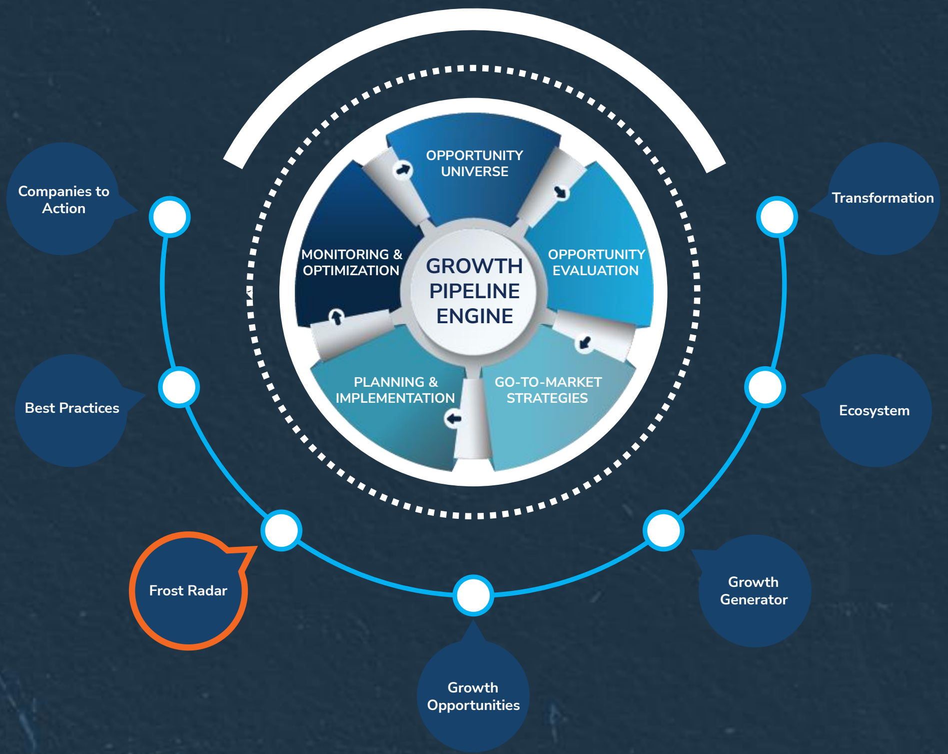
FROST & SULLIVAN

Frost Radar™: Consumer Identity and Access Management, 2024

A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines



PF9B-74
December 2024

Strategic Imperative and Growth Environment

Strategic Imperative

- The “C” in CIAM may refer to consumers, customers (partners, business-to-business [B2B], and/or business-to-consumer [B2C]), and/or citizens in the broader identity and access management (IAM) market. For this Frost Radar, Frost & Sullivan has focused on IAM vendors that provide solutions for consumers.
- The definition of CIAM, as with everything else in security, is expanding. Deep integration requirements, enterprise demands to consolidate vendors, and the changing threat landscape are helping to define the market.
- This analysis categorizes a CIAM provider as one that must offer access management and authentication, Vendors offer identity verification (IDV) as part of CIAM and enable integration with fraud detection and prevention (FDP) solutions to improve performance. This study recognizes IDV as a value-added component of CIAM.
- Workforce IAM is no longer sufficient for an organization that aims to build a robust identity security stack. The exponential rise in digital consumers has made CIAM pertinent. The increase in identity-based attacks has rendered consumers vulnerable, and governments and regulatory bodies are making adequate security an organization’s responsibility.
- The increase in digital consumers has amplified the demand for better digital experiences. The deployment of disruptive technologies as part of digital transformation initiatives is paving the way for modern CIAM.
- Artificial intelligence (AI), machine learning (ML), data analytics, biometrics, and blockchain are helping CIAM vendors to enhance outcomes.

Strategic Imperative (continued)

- Digitalization of products and services became essential during the COVID-19 pandemic, but often without adequate attention to security protocols. The resulting vulnerabilities were accentuated by the scale of data, lack of cybersecurity professionals, and changing regulations. To keep up with the dynamic scenarios, vendors are relying on automation and technology to secure consumers.
- Technology facilitates security against simple attack techniques, such as password spraying, and sophisticated attacks, such as man-in-the-middle (MiTM) and deepfakes.
- Technology-enabled security solutions improve accuracy and speed, which cannot be delivered with manual intervention. These technologies will soon become central to CIAM as companies acquire solutions created by experts in the field.
- Lean start-ups with a focus on innovation as well as digital businesses that have the resources to scale up rapidly intensify competition. CIAM vendors with experience must gear up with innovative products, solutions, approaches, and business models. A lack of proactive action will make it difficult to sustain in the evolving CIAM marketplace.
- The complexity of identity security creates silos and blind spots. Enterprises are unwilling to discard homegrown solutions developed over many years, and CIAM vendors must find a way to either integrate or orchestrate these systems.
- Not all vendors offer a system that can work effectively across the entire identity stack. This has led to the emergence of specialists that manage a niche area in the CIAM stack. Larger vendors continue to build on their capabilities with in-house solutions or acquisitions of complementary providers. The complexity and number of CIAM vendors will continue to increase as new approaches emerge and new identities are added.

Strategic Imperative (continued)

- The evolution of the identity stack has led to more collaboration between disparate segments of cybersecurity to improve the efficacy of solutions and reduce vulnerabilities. This has also created new opportunities for existing vendors and lowered entry barriers.
- CIAM ensures better security for external identities that are accessing corporate systems. This is to avoid problems related to stolen identities, synthetic identity, and credential stuffing and help clients protect consumer privacy and data.
- Many vendors are adding or integrating intelligence from capabilities such as identity, fraud detection, and citizen ID security to enhance outcomes.
- CIAM stakeholders include marketing and sales, operations, designers, and product teams. Cloud, CRM and operational software are some of the other industries in which CIAM solutions integrate.

Growth Environment

- The CIAM market is in the early growth stage. Frost & Sullivan expects market revenue to increase at a compound annual growth rate of 17.2% from 2024 to 2029 to reach $13.77 billion in 2029.
- As the number of digital consumers stabilizes after the surge that occurred during the pandemic, enterprises will focus on making infrastructure more secure. This trend is visible globally but will be more pronounced in North America, Europe, and some parts of the Asia-Pacific region because of greater consumer awareness and government and regulatory authorities' focus on compliance. Penalties are high and immediate, and non-compliance would result in loss of trust.
- Africa and Latin America also experience fraud, but low awareness among consumers, lack of security talent, and inadequate government attention enable fraudsters and bad actors to attack repeatedly. These regions' revenue contributions will remain small, but enterprises looking to grow globally will take the lead on CIAM in these locations as part of their implementation of best practices.
- BFSI, healthcare, and government lead in CIAM adoption, primarily because of strict data privacy regulations and the sensitive consumer information that they have access to.
- Large (2,500–9,999 employees) and very large (10,000 or more employees) enterprises typically have developers customize or build their own CIAM solutions. Small (fewer than 1,000 employees) and medium-size (1,000–2,499 employees) enterprises—collectively known as SMEs—commonly rely on out-of-the-box solutions or work with managed service providers, CSPs, and MSSPs to enable CIAM in their identity infrastructure.
- Vendors' journey from products to software licenses to subscriptions to converged solutions reflects their knowledge of the evolving industry. The workflows in solutions for on-premises and cloud-based infrastructures improve adoption.

Growth Environment (continued)

- Several factors contribute to the growth of CIAM market.
    - CIAM solutions are a vital component of enterprise digital transformation initiatives. CIAM solutions are important because they provide a seamless and secure front end to ensure a frictionless consumer journey.
    - Regulatory compliance demands that organizations assume more responsibility for protecting consumers or face monetary penalties and loss of trust. Regulations around the world mandate that organizations protect consumer information and adhere to strict guidelines to ensure data privacy Organizations must ensure compliance as more countries regulate the collection, use, and storing of consumer data in the next few years.
    - More CIAM solutions are equipped with advanced technologies. AI and ML enhance outcomes, enable personalized experiences, automate processes, enhance data management, and deploy next-gen authentication capabilities.
    - CIAM solution providers leverage their expertise and deep understanding of identity security and customer experience to enhance stakeholder outcomes across security, marketing, and sales. Vendors' leadership teams typically come with deep experience in the industry and understand trends and bad actors' modus operandi.
- CIAM solutions cater to multiple departments beyond IT and security, including compliance, marketing, operations, CRM, and strategy, accelerating adoption because stakeholders can use the dashboard in the ways that are most relevant to them.

Growth Environment (continued)

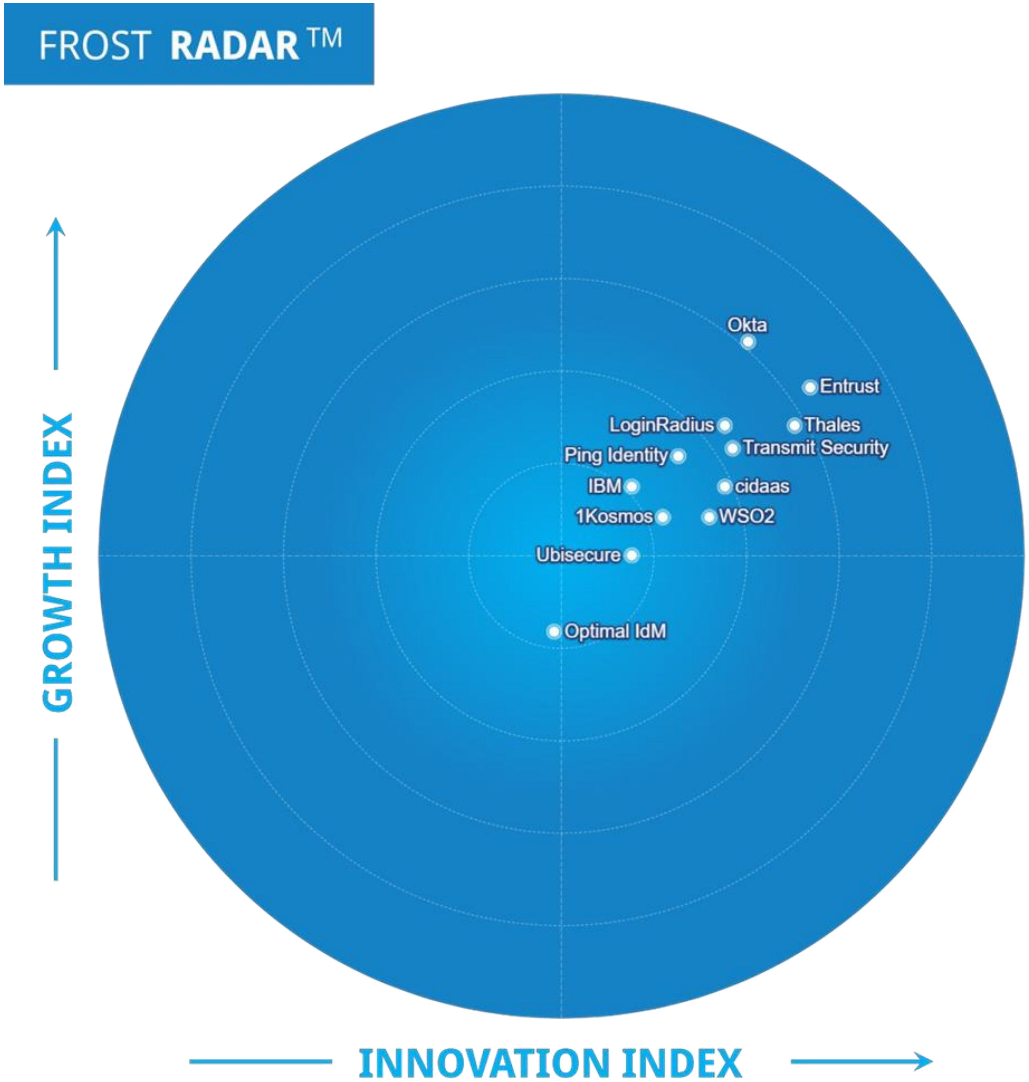
- Other trends that will affect CIAM in the next few years:
  - Privacy and consent management will enhance customer engagement and build trust.
  - In addition to other passwordless authentication methods, adoption of passkeys will increase.
  - A unified approach to CIAM, IDV, and fraud prevention will enhance security.
  - GenAI will enhance CIAM solution outcomes.
  - Companies are moving beyond homegrown CIAM to a more holistic CIAM.
- A Frost & Sullivan study related to this independent analysis:
  - Consumer Identity and Access Management, Global, 2024–2029

FROST & SULLIVAN

Frost Radar

Consumer Identity and Access Management, 2024

Frost Radar: Consumer Identity and Access Management, 2024



 Source: Frost & Sullivan

Frost Radar Competitive Environment

- Most vendors are observing more enterprise interest in CIAM solutions. While it may take some time before they can move away from homegrown solutions, the convenience of having the same vendor cater to different IAM users (e.g., workforces and external identities) is an attractive proposition.
- More than 125 vendors offer some component of CIAM. Competitive factors include cost; ease of implementation, integration, and use; advanced technologies; expertise; benefits across roles (IT, security, marketing, and compliance); scalability; support; customer relationships; partnership and innovation strategies; and user interface and experience. The first edition of the CIAM Frost Radar features 12 competitors.
- Many technology companies have launched security portfolios, and IAM is usually an important component. IBM, which offers CIAM capabilities along with other components of IAM, has a strong foundation with many large customers and resources that it can use for innovation.
- cidaas, Ubisecure, and WSO2 have roots in Europe but are looking to capture the global market with their growth and innovation plans.
- 1Kosmos, Entrust, and Transmit Security have established themselves as serious contenders in the last few years with a focus on identity-centric security and innovation. Their growth reflects the success of their strategies.
- LoginRadius is one of the few vendors focusing solely on CIAM. It also stands out for an API-first strategy to ensure that it fits well into the security stacks of larger enterprises.

Frost Radar Competitive Environment (continued)

- Okta, Thales, and Ping Identity are behemoths in the security industry that have completely changed the perception of identity security as they focus on strengthening this domain with new technologies, products, and services. Each has augmented capabilities over the last few years by acquiring innovative and growing competitors.
- Optimal IdM is one of the smallest providers on the Frost Radar and has a unique approach of maintaining a small core team. It offers other components of IAM as well, with some very large companies as clients.
- Vendors that recently entered the market, are already strong competitors, and are likely to be featured in future CIAM Frost Radars include Curity, Microsoft Entra External ID, Stytch, Descope, and Strivacity. Some vendors were not included in this analysis because of the lack of adequate information based on secondary research and their inability to provide information within Frost & Sullivan's stipulated time frame.

F R O S T & S U L L I V A N

Frost Radar

Companies to Action

Entrust

INNOVATION

- Entrust IDaaS, Entrust Identity Enterprise (Consumer), and Onfido's IDV solutions enable an end-to-end, secure consumer journey from onboarding and risk-based authentication to AI-driven biometric and document verification.
- Utilizing risk signals from other providers in addition to its own for continuous authentication, Entrust offers a range of authentication mechanisms including soft tokens, mutual authentication, push notifications, FIDO2/passkeys, and physical or digital cards.
- Entrust acquired Onfido in April 2024. At the time of the acquisition, Onfido had more than $140 million in revenue, more than 500 employees, and 1,200 customers globally. Terms of the deal were not disclosed.
- Onfido was one of the leading IDV providers. Its capabilities, such as FIDO2 authentication, will augment Entrust's portfolio and provide impetus to its growth and product strategy. Onfido's low-code, no-code orchestration engine and biometric authentication will enhance Entrust's IDV and know-your-customer (KYC) capabilities.
- Onfido Atlas™ is the AI technology layer that powers the IDV solutions, bringing more than 10,000 micro-models together to detect fraud, underpinned by liveness technology and anti-bias capabilities. Entrust's Onfido Fraud Lab is exploring the deeper integration of sophisticated spoof detection, accounting for emerging technologies such as deepfakes, into its CIAM solution.
- Its technology roadmap indicates the use of AI to improve reporting analytics and dashboards, such as authentication audit logs to highlight anomalous behaviors. It is also conducting verifiable credentials pilots.

Entrust (continued)

GROWTH

- With 54 years of experience, 3,500 employees, and a presence in 150 counties, Entrust has evolved into one of the leading providers of identity-centric security.
- Entrust's acquisition of Onfido was preceded by others, such as Evidos (2022) for digital signing and WorldReach (2021) for identity verification and KYC.
- The integration of Entrust IDaaS and Onfido's AI-driven biometrics IDV solution has enabled a unified approach to CIAM.
- Entrust also gained Onfido's revenue, employees, and customers, which are generating significant growth in Entrust's CIAM business, especially in Europe.
- Its growth will be fueled by a partnership program that includes other vendors in the ecosystem, MSSPs, and cloud marketplaces.
- With a large portfolio of adjacent capabilities, such as workforce IAM, machine identity, and certificate lifecycle management, and new features and capabilities launched since 2023, the company has many opportunities to cross-sell and upsell.

Entrust (continued)

FROST PERSPECTIVE

- Entrust’s acquisition of Onfido has enabled access to sophisticated technology being deployed for identity verification, which provides it with a significant edge over competitors. The use of AI and ML to enhance its capabilities as part of its roadmap will contribute to its growth.
- Entrust must focus on smooth integration and transition for clients, since the high-profile deal has raised expectations. The acquisition contributed to Entrust’s position as the Innovation Index leader, because Onfido has been recognized as one of leading innovators in the industry.
- Entrust’s global presence and CIAM portfolio will contribute to significant growth through cross-selling and upselling opportunities.
- Government and financial services clients are extremely discerning given the critical nature of their work. Entrust can leverage the experience from its deep penetration in these verticals in Europe and North America and utilize case studies of successful implementation to build confidence and new opportunities among potential buyers in other regions and verticals.

FROST & SULLIVAN

Best Practices & Growth Opportunities

Best Practices

1

A unified approach to CIAM, identity verification, and fraud prevention can enhance security It is necessary for a holistic security view, improving the efficiency and efficacy of solutions. This approach eliminates security gaps, streamlines operations, and improves compliance.

2

CIAM has outgrown homegrown solutions that started with providing a secure digital login experience. It has transformed into a promise of providing consumers with a holistic and consistent life cycle. This promotes revenue, brand loyalty, compliance, and security.

3

Many vendors are experimenting with embedding generative AI into their CIAM tools. The technology presents a significant opportunity for developers to create customized consumer IAM workflows, enhance CIAM outcomes, or automate certain repetitive tasks. Generative AI will enable admins to use insights proactively to enhance CIAM capabilities.

Growth Opportunities

1

The complexity in identity security is one of the biggest challenges to its adoption and growth. Third-party identity security APIs enable organizations to launch applications rapidly because developers can focus on nuances unique to their organization rather than building the entire software on their own.

2

The layered structure of identity security offers an opportunity to make CIAM more effective by adding components to the solutions. Identity verification is still considered a separate component of identity security. Its relevance to CIAM, especially in high-security use cases, cannot be overstated.

3

Passkeys enable a higher level of security than traditional passwords because they are resistant to phishing attacks. Passkeys simplify and accelerate the login process for users, eliminating the need to remember complex passwords and improving CX.

Frost Radar Analytics

Frost Radar: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a ROBUST growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar.

GI3

GROWTH PIPELINE
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive Mega Trends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGA TRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of Mega Trends can be found here.

II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com