STRATA
Identity Orchestration

THE COMPLETE GUIDE

What is Identity Orchestration?

> *In the future, vendors who are not doing the orchestrating will simply end up being orchestrated.*
> *- Gartner®[1]*

Multi-cloud identity management is hard. What if it doesn't have to be?

Identity and access management (IAM) today is at an enterprise's core. Everything runs on apps, and apps depend on identity. Global IT security spending in IAM **is expected to reach $16.7 billion by the end of 2023 (up from $12.3B just three years earlier)**, demonstrating the growing demand for solutions that address the challenges of multi-cloud and hybrid cloud.

With cloud adoption proliferating, identity data is everywhere. The new distributed reality of using multiple clouds and multiple identity service vendors makes for a complicated computing environment. Applications are scattered on private and public clouds as well as legacy on-premises IDPs resulting in security gaps, authentication issues, and poor user experiences.

Centralizing identity management into a single system is no longer an option because of the cost, complexity, and vulnerabilities that are inherently created.

Many identity and access management solutions were built for problems of the past. A new approach to managing identity that makes identity architectures simpler, more flexible, and less tightly bound to any single identity service vendor is the only viable solution.

Enter: Identity Orchestration.

We'll explore what Identity Orchestration is, how it works, where it fits in the IAM ecosystem, and the benefits it provides.

[1]Gartner, Innovation Insight: Journey-Time Orchestration Mitigates Fraud Risk and Delivers Better UX, Akif Khan, 10 June 2022

What is Identity Orchestration, and why should you care?

Identity Orchestration is a new, standard-based, software approach for managing distributed identity and access management (IAM). Through an abstraction layer, organizations can integrate multiple identity systems or providers (IDPs) across clouds and on-premises.Identity Orchestration provides a way to secure identity in hybrid-cloud environments.

It was created for today's computing environments to solve the big challenges that have emerged in recent years. With the rise of SasS and remote working came the proliferation of multiple cloud identity services, causing fragmentation and identity silos.

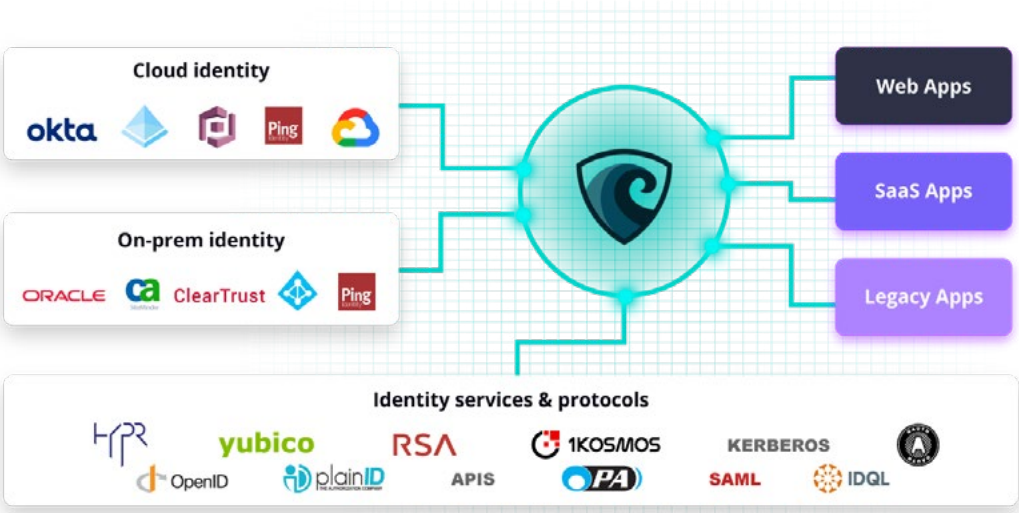
The use of multiple clouds in organizations has caused gaps in visibility, making identity and access management (IAM) unwieldy and manually intensive. Almost 60% of organizations that use multiple identity services or more than one cloud platform say that they deal with visibility gaps of policies, apps, and users.

In addition, more than 75% of workloads are still running on-premises behind legacy identity providers. Identity data is siloed in identity providers (IDPs) such as Active Directory, SiteMinder, OAM, LDAP directories, IDaaS platforms, and the IDPs built into public or private cloud platforms.

In addition, more than

75%

of workloads are still running on-premises behind legacy identity providers.



Identity Orchestration *integrates your apps, IDPs and services no matter where they run in the cloud or on-premises.*

Related reading:

The 2023 State of Multi-Cloud Report

Read the report

An Identity Orchestration platform bridges different identity operations in a seamless run-time experience. The software helps to provide consistent access to applications wherever they are running without changing the user access experience, rewriting any code, or recreating access policies in multiple identity systems.

In environments where identity systems are siloed, Identity Orchestration makes all components — which may not have been designed to work together — work as one. It does this by externalizing authentication and authorization from the applications themselves. Fragmented identities are integrated into an abstraction layer, which makes distributed authentication and authorization possible.

What can Identity Orchestration help you achieve?

Imagine being able to modernize and secure any application without rewriting code. What could you do with all those freed-up resources?

With Identity Orchestration software, IAM administrators can:

Streamline user authentication and authorization processes

Modernize applications without rewriting them

Choose to use best of breed identity management tools OR consolidate IDPs

With Identity Orchestration software, IAM administrators can streamline user authentication and authorization processes, modernize applications without rewriting them, and use best-of-breed identity management tools. By creating Orchestration Recipes, cloud admins easily combine different identity services distributed across clouds and IDPs into one cohesive identity fabric.

These services can include identity providers, directory services, threat detection systems, and APIs, allowing for comprehensive access control across all platforms. With this pattern in place, users' access to protected applications is fully controlled, authorization is externalized, and cross-cloud events can be easily audited, analyzed, and governed.

Identity Orchestration helps with a number of business use cases, such as modernizing legacy app identity, deploying passwordless/multi-factor authentication, enforcing authorization, and managing complex namespaces. It can also dramatically accelerate one of the top IAM priorities today: extending cloud identity capabilities to on-premises applications.

Being a vendor-agnostic solution for hybrid-cloud and multi-cloud deployments means Identity Orchestration software can work with most IDPs and identity services to secure both cloud and on-premises applications. It can also help organizations "move and improve" rather than "lift and shift" when migrating workloads off legacy identity providers to the cloud.

How does Identity Orchestration work?

Identity Orchestration abstracts, integrates, and orchestrates identity data to make it accessible through a consistent set of APIs and interfaces.

Things that were typically deemed very difficult by IAM practitioners, such as automating policy enforcement, configurations, and identities across any identity system, are expedited and simplified with Identity Orchestration software.

Authorization and authentication processes are externalized from applications through an abstraction layer. Those applications can then integrate with any identity system or service without changing application code or modifying configurations.

The software routes login requests to different concurrent identity providers or lookup-and-retrieve user attributes, groups, and other identity data from various identity stores.

Identity Orchestration ensures that the various steps of identity management occur in the right sequence. It takes identity system integrations and does specific operations with them in a particular order, creating runtime identity access flows for a user and governing what happens to that user from the beginning to the end of a user flow.

> *"The sheer number of identities that organizations must manage is nothing less than mind-boggling. In some cases, the figure can extend into the hundreds of thousands or even millions of people and devices. Historically, these identities would be spread across several internal "identity silos" that were hardcoded to business applications, legacy identity infrastructure, or a specific data center."*
>
> *- Gerry Gebel, Dark Reading*

Meet the identity fabric: The easiest way to connect all identity solutions

An identity fabric is an abstraction layer in a distributed identity management framework that is integral to Identity Orchestration software. It's what connects disparate identity silos and makes them work together as one. Your identity fabric integrates the existing IDPs, clouds, and identity services so that policies can be enforced consistently across all applications.

It uses orchestration to manage multiple identity domains on any number of clouds and weave them together so that they understand each other. It uses abstraction to:

- Manage identity across cloud and IDP vendors
- Modernize identity and migrate applications without rewriting
- Access identity policies and make them consistent across cloud services
- Automate authentication and eliminate custom coding through no-code integration

As an abstraction layer, it unifies distributed identity providers and infrastructures like MFA, directories, databases, APIs, authentication, and authorization providers. Developers can use a single abstracted API for the entire range of connected systems, enabling consistent identity and access across multiple clouds and vendors.

An identity fabric is not is not something you can buy on its own or off the shelf, but rather something that you can build through Identity Orchestration. Because it sits on top of your existing solutions, every identity fabric is different and unique to each organization.

How does an identity fabric work in practice?

An identity fabric discovers, abstracts, and integrates identity data across multiple identity domains. It then orchestrates identities and policies in distributed cloud services and presents that identity data consistently to hybrid and multi-cloud infrastructures.

This new approach to identity management respects the individual platforms you're managing — whether a cloud provider, like Microsoft Entra ID or AWS, or a SaaS application. You can define rules or policies for access and authentication in a central way, then convert the policies and distribute them across individual platforms or systems.

It inventories and maps elements of the extended identity system across multiple clouds. As a connecting layer that enables the orchestration of disparate environments, your identity fabric has interwoven threads connecting legacy infrastructures with cloud-based assets.

By decoupling identity from applications, an identity fabric eliminates the need to custom code identity into apps for cloud deployment. IT teams can use configuration, not coding, to 'wire' apps and identity, making it possible to easily switch one identity provider out for another. Or they can roll out a new identity service, like passwordless, to apps without rewriting the app.

Identity fabrics simplify identity management by creating a central control plane. It unifies policies and access controls across multiple identity systems, orchestrates policies, and enforces them at runtime. This intelligent and highly configurable system manages users' interactions with applications in real-time, providing a seamless and transparent experience.

Myth-busting: Key misconceptions about Identity Orchestration (or what Identity Orchestration doesn't do)

Identity Orchestration doesn't replace the built-in identity domains of cloud platforms like Amazon Web Services (AWS), Microsoft Entra ID, Google Cloud Identity, or Okta. Nor does it replace legacy IDPs like Oracle Access Manager (OAM) or Broadcom (CA) SiteMinder. Instead, it orchestrates identity data and policy across disparate Identity systems.

The foundation of true Identity Orchestration is that it is vendor-agnostic and works across all identity service providers. It automates the user flows across multiple cloud platforms and unifies any identity services without needing to rewrite code or refactor applications. It helps organizations modernize applications and transition to the cloud faster, at less cost, and more securely.

Identity Orchestration vs. SSO, workflows, and IDPs

Identity Orchestration is distinct from other traditional identity management systems, IDPs, SSOs, and workflows. It provides an overlay of identity and access management policy through a control plane and identity fabric.

Identity Orchestration is not an IDP

Identity providers (IDPs) store identities in a directory and enforce access control through roles and groups. Most IDPs also offer SSO, federation, and workflow capabilities. With Identity Orchestration, there's no dependency between the software and the customer, and it houses no organizational data, so PII is never at risk.

Identity Orchestration is not SSO or federation

Compared with SSO and federation, Identity Orchestration does not try to solve the problems of SaaS, SSO, or app management. It doesn't use password stuffing to integrate with non-standards-based apps. Identity Orchestration handles federated identity natively and doesn't rely on specialized federation software.

Identity Orchestration is not the same as workflows

Compared to workflows, Identity Orchestration is a runtime control plane process and not an administrative admin process that runs out of band, such as onboarding and off-boarding users into an organization. It works with many IDPs across clouds and on-premises rather than simply managing the workflows within one environment.

Solve the big IAM challenges facing the modern enterprise with Identity Orchestration

The forces of digital transformation create a mandate for technology that keeps pace with business and customer needs. Organizations are moving to the cloud, and now multi-cloud, but still have the majority of their workloads on-premises, and that's not going to change for the foreseeable future.

As organizations move to the cloud, they must manage their existing identity environments while adapting them to support hybrid infrastructures. They must also **accommodate new, cloud-centric use cases and integrate with new IDPs deployed during the transition.**

Many of these new identity services in the cloud only support standards-based application and service integrations. This creates an integration challenge when applications have long been integrated with legacy Identity providers built around proprietary mechanisms.

Some big problems that Identity Orchestration solves include:

- **The co-existence of old and new identity services**
- **IDP proliferation**
- **Multiple layers of identity**
- **Vendor lock-in**
- **Multi-cloud/ hybrid cloud fragmentation**
- **End of life/end-of-service of legacy identity providers**

PROBLEM 1

Multi-cloud and hybrid cloud fragmentation

As cloud adoption scales in enterprises, multiple cloud platforms are often chosen because different clouds have different specialized capabilities.

According to recent industry research,

Over 80%

of enterprises use three or more public clouds.

However, legacy IT infrastructures will endure as only 20% of workloads have moved to the cloud presently.

Multi-cloud and hybrid cloud environments drive the need for new and old systems to co-exist seamlessly to avoid fragmentation. Being able to manage identities across all clouds and legacy, on-premises identity management solutions is a top priority for IT and security leaders.

A hybrid and multi-cloud strategy requires fundamental changes in the way apps are architected, where they are deployed, and how they consume identity. These changes necessitate a new approach to identity designed to work in multiple clouds and provide a bridge between the old and new worlds of cloud-native technology.

PROBLEM 2

Multi-cloud and multi-vendor identity providers make consistent policy enforcement harder

Each time an enterprise adopts another cloud platform, it adds more identity silos to be managed. Each cloud service provider (CSP), such as AWS, Microsoft Entra ID, and GCP, requires your enterprise to use its built-in identity system to use its cloud platform. This also arises in the case of mergers, acquisitions, and divestitures where the transaction companies have different user groups on different IDPs.

Even organizations that have adopted an Identity as a Service (IDaaS) platform for cloud identity must still use the built-in identity service from the cloud platform.

Since cloud-native IDPs don't easily adapt to the needs of on-premises applications and legacy IDPs do not readily adapt to the requirements of cloud services, enterprises often deploy gateways and proxies in an attempt to implement last-mile integrations from legacy up or from the cloud down. The result is a series of square peg/round hole approaches that won't work as expected or leave serious functional gaps.

PROBLEM 3

Multiple layers of identity increase costs

The reality of modern cloud platforms is that enterprises must manage identity and policy for layered workloads, as well as the compute, network, and storage services on which they run. Managing identities along this “north/ south” axis is critical for security and compliance.

The ability to coordinate identity across infrastructure layers can determine the success of cloud adoption. Organizations have been managing identity manually in each layer, usually at considerable expense. Some enterprises have large teams with hundreds of administrators dedicated to manually managing distributed identity domains — this cost adds up quickly.

PROBLEM 4

Vendor lock-in

Switching clouds or making workloads and services portable across clouds requires the implementation of a new IDP with different policy models, APIs, and ways to identify users, group memberships, or roles for access control. Enterprises must overcome “identity lock-in” to support frictionless movement across clouds and gain the innovative capabilities of multi-cloud.

Today, organizations must rewrite apps to switch identity domains that use different sessions, APIs, and policies. Not only is this approach expensive and time-consuming, but it also requires technical expertise and introduces risk. Some organizations have deployed IDaaS single sign-on using protocols such as SAML, OAuth, and/or OIDC. These solutions are optimized for Software as a Service (SaaS) applications and don’t readily integrate with existing enterprise applications.

Apps and workloads designed pre-federation or not supporting federation must be rewritten. Federation is an SSO and authentication solution not designed to address how identities, policies, and last-mile application integrations are handled across different cloud platforms.

PROBLEM 5

End-of-life/end-of-service of legacy identity providers

As the cloud takes priority in boardrooms and budgets, legacy identity management vendors have deprioritized on-premises software investments and ended support for select versions of "legacy" products. Companies using software that has announced end-of-life or end-of-support must consider how best to migrate to a newer solution to avoid security risks.

Beyond security vulnerabilities, outdated legacy identity software also lacks essential features needed for digital transformation. Yet, many enterprises still rely on these products to protect applications at the core of their businesses. They can't easily migrate away from these products, making them susceptible to security risk, non-compliance, and being out of reach of zero trust.

PROBLEM 6

Skills gap/resource constraints

Modernizing legacy IDPs has historically required several quarters or even years of complex migration planning, execution, and validation.

Many organizations don't have the budget, human resources, and bandwidth to modernize by manually rewriting and consequently stay on outdated legacy identity software prolonging exposure from unpatched vulnerabilities and a lack of support for mission-critical systems. The cost is not only in dollars but in opportunity costs.

At a time when skilled software developers are at a premium, tying up valuable people's time on projects that are not going to create innovation sets organizations back.

What are the benefits of Identity Orchestration?

By nature, identity is tightly coupled to applications which makes it hard to untangle them from the identity services where they reside. Identity Orchestration coordinates multiple identity services into authentication and authorization user flows. The abstraction layer decouples apps from identity to allow consistent policy enforcement, modernization/moving to the cloud, increased cybersecurity, and identity resilience. Learn more about the benefits and how to put Identity Orchestration into practice.

Consistent policy enforcement for consistency across clouds

Policies across multi-cloud and multiple identity systems become fragmented, leading to security vulnerabilities, difficult management, and unreliable performance. Identity Orchestration simplifies and manages policy consistently across all apps using an integrated identity fabric.

Modernization/moving to the cloud

Moving off legacy identity systems to cloud-based ones means migrating all your applications from old to new, and traditionally, that required rewriting the code of each app. This is a daunting task when faced with updating or changing the code for hundreds or thousands of apps.

To meet the desire and requirements of moving to the cloud, Identity Orchestration is a no-code way used to modernize apps and enable the retirement of legacy identity infrastructure to cut budgets while allowing app modernization in minutes instead of months.

Increased cybersecurity

Cyber threats are growing exponentially, with passwords at the root of more than 85% of breaches. In a recent report, data breaches cost organizations an average of $4.35M last year.

Identity Orchestration improves your security posture by removing passwords and replacing them with passwordless or multi-factor authentication without rewriting apps.

Identity resilience

Identity is the front door to your apps and data, and when it goes down, all your apps are down. With downtime costs higher than ever, it's critical to improve the resilience of apps and data access at every layer. Identity Orchestration provides a resiliency layer to ensure your identity security is always available — across clouds, between on-premises, and the cloud.

Common business use cases for Identity Orchestration: How the smartest hybrid enterprises are putting it to use

Identity Orchestration can be used for any number of business use cases. From M&As to securing legacy apps and IDPs.

Mergers, acquisitions, and divestitures (M&A)

Enterprises merge, acquire, and divest businesses to fuel growth and respond to the need to transform. However, mergers, acquisitions, & divestitures can also cause identity management chaos. Combining multiple identity infrastructures so that employees, contractors, and partners can have access to essential systems while maintaining strong security controls is often messy.

To complicate matters, some business units within companies select different clouds based on the unique needs of their customers, leading to the use of additional identity layers. From an organizational perspective, M&As create situations where it is impossible to consolidate on a single IDP. Identity Orchestration can help navigate IAM without disrupting user experiences.

Securing legacy applications

Securing legacy applications (or non-standards-based applications) is a huge challenge for multi-cloud organizations today. The manual approach to upgrading identity providers can be impractical in terms of both time and cost. Many apps that run on commercial off-the-shelf software are often closed source, rendering rewriting impossible.

For those apps that can have code modified, custom coding takes an average of six months and $150,000 per app. Identity Orchestration makes it possible to modernize and uplift the security of hundreds or thousands of these apps without having to resort to rewriting them from scratch.

Coordinating identity policy management

Enforcing a common policy across a mixed set of clouds is paramount. Attackers take advantage of inconsistent access policies, poor visibility across clouds, and difficulties that arise when migrating policies.

The identity fabric that Identity Orchestration uses coordinates identity and policy across multiple layers of the cloud stack (from apps to PaaS services to IaaS computing, networking, and storage infrastructure) and coordinates across distributed identity silos. These north/south and east/west integration patterns are crucial to implementing a genuinely distributed approach to identity management.

How to get started with Identity Orchestration

Not all Identity Orchestration solutions are created equal. If it can't run on-premises as well as across multiple clouds, it's not truly Identity Orchestration. If you are looking for a solution that is built for the multi-cloud AND multi-vendor challenges of today, The Maverics Identity Orchestration Platform by Strata Identity can help.

Whether you need to modernize your legacy apps or orchestrate multiple IDPs or add passwordless authentication to all your apps without rewriting, we've got you covered. Learn about Identity Orchestration Recipes for a few of the possibilities. Try it now!

Modernize any app with any IDP in minutes. Join the 'Orchestration Kitchen' workshops

Discover Sessions

About Strata Identity

Strata Identity is the leader in Identity Orchestration for hybrid and multi-cloud environments. The orchestration recipe-powered Maverics platform enables organizations to integrate and control incompatible identity systems without changing the user access experience. By decoupling applications from identity, Maverics makes it possible to implement modern authentication, like passwordless, and enforce consistent access policies without refactoring source code. The company's founders created the IDQL (Identity Query Language) standard and Hexa open-source software for multi-cloud policy orchestration and are co-authors of the SAML standard for SSO federation.

For more information, visit us on the Web and follow us on LinkedIn and Twitter.

Solve the problems our clients are solving

Kroger · 3M · Minnesota · Carlsberg Group · Navy Federal Credit Union · syniverse

Identity Orchestration is changing everything. Strata is leading the way.

RSAC Innovation Sandbox 2022 Finalist · Gartner Cool Vendor 2020 · CSO 8 cybersecurity companies to watch · Microsoft Intelligent Security Association · Top 10 Black Cybersecurity Leaders 2021 · 2021 SINET 16 Innovator · Winner