why worth watching: IDlayr provides an enterprise-friendly single point of integration for businesses looking to deploy SIM-based authentication. IDlayr's APIs provide an abstraction layer on top of the disparate, individual APIs provided by Mobile Network Operators (MNOs).

Keyless Technologies

Keyless was founded in 2019 and is headquartered in London, UK. It is an 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.

Why worth watching: 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.

Micro Focus

Founded in 1976, Micro Focus is a British multinational software company headquartered in Newbury, UK. The company is one of the world's largest enterprise software providers and offers mission-critical technology and consulting services to thousands of customers. Micro Focus is also known for its long history of acquisitions, holding ownership in product lines of such vendors as Attachmate, NetIQ, and Novell.

Why worth watching: Micro Focus offers passwordless capabilities in Access Manager, supporting a variety of authentication methods including Kerberos, certificate-based, and integration with NetIQ Advanced Authentication. This integration enables passwordless access through FIDO2, FIDO U2F, Bluetooth, smartphone apps, facial recognition, fingerprints, NFC cards, and PKI.

Yubico

Founded in 2007 and headquartered in Santa Clara, California, Yubico, the inventor of the YubiKey, is a creator and major contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards, and a pioneer in delivering modern, hardware-based key authentication security at scale to customers in over 160 countries.

Why worth watching: Yubico’s solutions enable passwordless logins using the most secure form of passkey technology. YubiKeys work out-of-the-box across hundreds of consumer and enterprise applications and services, delivering strong security with a fast and easy experience.

© 2024 KUPPINGERCOLE ANALYSTS AG

Related Research

Leadership Compass: Passwordless Authentication for Consumers 2024.

Leadership Compass: Access Management 2023

Whitepaper: The Future is Passwordless. If you do it right.

Whitepaper: Simplifying and Strengthening Authentication with Passwordless Desktop MFA

Advisory Note: Maturity Level Matrix for IAM

Blog: Trends and Predictions - Passwordless Authentication

Copyright

©2024 KuppingerCole Analysts AG all rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing in-depth analysis, positions presented in this document will be subject to refinement or even major changes. KuppingerCole disclaims all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole does not provide any legal services or advice, and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

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 making 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.