KuppingerCole Report

EXECUTIVE VIEW

By John Tolbert
May 21, 2021

Strivacity Fusion

Strivacity Fusion is a multi-instance SaaS-based Consumer Identity and Access Management (CIAM) solution. Strivacity Fusion was built in the cloud using the modern micro-services architecture for maximum flexibility and scalability. Strivacity Fusion offers customers MFA and consent management options to help meet differing global requirements.

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

Content

1 Introduction

Consumer Identity and Access Management (CIAM) is an established specialty within Identity and Access Management (IAM) that has emerged in the last few years to meet evolving business requirements specific to consumer use cases. Many businesses and public-sector organizations are finding that they must provide better digital experiences for and gather more information about the consumers who are using their services. Enterprises want to collect, store, and analyze data on consumers to create additional sales opportunities and increase brand loyalty.

Consumer IAM systems are designed to provision, authenticate, authorize, collect, and store information about consumers from across many domains. CIAM solutions also work for many government-to-citizen use cases. Unlike workforce IAM systems though, information about these consumers often arrives from many unauthoritative sources. Information collected about consumers can be used for many different purposes, such as authorization to resources, or for analysis to support marketing campaigns, or Anti-Money Laundering (AML) initiatives. Moreover, CIAM systems must be able to manage many millions of identities, and process potentially billions of logins and other transactions per day. SaaS delivery of CIAM services is trending upwards and will likely remain the default choice for most organizations.

CIAM systems can aid in other types of regulatory compliance. Since GDPR took effect in the EU in May of 2018, collecting clear and unambiguous consent from consumers for the use of their data has become mandatory. Many CIAM solutions provide this capability, plus offer consumers dashboards to manage their information sharing choices. Moreover, CIAM systems can help corporate customers implement consistent privacy policies and provide the means to notify users when terms change and then collect acknowledgement.

The top features CIAM services provide are

- Authentication options: Email/phone/SMS OTP, mobile biometrics, behavioral biometrics, mobile push apps, FIDO, risk-adaptive and continuous authentication, and social logins (allowing users to login via Facebook, LinkedIn, Twitter, Google, Amazon, etc.). Consumer authentication components should permit risk-adaptive evaluation of runtime environmental parameters, user behavioral analytics, and fraud/threat/compromised credential intelligence to match the appropriate authentication mechanism to the level of business risk or as required by regulations.
- Privacy and consent management: Explicit user consent must be received for the use of their information. Consumer account dashboards are common mechanisms for providing users with consent monitoring, granting, and withdrawal options. Compliance with EU GDPR, Canada’s PIPEDA, and California’s CCPA are notable drivers.

- IoT device identity association: As IoT devices increase in popularity, consumers and business customer users will have greater need to associate their IoT devices with their digital identities. These identity associations between consumer and IoT objects will allow for more secure and private use of smart home, wearables, and connected cars.
- Identity analytics: Dashboards and reports on common identity attribute activities including failed logins, consumer profile changes, credential changes, registration tracking, etc.
- APIs: Allow access by 3rd-party applications to perform marketing analytics, CRM integration, security integration, provisioning/de-provisioning, consent auditing, and more. Many CIAM solutions support REST APIs, Webhooks, Websockets, and WebAuthn methods; JSON and XML formats; and LDAP and SCIM for provisioning.
- Account recovery mechanisms: When consumers forget passwords, lose credentials, or change devices, they need ways to get access to their accounts. Account recovery techniques include Knowledge-Based Authentication (KBA; but it is recommended to avoid this method as it is usually even less secure than password authentication), email/phone/SMS OTP, mobile push notifications, and account linking.
- Account TakeOver (ATO) protection: The inclusion of external and/or 3rd-party fraud and compromised credential intelligence for runtime evaluation of internal or external cyber threat or fraud information, such as known bad IP addresses/domains, compromised credentials, accounts suspected of fraud, fraud patterns, botnet behavior, etc., for the purpose of reducing the risk of fraud at the transaction level, especially ATO fraud.

Many CIAM vendors are taking an “API-first” approach to CIAM. API-driven CIAM architectures may be considered Identity API platforms and are best when instantiated as micro-services. Deploying CIAM functionality using Identity APIs aligns with the notion of Identity Fabrics.

IT departments should welcome CIAM initiatives, as they provide an opportunity for IT, usually considered a cost center to closely team with Marketing, a revenue producing center.

2 Product Description

Strivacity was founded in 2019 as a CIAM specialist endeavor. They are headquartered in Virginia. Strivacity Fusion follows the micro-services and serverless trend in solution architecture, which allows for optimum flexibility. Strivacity hosts in Amazon AWS and offers a multi-instance rather than multi-tenant approach as well as separate identity data stores per customer to achieve maximum data separation for clients.

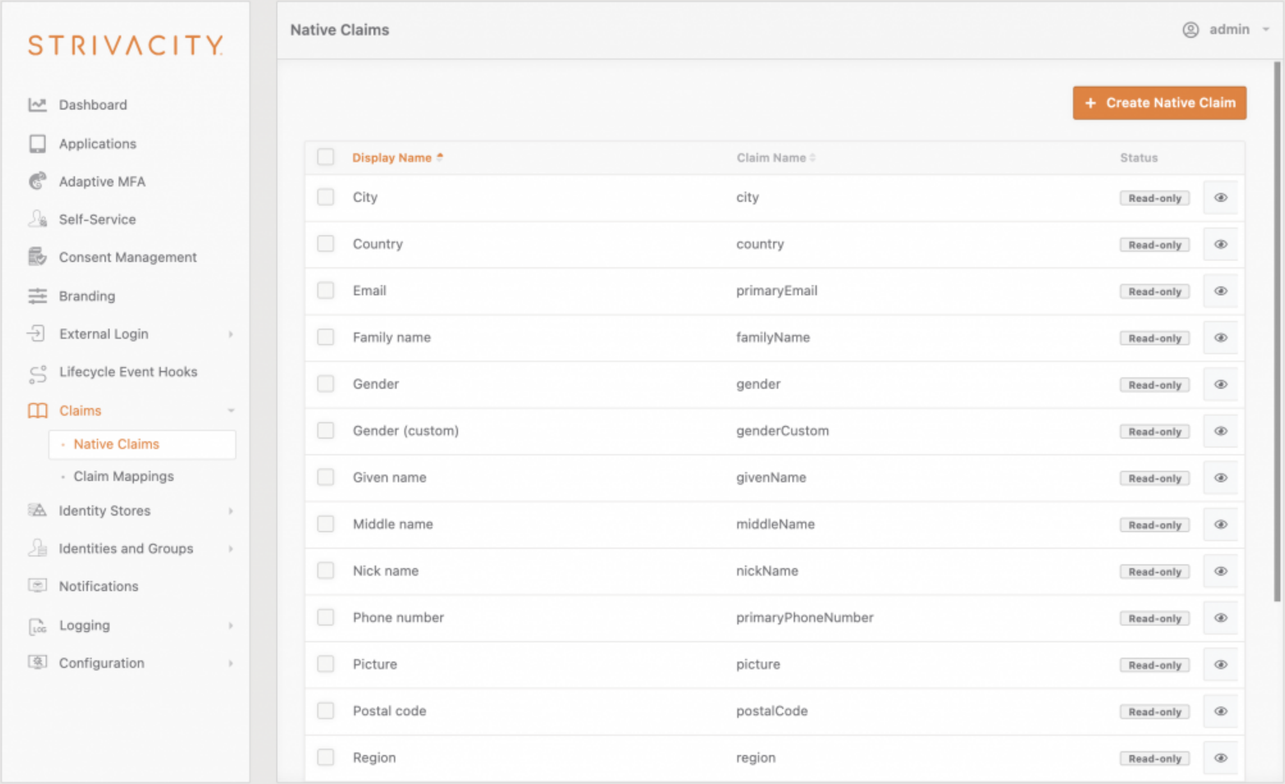
Strivacity Fusion facilitates white-labeling of login and consumer dashboards. Strivacity offers DNS branding options: customerdomain.strivacity.com or redirects to customer properties. Sub-branding scenarios are also available.

Fusion allows consumer self-registration, manual account creation by HR or help desks, and bulk import over APIs. Registration from social networks Facebook, GitHub, Google, Microsoft, and Twitter is supported, and provisioning from other identity providers can be configured. Strivacity partners with ID DataWeb for identity proofing functions, including mobile number matching, remote physical identity document verification, and dynamic Knowledge Based Authentication (KBA). Strivacity adheres to the progressive profiling concept, whereby customers can obtain pertinent information from consumers as needed rather than trying to get complete profile information at registration time.

Strivacity Fusion accepts email/phone/SMS OTP, magic links, and Google authenticator as both authentication methods and account recovery mechanisms. For the OTP options, Strivacity has email and telephony partners, or customers can choose their own. Breached password protection is enabled by default and additional queries against the haveibeenpwned compromised credential intelligence service can be configured. Strivacity imports IP reputation information and gets botnet detection capabilities from a combination of open source and commercial services. Fusion can also determine if user sessions are originating from TOR browsers and deny access if desired by customers. Additional intelligence services can be consumed if configured by customers. The built-in risk engine can also detect the use of new devices and impossible travel by consumers. Geo-fencing is on the near-term roadmap.

Consent management is a paramount concern for many organizations. Privacy regulations such as GDPR, PIPEDA, and CCPA are in effect, and new regulations are on the horizon in many regions around the world. Strivacity adheres to the principle of data minimization. Currently a proprietary method of consent tracking is used, but Strivacity will move to supporting Kantara Initiative’s Consent Receipt specification in the future. Fusion allows consumers to view, edit, download (in HTML or JSON format) and delete personal information. Fusion’s administrative facilities allow customers to gather age verification, to collect consent for marketing notifications, and to accept terms and conditions. Moreover, the Fusion interface allows site administrators to customize the terms and conditions for display and control response types.

Strivacity Fusion enables complete data normalization capabilities between incoming attribute data from identity providers and that which is used for access management policies by customers within the CIAM. The mapping of claims and attributes works bi-directionally for syncing accounts with external identity providers as well, due to support for OASIS and OIDC standard schemas. Fusion contains a built-in node.js IDE that allows customers to code up elements as necessary, such as API calls for attribute checks, runtime intelligence queries, and conditional changes for CSS and HTML. Customer admins can define bespoke attributes within the solution. The ability to customize and extend the platform gives customers more control over the consumer identity lifecycle.



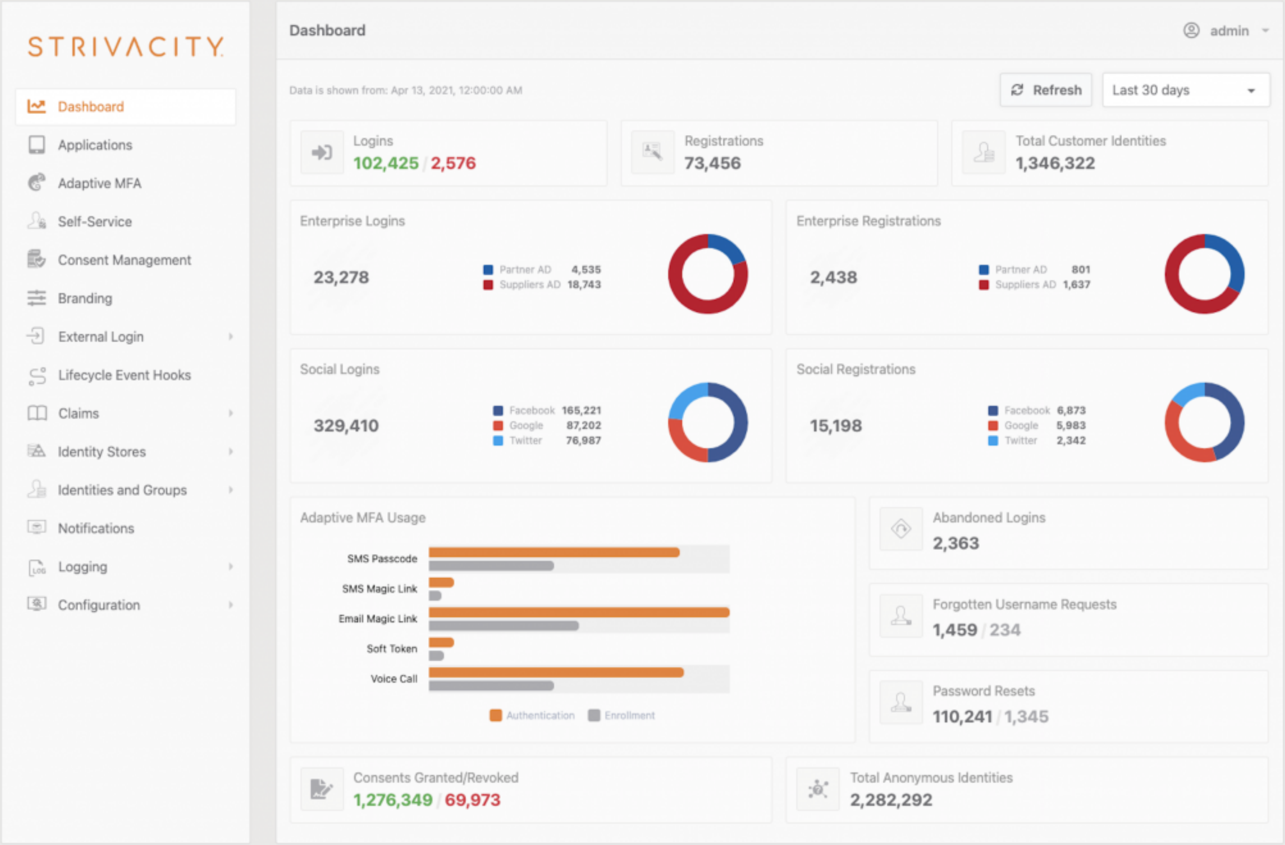
Display Name	Claim Name	Status
City	city	Read-only
Country	country	Read-only
Email	primaryEmail	Read-only
Family name	familyName	Read-only
Gender	gender	Read-only
Gender (custom)	genderCustom	Read-only
Given name	givenName	Read-only
Middle name	middleName	Read-only
Nick name	nickName	Read-only
Phone number	primaryPhoneNumber	Read-only
Picture	picture	Read-only
Postal code	postalCode	Read-only
Region	region	Read-only

Figure 1: Strivacity Fusion Administrative Console Claims Mapping (used with permission)

Fusion supports OAuth, OIDC, and SAML for federation and SSO with other web properties. Setting up SAML connections is relatively easy, as complete configurations can be imported from XML files. All functions available within the customer console are exposed via APIs which are governed by OIDC client credentials grants. APIs were designed and documented in Postman.

Customer administrators can be subject to the MFA requirements in accordance with the supported mechanisms listed above. Additional coarse-grained access controls can be implemented as IP address/range limitations per customer to the cloud-hosted admin console.

A number of pre-defined identity analytics reports are available through the customer portal. Login success/failures, authentication mechanisms used, and registration completions/abandonments are examples. Strivacity Fusion takes an application management approach. The top-level interface allows admins to quickly view, modify, and add applications for access by consumers. Different and/or multiple ID stores, including the aforementioned social network providers, can be leveraged per application instance. Strivacity has connectors for Adobe, Marketo, Salesforce, and ServiceNow, and they can work with customers to create more connectors for marketing analytics and automation systems as needed.



Data is shown from: Apr 13, 2021, 12:00:00 AM

Last 30 days

Logins 102,425 / 2,576

Registrations 73,456

Total Customer Identities 1,346,322

Enterprise Logins 23,278

Partner AD	4,535
Suppliers AD	18,743

Enterprise Registrations 2,438

Partner AD	801
Suppliers AD	1,637

Social Logins 329,410

Facebook	165,221
Google	87,202
Twitter	76,987

Social Registrations 15,198

Facebook	6,873
Google	5,983
Twitter	2,342

Adaptive MFA Usage

Abandoned Logins 2,363

Forgotten Username Requests 1,459 / 234

Password Resets 110,241 / 1,345

Consents Granted/Revoked 1,276,349 / 69,973

Total Anonymous Identities 2,282,292

Figure 2: Strivacity Fusion Dashboard (used with permission)

3 Strengths and Challenges

Strivacity Fusion aims to provide affordable CIAM services delivered via SaaS for organizations in multiple industry types, including those in high regulated markets. The micro-services multi-instance architecture enables scalability for customers with high volumes of consumer logins, consent actions, and profile changes. The use of separate and even multiple identity data stores per client facilitates maximum data separation and privacy, which is useful for privacy and security regulatory compliance.

Fusion is designed for administrative ease-of-use, with most features configurable through the standard interface. However, for customers with more advanced use cases to address, Fusion provides a full node.js IDE that supports custom CSS, HTML, and API integration to 3rd-party sources and applications. Strivacity offers development support for clients who need to extend the base set of capabilities.

Companies in the retail, entertainment, and media streaming sectors have been hit hard by fraud. Fraud reduction technologies are a requirement rather than a nice-to-have, especially for CIAM platforms. Strivacity partners with ID DataWeb to make fraud reduction intelligence, particularly identity proofing, available to their customers.

As a startup in CIAM, Strivacity is rapidly adding features and moving to capture market share. The platform will benefit from additional MFA options and a mobile SDK, which are planned. Support for FIDO2 and WebAuthn are also on the roadmap. More explicit support for CRM and marketing technologies will also be helpful. As consumers increasingly use smart home, wearable, and other types of IoT devices, demand for integrating device identity with consumer identity will grow.

STRIVACITY

Strengths

- Isolation-by-Design: separate SaaS instance and identity store(s) per customer
- Micro-services architecture for scalability
- Consumer data localization
- Consumers can view, edit, download, and delete profile information in accordance with privacy regulations
- No-code/low-code as well as full IDE customization options available
- Identity proofing and fraud reduction integration with ID DataWeb AXN

Challenges

- Early-stage startup looking to gain traction
- Additional MFA methods needed such as mobile biometric integration and mobile SDK
- No support for IoT device identity
- Additional CRM & MarTech integrations would be useful
- SOC 2 Type 2 certification in work

4 Related Research

Leadership Compass - CIAM Platforms
Leadership Compass - Privacy and Consent Management
Buyer\'s Compass - Consumer Identity and Access Management Solutions

Content of Figures

Copyright

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

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

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