LICENSED FOR INDIVIDUAL USE ONLY

The Forrester Wave™: Customer Identity And Access Management, Q4 2020

Tools And Technology: The Identity And Access Management Playbook

by Andras Cser
October 8, 2020

Why Read This Report

In our 32-criterion evaluation of customer identity and access management (CIAM) providers, we identified the 13 most significant ones — Akamai, Auth0, ForgeRock, IBM, LoginRadius, Microsoft, Okta, OpenText, Optimal IdM, Ping Identity, Salesforce, SAP, and WSO2 — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk (S&R) professionals select the right one for their needs.

Key Takeaways

ForgeRock, IBM, And SAP Lead The Pack

Forrester's research uncovered a market in which ForgeRock, IBM, and SAP are Leaders; Ping Identity, WSO2, Okta, Salesforce, and Auth0 are Strong Performers; and LoginRadius, Microsoft, Akamai, OpenText, and Optimal IdM are Contenders.

Consent Management, Identity Verification, And Scalability Are Key Differentiators

As older CIAM solutions become less effective at meeting the rapidly evolving security and privacy requirements of digital customer acquisition and retention processes, vendors that can provide comprehensive consent management, productized integration with identity verification, and scalability position themselves to deliver frictionless and delightful user management and accelerated time-to-value to customers and succeed in this market.

This PDF is only licensed for individual use when downloaded from forrester.com or reprints.forrester.com. All other distribution prohibited.

The Forrester Wave™: Customer Identity And Access Management, Q4 2020

Tools And Technology: The Identity And Access Management Playbook



by Andras Cser
with Merritt Maxim and Benjamin Corey
October 8, 2020

Table Of Contents

2 CIAM Converges Security And User Management

3 Evaluation Summary

9 Vendor Offerings

9 Vendor Profiles

Leaders

Strong Performers

Contenders

15 Evaluation Overview

Vendor Inclusion Criteria

16 Supplemental Material

Related Research Documents

The Forrester Customer-Obsessed Identity And Access Management Operating Model

The Forrester Wave™: Risk-Based Authentication, Q2 2020

Transform Your IAM Strategy To Succeed In The Post-Pandemic Era

Share reports with colleagues. Enhance your membership with Research Share.

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

© 2020 Forrester Research, Inc. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Unauthorized copying or distributing is a violation of copyright law. Citations@forrester.com or +1 866-367-7378

CIAM Converges Security And User Management

The CIAM market has been undergoing major changes over the past two years. CIAM is no longer just an extension of general IAM capabilities, and most enterprise IAM vendors now offer dedicated CIAM solutions. Vendors with IAM backgrounds, such as IBM, Okta, and Ping Identity, have been integrating platforms for business systems like CRM, web analytics, and privacy management into CIAM solutions. At the same time, vendors such as Akamai and SAP with more of a customer user management background have been expanding business system integrations and adding security capabilities such as provisioning, authentication, and authorization to their CIAM solutions.

As a result of these trends, CIAM customers should look for providers that:

- **Enable seamless, frictionless customer privacy and consent management.** As regional and global privacy regulations multiply, S&R pros' task to manage privacy and user consent to terms and conditions (T&Cs) while maintaining delightful customer security experiences is getting more complex. As a result, Forrester clients increasingly demand CIAM solutions with native, integrated consent management. Consent management should go beyond using an arbitrary customer user store attribute to indicate which version of a user agreement the customer accepted, instead providing the ability to manage multiple versions of agreements and generate granular reports on user acceptance of T&Cs.
- **Integrate with identity verification (IDV) solutions.** In (post) pandemic times, digital customer acquisition, onboarding, and retention are more critical than ever. To support faceless online approaches, CIAM solutions should offer productized integration with physical document verification solutions such as Onfido and Mitek; IDV solutions such as Equifax, Experian, GBG, LexisNexis, and TransUnion based on credit file headers; and social IDV solutions such as Socure and id.me. Drawing data from internal or third-party threat intelligence sources to supply context and further refine customer risk assessment during onboarding also reduces unnecessary customer friction and investigation labor.
- **Scale to large numbers of users in both technology and price.** Even small firms have huge customer user populations requiring management and digital authentication; media companies are a great example. Customers seek a CIAM vendor with a proven track record of serving tens of millions of customers with its CIAM solution; they also want vendors to provide sizing guides and performance guarantees under peak loads, including documented response times for new user registration, user self-service, and login procedures. CIAM vendors should offer pricing based on transaction volumes, number of active users, and total number of (active and inactive) users.[1]

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

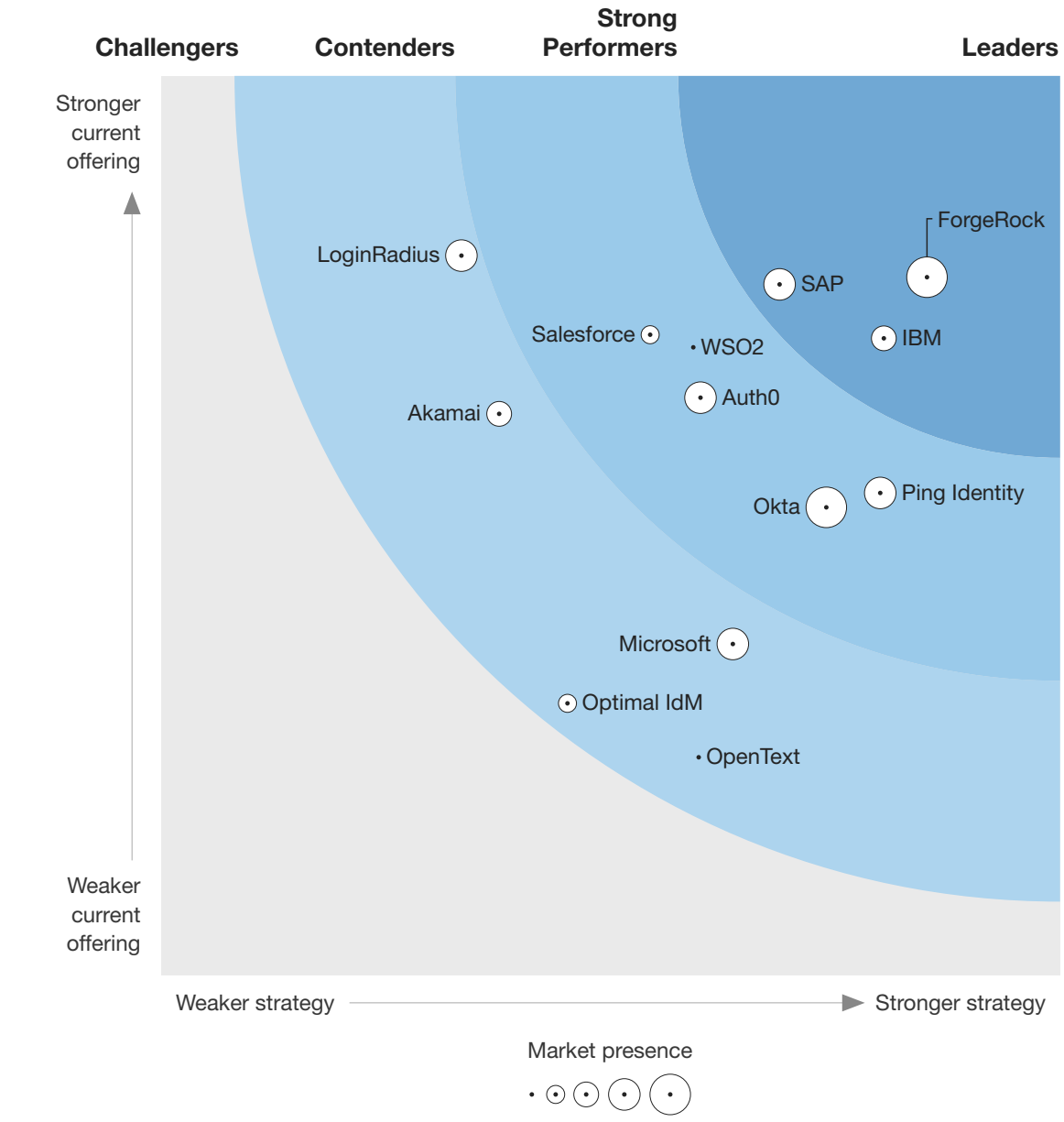
Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our reports on CIAM.

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 1 Forrester Wave™: Customer Identity And Access Management, Q4 2020



© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Customer Identity And Access Management Scorecard, Q4 2020

	Forrester's weighting	Akamai	Auth0	ForgeRock	IBM	LoginRadius	Microsoft	Okta
Current offering	50%	3.12	3.21	3.88	3.54	4.00	1.84	2.60
Data orchestration and user management	8%	1.00	3.00	5.00	3.00	5.00	1.00	3.00
Customer identity verification and registration	8%	3.00	3.00	5.00	1.00	3.00	1.00	5.00
Privacy, consent management, and profiling	7%	5.00	3.00	3.00	3.00	5.00	1.00	1.00
Customer authentication	7%	1.00	1.00	3.00	5.00	3.00	1.00	5.00
Customer self-service	7%	3.00	1.00	5.00	1.00	3.00	1.00	1.00
Business systems integration	7%	1.00	5.00	5.00	3.00	3.00	3.00	3.00
IDV and fraud management systems integration	7%	3.00	3.00	5.00	5.00	1.00	3.00	1.00
Reporting and dashboarding	7%	5.00	0.00	3.00	5.00	3.00	1.00	1.00
Active human users	7%	5.00	5.00	1.00	3.00	5.00	3.00	3.00
Number of brands	7%	5.00	3.00	5.00	3.00	5.00	1.00	1.00
Authentication attempts per hour	7%	5.00	5.00	5.00	3.00	5.00	1.00	1.00
Compliance	7%	3.00	5.00	3.00	5.00	5.00	5.00	5.00
Navigation and integrated environment	7%	3.00	3.00	5.00	5.00	5.00	3.00	3.00
Static and contextual documentation	7%	1.00	5.00	1.00	5.00	5.00	1.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Customer Identity And Access Management Scorecard, Q4 2020 (Cont.)

	Forrester's weighting	Akamai	Auth0	ForgeRock	IBM	LoginRadius	Microsoft	Okta
Strategy	50%	1.88	3.00	4.26	4.02	1.67	3.18	3.70
Execution roadmap	7%	3.00	3.00	5.00	3.00	1.00	5.00	3.00
Employees	1%	3.00	3.00	1.00	5.00	1.00	5.00	3.00
Developers	7%	1.00	5.00	5.00	3.00	3.00	3.00	5.00
Sales	7%	5.00	3.00	3.00	3.00	1.00	5.00	5.00
R&D investment	7%	1.00	5.00	5.00	5.00	5.00	3.00	3.00
Data orchestration, workflows, and user management	7%	1.00	3.00	5.00	1.00	1.00	1.00	5.00
Identity verification and registration	7%	1.00	3.00	5.00	3.00	0.00	1.00	3.00
Decentralized/self-sovereign identity	7%	1.00	1.00	3.00	5.00	1.00	5.00	1.00
Privacy, consent management, and profiling	7%	3.00	3.00	5.00	5.00	0.00	1.00	3.00
Authentication plans	7%	3.00	3.00	5.00	3.00	1.00	1.00	5.00
Identity analytics and threat feeds	7%	1.00	3.00	5.00	5.00	0.00	3.00	5.00
Business systems integration	7%	3.00	3.00	1.00	5.00	3.00	3.00	5.00
Support engineers	7%	1.00	3.00	5.00	5.00	1.00	5.00	5.00
Professional services	7%	1.00	1.00	5.00	5.00	1.00	5.00	3.00
Partner ecosystem	1%	3.00	3.00	5.00	5.00	5.00	5.00	3.00
Commercial model	7%	1.00	3.00	3.00	5.00	5.00	3.00	1.00
Market presence	0%	3.00	3.50	4.50	3.00	3.50	3.50	5.00
CIAM subscription revenue	50%	3.00	3.00	4.00	5.00	2.00	3.00	5.00
CIAM revenue growth	50%	3.00	4.00	5.00	1.00	5.00	4.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Customer Identity And Access Management Scorecard, Q4 2020 (Cont.)

	Forrester's weighting	OpenText	Optimal IdM	Ping Identity	Salesforce	SAP	WSO2
Current offering	50%	1.21	1.51	2.68	3.56	3.84	3.49
Data orchestration and user management	8%	1.00	3.00	1.00	3.00	3.00	5.00
Customer identity verification and registration	8%	1.00	1.00	1.00	3.00	3.00	1.00
Privacy, consent management, and profiling	7%	1.00	0.00	1.00	5.00	5.00	5.00
Customer authentication	7%	1.00	3.00	5.00	1.00	3.00	5.00
Customer self-service	7%	1.00	5.00	3.00	3.00	5.00	5.00
Business systems integration	7%	0.00	1.00	1.00	5.00	3.00	5.00
IDV and fraud management systems integration	7%	0.00	0.00	5.00	5.00	3.00	1.00
Reporting and dashboarding	7%	1.00	1.00	1.00	5.00	3.00	5.00
Active human users	7%	1.00	1.00	5.00	3.00	5.00	0.00
Number of brands	7%	5.00	0.00	5.00	3.00	5.00	5.00
Authentication attempts per hour	7%	1.00	1.00	5.00	3.00	5.00	3.00
Compliance	7%	1.00	1.00	1.00	5.00	3.00	1.00
Navigation and integrated environment	7%	3.00	3.00	1.00	3.00	5.00	3.00
Static and contextual documentation	7%	0.00	1.00	3.00	3.00	3.00	5.00

All scores are based on a scale of 0 (weak) to 5 (strong).

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

FIGURE 2 Forrester Wave™: Customer Identity And Access Management Scorecard, Q4 2020 (Cont.)

	Forrester's weighting	OpenText	Optimal IdM	Ping Identity	Salesforce	SAP	WSO2
Strategy	50%	2.99	2.26	4.00	2.72	3.44	2.96
Execution roadmap	7%	5.00	5.00	5.00	5.00	3.00	3.00
Employees	1%	5.00	1.00	3.00	5.00	5.00	1.00
Developers	7%	3.00	1.00	5.00	1.00	5.00	1.00
Sales	7%	3.00	1.00	5.00	1.00	5.00	1.00
R&D investment	7%	1.00	5.00	3.00	1.00	1.00	3.00
Data orchestration, workflows, and user management	7%	3.00	5.00	5.00	3.00	5.00	5.00
Identity verification and registration	7%	1.00	3.00	5.00	1.00	3.00	3.00
Decentralized/self-sovereign identity	7%	3.00	1.00	5.00	3.00	5.00	3.00
Privacy, consent management, and profiling	7%	5.00	3.00	1.00	3.00	5.00	3.00
Authentication plans	7%	1.00	1.00	3.00	3.00	3.00	5.00
Identity analytics and threat feeds	7%	5.00	1.00	5.00	3.00	3.00	1.00
Business systems integration	7%	1.00	1.00	3.00	3.00	5.00	3.00
Support engineers	7%	5.00	1.00	3.00	3.00	1.00	3.00
Professional services	7%	5.00	1.00	5.00	3.00	3.00	3.00
Partner ecosystem	1%	0.00	1.00	5.00	1.00	3.00	1.00
Commercial model	7%	1.00	3.00	3.00	5.00	1.00	5.00
Market presence	0%	1.00	1.50	3.50	2.00	4.00	1.00
CIAM subscription revenue	50%	1.00	1.00	4.00	2.00	5.00	1.00
CIAM revenue growth	50%	1.00	2.00	3.00	2.00	3.00	1.00

All scores are based on a scale of 0 (weak) to 5 (strong).

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

Vendor Offerings

Forrester included 13 vendors in this assessment: Akamai, Auth0, ForgeRock, IBM, LoginRadius, Microsoft, Okta, OpenText, Optimal IdM, Ping Identity, Salesforce, SAP, and WSO2.

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

Leaders

- **ForgeRock leverages new funding to refocus on CIAM.** Traditionally an on-premises IAM software platform, ForgeRock has largely ditched the open source, support-related business model and now generates revenue from subscription-based, commercial IAM offerings such as its cloud CIAM platform. Forrester estimates that the company generates two-thirds of its annual revenue from its CIAM solution. ForgeRock plans to enhance user personalization using self-service workflow trees, simplify authentication by extending FIDO2 WebAuthn to username-less login, and introduce behavioral analytics for authentication and authorization.

  The solution has a powerful workflow and policy abstraction called Trees that allows admins to create modular, customized, no-code or low-code workflows for all CIAM use cases, including registration, authentication, and self-service. Mapping data from existing user stores to the solution is easy. It supports early-stage, passwordless registrations out of the box; single sign-on (SSO) and validation flows are very broad and flexible. However, the solution's consent management and versioning are more complex to configure than those of other vendors. The solution includes selectable third-party multifactor authentication (MFA) integrations; customers report that writing ad hoc custom reports requires SQL query authoring.[2] It does not support access control lists for defining who can view which report. The solution is a great fit for firms that have many customer-facing applications with complex authentication and workflow requirements and those with established IAM or CIAM skills.

- **IBM has a renewed commitment to CIAM.** IBM's thought leadership in IAM has ebbed and flowed in recent years, but the firm has revamped its CIAM portfolio and created a cloud-based CIAM offering called IBM Security Verify. IBM successfully integrated its Trusteer risk-based authentication and web fraud management solution with its CIAM portfolio to create Security Verify. The vendor plans to implement continuous risk assessment for native mobile and web applications, implement a progressive trust workflow management process, and support developer and privacy experiences on the platform.

  The solution supports a broad range of authentication protocols, FIDO2, and biometrics and integrates with business intelligence solution Tableau. Integration with Trusteer and third-party identity verification and fraud management solutions is ahead of the competition, as are reporting

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

and dashboarding. However, customers report challenges with data integration workflows and role-based access control for administrators; invitations for registration also lag. Consent management and progressive profiling are rudimentary.[3] Out-of-the-box customer self-service (forgotten user ID recovery, user deregistration, and profile updates) and master data management (MDM) registration also lag behind. The solution is a great fit for firms that need to combine risk-based authentication with CIAM or revamp an existing IAM or web fraud management portfolio from IBM.

› **SAP elevates Gigya's security features to a complete CIAM solution.** After acquiring Gigya in September 2017, SAP debated whether to treat Gigya's technology as security or customer management. SAP decided to put it in customer data management; as a result, SAP is consistently adding security features — SSO improvements, push authentication, and risk-based authentication — to the solution's traditional user management capabilities. SAP plans to release server-side CIAM to enhance account takeover prevention, implement FIDO2 WebAuthn support, and introduce native screen sets that offer prebuilt workflows and app integration faster.

The solution offers outstanding consent management, expansive customer self-service, and a very well thought through CIAM administration interface. Leading marketing tools such as Adobe Campaign and Constant Contact and e-commerce portals such as Magento and SAP Commerce are preintegrated. However, it lacks FIDO2 WebAuthn support; there are no real risk scores for authentication; and customers complain about the lack of productized support for enterprise fraud management, MDM, or A/B alternative testing solutions. The solution is not available on-premises — only as a cloud-based identity-as-a-service (IDaaS) solution. It is a great fit for firms requiring extensive and complex consent management for users with differences in requirements across multiple geographies.

Strong Performers

› **WSO2 assembles open source and proprietary pieces into a versatile CIAM platform.** WSO2's CIAM solution comes from its identity management and governance platform. It has always focused on API- and standards-based IAM and comes with a comprehensive reference architecture. More than half of WSO2's employees work on product development. The vendor plans to launch a developer focused software-as-a-service (SaaS) CIAM cloud, introduce a hybrid cloud offering for customers that can't move their customer information to the cloud, and use machine learning (ML) and behavioral analytics to enable the CIAM solution to aid customers' A/B testing efforts.

The solution supports FIDO2 and offers full REST API support for integration that customers said was fairly easy to use. User administration, consent management, authentication, self-service, and business system integration are strong. Role-based access control for admins, passwordless authentication, forgotten user ID recovery, and notification management and dashboarding are also strong. However, the solution has no real SaaS/IDaaS offering, and managing multiple brands or online properties is cumbersome. It lacks built-in behavioral biometrics and device posture

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

management detection or integration; text-based, tabular reporting output requires a separate application. The vendor's compliance certifications are narrower than others. The solution is a great fit for firms looking for a cost-effective solution that they will operate themselves or have a managed security service provider operate.

› **Ping Identity doubles down on CIAM with PingOne for Customers.** Ping Identity's PingOne for Customers, an IDaaS offering dedicated to CIAM, offers MFA that developers can easily integrate into applications, profile management, and REST API-based CIAM policy management. Forrester expects that CIAM will ultimately comprise nearly half of Ping Identity's total revenue. The vendor plans to add integrated threat feeds to access policy definitions, launch Ping Portal to provide unified access to all Ping admin consoles, and create a new IDaaS service for privacy and consent management.

Customers love the solution's broad set of supported authentication standards, easy-to-use biometrics integration and recovery, productized integration with identity verification services, good progressive profiling, and extensive user management of enrolled devices. However, PingOne for Customers lacks FIDO2 support, and there is no role-based access control (RBAC) to view reports and A/B testing support out of the box. Much of the functionality we evaluated in this Forrester Wave — including the integration of MFA, fraud management systems, and risk-based authentication solutions — require firms using PingOne for Customers to install and configure Ping Federate and Ping Access as separate, likely on-premises components.[4] The solution is a good fit for firms with complex customer access management requirements and many on-premises applications that they must integrate into the SSO regime.

› **Okta focuses on scalability and performance management.** In 2019, Okta launched DynamicScale to respond to industry trends, consumer expectations, and customer CIAM performance issues and make performance more predictable. It provides a refactored, high-availability unit/cell-based IDaaS that can handle sustained high traffic loads. While customers will pay more for higher loads than before DynamicScale's introduction, the service ensures high availability of Okta's CIAM offering. The vendor plans to launch platform services to modularize its offering, enhance its Okta Identity Engine to accept third-party threat information, and launch a universal metadirectory to connect user repositories.

The solution offers good customer identity verification options, supports a broad set of authentication standards, and has an extensive list of regulatory compliance certifications globally. Okta's own integrated Threat Insight service provides context about users and their sessions to drive access policies. Productized support for third-party authenticators for MFA is also nice. However, the solution's consent management and dashboarding lag the competition. The solution lacks behavioral biometrics, a UI builder for profile management, and device posture management. Productized, out-of-the-box integrations with web analytics, marketing, and consent management solutions also lag behind. The solution is a good fit for firms looking for pure SaaS CIAM with minimal on-premises components.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

› **Auth0 enhances CIAM with threat and anomaly detection.** Auth0 launched its anomaly detection engine to provide its own threat intelligence tools and data sources such as IP address, domain, and password reputation. It also recently launched social registration, passwordless authentication, and a user migration feature that handles user password hashes elegantly. Auth0 has 660 employees globally, with a high focus on sales execution. The vendor plans to invest in CIAM platform capabilities, automate attack prevention using its anomaly detection engine, and enhance user context awareness and extensibility by onboarding partners into its integration marketplace.

The solution provides great user migration services and registration invite management. Account linking, credential-stuffing prevention, and lost MFA token replacement are ahead of the competition. Customers said that integrations with CRM and MDM solutions and web analytics platforms are particularly strong. However, the solution lacks FIDO2 support; mapping attributes from LDAP user data sources is cumbersome and requires more scripting than competitors. Explicitly adding system administrators is more complicated than with other vendors, and the solution offers minimal support for email-only, lightweight customer registrations.[5] Consent management and behavioral biometrics are also behind competitors. The solution is a good fit for companies transitioning from in-house-developed, app-specific, siloed authentication to centralized, orchestrated CIAM services.

› **Salesforce fortifies its CIAM with its customer data management platforms.** Building on the more than 150,000 customer organizations using its nonsecurity business solutions, Salesforce has been cross-selling its organically developed CIAM solution to its installed base.[6] The vendor plans to integrate Data Manager with its CIAM portfolio for a 360-degree view of the customer, release a suite of user privacy tools, and integrate its data management platform (via its 2017 acquisition of Krux) and customer data platform with its CIAM solution to help customers track and promote unregistered customer conversion.

Unsurprisingly, the solution has strong integrations with CRM, MDM, marketing, and analytics solutions — mainly Salesforce's own solutions. Reporting and dashboarding are visually pleasing and very versatile; CIAM admins can use report folders to customize who has access to which reports. Salesforce CIAM supports early-stage, email-only customer accounts; configuring the sending of classic registration invitations to customers is very flexible and easy to use. However, the solution lacks support for FIDO2 and WebAuthn. Progressive profiling is not quite productized; for many clients, it's very complex and difficult to set up. Configuring the registration of one-time password tokens is more elaborate than the competition, and there is no canned support for biometric integrations or A/B testing.[7] The solution is a great fit for firms planning to expand their Salesforce CRM or marketing tool investments to a full-fledged CIAM system.

Contenders

› **LoginRadius offers a technically strong and versatile CIAM solution.** It's no wonder that LoginRadius focuses heavily on CIAM: 73 of its 170 employees develop its CIAM solution. Considering its relatively small size, the vendor has an extensive network of implementation

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

partners with a proven track record of deals. The solution is available both as on-premises installed software and a cloud-based service, although LoginRadius did not disclose pricing for the cloud service. The vendor plans to implement real-time dark web monitoring, add continuous customer authentication to perform behavioral biometrics on users' actions to identify potentially fraudulent or harmful activity, and implement AI and ML for account protection and data enrichment.

The solution provides the broadest technical capabilities of those we reviewed in this Wave evaluation: User migration services are good, and the versatile, purpose-built consent management system comes with consent versioning. Support for email registrations and multiple brands and properties is extensive. The breadth of compliance certifications is impressive. However, RABC for CIAM admins lags behind, and setting up simple SSO requires much more scripting than the competition. Third-party, out-of-the-box MFA token support lags behind, and the solution lacks FIDO2 support. Customers said that the vendor's strategic plans lag other vendors in identity verification, privacy and consent management, and identity analytics and threat feeds. The solution is a good fit for firms with considerable marketing and developer skills but lacking CIAM skills.

› **Microsoft adds Identity Experience Framework to its CIAM solution for orchestration.** Thanks to strategic product management hiring, Microsoft is doubling down on CIAM by supporting open standards — such as OpenID Connect providers, Google ID support, and identity provider access token passthrough — and introducing the Identity Experience Framework (IEF), which allows for orchestration. Along with other vendors, Microsoft is also experimenting with active-user-based pricing models. It plans to integrate CIAM capabilities into Azure Active Directory; invest in user and entity behavioral analytics (UEBA) to support risk-based access management; and enhance the admin experience and provide automation to assemble, test, and report on workflows.

The solution has the most extensive set of compliance certifications and can serve millions of authentication requests per hour. User regions maintain data residency and compliance with diverse privacy regulations. The solution has remarkable out-of-the-box integration with Microsoft Dynamics using SAML/OIDC. Report access control and dashboard configuration are very usable. However, the solution is cloud-only; there is no on-premises version. It lacks support for FIDO2/WebAuthn support and a large array of functions such as email-only registrations, and requires that admins use and code in the relatively complex IEF or REST Graph API. There is no visual workflow designer. External user directory attribute mapping and consent management require customization using IEF programming. Customers report that changing user registration flows to support dynamic A/B testing is hard. The solution is a good fit for large multinationals with regionally varying data privacy requirements.

› **Akamai offers hosted login and an updated registration builder.** The acquisition of Janrain in 2019 catapulted Akamai, which had limited IAM experience, into the CIAM space. Akamai has continued to add features to the CIAM solution, including webhooks, hosted login, and updated the registration builder. It plans to implement adaptive authentication with risk signals, implement edge authentication using its content delivery network infrastructure to block hackers as early as possible, and expand the ecosystem of data integrations to business intelligence platforms.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

The solution has good reporting and dashboarding capabilities and manages large numbers of identities and brands. It offers identity verification flows for registrants and flexible consent revocation services. A built-in authorization server can manage business entitlements in portals. Scoping for CIAM admins and report access management are granular. However, the solution lacks FIDO2/WebAuthn support. Adding LDAP user stores requires professional services; user migration requires complex middleware and integration. In our assessment, the solution and most of its integrations with business systems such as MDM, web analytics, and enterprise marketing focus on privacy by design and are not productized or exposed to the same degree as the competition. Our impression from customer conversations was that Akamai spent time trying to recover its CIAM development momentum after the Janrain acquisition, leading to delays in keeping up with the competition. The solution is a good fit for global security-minded firms looking to protect critical properties using serverless computing, distributed denial of service attack protections, and bot management front-ended CIAM.

- **OpenText builds on Covisint's CIAM assets.** OpenText expanded its CIAM portfolio to allow interoperability across its nonsecurity product portfolio. During the 12-month period ending on the cutoff date, the vendor has also implemented system for cross-domain identity management (SCIM) and U2F and made various improvements to CIAM workflow and user migration. The vendor plans to create a low-code development environment to empower developers to automate the build-out of CIAM environments, integrate the OpenText privacy center with its CIAM solution, and introduce a productized interface to OpenText Experience to enable omnichannel CIAM, A/B testing, and call center CIAM optimization.

  OpenText's CIAM solution capitalizes on its expertise in identity federation and trust in B2B2C IAM and has a good set of IAM functionality for the internet of things (IoT). The solution has useful risk-based authentication and comprehensive features for replacing lost MFA tokens. Multitenancy administration — the scoped administration of hierarchies of tenants — is very good and broadly adopted by customers. Controlling access to reports is functional and flexible. However, the vendor has no CIAM implementation partners, greatly limiting its ability to increase its solution's customer reach.[8] Productized support for multiple brands or properties, privacy and consent management, progressive profiling, early-stage (unauthenticated) customer accounts, and consent revocation are not exposed to CIAM admins to the same degree as the competition.[9] The solution may be a good fit for firms looking for scalable IoT IAM device management as a building block of their CIAM strategy.

- **Optimal IdM has a fully cloud-hosted CIAM solution.** The vendor improved its federation and LDAP integration capabilities and added multitenancy support to OptimalCloud. The solution also offers APIs for easy integration. Optimal IdM spends a lot on innovation; Forrester estimates that it spends half of its CIAM revenues on CIAM research and development. It plans to expand the CIAM solution's API set for easier integration at end user customers and partners, implement true UEBA to analyze data that the vendor's OptimalCloud solution stores in Splunk, and improve its SCIM provisioning engine.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

The solution's attribute mapping is good, and it has SCIM and CSV-based admin user provisioning capabilities. It has decent support for multiple hierarchies of tenants. Typing pattern analysis provides added protection against account takeovers, and the solution explicitly supports user self-deregistration and user profile update self-service. However, it lags other solutions in productized consent management and integrations with business systems like CRM and MDM. IDV and fraud management solution integration also lag behind. Customers and Forrester found that reporting and dashboarding are largely missing. Further, the vendor has no ecosystem of systems integrator partners. The solution is a good fit for organizations wanting to use one integrated solution for both workforce and customer identity and access management.

Evaluation Overview

We evaluated vendors against 32 criteria, which we grouped into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include data orchestration and user management, customer identity verification and registration, privacy, consent management and profiling, customer authentication, customer self-service, business systems integration, IDV and fraud management systems integration, reporting and dashboarding, scale, compliance, integrated environment, and static and contextual documentation.
- **Strategy.** Placement on the horizontal axis indicates the strength of each vendor's strategy. We evaluated the execution roadmap, market approach, CIAM R&D investment, CIAM solution enhancement, depth of support professional services, and partner ecosystem.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's annual CIAM subscription revenue and growth.

Vendor Inclusion Criteria

Forrester included 13 vendors in the assessment: Akamai, Auth0, ForgeRock, IBM, LoginRadius, Microsoft, Okta, OpenText, Optimal IdM, Ping Identity, Salesforce, SAP, and WSO2. Each of these vendors has:

- **A thought-leading, productized portfolio of products and services.** We included CIAM vendors that demonstrated thought leadership and solution strategy execution by regularly updating and improving their productized product and model portfolio. Customers of vendors had to report that the solution is purpose-built for customer-facing identity and access management.
- **Annual CIAM revenues of at least $4 million with at least 9.5% growth.** We included vendors that have at least $4 million in combined revenues from the CIAM solution and at least 9.5% year-over-year growth in CIAM revenues.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

- **Mindshare with Forrester's end user customers.** The vendors we evaluated are frequently mentioned in Forrester end user client inquiries, vendor selection RFPs, shortlists, consulting projects, and case studies.
- **Mindshare with vendors.** The vendors we evaluated are frequently noted by other vendors during Forrester briefings as viable and formidable competitors.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.



Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Supplemental Material

Online Resource

We publish all of our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

The Forrester Wave Methodology

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by July 10, 2020 and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] Transactional pricing is also known as pay-as-you-go pricing. Pricing based on the number of active users means that a customer pays only for those users that log in during a given month. Pricing based on the total number of inactive and active users means that a customer pays a flat per-user annual fee.

[2] However, the vendor provides integration guides for Daon, Entrust, and others.

[3] The vendor plans to improve consent management in the second half of 2020.

[4] The situation was quite similar in our last workforce IAM IDaaS Wave. See the Forrester report "The Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise, Q2 2019."

[5] New admins need to be explicitly invited and cannot be designated based on Active Directory group memberships. Email-only, lightweight customer registrations are planned.

[6] Source: Salesforce (https://www.salesforce.com/campaign/worlds-number-one-CRM/).

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

[7] Login flows provide many ways to do progressive profiling, from drag and drop to a full programmatic experience. Biometric integration is built into the mobile SDK.

[8] Additionally, the vendor's CIAM product modernization and citizen developer efforts will enable it to leverage its broad network of business partners to deliver solutions.

[9] The vendor has its own global services organization for CIAM project implementation.

© 2020 Forrester Research, Inc. Unauthorized copying or distributing is a violation of copyright law.
Citations@forrester.com or +1 866-367-7378

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.