STRATA
Identity Orchestration

The ROI of Application Identity Modernization & Legacy IDP Migration

Identity Orchestration
Return on Investment 2023

Situation Overview

Strata Identity interviewed 50 leaders at Fortune 1000 companies about their application identity migration and IDP modernization strategies. The report outlines key takeaways from the interviews and real customer data that can help organizations achieve better and more expedient results from their modernization efforts.

Today's enterprise computing infrastructures consist of a complex mix of public cloud, private cloud, and SaaS apps. Typically, each of these systems has its own built-in identity and access management (IAM) implementation.

Organizations increasingly have multiple public clouds (AWS, GCP, or Microsoft Azure to name the big players), which leads to identity silos to manage. Migrating apps from a legacy identity provider to a cloud Identity   provider requires the associated identity to migrate as well.

Traditional approaches to identity migration and modernization require recoding all legacy apps to be able to work in the cloud. It is an expensive process that takes a long time. Often, the ability to custom code/refactor each app, the expertise of the IAM infrastructure, and the knowledge of how the apps are integrated is a painful discovery process.

Apps require identity (login, SSO, and password management, etc.) which has likely been custom coded to work with older identity systems. One to one customization leads to pervasive lock-in between the apps, the legacy IDPs, and the platforms/vendors the apps run on. **Lock-in forces millions of dollars in IT spend — managing, upgrading, and maintaining legacy identity infrastructures.**

Identity management challenges to modernization

The organizations represented in this report identified the many obstacles their identity teams face:

Multi-cloud adoption.

Most organizations are actively adopting public clouds for their business activities. In fact, many are moving to three or more public clouds to achieve their business and technology goals. Additionally, many continue to implement private cloud technology on-premises utilizing products from companies such as VMware, Red Hat, and Microsoft.

New identity silos to manage.

Each new cloud platform creates another silo of identities. This can be quite challenging for network and security administrators. There is a lack of visibility with no single pane-of-glass for managing identities, access, and policies.

Legacy identity lock-in.

Applications that are were hardcoded into an older identity systems are locked in. An application would traditionally need to be refactored before it can use a different identity system or move the cloud.

Skills shortage.

Legacy applications may be five or more years old and the people who wrote them are no longer with the company. The individual who integrated the identities with the application are also gone. Finding talent to address these challenges is scarce and expensive.

TABLE 1

Infrastructure, identity systems and apps in use

What infrastructure do you run?	Typical
Public Clouds	3.5
Private Clouds	1.5
On-Premises Identity Systems	3
On-Premises Apps	50
% of Apps Migrated To Cloud	10%

Technical debt and refactoring

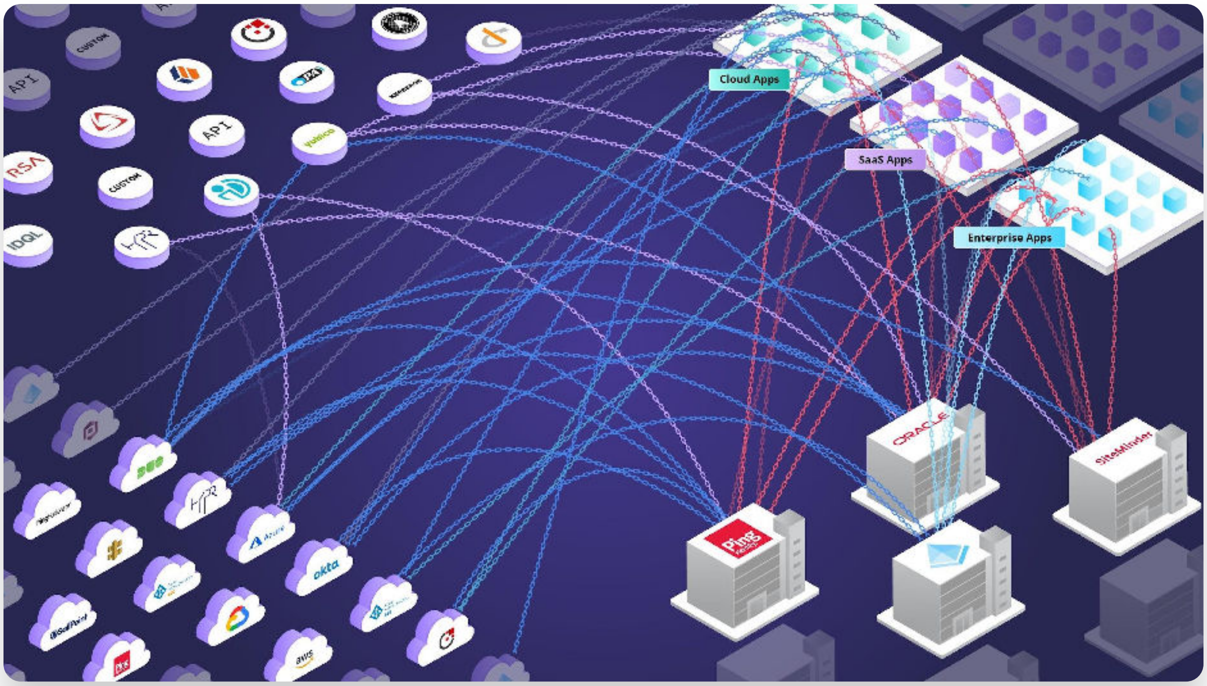
With the majority of apps integrated with legacy identity using custom ‘last mile’ code, each app must be rewritten or refactored to work with the new identity system. Manually refactoring or rewriting apps is expensive, time consuming, drudge work that often results in throwing good money after bad.

Companies need to become more agile and have indicated are looking for ways to improve their development processes. This means that manual migration approaches must give way to automated approaches.

It also means that **developers, who are often pressed for bandwidth, are better utilized to work on leading edge projects rather than trying to retain and get them excited about a legacy identity migration project.** A developers’ time is better spent on innovation and building new customer experiences and digital products than doing tedious migration work.

FIGURE 1

Migrating to a new identity system requires rewriting the apps to accept the new form of SSO. And, identity data and policies must be translated from old to new. The old way meant integrating each app with each identity provider with custom code and manual effort..



Standards-based and non-standards-based applications

Most applications fit into two categories: standards-based and non-standards-based. Standards-based apps are newer and can accept modern authentication, such as SSO and MFA or passwordless, to SaaS apps by leveraging identity protocols like SAML (Security Assertion Markup Language) or OIDC (OpenID Connect).

Non-standards-based applications (also called legacy apps), such as those reliant on cookie-based sessions, cannot consume modern authentication methods. These apps are the most common still today in organizations, but also put the most strain on resources to recode.

Organizations that Strata interviewed reported a range of complexity for how difficult app identity migration based on the complexity, age and build of the app. They ranged from simple standards-based apps that use SAML or OIDC to complex apps that use the proprietary cookie sessions popular with first generation web access management (WAM) platforms.

TABLE 4
Most common ways apps and identities are integrated (most apps are non-standards-based)

How are your apps and Identity integrated? (multiple response allowed)	**Typical**
SiteMinder Cookies (SMSESSION)	**78%**
Oracle Access Manager Cookie (OAMSESSION)	**72%**
HTTP Headers	**24%**
SAML	**19%**
JWT	**11%**
OIDC	**13%**
Other	**5%**

Identities are distributed across multiple systems

Organizations are managing identities across many identity systems. Below are the most common on-premises and cloud based identity management systems in use today.

TABLE 2

On-prem identity providers in use

What on-prem identity do you run?* (multiple response allowed)	**Typical**
Active Directory	**78%**
Oracle Access Manager	**29%**
Broadcom/CA SiteMinder	**13%**
IBM Tivoli Access Manager	**26%**
Ping	**14%**
ForgeRock	**5%**
Other	**13%**

TABLE 3

Cloud identity platforms in use (by organizations using more than 1identity service).

What cloud identity do you run?* (multiple response allowed)	**Typical**
Azure AD	**69%**
AWS Identity, Cognito	**34%**
Okta	**25%**
Google Cloud Identity	**21%**
Other	**24%**

*Strata's State of Multi-cloud Identity Report 2021

Legacy identity systems limitations

The leaders in our study shared whether they felt their legacy identity systems were adequate for today's challenges and which use cases are not being met with first generation identity software. They shared 5 common limitations:

1ST MAIN LIMITATION:
End of life (EOL)/end of service (EOS):

The mega legacy identity system vendors have publicly announced their mandate to focus on the cloud, consequently redirecting resources away from on-prem software. This reprioritization has led on-premises legacy software to reach end of life (EOL)/ end of service (EOS) as resources are redirected, draining away technical and support resources.

2ND MAIN LIMITATION:
Outdated versions of identity software:

The EOL/EOS problem is compounded by the fact that over 50% indicated they're running two or more releases behind the current release. Companies usually lack budget and resources to upgrade at every release and, once behind, it's hard to catch up. Getting on the current release often requires sequential upgrades which is time-consuming and difficult.

3rd MAIN LIMITATION:
Compliance and security risks:

Running older versions of software not patched and continually updated by vendors, creates additional new security risks. Legacy identity built before the notion of zero trust was conceived does not work in the cloud. The assumption of a secure perimeter — used by older technology — cannot be assumed in the cloud. Compliance is also a key concern because many mission-critical applications cannot run if they're outside of vendor support.

> *"Without Strata, Kroger could have been spending hundreds of thousands of hours redeveloping applications."*
>
> Cloud information Security Manager, The Kroger Company

4TH MAIN LIMITATION:
Incompatible with hybrid multi-cloud:

Our interviews corroborated that legacy identity architectures do not support the needs of distributed multi-cloud architectures. These older identity systems don't work in cloud-native platforms with their microservices and ephemeral architectures. Additionally, legacy identity systems extensively utilized proprietary cookies for sessions as they were released before standards such as SAML, JWT, OIDC were available.

5TH MAIN LIMITATION:
Complex and expensive:

A big challenge is the cost of maintenance to support multiple legacy identity applications. Each application is integrated with its own identity session system. Legacy identity software often runs on dozens of servers (sometimes hundreds) and requires complex infrastructure like networking, storage and integration with web tier. Retaining developers who want to work on legacy systems is difficult and expensive.

Enterprise IT Environments are more complex and distributed than ever before.

Strata provides a simple and cost effective way to address these challenges with modernization and migration.

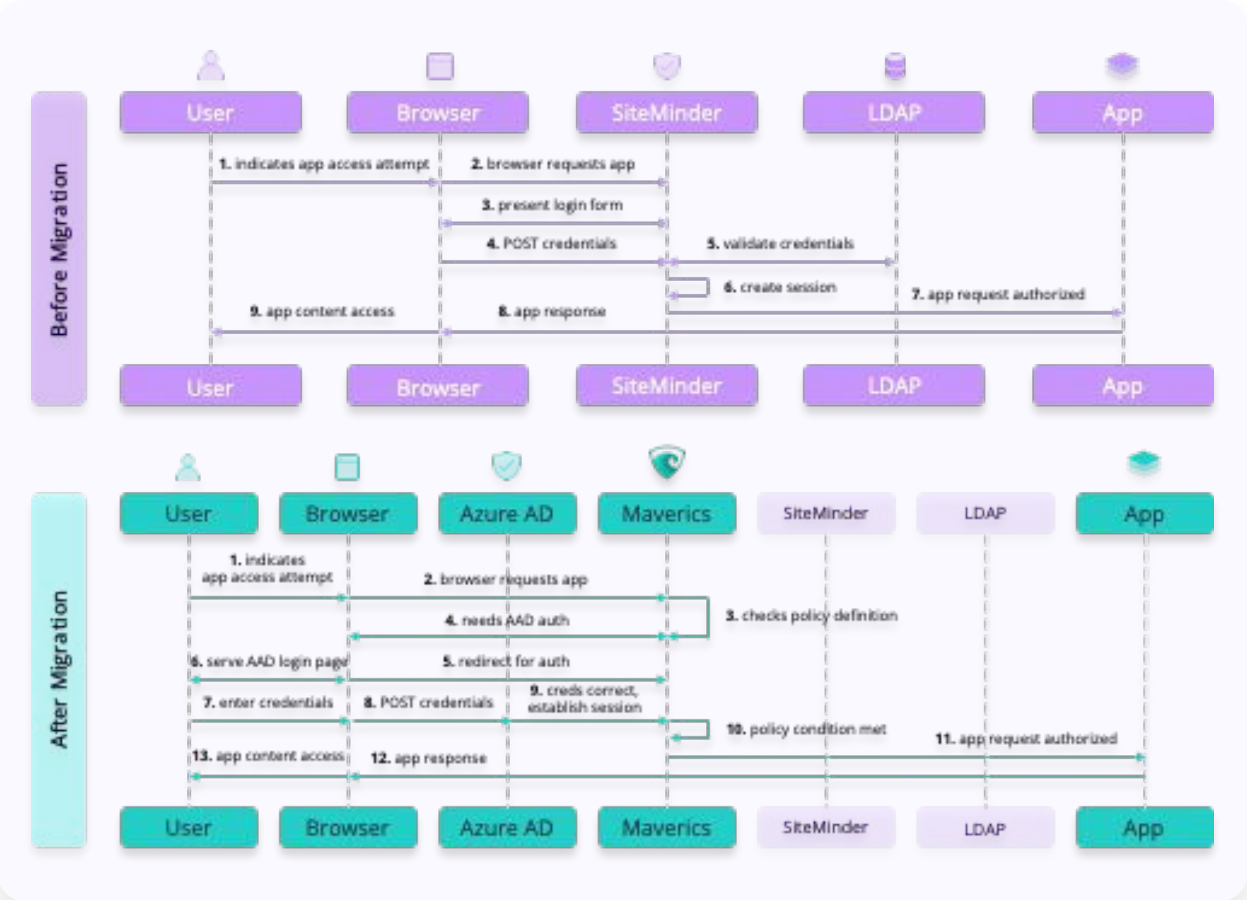
The Maverics Identity Orchestration Platform by Strata

Strata created Maverics, the first **Identity Orchestration** platform—it is natively engineered to work seamlessly across multiple clouds and integrate legacy on-premises systems with modern cloud-based identity.

Maverics enables app identity to be migrated from one identity system to another quickly through the use of an identity abstraction layer without any app rewrites. *Figure 2 illustrates the Maverics abstraction layer.*

FIGURE 2

Strata's software-based approach eliminates the need to rewrite apps and allows for moving the application authentication from a legacy IDP to a modern cloud one without the need to refactor the apps.



Measuring ROI using Strata's Maverics Identity Orchestration Platform

With Strata's distributed multi-cloud architecture, organizations can confidently migrate and accelerate their move to the cloud, while realizing significant hard-cost savings and faster migration project completions.

Using Strata's software, organizations see significant ROI both immediately and ongoing. A detailed analysis of an identity migration experience is found in the following section.

Figure 3 below shows potential cost savings when using identity modernization software instead of rewriting apps. The graph also illustrates the before and after cost savings that can be achieved from skipping rewrite/refactor apps.

FIGURE 3
Savings from identity modernization without rewriting apps using Strata's ROI methodology

Strata ROI calculation for 100 non-standard Apps + 50 standards-based apps breaks down like this:

✔ Total money saved from avoiding app rewrites = **$17.5M**
✔ Total infra costs saved from retiring legacy IDP = **$7.5M**
✔ Total for Maverics investment for the 150 app count = **$510K**

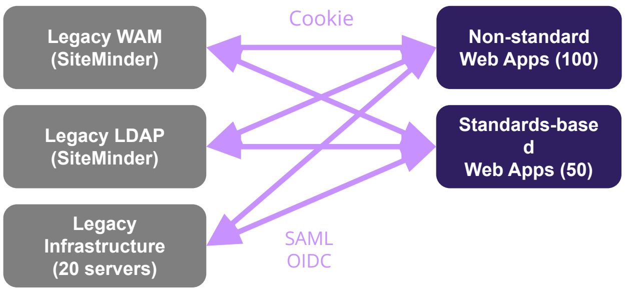
To calculate ROI, we take the cost difference, over the Maverics investment.

✔ $24,490,000/$510,000 = **4802% ROI**

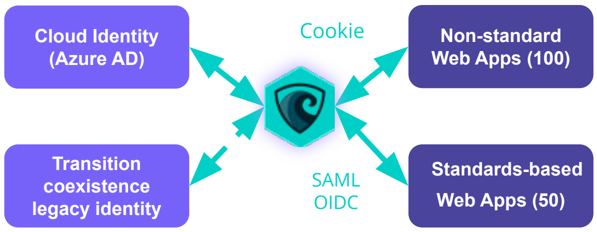
*ROI varies based on the number of apps migrated and the costs associated with rewriting each app.

Strata modernization ROI analysis worksheet

Current State



Future State


Cloud Identity (Azure AD)
Transition coexistence legacy identity
Cookie
SAML
OIDC
Non-standard Web Apps (100)
Standards-based Web Apps (50)

Strata Modernization ROI

Number of standards based apps	50	Number of non-standards based apps	100	Number of IDPs	2

Infrastructure and support costs	Annual legacy app support and license	**$5,000,000**
	Annual legacy Identity Infrastructure	**$2,500,000**
Total infra costs	Total for app support and infra of legacy identity	**$7,500,000**
App rewrite costs	One standards based app	**$50,000**
	One non-standards based app	**$150,000**
Total app rewrite costs	Cost to rewrite all apps	**$17,500,000**
Opportunity costs	Weeks to rewrite an standards based	**12 weeks**
	Weeks to rewrite a non-standards based app	**24 weeks**
Total opp costs	Week to rewrite both types of apps	**3000 weeks**
Maverics Investments	Price per month per App	**$250**
	Price per month per IDP	**$2,500**
Total Yearly Maverics Investment	Based on per App and IDP pricing	**$510,000**

Infra support costs + Total app rewrite costs = Total current costs
(Total current costs - Maverics Investment) / Maverics Investment = ROI

ROI	**Return On Investment**	**4,802%**
	Payback period	*****

Model your potential ROI with Strata's free calculator

Try Strata's ROI calculator

Let's run the numbers: Identity Orchestration impact for app identity modernization

Using software to automate the migration and modernization of identity greatly improves a business' hard-cost savings, reduces opportunity costs, and provides the foundation to enable new, modern security capabilities in the future.

Additionally, these organizations saved considerable time performing migrations and modernization initiatives. The range in cost savings account for the number of environments an organization has and legacy app complexity. As shown in the table below, organizations that move from legacy to modern cloud identity systems can realize significant hard-cost savings.

Average hard cost savings

TABLE 5
Achieving cost savings through legacy IAM cost avoidance

Avoided Cost	Est. Savings
Rewriting apps to work with a new identity solution	$50,000-$150,00/app
Ongoing support and maintenance license for legacy identity software	$5,000,000
Maintaining compute infrastructure used by legacy identity	$2,500,000

TABLE 6
Achieving time savings through automation

Avoided Time Expenses	Est. Savings
Not rewriting apps to work with new identity solution	12-24 weeks/app

Benefits of migration & modernization with Maverics Identity Orchestration

The traditional way to modernize identity requires significant budget and time, driving classic identity migrations to be complex and expensive multi-year endeavors.

Strata's Maverics Identity Orchestration Platform can yield an ROI of almost 5000%. The savings are realized in weeks to months rather than years — the amount of time it would have taken to manually rewrite and migrate a handful of apps. With Strata, organizations can modernize for good and see the following benefits:

- ✓ **Identity that supports distributed architectures** running natively on multiple clouds.
- ✓ **Modernize in weeks**, rather than years and never have to rewrite an app.
- ✓ Use of **modern cloud identity capabilities** like MFA, passwordless, and mobile.
- ✓ Access to a **modern cloud-native platform** with capabilities like microservices, containers, like auto-scaling, and DevOps.
- ✓ **Improved security** from using continually updated software vs. old, outdated, non-supported software.
- ✓ **Improved compliance** by running on modern identity platforms that support GDPR and other regulations.
- ✓ **Freedom from vendor lock-in** by decoupling apps from IDPs or multiple cloud services.
- ✓ **Coexistence to incrementally migrate** and avoid the risks of a big bang migration approach.

Benefits of migration & modernization with Maverics Identity Orchestration

A thoughtful, integrated identity modernization strategy is perhaps more critical than ever to save costs by retiring legacy infrastructure, manage risk, and drive an efficient project that sets your business up for success.

Strata's Maverics Identity Orchestration Platform empowers identity architects and business teams to create seamless and secure identity experiences across multi-cloud and hybrid-cloud environments and modernize legacy applications — without any rewriting apps.

With Maverics, organizations have realized an average **ROI of 4800%, saved more than seven million dollars (US) in hard costs, and completed migrations in months instead of years — approximate time saved for migrating 50 standards based and 100 non standards based apps equates to 57 years in developer hours!**

Strata built our software to solve the challenges of distributed identity infrastructures. It's a new **approach to migrating applications and modernizing identity** for multi-cloud and hybrid environments.

Maverics easily enables organizations to migrate identity to the cloud, use multiple clouds, and supports hybrid deployments. The Maverics abstraction layer eliminates the need to write custom code to integrate each application.

In addition to the monetary savings, businesses realize the benefits of **increased agility, improved security, and future-proofing** with Strata's Maverics Identity Orchestration platform.

Kroger Customer Modernization Story

Kroger needed to modernize the authentication and authorization of their mission-critical applications in a short amount of time. The retail grocery giant had both consumer-facing apps and internal apps that every person at the company relied on daily.

With 400 applications spanning from in-house built using a variety of technologies and programming languages, to commercial off-the-shelf applications, Kroger estimated that migration could take years and cost millions of dollars.

Strata immediately saved Kroger millions of dollars in custom coding, manual testing, and validation work — plus, years-worth of migration projects. They also slashed legacy infrastructure expenses by retiring legacy identity software and related infrastructure.

Before Strata

- ✓ Fortune 25 retailer - $140B annual revenue
- ✓ Massive SiteMinder footprint with expensive maintenance
- ✓ Inability to support modern authentication and MFA
- ✓ Legacy tech debt was ***slowing digital transformation*** and Kroger's move to a self-service IT model
- ✓ Facing ***$60m/150 year (cumulative coding time)*** project to modernize 400 critical applications

After Strata

- ✓ Fabric in place – permanent flexibility to innovate and ***change*** as business environment changes
- ✓ Off of SiteMinder in 12 months and for ***less that 1%*** of the cost of the refactoring approach
- ✓ Self-service IT initiative accelerating
- ✓ ***Simplified and more secure authentication*** for Kroger's associates and customers
- ✓ Kroger identity team with ***never have to consider*** an application rewrite again. ***Ever.***

Read the full story

Now you’ve modernized. What’s next?

Strata brings a new generation of identity management capabilities for organizations operating in the hybrid, multi-cloud world. Identity Orchestration with Strata future-proofs your organization by keeping you permanently modern and allows you to make the most of your existing identity investments. With Strata’s Identity Orchestration platform you can experience:

Increased flexibility – Freedom from lock-in allows you to choose cloud platforms and identity platforms independently.

Faster project completion – Using software instead of manual effort to significantly reduce cycle times.

Improved security – Integrated identity silos for easier management of different infrastructures across multiple cloud providers.

Enhanced development – Modernized developer access to identity, reduced dependency on legacy development and upgrades.

Time & cost savings – Retiring legacy software and related infrastructure, avoiding manual work services, and avoiding training on legacy technologies.

Multi-cloud readiness – Ability to move to the cloud and from one cloud to another and natively manage identity across distributed clouds.

Increased revenue – Better customer experience enabled by digital transformation that leads to increases in gross profits from online channels, powered by identity modernization.

Improved agility – Ability to mix-and-match infrastructure, such as moving to Google Cloud from AWS or swapping identity domains from SiteMinder to Okta, for example.

Contact your Strata representative today to learn more about how you can get started with your identity modernization and migration journey. Contact **sales@strata.io** or visit us here: **strata.io/demo**

Report framework

This report is the result of survey data and actual statistics from existing Strata customers. The field and primary research conducted in conversations with 50 leading innovators at Fortune 1000 organizations. These organizations are concentrated in regulated industries subject to compliance including financial services, insurance, healthcare, and global technology enterprises.

About Strata

Strata is pioneering the concept of Identity Orchestration for distributed, multi-cloud identity. Strata's **Maverics Identity Orchestration Platform** enables companies to seamlessly unify on-premises and cloud-based authentication and access systems for consistent identity management in multi-cloud environments. Strata's unique distributed approach to identity enables organizations to break decades-old vendor lock-in that has prevented a broader transition of enterprise workloads to public cloud infrastructures.

Strata's founders co-authored the SAML open standard for identity interoperability, created the first cloud identity services, delivered the first open-source identity products, and are now building the first distributed identity platform — Maverics.

To learn more, visit us at **Strata.io**

STRATA
Identity Orchestration