KuppingerCole ANALYSTS

Executive View Omada Identity Cloud

Nitish Deshpande

November 25

EXECUTIVE VIEW

This KuppingerCole Executive View looks at the challenges organizations face in managing identity lifecycle, access governance and compliance across diverse environments. A technical review of the Omada Cloud Identity platform is included.

Content

Figures

Introduction

Traditional identity management approaches often rely on disparate systems that provide limited insight into access relationships across the enterprise. Without a unified identity data model, organizations struggle to correlate identity and entitlement information from multiple sources. This hinders their ability to make informed access decisions, slows onboarding and offboarding, and increases the likelihood of excessive or orphaned entitlements. The operational impact is further compounded when identity teams must rely on manual, repetitive tasks to manage access, review entitlements, and address issues that could otherwise be automated to free resources for higher-value activities.

The market is shifting toward unified identity platforms delivered as a service. These platforms consolidate identity lifecycle management, access governance, policy enforcement, and reporting into a single, centrally managed environment. A unified approach allows consistent application of policies across systems and applications, facilitates centralized monitoring, and streamlines compliance reporting. For administrators, it simplifies management by providing a single interface for provisioning, certification, workflow execution, and analytics. For end users, it offers a more consistent and efficient user experience, including self-service capabilities for access requests, password resets, and profile management.

Cloud-delivered IGA offers distinct operational advantages over traditional on-premises deployments. The ability to provision and be operational within hours, automatic application of security updates, and elastic scalability align well with organizations' need for agility. High availability and disaster recovery capabilities, along with modern security controls such as web application firewalls, further support business continuity and risk mitigation. By integrating with both cloud and on-premises systems, often without requiring complex firewall changes, these platforms help bridge the gap between legacy infrastructure and modern services.

From a governance perspective, advanced capabilities such as AI-driven role discovery, access analytics, and dynamic policy enforcement are becoming standard. These features support the reduction of role sprawl, enable more targeted certifications, and improve the accuracy of access reviews.

- Role mining, when supported by machine learning, can surface access patterns and suggest optimized role structures.
- Access analytics can identify anomalies, orphaned accounts, and policy violations in near real time.
- Automation plays a critical role not only in provisioning and deprovisioning but also in orchestrating workflows that respond to changes in risk posture or business context.

The compliance landscape continues to be a driver for IGA adoption. Regulatory frameworks such as GDPR, HIPAA, SOX and CCPA require organizations to demonstrate control over access to sensitive data, maintain audit trails, and enforce least-privilege principles. Automated certification campaigns, segregation of duties controls, and detailed reporting capabilities are fundamental to sustaining compliance and avoiding penalties. In parallel, there is a growing emphasis on "evergreen" operations, where platforms continuously apply functional updates and security patches without service disruption, keeping organizations aligned with evolving security and regulatory expectations.

In this KuppingerCole Executive View report, we examine Omada Identity Cloud, an IGA-as-a-Service platform that delivers unified identity lifecycle management and access governance through a cloud-native architecture, combining operational efficiency with advanced analytics, AI-driven insights, and policy-based automation to address complex enterprise requirements.

Product Description

Omada, headquartered in Denmark, counts among the established providers of solutions for IGA. Founded in 2000, Omada provides Omada Identity Cloud with a full range of IGA capabilities for customers wanting a cloud-native SaaS solution.

Omada has released its next generation of its Omada Identity Cloud service, built on a fully cloud-native platform. This platform is the basis for delivering all future features to Omada's customers. The platform is multitenant compute and uses zero-trust architecture exposing all core functionality through APIs. The integration capabilities of this platform allow data to flow in and out seamlessly.

Omada supports a wide range of out-of-the-box and configurable connectors for SaaS systems but support for certain legacy on-premises systems is limited. Omada provides a connector community for peers to share, generate and install connectivity packages that are easy to deploy.

For broader integrations, Omada exposes capabilities via SOAP, REST, SQL, OData and GraphQL APIs. These APIs are used for integration with third-party tools, accessing data within the solution, and managing the cloud platform itself.

Omada's Identity Cloud platform centralizes identity lifecycle management and access governance into a single, cloud-delivered environment.

Organizations can be operational within two hours of ordering thanks to rapid provisioning. The platform is continuously updated with functional and security enhancements through an evergreen delivery model.

The design focuses on removing operational friction. Routine hotfixes and updates are applied automatically, while administrators retain control over environment configuration and upgrade timing via the Cloud Management Portal.

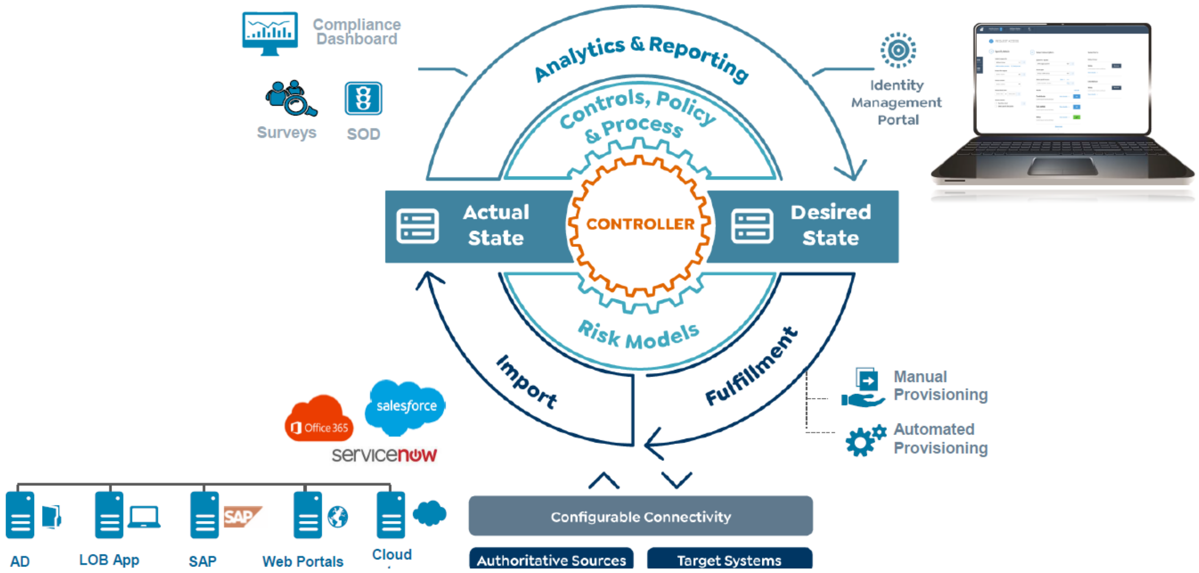

Figure1: Omada Identity Cloud (Source: Omada)

The platform covers established IGA capabilities such as provisioning, deprovisioning, access requests, role management, segregation of duties (SoD) enforcement, and certification campaigns.

On top of these foundations, the platform delivers advanced capabilities in analytics, AI-driven decision support, and policy-based automation. Its Cloud Application Gateway enables secure connectivity to both cloud-hosted and on-premises systems without the need for complex firewall rule changes, ensuring integration flexibility.

Omada's Role Insights, Access Navigator, and Data Quality dashboards deliver visibility into identity relationships, access assignments, and governance data health, allowing organizations to make informed, timely decisions.

Finally, with the embedded multi-lingual AI assistant Javi, Omada Identity Cloud brings governance workflows directly into collaboration tools. Users can approve access, review roles, and act on compliance tasks in context, without switching systems.

Cloud Application Gateway (CAG)

The Cloud Application Gateway provides secure connectivity between Omada Identity Cloud and target systems, whether cloud-based or on-premises. It operates using outbound-only TLS 1.3 connections thus eliminating inbound firewall changes which is a frequent barrier in enterprise integration projects. CAG supports imports, provisioning, schema discovery, and connectivity validation, ensuring that governance processes extend seamlessly across heterogeneous environments.

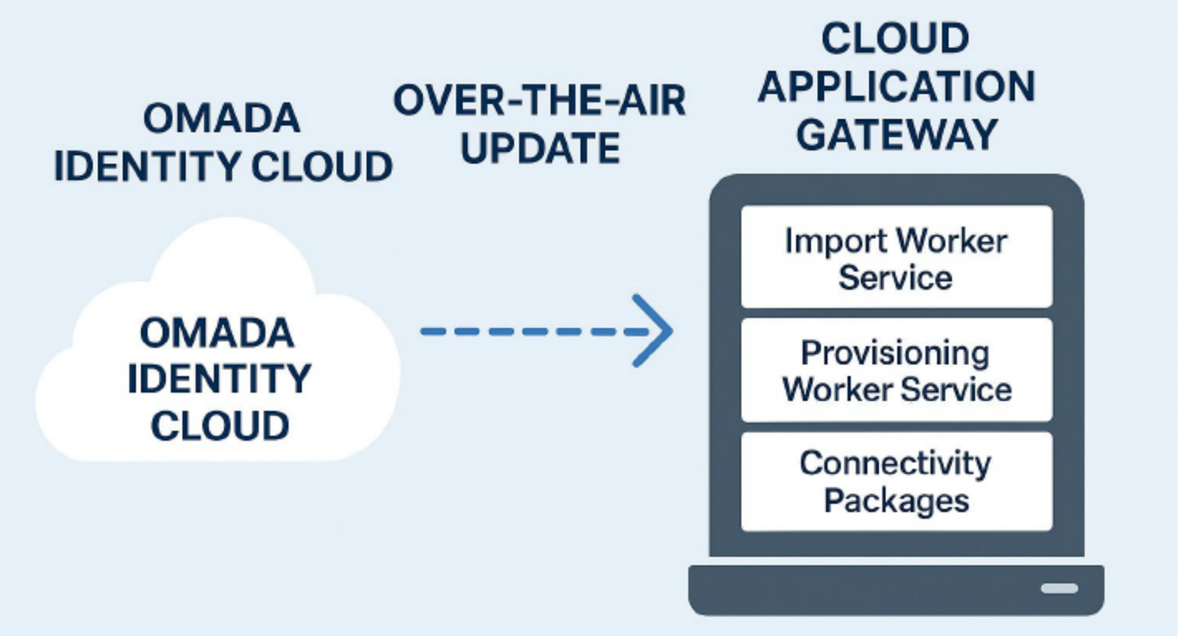

Figure 2: Cloud Application Gateway (Source: Omada)

Its automated over-the-air update mechanism keeps connectivity components current without manual effort, reducing operational overhead.

Looking ahead, Omada is introducing a zero-knowledge model that will allow customers to manage their own decryption keys, strengthening control over sensitive integration data.

With its security-first design, CAG is particularly effective for connecting to systems in regulated or security-sensitive environments where minimizing network exposure is essential.

Cloud Management Portal

The Cloud Management Portal provides self-service control over all Omada Identity Cloud environments, including production, non-production, and configuration-only instances.

Production environments are designed for high availability, ensuring seamless, uninterrupted service with geo-redundancy and comprehensive disaster recovery protocols. This setup supports business-critical operations with stringent SLA adherence.

Meanwhile, non-production instances offer a safe environment for configuration and testing, isolated from live systems to prevent unapproved changes from affecting operations. This separation allows businesses to innovate and test new features or updates under realistic conditions without the risk to operational stability, thereby fostering an agile yet secure development lifecycle.

Administrators can choose to upgrade immediately while keeping services available, or schedule updates to align with internal change management. The portal also supports CI/CD integration and provides SLA monitoring through automated probes, giving organizations visibility and control over their environment lifecycle..

Dynamic Roles and Contextual Policy Enforcement

Omada Identity Cloud addresses the challenge of role inflation by enabling dynamic, attribute-driven role assignments. Attributes such as department, location, or business unit can define role membership, and dynamic inheritance allows for sub-role and permission assignment without creating redundant static roles. This approach maintains flexibility while controlling access proliferation.

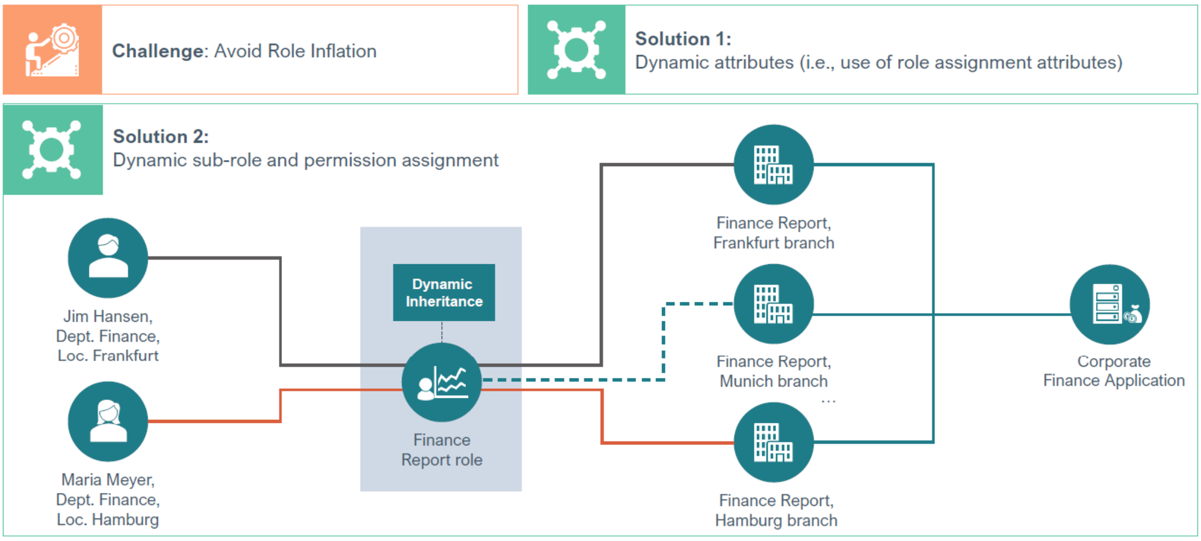
Challenge: Avoid Role Inflation
Solution 1:
Dynamic attributes (i.e., use of role assignment attributes)
Solution 2:
Dynamic sub-role and permission assignment
Jim Hansen, Dept. Finance, Loc. Frankfurt
Maria Meyer, Dept. Finance, Loc. Hamburg
Dynamic Inheritance
Finance Report role
Finance Report, Frankfurt branch
Finance Report, Munich branch
...
Finance Report, Hamburg branch
Corporate Finance Application

Figure 3: Dynamic Roles and Contextual Policy Enforcement (Source: Omada)

Policy enforcement extends across organizations, business processes, roles, and resources, supporting sophisticated segregation of duties (SoD) scenarios. SoD conflicts are detected automatically during department changes, when granting new rights, or when business roles or rules change.

Built-in mitigation workflows, including time-limited exceptions, thus allowing legitimate business needs to be accommodated without compromising control.

AI-Driven Role Insights and Access Analytics

Role Insights leverages machine learning to analyze identity and entitlement data, surfacing access clusters and detecting anomalies. This allows role engineers to filter and fine-tune roles based on business context, applying best-practice methodologies informed by over two decades of project delivery experience.

The Access Navigator dashboard complements this by presenting interactive, filterable views of identities, systems, assignments, contexts, accounts, and resources. Governance teams can save filter sets, share them for collaborative analysis, and export findings in CSV or image formats for reporting. Together, these capabilities support a continuous improvement cycle for role design, entitlement hygiene, and access review efficiency.

Compliance Workbench and Data Quality Dashboards

The new Compliance Workbench provides a single dashboard showing key compliance metrics: orphaned accounts, separation of duties (SoD) violations, approved policy-based access, and direct access assignments that bypass standard approval workflows. This unified view accelerates issue resolution and simplifies audit reporting.

The Data Quality Dashboard complements this by flagging orphaned accounts, unused entitlements, accounts without owners, and resource assignments pending deprovisioning. Highlighting these hygiene issues enables administrators to proactively remediate risks. This reduces the likelihood of lingering high-risk entitlements and ensuring cleaner governance datasets.

AI Assistant – Javi

Javi is Omada's multi-lingual AI assistant embedded into collaboration platforms like Microsoft Teams delivering governance actions directly to users' workspace. Javi supports a conversational experience powered by GenAI for business processes such as compliance and identity access reporting, requesting and approving access, notifications and much more.

Javi supports fuzzy search for access requests. This reduces the need for users to know exact entitlement names. It also generates AI-driven descriptions for roles and resources which can enhance reviewer's understanding about the specific role/ resource. Overall, Omada enables real-time, conversational access to governance data, by integrating analytics and reporting into the assistant.

Disaster Recovery and High Availability

Omada Identity Cloud operates with a standard SLA of 99.5% availability, with an optional 99.9% SLA for organizations requiring higher uptime guarantees. Disaster recovery planning is built into the service, with a recovery point objective (RPO) of 15 minutes and a recovery time objective (RTO) of 270 minutes. Failover to alternative data centres within the same region is part of the architecture, and DR procedures are regularly validated.

This resiliency is paired with multi-tenant elasticity for compute resources and dedicated persistent storage per customer to ensure both performance and data isolation.

Analytics-Driven Governance Decisions

Beyond role and access analysis, Omada Identity Cloud includes advanced reporting capabilities through its enhanced dashboards. The platform supports real-time operational analytics, policy lifecycle management, master data quality analysis, and provisioning visualization.

Actionable analytics link governance insights directly to remediation workflows, allowing administrators to act on risk indicators without leaving the reporting view. Scheduled reporting and integration with external business intelligence platforms via streaming services allows organizations to incorporate identity governance metrics into broader operational analytics strategies.

Through its combination of automation, analytics, and intuitive user engagement, Omada Identity Cloud solidifies its role in the IGA solutions space. Its comprehensive scope can be tailored to address current identity governance challenges while staying future-ready to address evolving technological landscapes.

Strengths and Challenges

Omada Identity Cloud is a mature IGA-as-a-Service platform. It combines lifecycle management, governance, and advanced AI-driven automation to streamline identity processes. The platform offers secure connectivity through the Cloud Application Gateway, dynamic role management, and SMART Certification to address compliance challenges. Analytics dashboards enhance visibility into access relationships and data quality, while the multilingual AI assistant, Javi, embeds governance into collaboration platforms for faster, contextual decision-making. Built on a zero-trust architecture, with API-driven integrations, rapid provisioning, evergreen updates, and built-in disaster recovery, the platform balances governance rigor, operational agility, and user-centric design. Features like Role Insights and Access Navigator help organizations continuously optimization identity and access governance practices.

However, Omada Identity Cloud faces a few challenges, particularly in supporting legacy on-premises systems, which may be an issue for customers with significant legacy infrastructure. Another area for potential improvement is the expansion of its partner ecosystem to enhance its market presence beyond current regions. Despite these hurdles, the ongoing development of its AI capabilities and automated over-the-air update mechanisms for its Cloud Application Gateway are promising steps towards broadening its integration capabilities.

Omada Identity Cloud is best suited for medium to large enterprises across North America and EMEA, particularly those in regulated industries such as finance, healthcare, and public services.

Its cloud-native architecture and robust governance features make it a strong candidate for organizations seeking to address their identity lifecycle and access governance processes. Dynamic roles, policy-based automation, and compliance dashboards serve various use cases, from managing access requests to conducting AI-driven role analysis.

Enterprises looking to bolster their governance framework with a modern, cohesive IGA platform should consider Omada Identity Cloud as an option.

Strengths

- Unified identity governance platform combines lifecycle management and access governance in a single SaaS environment.
- Secure, outbound-only connectivity to cloud and on-premises targets via Cloud Application Gateway with automated over-the-air updates and planned zero-knowledge encryption.
- AI-Driven Role Insights leverage machine learning–based discovery of access clusters and outliers for role optimization.
- Role insights and Access Navigator Dashboard provides interactive analytics on identities, accounts, resources, and contexts with exportable reports.

- AI Assistant “Javi” is an embedded, conversational, multi-lingual governance assistant integrated into collaboration tools such as Microsoft Teams.
- Cloud Management Portal supports full administrative control of cloud environments, upgrades, and operational monitoring.
- SLA-supported high availability and disaster recovery.

Challenges

- Customer base still concentrated in EMEA and North America
- Specialized environments may require additional customization
- Full feature set could be complex for smaller organizations
- Limited support for some legacy on-premises systems

Related Research

Advisory Note: Modernizing Authorization: Policy Based Access Management
Buyers Compass: Policy Based Access Management
Leadership Compass: Identity Governance and Administration
Leadership Compass: Identity and Access Governance
Leadership Compass: Policy Based Access Management
Leadership Compass: Access Management
Leadership Compass: Customer Identity and Access Management (CIAM)
Leadership Compass: Cloud Infrastructure and Entitlement Management

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 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.

Copyright

The conclusions, recommendations, and predictions in this document reflect KuppingerCole's initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinements or significant changes. KuppingerCole disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole assumes no liability for errors or inadequacies in the information contained in this document. Any expressed opinion may change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Their use does not imply any affiliation with or endorsement by them.

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.