KuppingerCole Report

Executive View

WSO2 Asgardeo

WSO2 has been a leader in CIAM innovation for years. WSO2's primary design and deployment models have been to leverage open source for on-premises installations. With Asgardeo, WSO2 launches a complete multi-tenant SaaS solution for CIAM, aimed at developers. Asgardeo features an all-new architecture to speed CI/CD for customers. WSO2 embraces technical standards to promote interoperability, and many out-of-the-box API integrations are available in their marketplace to facilitate integration with customer applications.



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

Content

Introduction 3

Product Description 5

Strengths and Challenges 7

Related Research 8

Copyright 9

Introduction

Consumer Identity and Access Management (CIAM) is an outgrowth from enterprise Identity and Access Management (IAM) that has become a substantial market of its own. CIAM solutions are designed to meet evolving technical requirements for businesses and other organizations that deal directly with consumers and citizens. 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 in order to enhance the ability to match product and/or services with market demand and individual interest 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.

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, facilitate marketing automation, CRM integration, security integration, provisioning/de-provisioning, identity proofing, consent auditing, and more. Measures support for REST APIs, Webhooks, Websockets, WebAuthn; 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.

Product Description

WSO2 was founded in 2005. They are headquartered in the Bay Area and have offices and customers around the world. WSO2 builds products and services on top of an open-source base, licensing by the Apache 2.0 framework and providing support via annual subscriptions. In their broader portfolio, WSO2 has solutions for Open Banking, Open Healthcare, and API Management. WSO2 Identity Server is their IAM and CIAM solution for on-premises deployments. WSO2 Identity Server was an Overall, Product, and Innovation Leader in the previous edition of the KuppingerCole CIAM Leadership Compass. Asgardeo is their CIAM and IDaaS offering. Choreo is their cloud-native engineering platform for API developers, which allows developers to build microservices-based applications in both low-code and pro-code environments.

WSO2 is designing Asgardeo for a wide variety of customer types, from small to medium sized businesses and organizations as well as enterprises. This cloud-hosted service enables rapid deployment and time-to-value. Choreo and Ballerina, which is based on open-source, provide the means for customer developers to connect and extend Asgardeo to their own applications and 3rd-party API services.

WSO2 has industry specific profiles for their IAM solutions covering automotive, banking and finance, energy and utilities, healthcare, insurance, media and entertainment, pharmaceuticals, and retail. Advanced connectivity can be configured between Asgardeo and industry vertical applications using Choreo and their API Manager.

Asgardeo can be white-labelled by customers for consistent branding. Consumers can self-register using email or any OpenID or SAML-based social network credential. Organizations migrating to Asgardeo from another IAM or CIAM solution can bulk import user information via LDAP, SCIM, or through connectors to various cloud service APIs. WSO2 supports several account recovery options, including Knowledge-Based Authentication (KBA), email and SMS links, and cross-linking to most other IDaaS.

Consumers are tired of creating and remembering passwords, and organizations hosting consumer identities realize that password authentication is fraught with problems, which is leading to increased adoption of passwordless authentication mechanisms. The FIDO Alliance standard has powered the uptake of passwordless authentication methods. WSO2 supports FIDO U2F and 2.0, but the solution is not certified yet. Asgardeo accepts a large number of authenticators, including email/phone/SMS OTP; mobile push notifications via Duo; and 3rd-party apps including Aegis, Amazon, Authy, Basecamp, Google, LastPass, Microsoft, Okta, SaaSPass, and Yahoo. They have connectors for Veridium Biometrics and Aware Knomi for mobile biometrics, but Android and iOS native biometrics are not supported but are on the vendor's roadmap.

Single Sign-On (SSO) is an important requirement for most companies in both workforce IAM and CIAM scenarios. For large enterprises with multiple brands, SSO between all affiliated sites is expected by consumers and therefore is essential. Asgardeo supports all federation standards, including JWT, OAuth2, OpenID Connect, and SAML. A new Market Place will be available in 2022 for many common business application types including Business Intelligence (BI), Customer Relationship Management (CRM), email, Enterprise Resource Planning (ERP), e-signature services, marketing automation, office productivity, publishing, and more.

An initial, low assurance authentication event is often insufficient for some kinds of transactions, according to many organizations' security policies. Asgardeo supports adaptive authentication, which brings contextual risk analysis to bear on individual transaction requests. Asgardeo can be configured to examine user attributes, user behavioral analysis, and previous authentication assurance levels against policies governing the request type. Authentication sequences can be defined within the administrative UI. Many pre-built scenarios exist which can be customized as needed, such as for IP allow lists, discovery of new devices, login attempt failures, concurrent session limits, and authentication context reviews. Looking deeper, WSO2 plans to utilize Azure ML and HDInsight for risk analysis.

With fraud on the rise globally, evaluating additional feeds of information that can help reduce the risk of Account TakeOver (ATO) attacks is a paramount concern for most consumer-facing businesses.

WSO2 has been a pioneer in API enablement of identity functions. Identity Server and Asgardeo both support API integration with other IAM and security solutions. Moreover, WSO2 API Manager (a separate product which was rated as an Overall, Product, Innovation, and Market Leader in the KuppingerCole Leadership Compass on API Management and Security) can be used to secure and manage IAM and other APIs developed and exposed by customers.

One of the core requirements for CIAM solutions is to produce identity analytics reports for their customers. Identity analytics are general indicators of activity useful for trend analysis, but are also important for security, as input for User Behavioral Analysis (UBA) for risk analysis and as indicators of brute force password guessing and credential stuffing attacks. Asgardeo plans to provide identity analytics reports covering consumer registration events, user profile changes, changes to credentials, failed login attempts by user, etc.

As consumer IoT devices continue to rise in popularity and number, CIAM solutions are increasingly called upon by customer organizations to manage and link IoT device identities with consumer identities. Consumers expect to be able to use their existing digital IDs seamlessly and safely with newly purchased smart devices. IoT device identity management is more complex than simple one-to-one pairings. Home automation devices, electronics, connected cars, etc. are often used by multiple people within the same household, so one-to-many and many-to-many management schemes are necessary to support real-world identity relationships. IETF's OAuth2 Device Flow (OA2DF) is a widely accepted standard that is implemented by device manufacturers for the purpose of device-to-human identity association. WSO2 customers use their solutions for associating and managing device identities for use cases such as connected cars, medical equipment, and integrating with smart speakers such as Amazon Alexa. Asgardeo does not at present include a dedicated user dashboard for these functions, but customers can craft their own using the built-in developer tools.

Privacy and consent management are top concerns for many organizations. Privacy regulations such as GDPR, PIPEDA, and CCPA/CPRA are in effect, and new regulations are on the horizon in many regions around the world as well for more states within the US. Asgardeo allows consumers to view, edit, and delete personal information within a self-care app. Users may also manage credentials and links to other accounts. Permissions for data usage can be given and revoked. Consumers can export their data in accordance with GDPR and delete accounts. Identity Server supports the Kantara Initiative User Managed Access (UMA) and Consent Receipt specifications. Granular family management is on the product roadmap.

As a cloud resident solution, Asgardeo is hosted within Microsoft Azure. The product architecture is based on modern principles of microservices. Consumer profile storage is flexible, in that, Asgardeo supports LDAP, SQL, and NoSQL type databases. Additional attribute types are configurable by customers if needed. The aforementioned standards support allows easy connections to most compliant IDaaS providers, and out-of-the-box integrations are available for Microsoft Azure AD, Okta, OneLogin, Ping Identity, etc.

Asgardeo is a purpose-built cloud CIAM solution derived from WSO2's robust Identity Server and is designed to scale on demand for peak customer loads. WSO2 reports that some customers achieve more than 1 million logins per hour with a latency of no more than 250 ms. Asgardeo has a 99.9% uptime SLA.

Asgardeo interoperates with customer security infrastructure. Asgardeo can output event information via Azure services to SIEMs. Customer data is protected by MFA for admins and database encryption.

Asgardeo is aimed at developers from SMBs to enterprise who need to revamp consumer identity or add consumer identity functions to existing Line of Business applications. Toward that end, Asgardeo features intuitive administrative and developer consoles that allow both low-code and pro-code programming approaches. Moreover, WSO2 recognizes that "developer" is not a monolithic term. Some developers need to build complex applications with deep integration with CIAM solutions. Others may only need to assemble API communications between CIAM, CRM, and Customer Data Platforms. Developers can use the low-code flow-chart style interface within Choreo to build APIs, integrations, services, and applications that can be used by Asgardeo. Many common APIs and widgets can be visually selected, and others can be configured with just a few lines of configuration information. The developer UI allows for program testing, and changes within the underlying code can be pushed directly to Kubernetes in production instances when ready.

Strengths and Challenges

WSO2 has a good reputation in IAM for their open-source integration model and service support, as well as for incorporating innovation and conformance to relevant industry standards. Asgardeo is a new entrant to the CIAM SaaS market, but it has a strong lineage from its on-premises antecedent, WSO2 Identity Server. WSO2 is expanding their market potential by offering Asgardeo, filling in a gap in the portfolio. Identity Server will continue to serve medium to large enterprises that prefer on-premises deployments. Asgardeo will be a good choice for organizations ranging from SMBs to enterprises who are launching new CIAM services and/or migrating from other developer-focused CIAM / API platforms.

Given Asgardeo's target audience, the low-code / pro-code interface within Choreo will be beneficial for customers who both need to build quick API connections between solutions and those who need to design more complex consumer-facing applications. Asgardeo features a flow-chart style interface for constructing authentication flows. Many common selections are available by default within the UI. Code samples and instructional videos are readily available online. Asgardeo with Choreo can work together to build customized APIs and full applications.

Asgardeo has multiple choices for authenticators and a built-in risk engine to provide risk adaptive authentication. WSO2 supports FIDO authentication standards and certification is planned for 2022. Customers can tweak authentication policies or build them from the ground up, defining

equivalences among authenticators and sequences for situations of increasing risk. Identity analytics reports are present, and all pertinent data can be exported to external security and marketing analytics tools for processing thanks to the comprehensive support for communications protocols.

Asgardeo draws good privacy and consent management features from its Identity Server progenitor. Asgardeo provides user self-service portals that enable consumers to view, edit, export, and/or delete consent actions and personal information in accordance with prevailing privacy regulations. Development of family management is expected.

Asgardeo has good basic integration with consumer IoT device identities. Adding an extensible IoT device management portal for consumers would likely be useful for customers.

Strengths

- Cloud-hosted and designed to help developers add CIAM to applications
- Low-code and pro-code options within the same interface
- Associated Choreo and API Manager products enable customers to easily integrate their own and public APIs into new applications and secure them
- Flow-chart style admin and developer interfaces
- Good selection of MFA options with flexible policy editing
- Many pre-built connectors for other IDaaS and SaaS applications
- Comprehensive support for most every IAM standard including Kantara UMA and Consent Receipt
- Straightforward monthly active user licensing model allows for consistent predictability for customers who need to control costs

Challenges

- Lacks family management
- Customers must create their own smart IoT device identity integration dashboards for consumers
- Supports FIDO and FIDO 2.0 certification is planned for 2022

Related Research

Leadership Compass - CIAM Platforms

Leadership Compass - Consumer Authentication

Leadership Compass - Identity API Platforms

Leadership Compass - API Management and Security

Leadership Compass - Identity Fabrics

Leadership Compass - Enterprise Authentication Solutions

Leadership Compass - Access Management

Copyright

©2022 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 deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim 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 do 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 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.