KuppingerCole Report

EXECUTIVE VIEW

By Martin Kuppinger

September 03, 2021

One Identity Manager On Demand

One Identity Manager On Demand is the IDaaS solution of the established One Identity Manager. It comes with feature-parity for all established IGA capabilities, including connectors to target systems and governance capabilities. One Identity supports IDaaS deployments with continuous updates and defined segregation of customizations from code. One Identity Manager On Demand counts amongst the most feature-rich IDaaS solutions available on the market.

By **Martin Kuppinger**
mk@kuppingercole.com

Content

1 Introduction

IAM (Identity & Access Management) today is at the core of enterprise IT infrastructures when it comes to managing the digital identities of employees, partners, customers, but also devices and things, in the digital business, and for protecting digital corporate assets. IAM, as the name states, is about managing identities and their access. This involves managing user accounts and their entitlements as well as their access across the variety of systems and applications in use in organizations.

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 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 and to smart manufacturing, digital assets are becoming "crown jewels" even for more traditional businesses such as mechanical engineering.

Protecting digital assets, the systems, and applications in an IT environment of growing complexity and of a hybrid nature while facing ever-increasing attacks, involves several actions organizations must take. Protecting against internal and external attackers requires a well-thought-out understanding of risks and countermeasures.

Among the core elements of every infrastructure, we find IAM. IAM done right ensures that identities, their user accounts and passwords, and their access entitlements are well-managed and that authentication works as expected. IAM thus reduces the attack surface by helping organizations moving towards the "least privilege" principle. IAM provides the tools to automate processes around managing users and access entitlements, but also for regularly reviewing these and identifying, e.g., excessive entitlements.

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

IAM is the tool for implementing the workflows and automated processes for onboarding users and granting them access. Again, if done right, IAM can enable organizations 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 at runtime.

Over the past few years, we have seen a convergence of traditional IAM deployments that run on premises towards IDaaS. IDaaS is one of the fastest growing market segments of IAM characterized by cloud-based delivery of traditional IAM services. The market, driven largely by web-centric use-cases in its early days, now offers full-fledged delivery of IAM capabilities irrespective of application delivery models. The IDaaS

market has registered significant growth over the last few years primarily driven by the need of organizations to achieve better time-to-value proposition over on-premises IAM deployments. IDaaS solutions offer cloud-ready integrations to extend an organization's IAM controls to meet the security requirements of their growing SaaS portfolio.

The IDaaS market has evolved over the past few years and is still growing, both in size and in the number of vendors. However, under the umbrella term of IDaaS, we find a variety of offerings. IDaaS in general provides Identity & Access Management capabilities as a service, ranging from Single Sign-On to full Identity Provisioning and Access Governance for both on-premises and cloud solutions. These solutions also vary in their support for different groups of users - such as employees, business partners, and customers - their support for mobile users, and their integration capabilities back to on-premises environments.

This KuppingerCole Executive View report focuses on One Identity Manager On Demand. One Identity is one of the leading, established vendors in IAM, with specific focus on IGA and PAM. One Identity Manager On Demand is the IDaaS version of their established on-premises flagship product One Identity Manager.

2 Product Description

One Identity Manager OnDemand is the IDaaS version of One Identity Manager. In contrast to other vendors, One Identity took a different approach for its IDaaS solution. It neither is just a lift-and-shift of an existing solution to some sort of SaaS delivery, nor is it a completely new product. Over the past years, One Identity already has invested significantly in modernizing the on-premises version of the One Identity Manager, specifically in modularizing its architecture. One Identity Manager On Demand builds on that, meaning that there is virtually no trade-off in functionality when choosing One Identity Manager On Demand, compared to the traditional One Identity Manager. The only major functional difference is that the Data Governance Edition is not available as SaaS.

On the other hand, One Identity had to master the challenge of delivering a true IDaaS solution based on this technology. Requirements for such IDaaS approach, in the definition of KuppingerCole, e.g., require an API-first integration and customization approach; segregation of customizations to make them resilient to the impact of updates; efficient and continuous updates and patches, managed by the provider; and scalability and elasticity in deployment. We don't expect the solution to be truly multi-tenant. On one hand, many customers, specifically in areas with sensitive data such as IAM, refrain from full multi-tenancy. On the other hand, modern single-tenant deployments can be managed well with automation, delivering the continuous update and patching to the customers, while leaving data and customizations untouched in the customer's tenant.

One Identity has intensively worked to balance the IDaaS requirements while keeping the technical strength. Customizations are consequently isolated, and customer extensions remain untouched during updates. The web front-end has been rewritten and is based on Angular, consuming APIs that are exposed by the API Server component. Thus, front-end and backend are segregated, allowing to manage customizations at the front-end, as well as orchestration to other solutions, based on APIs and isolated from the backend.

Updates are provided continuously, based on the Azure platform update mechanisms and ubernets. Customers receive notifications, and updates take place over a defined period. Additionally, customers by default have two instances of One Identity Manager On Demand, one for pre-production and testing, and the other for the production environment. Based on the technical features as well as checklists and best practices provided by One Identity, customers shall be well-able to benefit from the IDaaS characteristics, while having a comprehensive set of capabilities to build on.

From a capability perspective, One Identity Manager On Demand comes, as mentioned, with almost the full feature set of the traditional on-premises version. Connectivity to systems that are running on-premises still utilizes the broad set of connectors for these solutions, while SaaS solutions can be integrated via Starling Connect, another SaaS service provided by One Identity, which integrates to SaaS services via the SCIM 2.0 standard (System for Cross-Domain Identity Management). Specific strengths such as SAP certified, deep integration into SAP environments is available in the on-demand version of One Identity Manager as

well.

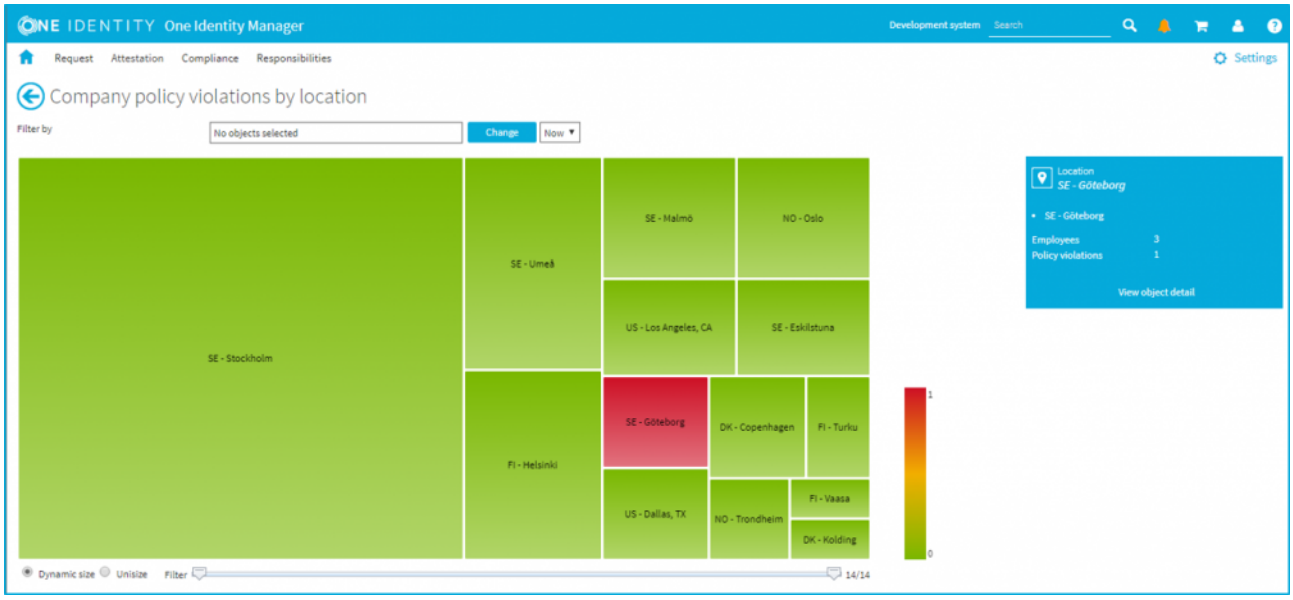

Figure 1: The Governance Heatmap is one of the features of the One Identity Manager user interface (Source: One Identity)

Other feature areas include User Lifecycle Management, Access Governance, and Self-Service Access Portals. For Access Governance, One Identity has added a Governance Heatmap as one of the new features, providing insight and drill-down into the status of Access Governance across various types of systems and users.

One Identity Manager On Demand continues on the evolution that has been demonstrated by One Identity in the on-premises One Identity Manager, with shifting to a modular architecture and segregation of customizations.

3 Strengths and Challenges

With its approach for One Identity Manager On Demand as the IDaaS offering, One Identity, at first glance, seems to take a lift-and-shift approach. However, in contrast to other vendors, One Identity builds on a modern, modular, and API-based architecture, which allows for delivering continuous patches and updates to the tenants at scale, as well as for isolating customizations, orchestration, and integration so that these remain untouched by updates.

The advantage of this approach is that One Identity Manager On Demand provides the same, comprehensive feature set as the on-premises One Identity Manager, with very few exceptions. Thus, customers can build on a proven, feature-rich solution, but on the other hand benefit from the advantages of an IDaaS deployment.

What we miss is a published standard pricing model that is consequently based on a pay-per-use approach. For IDaaS solutions, we expect vendors to take such approach, shifting away from traditional licensing to consequently implemented subscription models based on current usage.

One Identity Manager On Demand is an interesting solution in the evolving IDaaS IGA market. It delivers to the expectations we have on IDaaS solutions, despite being based on the traditional on-premises technology. Due to that foundation, it is a very feature-rich solution that caters to the need of customers in the complex space of IGA.

Strengths

- Comprehensive IGA feature set, with overall feature-parity to on-premises solution
- Very broad set of connectors for on-premises and SaaS targets available
- Deep integration into SAP environments, SAP-certified
- Defined segregation of customizations, ensuring that these remain untouched by updates
- Comprehensive set of APIs
- Angular-based web-UI, utilizing the backend APIs, segregating front-end and backend
- Pre-production environment for testing being available to tenants by default
- Continuous delivery of patches and updates to tenants with notification period
- Utilizes capabilities of Microsoft Azure and Kubernetes for efficient rollout of patches and updates

Challenges

- Licensing model is not published as a pay-per-user/month model
- Data Governance capabilities not available in the product, in contrast to the on-premises version
- Starling Connect kept as a separate component
- Not a multi-tenant solution, but well-thought-out approach for patching and updating tenants
- Currently only available on Microsoft Azure, also due to utilization of Microsoft SQL technology

4 Related Research

Leadership Compass Identity Governance & Administration 2021 - 80516
Executive View One Identity Active Roles - 80413
Executive View One Identity Manager - 80310
Market Compass IGA Solutions for ServiceNow Infrastructures - 80515

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.