kuppingercole ANALYSTS

Omada Identity Cloud

Nitish Deshpande

August 1, 2024

EXECUTIVE VIEW

This KuppingerCole Executive View report looks at Omada's SaaS solution, Identity Cloud. This report will highlight new features in the latest release and provide an overview of the IGA capabilities of the solution. The report concludes by outlining the strengths and challenges of the solution.

Content

Introduction 3
Product Description 4
Strengths and Challenges 8

Figures

Figure 1 Omada Identity Cloud compliance workbench dashboard 6
Figure 2 Omada Identity Cloud analytics dashboard 7

Introduction

IAM (Identity and Access Management) solutions are essential components of enterprise IT infrastructures for managing the digital identities of employees, partners, customers, but also devices and things, in the digital business, and for protecting digital corporate assets. IAM systems manage user accounts and their entitlements as well as their access across the variety of systems and applications in use in organizations.

Identity Lifecycle Management remains a core IAM requirement, but Access Governance is becoming a more sought-after capability for organizations requiring better visibility and control over governance functions and access entitlements across IT infrastructures. Governance solutions can run the gamut of providing simple reporting and dashboarding but can include more advanced capabilities that can include AI and/or machine learning techniques enabling pattern recognition to deliver valuable intelligence for process optimization, role design, automated reviews, and anomaly detection. Identity Governance and Administration (IGA) encompasses the capabilities in IAM market that broadly deal with end-to-end identity lifecycle management, access entitlements, workflow and policy management, role management, access certification, Separation of Duties (SoD) risk analysis, reporting and access intelligence for business-related insights to support effective decision making, enhanced auditability and improved security. IGA can also contribute towards removal of manual processes by automating tasks such as access reviews, access certifications, triggering workflows and others.

Over the past several years, organizations have been facing multiple changes affecting their security posture. The perimeter which separated the internal network from the outer world does not have the same relevance it had before, with remote and mobile users accessing internal systems, with integrating business partners and customers into business processes, and with the shift to cloud applications. On the other hand, the value and relevance of digital corporate assets and intellectual properties have increased. With the shift to connected things, digital assets need more robust security to avoid data breaches and unauthorized access.

IAM done right ensures effective management of identities and their various supporting components such as their user accounts and passwords, and their access entitlements, and attributes, while making sure authentication works as expected. IAM if not done right increases the attack surface. IAM provides the tools to automate processes around managing users and access entitlements, but also for regularly reviewing these and identifying orphan accounts, excessive entitlements, static entitlements, policy and SoD violations, unauthorized access, and in general centralized governance visibility.

On the other hand, IAM also plays a vital role for business enablement, when it comes to the need of employees, contractors, business partners, and customers to access certain applications, systems, and data. IGA (Identity Governance and Administration) as one of the core disciplines within IAM helps in managing identities and avoiding orphaned accounts, and in restricting entitlements according to the least privilege principle as a core concept of regulatory compliance. Thus, it helps in achieving regulatory compliance, but also is a central element in reducing the attack surface for both external and internal attacks. Beyond that,

there is an emerging demand for supporting things (IoT) and devices, specifically when creating new digital services.

IGA products support the consolidation of identity information across multiple repositories and systems of record such as HR and ERP systems in an organization's IT environment. The identity information including user accounts, associated devices, associated access entitlements and other identity attributes are collected from across the connected target systems for correlation and management of individual identities, devices, users, groups as well as roles through a centralized administration console.

IAM tools should enable implementing the workflows and automated processes for onboarding users and granting them access; however, not all solutions are capable of performing this task. IAM can enable organizations to manage identities by optimizing the onboarding and change processes, but also ensure that entitlements are revoked, and accounts are deleted or deactivated once they are no longer required. Moreover, IAM also manages access through various access control policies, Just In Time (JIT) provisioning, adaptive authentication, and dynamic authorization.

This KuppingerCole Executive View report focuses on Omada Identity Cloud, an IGAaaS offering provided by Omada, a leading IGA (Identity Governance & Administration) vendor headquartered in Denmark. Omada Identity Cloud has its roots in the established on-premises IGA solution of Omada but has been rebuilt to allow for efficient delivery as a service.

Product Description

Founded in 2000, Omada provides Omada Identity Cloud for customers wanting a SaaS solution – delivering a full range of IGA functionalities.

Omada is one of the leading vendors in the IGA market. Omada provides an advanced feature set for core IGA capabilities such as identity lifecycle management, access governance, identity provisioning, and compliance reporting. Omada offers an accelerated deployment offering that uses a best practice framework that allows customers to be operational within 12 weeks. This package is part of their standard offering. Omada Identity Cloud core components include a set of cloud-native services including a Data Pipeline service, a Provisioning service, a Workflow automation service, a Role and Policy engine service an Identity analytics service and a cloud management portal. Omada is constantly innovating its Identity Cloud offering with continuous service updates and planned solution updates released every six weeks.

The Omada Identity Cloud Platform supports a wide range of out-of-the-box and configurable connectors. It supports a connector community for peers to share, generate, and install connectivity packages. Standards-based connectivity builds on the established SCIM

standard which supports identity provisioning including support for SCIM 2.0, while API-based connectivity utilizes standard APIs such as REST, SQL, GraphQL, and SOAP.

Omada has a developer portal called the Omada Hub which has documentation, tutorials, videos, and a forum for questions and answers. Omada supports JavaScript and .NET programming languages which can be leveraged to offer connectivity to all other mainstream programming languages. Omada supports Java by easily using the JavaScript Engine class to invoke the JavaScript from their SDK. For Python, JavaScript can be invoked by using node.js. For C/C++, one can leverage the EM_JS macro or call the script directly from emscripten_run_script. For Ruby, a developer can invoke JavaScript using ExecJS.eval and for Go it can be done by using the Syscall/js package. Lastly both iOS and Android have several methods to call JavaScript on the device. Omada's identity lifecycle management allows control of identities as per context, association, or roles including review of access right. Access review for all identities including external identities is available.

The latest version release is focused on a variety of performance enhancements, implementation of AI and machine learning for chatbots, access recommendations and new features for compliance and analytics. Omada has invested in a GraphQL API for business logic which is used for integration with third-party portals such as the ServiceNow portal for access request and approvals through its standard interface. No additional license cost is required on the ServiceNow site although customers will need ServiceNow accounts.

With the introduction of this GraphQL API, it is now possible to support chatbot interfaces. Customers can integrate with Omada to perform access requests via GraphQL APIs through third-party applications. AI analysis of user access management data is supported by the solution by using unsupervised machine learning to provide role suggestions. This new GraphQL API provides a new method for evaluating policies during requests by simulation assisted by the Role and Policy engine service, the policy evaluation is a new method and is doing a simulation call to the role and policy engine whereby it returns the result.

Omada has built a new access request framework which is being updated regularly to provide new services. Omada's approach is that through a single browser, IGA configuration for process workflows, policies, and connectors is completely possible. The generic web service framework has a new updated UI which allows customers to configure the web services connectors. JSON references path and template enhancements have also been added to the connector framework. Further enhancements around connectivity include support for Microsoft EntraID.

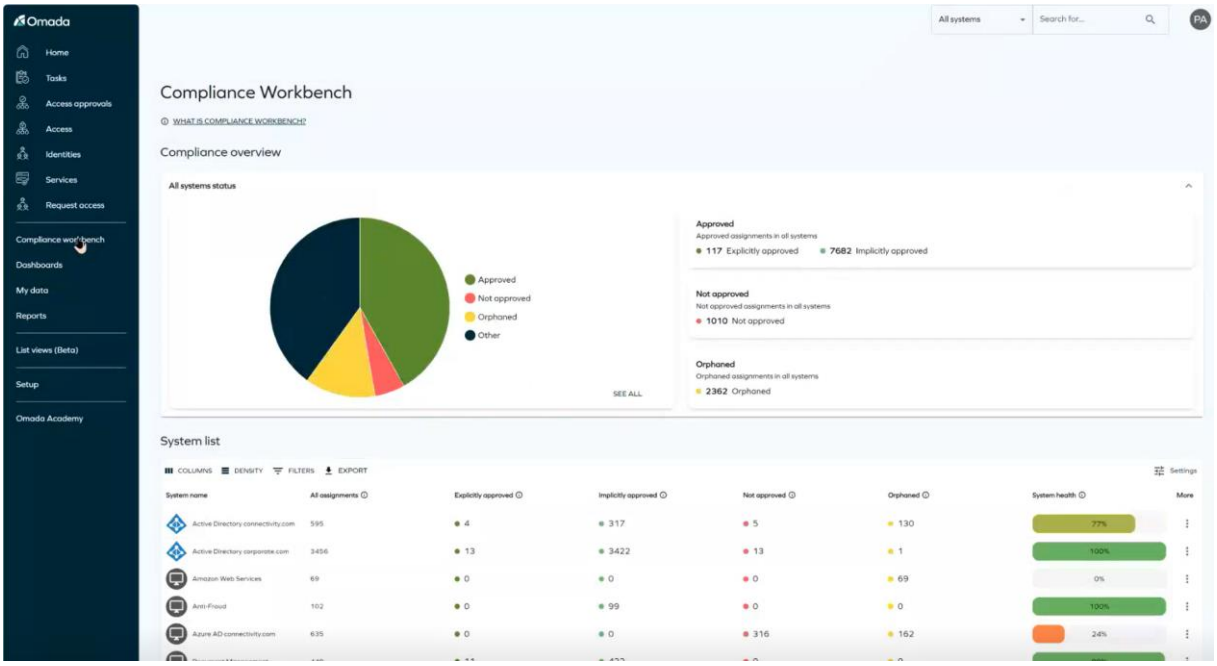

Figure 1: Compliance workbench dashboard (Source: Omada)

Omada compliance workbench provides a unified view of the compliance state of all access rights across all systems. The workbench dashboard is actionable to drive access review and certification campaigns. The workbench dashboard also provides a comprehensive view of the system and can help customers understand the overall system health metrics based on parameters such as unapproved access and orphaned accounts.

Omada Identity Cloud now offers a new Identity Analytics dashboards. This new interactive dashboard and reporting capability displays advanced data and identity analytics. The dashboard insights provide information about the status of certifications, characteristics of SLAs, ongoing campaigns, and historical data. Omada Identity Cloud also has a new dynamic audit trail dashboard powered by analytics. The landing page of this dashboard is graphical and statistical with a modern data visualization interface highlighting widgets related to decisions made in a week compared to total requests inbound, rate of approved access, breakdown of activities carried out in a week, and top resources requested for access. Dashboards can be customized through the available set of filters. The audit trail can be downloaded either as a CSV file or as an image.

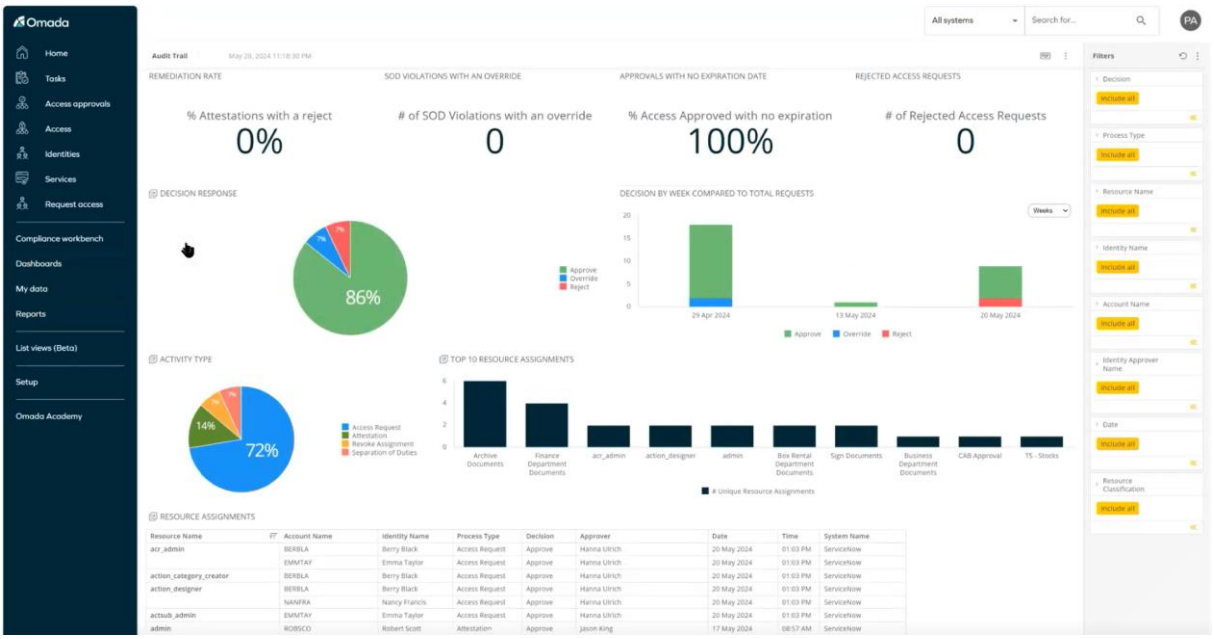

Figure 2: Configurable analytics dashboard (Source: Omada)

Omada has a new AI-powered chatbot assistant that provides technical and general information about the product and the overall IGA topic on demand. Customers and partners can both have access to the chatbot which is trained on enablement material and product documentation. The interface for the chatbot is user friendly and the responses from the chatbot are comprehensive. It covers a wide variety of topics with related links provided at the end of responses.

Omada's peer access analysis and peer recommendations provide rule-based automation to recommend access based on roles and highlight outliers. The role mining engine supports role analytics and role discovery. The solution uses advanced machine learning algorithms for role discovery. The current version of the solutions uses PowerBI as the client viewer, however, Omada plans to offer a Role Insights view within the Identity Analytics dashboards. In-house Machine Learning algorithms also allow the user to see how resources are related to roles and identify patterns.

Omada also provides bottom-up role discovery where if a user has all the characteristics of a role, then the role is implicitly assigned. The solution uses AI for recommending access requests based on peers via a thorough analysis. The solution supports continuous validation of access policies, automation of migrating controls, closed-loop reconciliation, automatic case management, and context modeling.

The access request page user interface now shows enhanced details such as policy and risk checks. If an access request can result in a conflict, then the user is alerted about the implications which can help to improve security and compliance. The access request page displays real-time insights into access requests and violation status.

The cloud management portal has a modern user interface. It is a delegated self-service portal for customers on their own cloud environments. Cloning of the environment is also supported through this portal. Omada Identity Cloud supports a wide range of connectors

totalling over 150 through the connectivity manager in the cloud portal. User management is supported through the cloud portal. Omada supports full configuration of cloud environments through the cloud portal. Omada does not enforce upgrades, but environments can be set for auto upgrade.

Omada has extended its support for generic SSH connectivity to simplify integration with on-premises servers to manage user data. There is also a new SAP Concur connectivity package that allows users to directly manage access within Omada and connect directly with SAP Concur by enforcing SoD policies.

Omada has created a next generation microservices based architecture, called Horizons, which operates within the Omada Identity Cloud Service. This new architecture will be the base for delivering all future features to Omada's customers. This platform modernizes data ingestion with a focus on real-time data processing and streaming data at all times. The platform is multitenant and uses a zero-trust architecture which is fully exposed via APIs. The integration capabilities of this platform allow consumption of the data in both directions.

Strengths and Challenges

Omada continues to enhance the Identity Cloud platform with new features leveraging AI and machine learning. It is focused on providing a flexible update policy, thus supporting improved flexibility. The updates are under the control of the customer with updates in short intervals every six weeks.

Omada continues to enhance its strength in Access Governance, with several new and enhanced capabilities. From our perspective, Omada on the one hand gives customers a great degree of flexibility in adapting the solution to their needs, and on the other hand provides best practices processes, KPIs, etc. This combination allows customers to build and customize the solution to their needs, based on best practices and a no-code approach, and benefit from the two decades of practical experience Omada has gathered.

Omada is focused on medium-sized and enterprise-size customers. Most of its presence is based in North America and EMEA. Their roadmap includes a, enhanced role mining, and delivery of new dashboards at regular intervals. A collaborative role discovery tool for managers and other leaders to create roles for their populations is also planned in the roadmap.

Strengths

- Covers all major capabilities related to IGA such as identity lifecycle management, access governance, and identity provisioning management including transfer of identity
- Supports wide range of authenticators for user and admins self-service
- Unique configurable connector community
- Supports all capabilities related to identity lifecycle
- AI and machine learning implemented for various tasks such as role discovery, access recommendations, and analysis of access management data

- Omada compliance workbench provides unified view of compliance state of all access rights across all systems
- Reporting model uses advanced analytics dashboard which can be configured
- Supports all deployment models
- Modern, flexible user interface
- Provides an Accelerator Package as a standard part of their offering to deploy the solution within 12 weeks
- Continuous delivery of updates and patches, with ability for tenants to control when these are applied rather than forced updates
- Efficient approaches for managing SoD controls and conflicts as well as recertifications

Challenges

- Limited customer presence outside EMEA and North American market
- Partner ecosystem is good but missing global reach
- Omada provides primary support to JavaScript and .NET but if required, can also support other programming languages through invoking relevant nodes and macros

Related Research

Leadership Compass Identity Governance & Administration 2022
Executive View Omada Identity Suite
Leadership Compass Identity as a Service (IDaaS)
Leadership Compass Access Governance 2023
Market Compass IGA Solutions for ServiceNow Infrastructures

About KuppingerCole

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

Copyright

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

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

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