KuppingerCole Report

WHITEPAPER

By Paul Fisher

July 02, 2021

The future of IAM lies in the cloud and as a service

IAM software and tools have traditionally been installed and run on-premises by the organization itself. In recent years, the growth in identities operating across cloud and digital services has seen vendors offering IAM solutions as a service to assist with this growing complexity and concomitant security challenge. This IDaaS market, with its ease of adoption and cloud-native integrations, is slowly overtaking the on-premises IAM market.

But even while the flexibility, security and scalability of IDaaS makes sense for many businesses, a third option is becoming popular. This is IDaaS designed by a third-party integrator using best of breed identity components to build an IAM solution that is bespoke to operational and budgetary requirements and can also be operated by the integrator if the customer chooses.

By **Paul Fisher**
pf@kuppingercole.com

Content

1 Introduction

At its most fundamental, Identity and Access Management (IAM) software provides secure access to services, applications and data centres located across an organization. In modern digital organizations the identities of those seeking access can belong to users, customers, applications and IoT devices.

IAM software and tools have traditionally been installed and run on-premises by the organization itself. In recent years, the growth in identities operating across cloud and digital services has seen vendors offering IAM solutions *as a service* to assist with this growing complexity and concomitant security challenge. This IDaaS market, with its ease of adoption and cloud-native integrations, is slowly overtaking the on-premises IAM market.

Identity as a service (IDaaS) refers to services provided via the cloud or through SaaS (software-as-a-service) systems for identity and access management. It provides cloud-based authentication provided and managed on a subscription basis by third-party providers.

But even while the flexibility, security and scalability of IDaaS makes sense for many businesses, a third option is becoming popular. This is IDaaS designed by a third-party integrator using best of breed identity components to build an IAM solution that is bespoke to operational and budgetary requirements and can also be operated by the integrator if the customer chooses.

With IDaaS vendors slowly bridging the gap with traditional on-premises IAM software in terms of depth of functionalities, they now present a strong alternative for organizations to replace existing on-premises IAM deployments. The market is seeing different demands. There are those organizations that may be at the start of IAM journey and happy to subscribe to a fully managed service for all its identity management needs.

Then there are those, often larger, organizations, which have already invested in on-premises IAM platforms integrated with legacy IT but wish to add IDaaS for newer identity projects or replace legacy systems altogether. They will be looking for frictionless operation between the two. We will discuss these options and offer guidelines for choosing the right provider further in this Whitepaper.

Some identity vendors are already supporting pre-configured cloud based IDaaS services for Access Management, single sign-on, user provisioning, mobile identity, compliance, and both multi-factor and adaptive authentication.

Given the increased complexity of managing identities across multi-cloud infrastructures, on-premises, and remote locations it makes sense to outsource identity management for many tasks and users, leaving the choice of authentication protocols to IAM experts. The good news is that multiple options now exist for customers to manage identity more efficiently in the hybrid and mixed IT environments that proliferate today.

2 Highlights

- Why for IAM to operate at maximum efficiency it should be designed as part of an Identity Fabric model based on KuppingerCole's principle.
- As digital transformation continues apace, many organizations are struggling to cope with rising numbers of identities.
- IAM sometimes gets left behind is because IT and Security management tiers are left out of the digital decision-making hierarchy.
- The shift to cloud, IaaS, SaaS means that legacy IAM struggles to keep up with identity demands and IDaaS is one solution that organizations should consider.
- With the increase in demand for secure access and authentication right across the extended enterprise, the limitations of multiple platforms and glued together authentication protocols will become more pronounced.
- Outsourcing IAM relieves the burden of technical support and maintenance from in-house teams that may already be stretched.
- If required, IDaaS can also be run as a managed service by a third party further reducing cost and transferring all security and maintenance responsibilities to the provider.

3 Identity and Access Management in a digital landscape

It is clear to KuppingerCole that Identity is central to the efficient and secure operation of digitally transformed businesses. After all, in the expanding universe of digital organizations everything is connected and co-dependent, and all the functions within are dependent on someone or something granted access to digital tools they need to their job.

Add the threat of unauthorized access and resulting cyber-attacks from bogus identities to the blend, it is apparent that IAM assumes a new frontline role in protecting the organization.

Identity Management in the digital landscape in modern organizations must fulfil two fundamental tasks: facilitate the efficient flow of authentic identity and protect the business from the threats contained in unauthorized access.

3.1 The Identity Fabric and IAM

KuppingerCole has identified that for complex, modern enterprises to operate closer to optimal efficiency, and for employees to achieve greater productivity, IAM architectures should be underpinned by an Identity Fabric model. This unifies a core set of Identity focused services that perform Authentication, Access Management, Identity Management and Access Governance. These are connected to users, applications and data sets via clusters of connectors, scripts and, increasingly, APIs.

The precise structure of an Identity Fabric will be determined by analysis of the major capabilities required by an organization, which should be based on specific IAM use cases (such as managing access of customers to an ecommerce system) and the required technical capabilities.

Ideally the capabilities required by the organization will be delivered in a digital architecture that includes containers, Kubernetes and microservices. However, in many organizations this type of environment will be shared with legacy architectures which will require an Identity Fabric design that can manage access across both. For an Identity Fabric to meet desired lean business goals (delivering maximum value), it must be capable of adapting to existing IAM processes in legacy environments as well as full digital environments -- and to move those legacy components into full digital environments at some stage. To do this successfully may be beyond the scope of many organizations and who look for managed services to operate at least some parts of their Identity Fabric.

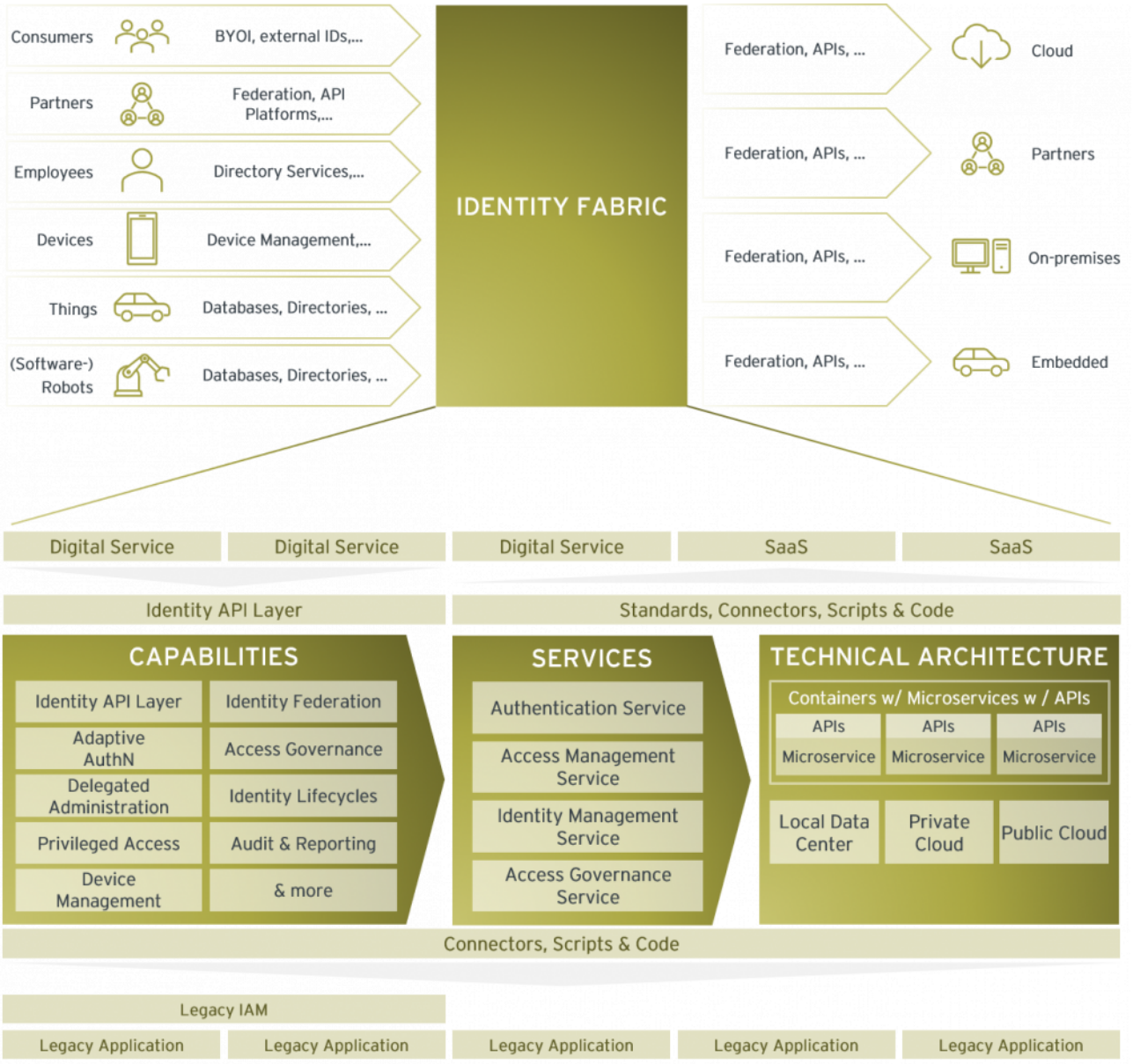

Figure 1: An Identity Fabric sits at the heart of an organization and its design will enable all types of identities to connect to services, data and applications (Source: KuppingerCole).

3.2 The complications and the challenges for IAM in digital environments

While the Identity Fabric remains the model for IAM, many organizations will find themselves already challenged by the demands of access management as their organizations become more digital. Often the process of digital transformation is led by LOBs who do not always consider the security and access management challenges it brings as a side effect. But to truly benefit from the perceived gains of digital transformation, organizations need to ensure IAM processes are in tune with the changes being made elsewhere.

Those changes will be in IT and business processes and include new development processes and delivery models, increased pace of innovation, rapid and continuous software development through the emergence of agile DevOps teams, automation, ubiquitous collaboration tools, enhanced data governance, customer access to networks and cloud delivery of services. Additionally, organizations are beginning to invest in projects based around Big Data, IoT, machine learning and Artificial Intelligence to further their digital transformation journey.

All of this creates exponentially growing types and amounts of data which require innovative applications & business models. It also rapidly introduces new and increased numbers of identities that need access to new digital assets forged in the heat of transformation, as well as the legacy infrastructure that in many cases sits alongside.

Importantly, the identities will not only be those of regular employees but also those of partners in the supply chain, contractors, customers. To those we can add in non-human identities such as applications, service accounts and IoT devices.

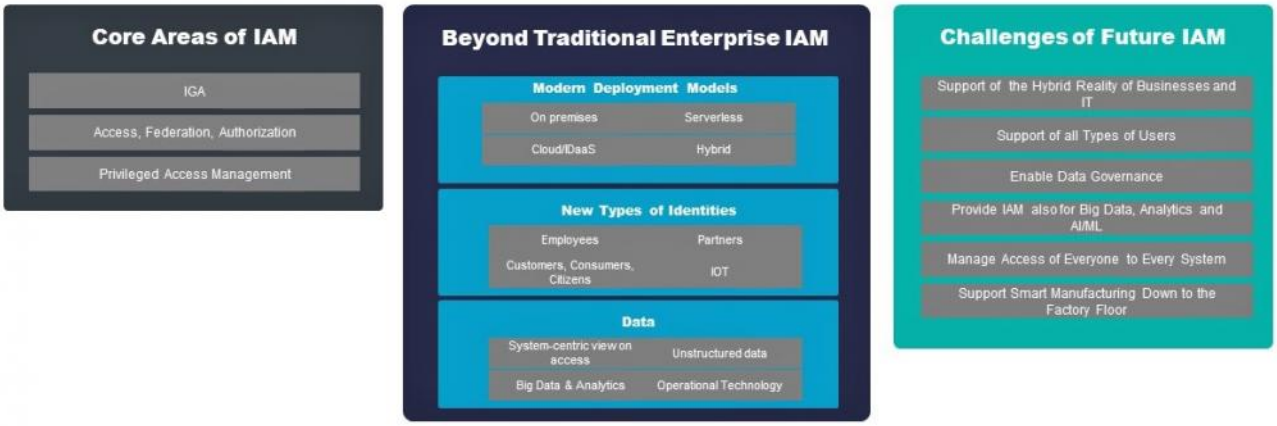

Figure 2: From core tasks to future challenges, how IAM is evolving to meet the demands of digital transformation happening in modern organizations (Source: KuppingerCole).

3.2.1 Numerous authentication protocols add to IAM challenges

Authentication is a core component of Identity and Access Management (IAM) and enabled by several different protocols on which the authentication and authorization process can be designed. Digital transformation has increased the need for robust standards that can work with remote working, multi-cloud environments, IoT, APIs and DevOps. Currently there are nine major authentication protocols in use, each with strengths and weaknesses, some are compatible with others, some not. Most are based on open-source designs making them adaptable and interoperable.

With such choice available it is probable that many organizations will find parts of the organization use different authentication protocols to others as in-house engineers or those leading an IT procurement have favoured one protocol over another. This mix of authentication protocols will have undoubtedly been created during incremental adoption of various IAM tools and platform by different departments and managers over the years. This is a normal condition for most modern organizations as they grow and adapt but it is not an ideal position as the organization must rely on all these platforms and their protocols to communicate without friction to services and resources and rely on IT engineers to ensure that workarounds are found when they do not.

This is not necessarily a problem if it is managed well, and that access is not delayed or prevented. But *managing* is the operative word, and this can consume a lot of time when things do not work out and it may be that the organization finds this web of different protocols and IAM platforms difficult to manage. Remember also that some of these protocols are now thirty years old and were written for very different times.

Work continues by Identity Providers, open-source communities, and the wider industry to update these protocols to make them more secure and better performing in today's fast paced hybrid environments. The addition of biometrics, multi-factor authentication (MFA) and encryption over time has also strengthened authentication but there is always room for further development. Increasingly, technology like the protocols at the heart of IAM platforms may prove too granular for fast moving organizations to think about, preferring to leave that choice to IDaaS providers where the solution is simply expected to work, and let people get on with their jobs.

3.2.2 Changing traditional attitudes to managing identities in business environments

As identities multiply, organizations need to rethink their approach to IAM. With the increase in demand for secure access and authentication right across the extended enterprise, the limitations of multiple platforms and glued together authentication protocols will become more pronounced.

The adoption of Identity Fabrics is desirable if business and IT leaders are to enable access by everyone and everything to every service as required, with security and without latency. This requires, ideally, one single, integrated, and highly scalable IAM platform for current, emerging and future digital services that are the desired outcome of digital transformation. Such a platform must also be capable of bridging to existing IAM tools, if they need to be retained for operational reasons, and to legacy IT stacks and applications, data and services.

But it also means making some tough decisions on unifying IAM and changing some long-held ideas about securing identity in the workplace. For example, the idea that employee and customer identity management should remain segregated from a technology and process perspective. Traditional security thinking has always been about separation to prevent unauthorized access or infection by malware. The problem is that modern business practice in many sectors requires that customers are brought right into the business and allowed direct access through CIAM.

While organizations need to integrate consumers into the system in compliance with regulations, this is made even more challenging by the fact that consumers increasingly want to retain control over their identity by bringing their own identity (BYOI). Organizations thinking about the future of identity will have to take that into consideration and plan accordingly to ensure they can use identities maintained by third parties.

The same is true of third parties, vendors and supply chain partners. Separating all these identities is time-consuming, calls for a duplication of IAM efforts and will undoubtedly result in technical redundancies and inefficiencies when adapting to new business requirements. And of course, organizations must adapt to and manage all the new identities from things, machines and applications. For many organizations this will mean a rethink and investigation of the potential of IDaaS that fulfils the principle of the Identity Fabric, and fully reshapes how IAM is conducted.

4 The Advantages of IDaaS for business

IAM is shifting from an IT security-based exercise and a supporting function for the business to one that sits at its core and dynamically facilitates the flow of identities through the organization, much like the heart regulates blood flow through the body into its constituent parts.

This also changes the responsibilities on vendors, consultancies, and system integrators involved with IAM, transforming their role from a technical function to a business play. Only when understanding the business cases, can the transformation of IAM, and by extension, IDaaS be done right.

There are immediate business advantages to deploying IDaaS in the enterprise. These include:

- Outsourcing IAM relieves the burden of technical support and maintenance from in-house teams that may already be stretched.
- The absence of on-premises installation and deployment lowers Total Cost of Ownership (TCO) while reducing Time to Value for the IAM platform.
- IDaaS can be run on AWS or other cloud services removing the need to host on in-house servers or data centres
- If required, IDaaS can also be run completely as a managed service by a third party further reducing cost and transferring all security and maintenance to the provider.
- The organization benefits form automatic software updates and access to expert knowledge from IDaaS providers.
- Identity provided as a service is likely to deliver best in breed capabilities that would be hard to deliver in a home grown IAM platform.
- IDaaS provides SSO access for users from any end point as authentication is processed in the cloud.
- A hosted IAM service can grow and adapt to the changing needs of an organization.
- With modern IDaaS access features, there is no need for end-users to remember multiple account credentials.
- System administrators can reduce the number of user accounts they have to manage.

The shift to a services-based model will require a change in the way IAM is deployed to a centralized model capable of supporting both outbound and inbound services or microservices delivered in a variety of ways.

IDaaS companies supply cloud-based authentication or identity management to enterprises through subscription plans. It allows enterprises to use single sign-on, authentication, and access controls to provide secure access to their growing number of software, services, data centres and other SaaS applications.

5 IDaaS delivery services from iC Consult

iC Consult is a specialist IAM integrator that for nearly 25 years has provided IAM solutions to organizations looking to shift Identity Management to the cloud as part of digital transformation. The company has around 350 consultants with offices in German-speaking countries, UK, USA, China and elsewhere.

5.1 Two levels of IDaaS from iC Consult

iC Consult offers two IDaaS solutions as part of its consultancy services. For those customers that are new to IDaaS or IAM it offers standard IDaaS with a choice of leading off the shelf IDaaS platforms such as Okta, Sailpoint or others. The company then integrates and adapts these into the client IT landscape as part of its offering. This gives the client the ability to leverage the full platform without any deployment learnings and get continuous support from an iC Consult Customer Value Manager. It also means that new features are handled by the provider in a standard MSP manner, leveraging new features provided by the IDaaS platform to create immediate value for the customer. The company also offers support for integrated applications etc. on top of the vendors basic support for the platform.

An advantage of this approach is that iC Consult can choose from the wider IDaaS market, maintaining vendor independence to find the right IDaaS solution for clients. Customers benefit from the company's core competencies in IAM architecture and design as well as IAM implementation and integration. The service is well suited to mid-size to larger enterprises and fast-moving organizations that have less time to spend on procurement and configuration of IAM. Larger enterprises may look to iC Consult to design IAM for hybrid architectures, too. The second option is to run the entire platform as a managed service from the ServiceLayers cloud on behalf of the customer and is outlined in detail below.

5.2 iC Consult Service Layers: Identity and Access Management as a Managed Service

The Service Layers platform takes the IDaaS model a stage further by offering the IAM consultancy services described above but delivers the final IAM design as a Managed Service to the client. Based on a combination of ForgeRock, Ping Identity and One Identity solutions, Service Layers boasts a range of other technologies for delivering integrated, customized services from various IaaS (Infrastructure as a Service) platforms such as AWS (Amazon Web Services), Microsoft Azure or Google Cloud Platform (GCP).

The Service Layers approach is to build on best-of-breed products, fully automate the infrastructure deployment and management ("infrastructure as code") and the configuration ("configuration as code"), which allows for rapid deployment and customization on behalf of the client. Unlike some IDaaS vendors\' common approach, Service Layers uses dedicated instances for each customer, so no runtime components are shared across customers. Thus, Service Layers can automate the infrastructure and configuration management, resulting in a cost reduction for operations compared to traditional, manual operating models.

The entire architecture is based on microservices and containers making it modern and flexible. Microservices allow for defining small, functional blocks with well-defined APIs and flexible reusability. Such microservices as well as the pre-configured services of the applications used are packaged into containers, orchestrated by Kubernetes. These can be run on various types of infrastructures, including private and public cloud environments.

Based on that, Service Layers delivers a managed service platform that not only consists of IAM tools but also the entire runtime environment. This includes:

- Underlying cloud infrastructure and operations environment
- Functional components, based on best-of-breed products with extensions by Service Layers
- Customizations
- Defined processes for efficient operations of the entire infrastructure

Service Layers is designed for large enterprise clients and medium-sized businesses. Data centres and operations are available in various regions, including GSA (Germany, Switzerland, Austria), Russia, China, and the U.S. The ability to provide regional IAM Managed Services source with hosting locations in the China and Russia markets is considered a unique selling point.

The company counts manufacturing among its customers, which frequently have factory plants in some or all these regions and countries as well as a large customer base, and which need consistent IAM and CIAM services and operations across these regions.

Due to delivering the service on microservices and container-based architecture, Service Layers also integrates a consistent DevOps approach, allowing for agile delivery and enhancements of the service for developer environments. This includes features such as CI/CD pipelines, auto-scaling and more. Service Layers focuses on full automation of both the delivery pipeline and operations, by making use of common, modern DevOps infrastructure components. These include: Gitlab, Helm, Docker Containers, Kubernetes, Swagger, and many more. For various functional capability enhancements and customizations, additional established infrastructure components such as Elasticsearch or PostgreSQL are used.

While Service Layers provides a high degree of component re-use amongst customers and thus efficient delivery, data is fully segregated, and deployment and configuration options remain flexible due to separated deployment instances for each customer. Customers can decide the following:

- The deployment model and cloud to use
- The level and availability of support
- The amount of customization

The deployment/service can also be done directly into the customer's preferred cloud infrastructure. This helps customers to apply their governance and compliance rules as well to get better pricing conditions from their existing Cloud providers.

Service Layers standardizes operations, patch management, and other services across all customers, based on their automation approach, reducing costs for all clients. Furthermore, each customer instance is supported by a defined project team for both customization and operations.

Other notable features include quick and easy access to online properties. This includes registration via social and mobile login, multi-factor authentication (MFA), and integrated self-services for a first-class user experience. Service Layers provides the basis for quickly onboarding new colleagues and efficiently assigning or adjusting all authorizations.

Fast logins, MFA and extensive user self-administration improve user performance and simultaneously reduce the service desk's workload. A customizable role management system automatically grants employees the authorizations they need while protecting sensitive data.

6 Recommendations

KuppingerCole Analysts believe that IAM must evolve to become a background service akin to a utility that is easy to consume and flexible in supporting emerging business requirements. Not all organizations will be able to attain this goal immediately but IDaaS goes some way close, while a fully managed IDaaS setup goes a step further for many organizations. We recommend that organizations take the following steps in planning their IAM requirements:

- If you are starting with a clean slate assess your IAM needs now and in the future, and plan accordingly.
- Identify the gaps between the current and desired state of IAM in your organization.
- Identify which existing technologies, if any, can be used and whether these need to be migrated to a services-based model and plan for a phased migration.
- If current IAM platforms, policies and software look as if they will not meet future requirements, be prepared to junk.
- Ensure that any replacement solution fits the organization, its culture, risk and security parameters, and dominant IT architecture.
- Put Identity Access at the heart of your organization by adopting the Identity fabric model as designed by KuppingerCole.
- Accurately understand the types of identities that must be served after digital transformation, which may include customers, vendors, and non-human things (IoT).
- Remember the types of Identity in usage may change over time and any IAM platform must be adaptable enough to accommodate these.
- Identify and quantify your organization's capacity to procure, deploy and run IAM across the entire organization and be bold about any resource limitations.
- Allow for the specific requirements of DevOps and other specialists to be incorporated into any IAM platform.
- Analyse how IAM will operate within hybrid IT environments including cloud, networks and IaaS services
- Decide if you can manage Identity on-premises, IDaaS or as a fully managed service from a service provider.

- If necessary, bring in a consultancy to advise on your IAM strategy.

KuppingerCole can assist you with these tasks. Talk to one of our KuppingerCole expert advisors on how to perform maturity assessments, organize IT departments, and choose the right IAM solutions for your environment.

7 Related Research

Buyer's Guide: Consumer Identity and Access Management Solution - 80111
Architecture Blueprint: Hybrid Cloud Security - 72552
Advisory Note: Cloud Services and Security - 72561
Buyer's Guide: Consumer Identity and Access Management Solution - 80111
Insights: Identity and Access Management
Leadership Compass: Access Management - 800257
Leadership Compass: Access Governance & Intelligence - 80098
Leadership Compass: Access Management & Federation - 71147
Leadership Compass: API Management and Security - 70311
Leadership Compass: Cloud-based MFA Solutions - 70967
Leadership Compass: Consumer Authentication - 80061
Leadership Compass: IDaaS Access Management - 79016
Leadership Compass: Identity API Platforms - 79012

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.