KuppingerCole Report

EXECUTIVE VIEW

By Richard Hill
October 20, 2020

# ideiio

Identity Governance & Administration (IGA) is not only for large enterprises but organizations of all sizes to reduce the risk of user access to applications, systems, and data and ensure compliance with applicable laws and regulations. ideiio focuses on providing a straightforward and easy way to deploy and use IGA in organizations regardless of its size.

By **Richard Hill**
rh@kuppingercole.com

# Content

# 1 Introduction

Regardless of an organization's size, there is always a level of risk associated with user access to an organization's applications, systems, and data. At the same time, organizations strive to remain relevant through digital transformations of their services and emerging technology initiatives such as the digital workplace, DevOps, security automation, and the Internet of Things.

Cost savings and license management are key considerations for organizations, especially in the mid-market. IT solutions that provide automation and workflows save time and reduce human error, contributing to lower IT costs. Solutions providing flexible licensing models can also help to reduce costs.

To stay competitive and compliant, organizations must actively seek new ways to assess and manage security risks without disrupting the business. Therefore, security leaders urgently need to continually improve upon the organization's security posture by identifying and implementing appropriate controls to prevent such threats.

Identity Governance and Administration (IGA) concerns the IAM (Identity and Access Management) extended capabilities that broadly deal with end-to-end identity life-cycle management, access entitlements, workflow and policy management, and role management, access certification, SOD risk analysis, reporting, and access intelligence. A self-service user interface allows for requesting access, profile management, and password resets. Configurable connectors, either cloud-native or based on gateways back to on-premises environments, offer automated user Lifecycle Managementto both on-premises as well as SaaS applications.

As IGA becomes a vital security risk and management discipline directly impacting any organization's security posture, a lack of basic IGA capabilities can leave organizations exposed to risks originating from inefficient administration of identities and access entitlements, poor role management, and a lack of adequate auditing and reporting. These risks range from identity thefts to unapproved and unauthorized changes, access-creep, role bloating, delays in access fulfillment, orphan roles and accounts, or SOD conflicts leading to occupational and other internal fraud. Many past incidents in the news have emphasized the need to have better IGA controls for organizations of all sizes across all industry verticals.

IGA also refers to the increasingly integrated Identity Lifecycle Managementand Access Governance markets. Identity Provisioning focuses on tasks related to administering access fulfillment and entitlements throughout an identity life-cycle. Access Governance provides necessary (mostly self-service) tools for businesses to manage workflows and access entitlements, run reports, access certification campaigns, and SOD checks. Access intelligence is the analytics layer over Identity Lifecycle Managementand Access Governance that offers business-related insights to support effective decision making and potentially enhance governance.

ideiio, established in 2019 is a vendor in the IGA market, spun out from, and remaining part of the ProofID group – an IAM professional services provider and system integrator. Headquartered in Manchester, UK, with offices and development teams in Colorado Springs, US – ideiio builds upon the pre-existing and mature ProofID IGA product. ideiio provides a suite of IGA capabilities that can be deployed and used in a more straightforward manner by organizations of any size, although primarily targeting mid-market to enterprise customers.

# 2 Product Description

The mid-market segment is characterized by unique IAM challenges that large IAM solution providers often ignore. IAM requirements of mid-market organizations frequently fail to be on the list of primary design considerations for most (large) IGA vendors. Furthermore, it is increasingly brought to KuppingerCole's notice that SMBs also receive a low level of service and customer support compared to larger customers.

The IGA segment's mid-market requirements vary significantly due to mid-market organizations' needs to have simpler IGA deployments focusing on achieving low-cost IT efficiency. While resource availability remains a constant challenge for most mid-market organizations, the inadequate support and investment from business stakeholders for IT security adds to the growing list of challenges for IGA, which remains one of the most expensive and complicated security implementations.

Since the unique IGA challenges of small and medium-sized organizations result in non-uniform adoption of IGA technologies across organizations, there’s a growing need for IGA products and solutions that cater to simpler IGA needs that meet the unique IGA challenges of mid-market organizations. ideiio is available as a SaaS offering. ProofID, with its more mature IAM professional services and systems integration expertise, offers ideiio as a managed service. ideiio is targeted at the generic IGA needs of the mid-market segment in the EMEA and North America regions.

ideiio is designed and developed to meet the IGA requirements primarily of mid-market organizations and has achieved notable success in B2B implementations, as well as in the higher education industry.

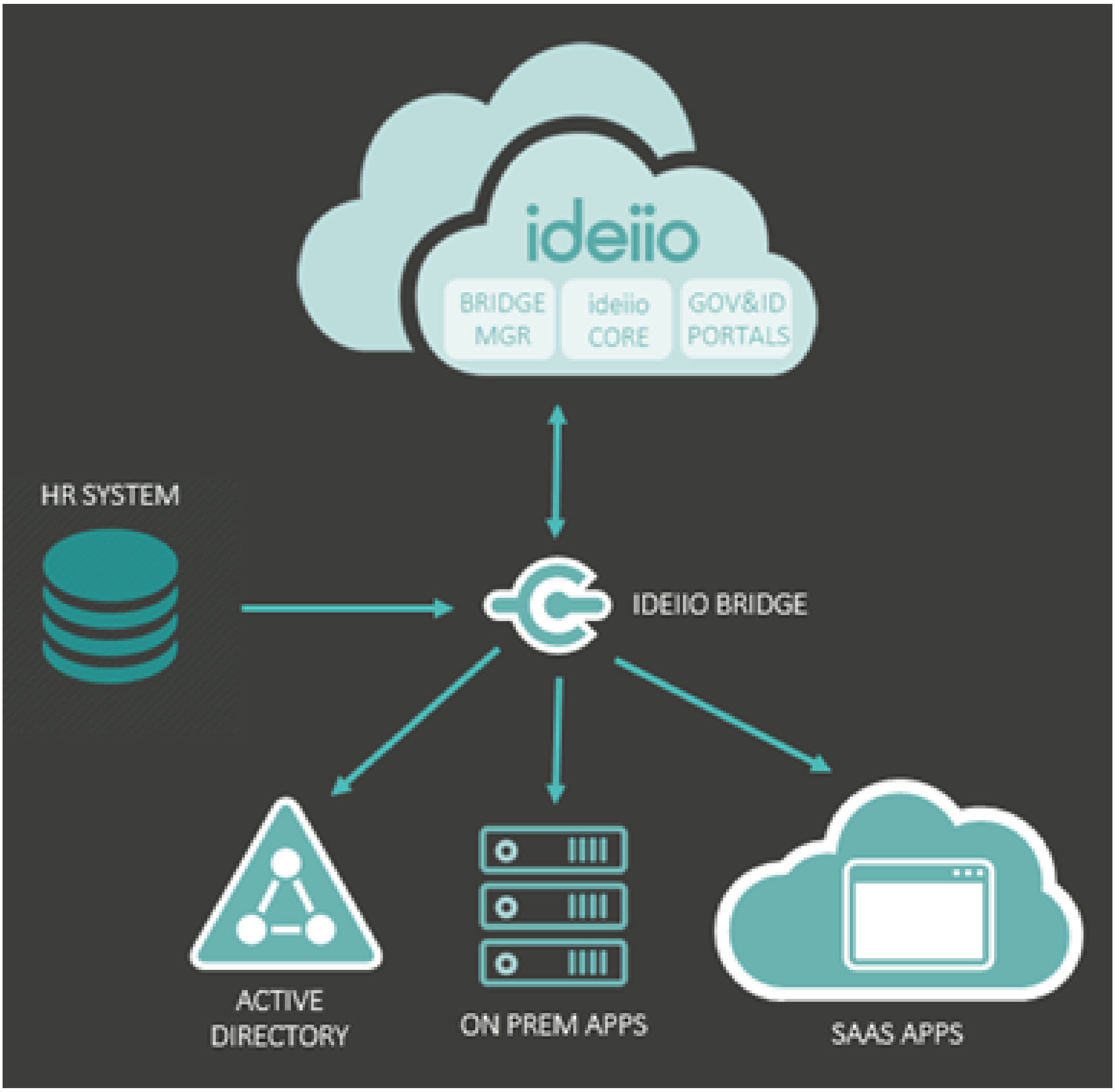

Figure 1: High-level architecture of Ideiio (Source: ideiio)

ideillo IGA Suite

The ideillo IGA solution consists of four architectural components, all of which are a part of the ideiio suite's license model, which is designed to minimize costs for the cost-conscious midmarket sector:

- ideiio Bridge & ideiio Bridge Manager
- ideiio Core
- ideiio Identity Portal
- ideiio Governance Portal

ideiio Bridge is used as the interface to both source and target application for automatic creation, updating, and deleting user accounts (Lifecycle Management). Also, the ideiio Bridge can be deployed as a standalone component for more complex Lifecycle Managementuse cases. ideiio Bridge is capable of providing bi-directional data mapping and transformations. The ideiio Bridge can be deployed on-premises or hosted in the cloud. Regardless of where ideiio Bridge resides, all of the bridge administration occurs in the ideiio Bridge Manager, hosted in the cloud. Built upon a Java and J2EE architecture framework, ideiio Bridge can integrate out-of-the-box (OOTB) with the most commonly available data source and repository types, including LDAP, Active Directory, SQL databases, SCIM, REST APIs, and other flat files (CSV) as identity stores for identity data synchronization. ideiio can act as an identity store or readily integrate with others.

ideiio Core is the web-based administrative interface in the cloud in which administrators can configure the ideiio system. ideiio Core is where the IGA functionality like role-based access control, access policies, and workflows can be configured and maintained.
ideiio Identity Portal interface also resides in the cloud and provides end-users access to their identity data and allowing them to request access to applications and is designed to be user intuitive.

ideiio Governance Portal is cloud-based and provides managers access to ideiio’s access certification functionality for governance and other compliance tasks.

### IGA Features

ideiio lifecycle management covers use cases such as synchronizing identities from HR or processing the joiner/mover/leaver scenarios. ideiio supports a wide range of popular identity repositories as well as providing its own identity repository. Schema extensions are also supported through the ideiio bridge.

Identity Lifecycle Managementto target applications is accomplished through ideiio bridge or as a standalone ideiio Lite offering, suitable for SMBs or organizations taking their first steps with Identity Lifecycle Management. Out-of-the-box on-premises Identity Lifecycle Managementconnectors provide good support for Microsoft applications like Active Directory, SharePoint, Exchange, SQL Server, or Lync/Skype for Business. Generic connectors are provided for LDAP, JDBC, Text, and SCIM. Connectors to popular SaaS applications like Azure AD, O365, AWS, G-Suite, Workday, Zoho, Bamboo HR, Orange HR, and Microstrategy are given out-of-the-box. User Lifecycle Managementcan also be automated for non-SCIM applications.

Audit information for all administrative activities is recorded, including object, subject, timestamp, action, result, and modified data. Also, an audit API is available for the retrieval of audit events. IGA reporting includes reports on access certification, group, privileged access, roles, user access, and identity matching across applications. ideiio Bridge can provide identity matching reports that can recognize common users across multiple applications based upon complex attribute filters.

User self-service capabilities are available through ideiio Identity Portal, allowing end-users to request access to applications, roles, and entitlements. The cataloging is role-based, thereby allowing users to only see and request access from a list of pre-approved resources and applications that they should be entitled to. Support for application entitlements allows ideiio to define and manage user’s access at a fine-grained level for individual applications. It can also support consumer or citizen use cases through ideiio’s selfregistration workflows. Application access can be granted without approval, or ideiio Identity Portal can be configured to have users go through multi-step approval workflows before access is granted.

ideiio access governance support covers role management and access certification through the configuration and execution of certification campaigns. Micro certification is also supported based on the expiry date and associated policies. ideiio also supports basic segregation of duty (SoD) checks based on defined policy rules. Advanced identity and access intelligence features to support risk-based analytics or advanced segregation of duty (SoD) analysis are, however, not yet supported by ideiio but are featured on their product roadmap.

ideiio supports administrative authentication via SAML, OpenID Connect, or username/password. End-user self-service authentication provides a username/password option, as well as support for OIDC in which ideiio Core can act as an OIDC server. Integrations with third party authentication systems such as PingFederate or Okta are also supported.

ideiio delegated administration gives out-of-the-box delegated administration features in which administrator permissions can be delegated to another identity for a limited period of time. Also, both policies and management of a subset of identity’s lifecycle can be delegated to a department or external organization. Users can be mastered directly in ideiio and gives the tools to accomplish this for B2B and supply chain customers as examples.

ideiio User Search provides end-user directory searches allowing end-users to look up other end users and their details such as email address or phone number. This is accomplished by leveraging the identity and their attributes within ideiio. ideiio White Pages can also be used as a added capabilitity to other directory services such as Active Directory, Universal Directory, or PingDirectory.

### DevOps Support

DevOps need support options for their tools, automation, and continuous integration processes. Integration with other systems also requires access to APIs, and developer uses APIs directly or indirectly using SDKs in application to interact with services. ideiio provides both the APIs and SDKs for this purpose.

ideiio's APIs are REST-based and provide access to most of the solution's capabilities. SDKs are available for both Java and PHP programming languages. ideiio SDKs also offer a high level of access to ideiio's functionality. An SDK is also provided for the ideiio Bridge that allows the creation of custom Lifecycle Management connectors and its transformation logic processes.

### Deployment Models and Integration Options

With the options to be deployed in the public cloud (AWS) for IDaaS IGA, ideiio offers the flexibility to be deployed in a private cloud or on-premises environment in a multi-tenant fashion, depending on the customer’s deployment preferences. Since ideiio is hosted in AWS, customer can specify their preferred region using AWS Regions and Availability zones. Data Centers are based on customer data location requirements.

Other deployment options include on-premises or a hybrid model in which ideiio bridge resides on-premises and management aspects of the solution from the cloud. A hosted managed service is also available through ideiio’s partner ProofID.

ideiio offers bi-directional OOTB integration with Ping Identity for access management. Ping Identity, with its multiple authentication methods, offers MFA for users. The integration, particularly with Ping Federate, offers a means for exchanging authentication information, user attributes, and access entitlements for a fine-grained authorization to the requested application or resources, whether on-premises or in the cloud. ideiio also provides an Identity Lifecycle Managementintegration for Okta via the Okta AP as well as integrations with other Access Management vendors through open standards such as SAML and Open ID Connect

# 3 Strengths and Challenges

ideiio is primarily aimed at mid-market customers and offers a solution that covers most aspects of IGA preferred by SMB organizations to jump-start their IAM journey. Provided as a public cloud service hosted in AWS with the option of on-premise deployment and as a managed service, ideiio addresses generic IAM requirements around identity lifecycle management, including identity fulfillment, password management, and access governance in one product. Its ‘identity bridging’ architecture approach requires additional components to be installed but facilitates faster and easier deployment options for customers to onboard IGA without much effort from the integration and service delivery teams.

The IGA capabilities offered by ideiio remain broad in scope but, unlike vendors targeting the enterprise space, relatively limited in the depth of functionality in a way that is suitable for most SMB organizations to meet their generic IGA requirements while allowing for easier and faster deployment, thereby delivering the desired time to value proposition. ideiio offers SDKs and scripting capablilities to address more complex use case typically seen in Enterprise deployments.

ideiio has some limitations but plans to include advanced support for identity analytics, advanced SOD controls, and access governance in future product releases that target primarily enterprise customers with a need for baseline IGA capabilities, as well as to enable its customers to detect and prevent identity thefts more effectively.

While most of its IGA product business is currently in the UK and neighboring countries, ideiio is actively expanding its IGA business in the US, through its development and operational facility in Colorado Springs, CO.

ideiio can cover the full-size range of businesses looking for IGA solutions, such as ideiio Lite for standalone user Lifecycle Managementfor smaller organizations, IGA & Lifecycle management utilizing ideiio core, bridge and ID portal for midmarket companies, or enterprise IGA using the full ideiio suite.

Combined with a good understanding of IGA requirements for mid-market customers due primarily to its IAM professional services heritage from ProofID, ideiio offers good coverage of fundamental IGA features to meet the distinct and emerging IGA requirements mid-market. With a strong presence in the Higher Education vertical, ideiio's technology and inbuilt workflow templates are well aligned to this sector's IGA requirements. It also finds appropriate relevance within mid-market B2B use-cases due to its straightforward deployment approach and configurable options.

ideiio presents a viable alternative to several prevalent IGA vendors for SMBs to meet their distinct IGA requirements. ideiio is becoming an established IGA vendor for mid-market organizations and should be a consideration for this IGA market and leverage its industry expertise and experience.

## Strengths

- A focussed approach to IGA for addressing mid-market IGA requirements
- ideiio Lite offers a low impact way for smaller organizations to get started with identity lifecycle management
- ‘Identity bridging’ approach enables easy extension into cloud and partner networks
- Flexible Java-based architecture
- API and SDK support for DevOps
- Good baseline IGA capabilities
- Delegated administration support for B2B use cases
- ideiio User Search provides addon value to other directory services
- Years of IAM systems integration experience
- A well thought out product development roadmap

## Challenges

- Primarily focused in the EMEA region, although increasing presence in North America
- Limited technology integrations and partner ecosystem, although growing in Europe
- Missing intelligent governance & risk insights through AI or analytics dashboards

# 4 Related Research

Leadership Brief: Typical Risks and Pitfalls for IGA Projects - 72580
Leadership Compass: Identity Governance and Administration – 80063
Leadership Compass: Access Governance and Intelligence - 80098

# Content of Figures

# Copyright

©2020 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 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 back 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.