KuppingerCole Report

EXECUTIVE VIEW

By Richard Hill
November 16, 2021

Simeio Identity Orchestrator

Simeio Identity Orchestrator (IO) is a solution that helps integrate and orchestrate other IAM solutions while also adding a series of own capabilities. Simeio IO allows customers to connect and direct their existing IAM infrastructure in a modern and more efficient way. Using Simeio IO, customers can converge existing IAM siloed solutions that Simeio can then operate as an MSP or IDaaS. Simeio IO offers improved application onboarding, IAM analytics, with a unified single pane of glass and mobile application.

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

Content

1 Introduction

IAM (Identity & Access Management) today is at the core of enterprise IT infrastructures when it comes to protecting digital corporate assets. IAM, as the name states, is about managing identities and their access. This involves managing user accounts and their entitlements across various systems and applications in use throughout organizations.

Over the past several years, organizations have been facing multiple changes affecting their security posture. The perimeter that separated the internal network from the outer world does not have the same relevance before, with mobile users accessing internal systems, integrating business partners and customers into business processes, and shifting 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 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 a hybrid nature while facing ever-increasing attacks forces organizations to take action. Protecting against internal and external attackers requires a well-thought-out understanding of risks and countermeasures.

IAM is a core component in every security architecture. IAM "done right" ensures that identities, credentials and authenticators, and access entitlements are well-managed. IAM thus reduces the attack surface by helping organizations move towards the "least privilege" principle. IAM provides the tools to automate processes around managing users and access entitlements and regularly reviewing these and identifying, e.g., excessive entitlements.

On the other hand, IAM also plays a vital role in business enablement when it comes to the needs of employees, contractors, business partners, and customers to access specific applications, systems, and data. IAM is the tool for implementing the workflows and automated processes for onboarding users and granting them access. Again, if done right, IAM can help organizations by optimizing the onboarding and change processes, ensuring that entitlements are revoked and that accounts are deleted or deactivated once they are no longer required.

Under the umbrella of IAM, we can differentiate between the "core IAM" or -- as it is called frequently today -- IGA (Identity Governance and Administration), and the broader definition of IAM, which includes additional capabilities such as Privileged Access Management, Web Access Management, Identity Federation, and more. IGA, in fact, is an umbrella term for two of the core elements of IAM, which are Identity Provisioning and Access Governance. Identity Provisioning supports automating processes for creating and managing user accounts and their high-level entitlements across various systems and applications in use. At the same time, Access Governance adds the governance layer for analyzing entitlements, regular reviews, recertification, and efficient access request workflows. However, other capabilities such as Access

Management are of equal relevance.

Over the past few years, we have seen a shift from traditional IAM deployments that run on-premises towards IDaaS. IDaaS is one of the fastest-growing market segments of IAM characterized by the cloud-based delivery of traditional IAM services. The market, primarily driven by web-centric use-cases in its early days, now offers full-fledged 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 metrics 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 number of vendors. However, under the umbrella term IDaaS, we find a variety of offerings. IDaaS, in general, provides Identity & Access Management and Access Governance capabilities as services, ranging from Single Sign-On to full Identity Provisioning and Access Governance for both on-premise and cloud solutions. These solutions can also vary in their support for different users, such as employees, business partners, and customers; their support for mobile users; and their integration capabilities back to on-premise environments.

In this executive view, we discuss how Simeio's Identity Orchestrator can help create a unified IAM infrastructure by connecting and directing other IAM solutions across all areas, from Identity Lifecycle Management (ILM) to Access Management and Privileged Access Management (PAM), with a range of capabilities provided as part of the Simeio solution itself.

2 Product Description

Simeio is a US-based vendor in the IAM market, delivering their Simeio Identity Orchestrator as a solution that supports customers in orchestrating IAM solutions that they have in place or that they deploy in addition to their current solutions. Thus, Simeio Identity Orchestrator (IO) is not a full-fledged IAM suite that delivers each and every capability on its own, but -- as the name indicates -- an orchestration platform. Moreover, Simeio IO adds a range of capabilities beyond what standard solutions provide.

The focus of Simeio IO is multi-fold:

- It allows the integration of multiple IAM services into a unified solution, e.g., coordinating and addressing use cases spanning numerous areas of IAM.
- It enables the replacement of some IAM services through the ability to orchestrate with different solutions, and -- even more important -- by adding a consistent layer on top of other vendor solutions.
- It simplifies customization by providing an API layer across multiple services. This also abstracts the underlying services. Thus, customers afterward can migrate the underlying IAM systems with limited impact on user experience and integrations to other systems. Consistent APIs will reduce the need for code changes in dependent services.
- A single Simeio IO deployment can work across multiple solutions, regardless of deployment models, simplifying deployment and operations.
- It allows customers to move away from siloed IAM infrastructures toward a unified platform, which aligns well with the "Identity Fabrics" paradigm defined by KuppingerCole.
- Allows for the automation of manual tasks and policies for monitoring and remediation of malicious actors and events.

Simeio has grown significantly and has become a contender in the IAM services market, with more than 600 employees, operating in more than 60 countries, and owning multiple Security Operations Centers (SOCs) for running the IAM operations of their customers.

Simeio is distinguished from other vendors that offer integration platforms or, more commonly, integrated offerings spanning multiple IAM tools, in both the breadth of their own capabilities provided, and in the breadth and number of IAM solutions supported. Simeio IO comes with integration capabilities for about one dozen IAM vendors, covering all major areas such as:

- IGA (Identity Governance & Administration)
- Access Management
- PAM (Privileged Access Management)
- Risk Intelligence

Simeio IO bridges the gap many organizations today have with multiple IAM siloes: both horizontally with PAM, IGA, and Access Management being implemented and operated independently and vertically across different identity repositories containing workforce, business partners, and consumer identities.

Many of today's use cases overlap. Identity verification and self-service registration might apply to both customers and certain groups of partners. In contrast, other partners such as contractors are frequently closer to their own workforces in their processes. On the other hand, dealing with first-line worker access might be closer to customers in the methods applied than to other members across the workforce. Thus, integrated approaches provided by Simeio IO can significantly increase efficiency and reduce complexity in IAM infrastructures.

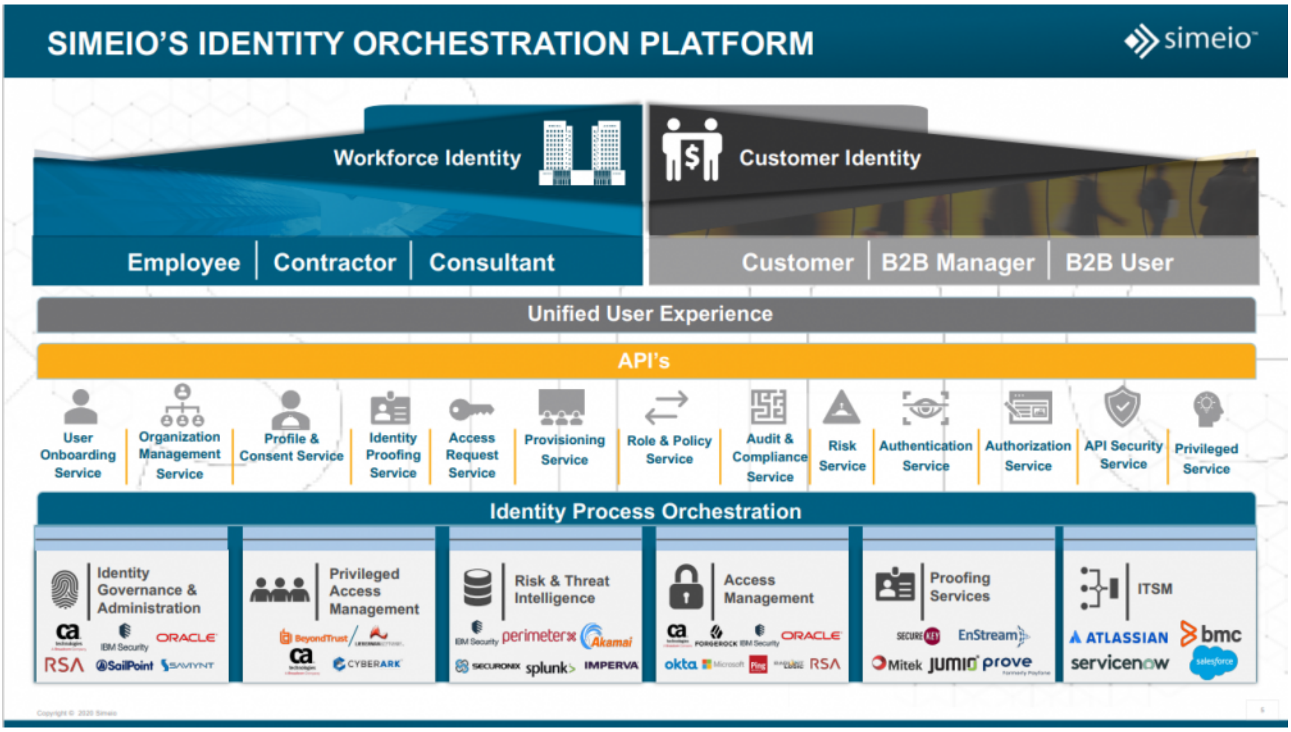

Figure 1: The architecture of Simeio Identity Orchestrator (Source: Simeio)

Product Architecture

From a product architecture perspective, Simeio IO comes with integrations for both existing IAM solutions and applications, based on what Simeio calls their plug-in framework. Simeio IO then provides a range of unified services, from administration and governance to a service tier that supports, for example, RBAC (Role-Based Access Controls), authentication, and the underlying framework composed of other security services, databases, and other capabilities. Below that is a unified data tier that maintains data that is used throughout various integrations and target applications.

Simeio utilizes a microservices architecture to deploy its capabilities and exposes them via REST APIs. The Simeio IO web UI and mobile app are built on this layer of APIs and customized REST API clients can also interface with this layer too. For example, this allows for the creation of digital services based on standard identity services provided by Simeio IO while mitigating the risk of changing these digital services when some of the underlying integrations change. Simeio IO, in essence, creates an abstraction layer. With this approach, Simeio IO presents a unified platform for IAM that can integrate their customers' current IAM landscapes and thus also support gradual migrations to modern Identity Fabric architectures. The Simeio IO approach minimizes user interfaces such as user self-service facilities and applications that consume identity services.

New Simeio IO Capabilities

Simeio IO continues to innovate and simplify the application onboarding process with its recently introduced *NextGen Application Onboarding* service as an end-to-end automated onboarding capability that runs on its orchestration platform. The service allows for the distribution of application ownership through a self-service process. Made simple is the ability to pull information from a configuration management database (CMDB) or other centralized information locations. Simeio provides predefined access request questionnaires for applications access requests with information prefilled from the CMDB and the ability to customize layers of the questionnaire. Permissions can also be defined, allowed groups made visible, and entitlements imported via REST-based connectors as needed. Workflows, such as manager approval or manager and resource owner approval, can be selected. Provisioning options are available for both connected and disconnected applications. For connected applications, a JSON file with configuration parameters, data mapping, etc., can be used with the REST-based connectors. Similar questionnaires can be used for the PAM and SSO capabilities as well.

The Simeio *IAM Analytics* takes an analytics and remediation perspective. For example, an organization using a third-party IGA solution like SailPoint or Saviynt can use the analytics capabilities through the Simeio IO integration providing a cross-services and cross-platform analytics solution. On the near-term roadmap is remediation features across various identities as Simeio continues its focus on increasing its aggregate identity store capability. Remediations could come in the form of identifying the need to make policy changes to remediate events like high authentication failures or SoD violations, for example. Simeio can use the logs and events from the other integrated third-party AM, IGA, and PAM solutions to identify issues and remediate them. The Simeio IAM Analytics also gives visibility into IAM KPIs and tracks ROI. Views into the analytics results allow for pre-configured and persona-based dynamic dashboards.

Simeio also offers a more unified UI that gives a single interface for all IAM services under its control, including integrated third-party IAM solutions. The third-party IAM solutions like Saviynt, CyberArk, or Ping

Identity, can be plugged into the Simeio IO platform using connectors. Once a third-party solution is plugged in, the capabilities of that solution can be turned on or off, configured, and defined rules within the Simeio IO UI. This capability allows organizations to orchestrate the underlying IAM solution while making the aggregated functionality seamless to the users. User self-service and admins can request application access from a catalog and track the approval process through the UI. Simeio also provides a mobile app to allow users to request and view the process details and enable management to approve requests from the same mobile app.

Integrations, Deployment and Delivery Models

Simeio IO provides a solid ability to integrate with other third-party solutions across the IGA, Access Management, and PAM verticals. For IGA, Simeio IO can integrate with other third-party IGA controls such as Saviynt, RSAS, Oracle, and SailPoint using SCIM, REST, or Custom APIs. Integration models for external access management solutions like Ping Identity, ForgeRock, Okta, and Microsoft are accomplished using SAML, OAuth, or WS APIs. Regarding PAM, Both CyberArk and BeyondTrust can be integrated with Simeio IO using a SOAP or REST API and access via a command-line interface (CLI).

Notably, implementation of Simeio IO still will require system integrator work and customization. Still, Simeio has extensive experience dealing with the rapid orchestration of a significant number of leading IAM solutions in the market.

Simeio not only provides the technology but also acts as the operator as well. Thus, deployment can be part of a managed services package, with existing solutions still running on-premises and Simeio working as MSP (Managed Service Provider). Simeio can also operate all services as cloud-delivered IDaaS on behalf of customers. As is common practice, Simeio provides SLAs for availability, response time, resolution time, and performance in these models.

3 Strengths and Challenges

Simeio IO follows a well-thought-out approach for adding a centralized layer on top of existing IAM solutions. This enables orchestration amongst multiple solutions by abstracting these functions. However, Simeio goes beyond merely integrating existing solutions and adds a range of their capabilities in a modern microservices architecture.

A strength of Simeio IO is the broad support for existing IAM solutions and their partner ecosystems. Its identity process orchestration allows for tie-ins to the identities of its many third-party integration partners. Simeio IO\'s ability to abstract the functionalities of the third-party solution with is UI driven and executed through its APIs and microservices gives the ability to provide the functionality through Simeio IO\'s web and mobile UIs. This allows customers to unify existing solutions into a common IAM infrastructure while facilitating the gradual migration of underlying IAM services. Thus, deployment and management complexity can be reduced while flexibility for modernizing the existing IAM infrastructure is greatly enhanced. Simeio IO aligns well with the KuppingerCole Identity Fabrics paradigm as a foundation for modern IAM infrastructures.

Simeio also acts as the MSP or IDaaS provider, depending on the target operating model chosen by the customer. Thus, customers can get full service from Simeio, complete with Simeio's own technology and deployment and operations services.

Customers should be aware that Simeio IO is not a full-fledged IAM suite that supports every capability by itself but also requires underlying solutions. Furthermore, integration of existing products, despite the standard support, will commonly require some level of customization, specifically for legacy IAM solutions that have been heavily customized over time. However, Simeio IO continues to make progress on simplifying the integration and controls over those underlying third-party solutions.

Overall, Simeio IO is a well-thought-out solution for orchestrating existing and new identity services, helping customers move away from siloed solutions allowing customers to optimize and modernize their IAM infrastructures more efficiently.

Strengths

- Well-thought-out approach on orchestrating existing IAM products.
- NextGen Application Onboarding service
- Broad partner ecosystem, involving many of the established vendors.
- Improved analytics with future remediation capabilities
- Consistent set of REST APIs for abstracting vendor solutions from applications that consume IAM services, and from the user interface.
- Unified single pane of glass UI and mobile app
- Provides a single sign-on experience across all IAM services.
- Simeio acts as a product vendor with an independent roadmap, while also operating as MSP and IDaaS.

Challenges

- Though they are active in most regions, the primary market of Simeio is still North America, with a good ability to execute in that region; however, it has a limited system integrator partner network on a global scale
- Some limitations for DevOps support (CLIs, SDKs), although REST APIs are available
- Despite having a broad partner ecosystem, not all IAM products are supported out-of-the-box.
- Deployment might require a varying level of customization, depending on the type of and state of solutions to be integrated.

4 Related Research

Executive View: Simeio IAM for SMB - 79071

Leadership Brief: 10 Top Trends in IAM -- 80355

Leadership Brief: Access Reviews Done Right - 80195

Leadership Compass: Identity Governance & Administration 2021 - 80516

Leadership Compass: Identity as a Service (IDaaS) - IGA - 80511

Leadership Compass: Identity Fabrics - 80514

Market Compass: IGA Solutions for ServiceNow Infrastructures - 80515