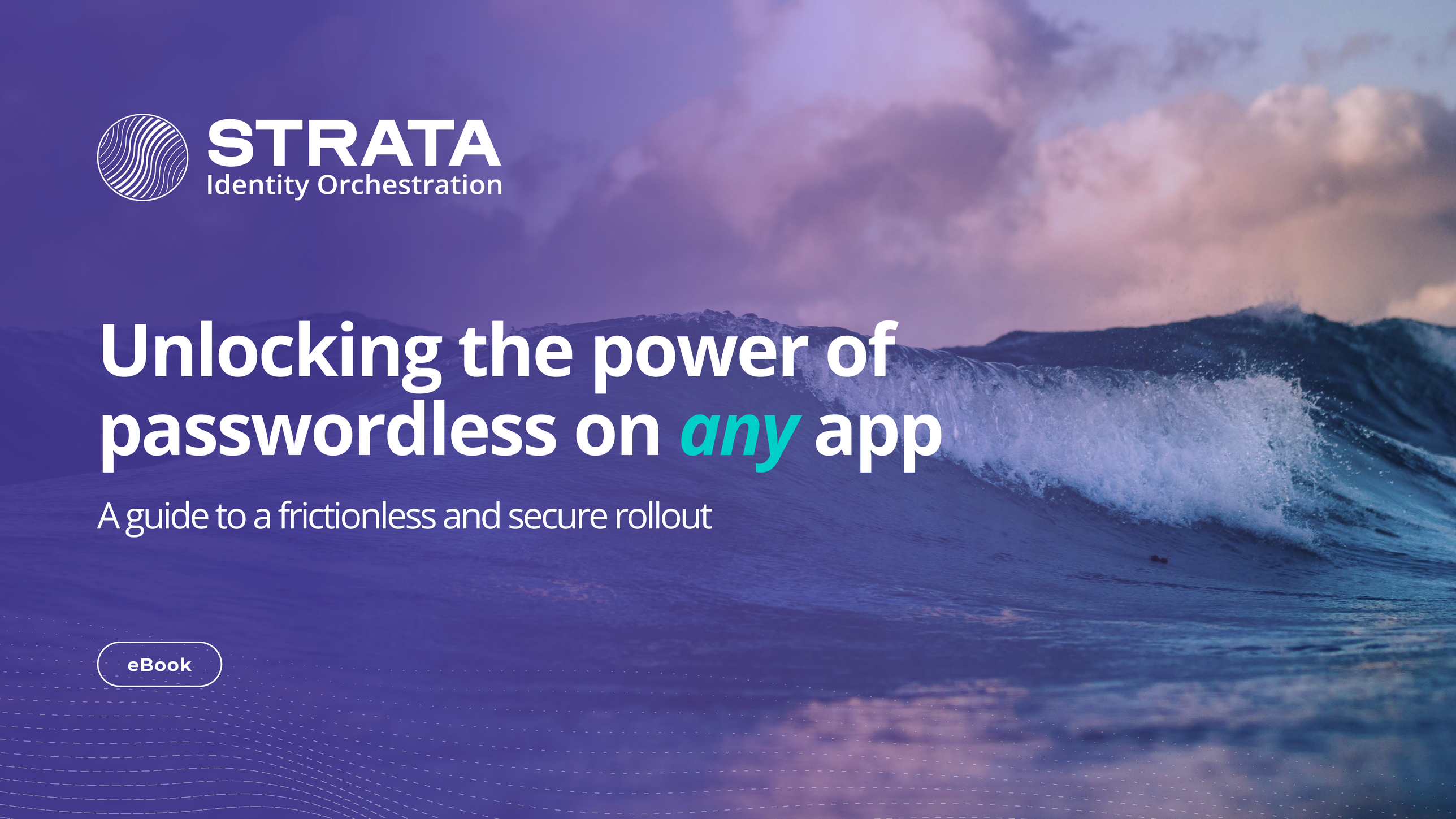

STRATA
Identity Orchestration

Unlocking the power of passwordless on *any* app

A guide to a frictionless and secure rollout

eBook

Passwords are at the root of most cyber evil today. According to IBM's Cost of a Data Breach report, using stolen or misused credentials is the most common cause of a data breach. The same study also reported that ***a data breach in the United States costs an organization an average of USD 9.44 million — and the number of breaches is set to increase.***

Passwords are ubiquitous but problematic. Organizations loathe passwords because they aren't secure; users don't like them because they're hard to remember. Patchwork attempts to improve password security often further complicate the user experience. So therein lies the question: why doesn't everyone stop using personal credentials altogether and go passwordless?

While great in theory, it's not that simple. Achieving a true passwordless state requires that all apps are decoupled from the associated identity provider (IDP) and can accept modern authentication methods. Organizational readiness aside, the other significant challenge is rolling passwordless out in a frictionless way so that people will use it — and it works.

When done right, passwordless authentication makes organizations and user identities more secure. Yet few organizations attempt adopting passwordless because it seems too overwhelming.

While the challenges of making passwordless a reality for legacy apps are significant, with the right partner, they are entirely solvable. This ebook sheds light on the biggest obstacles associated with modernizing legacy web applications with passwordless and outlines a path to adoption using Identity Orchestration that any organization can follow.

Part 1

Understanding passwordless authentication

Passwordless authentication is an advanced form of multi-factor authentication (MFA) that can solve many organizations' biggest security challenges. While some may be familiar with the basics of passwordless authentication and how it works, making it work for their organization is an entirely different story.

Why is passwordless authentication important?

Is passwordless authentication important? Yes! It protects organizations against credential theft, which can lead to cybersecurity breaches. Hackers are good at social engineering, exploiting the use of default passwords or sharing passwords. Even the most sophisticated security solutions are at risk if user information is part of the authentication process.

For this reason, zero trust security architecture (ZTA) is a top priority for many enterprises today — a priority that can only be achieved when the entire IT architecture is secure. A secure architecture is a modernized one; in other words, there are no passwords, and all gaps are closed so that hackers can't infiltrate the identity perimeter (and users can't thwart efforts).

Even if you've been putting off trying to achieve ZTA, the stakes for creating a secure environment have gotten higher with the United States government's Executive Order on Improving the Nation's Cybersecurity and the Office of Management and Budget's (OMB) Federal Zero Trust Strategy. Ignoring ZTA means getting cybersecurity insurance will be tricky or incredibly expensive — a huge frustration and a massive liability.

What are the challenges with passwordless authentication for legacy apps?

Moving to passwordless or MFA authentication methods to protect web applications is a must do today. Most organizations can fairly easily make the switch for cloud-based apps, but what about legacy, on-premises, and custom applications?

There are huge challenges in front of you before making passwordless work for legacy apps. Why? They were built in a different era, one in which applications were protected inside the firewall of your on-premises IDP. They were created before the cloud and don't speak the same language as modern authentication tools.

Legacy applications

It's nearly impossible to add passwordless or modern MFA authentication to legacy apps on-premises without modernizing them. Traditionally, modernizing apps meant manually recoding each one individually — something most budgets and IT teams cannot accommodate.

App owners

App owners bring their own set of challenges, as they are required to change the way they work to support passwordless flows. This behavior isn't due to malice or distrust — they're busy doing what they do, and getting them to embrace a new process can cause a blocker.

End users

Users present another unique challenge. Typical passwordless authentication flows require users to register a verification factor or device. However this means that the process will appear different than the user expects. If users have to abandon their familiar password-based login pages, they may resist this change or cause an expensive increase in IT support inquiries.

Multiple solutions

Finally, there may be a need to support multiple vendors' passwordless solutions. Some passwordless solutions, for example, pose app-level integration challenges. These need software development kits (SDKs) to support even simple flows, which may make it tough to add behavioral analytics.

Part 2

Moving to passwordless authentication

When transitioning to passwordless authentication, some planning guidelines include assessing readiness, choosing a passwordless provider, planning a smooth deployment, convincing stakeholders, and guiding end-users to adopt something new.

On the technical side, perhaps the biggest challenge of implementing passwordless authentication is that older applications were typically built before modern identity systems even existed. Legacy apps simply aren't able to use passwordless authentication unless code is completely rewritten. Often, recoding applications isn't merely formidable — it's impossible. Keep reading to explore how to make the impossible possible.

Evaluating passwordless authentication readiness

Passwordless authentication may be a golden ticket worth pursuing, but it is a big jump depending on the starting point. Because any digital transformation is on a continuum, its trajectory will be influenced by the amount of tech debt in front of the organization's modernization maturity.

Here are some common scenarios to help determine an appropriate starting point in the journey to passwordless authentication:

Ready to secure any app with Strata and HYPR passwordless authentication.

Learn more

Legacy applications

These organizations have not moved to the cloud and don't have a modern IDP. Though uncommon today, they still exist and have many steps to address before achieving passwordless. Moving forward to modern authentication should still be the objective and there are ways to scale faster today than there were five years ago.

Combination of cloud and on-presmises

These organizations have a modern IDP, and some apps are on the cloud(s), but many are still on-premises and have not been modernized to be able to work with modern authentication. They are likely using single sign-on (SSO), two-factor authentication (2FA), or MFA, maybe even a version of passwordless as part of their MFA process.

Ready for passwordless

This is a small group that's getting louder. To be ready for passwordless means that all apps are in the cloud or that on-premises apps have a way to speak to an IDP through an abstraction layer sometimes referred to as an identity fabric.

According to a 2022 report from the Enterprise Strategy Group, 17% of organizations have started to eliminate passwords selectively, and 37% are actively testing eliminating passwords. These results indicate that passwordless authentication is becoming a strategic initiative; however, it's not yet achieved widespread implementation.

There are many subplots on the identity modernization continuum that fall in between the three noted here, but the bottom line is a modern IDP is required to get started. Then, applications themselves must either natively be able to speak to the modern authentication protocols, or there must be an abstraction layer in front of those apps. More on the latter in section three below.

How to choose a passwordless provider

Choosing a passwordless provider is an important decision, and there's more to it than cost considerations. Popular vendors include Microsoft, Okta, Hypr, Yubico, and 1Kosmos, each varying in their approaches to passwordless authentication. Some provide several options for implementation, while others are more limited. But more options aren't necessarily better — what matters is finding a method that best fits the way the organization operates.

Beyond their products being FIDO2 compliant, we lay out some considerations when selecting a passwordless provider:

No passwords anywhere

Make sure the provider doesn't use passwords in any way. For example, some providers store passwords within their architecture. Users must create a password when they set up their accounts to be used as a recovery method — this disqualifies the vendor from being a true passwordless solution.

Cross app compatibility

Ensure that the user experience is seamless and that there's no need to reauthenticate when users go to different channels. Whether users switch between browsers, web applications, or devices, a passwordless provider should offer users a consistent experience.

Use cases

Look for a solution that will easily accommodate every way you want to use passwordless authentication, such as file encryption, digital document signing, and system logins.

Scalability

It's important to have a passwordless provider that can adapt — consider future mobility needs and the implications of a growing business.

Vendor credentials

Just because a vendor provides a security solution doesn't mean that the vendor itself is secure. Don't settle for a vendor that isn't approved for use by government authorities or can't prove their own compliance credentials.

Ability to deploy on legacy apps

Some organizations might wonder how legacy applications will limit passwordless provider choice. Any passwordless vendor would usually be unable to touch legacy apps without extensive custom code, but the following rollout allows you to choose any provider that makes sense for your organization.

Rolling out passwordless authentication

Make modern identity protocols work on any application

It will be difficult or impossible to migrate legacy applications to passwordless until they can work with modern identity protocols. Applications that are unable to communicate with a modern identity provider cannot use passwordless authentication. In the past, this often meant that older apps were discarded if updating was too precarious — a sacrifice in the quest for modernization.

Rewriting applications' code is typically performed so they can speak to modern identity protocols. ***This process can take the better part of a year plus cost half a million dollars just for one application***, which simply isn't viable for many organizations.

Identify a test group of people + test application

Start with a small user group who have already bought into the idea of going passwordless. It's ideal for this group to be from within the same department with a legacy application that's unique to them. For example, it would be wise to select a small finance group using an accounting app that no one else in the organization touches.

Don't worry about the application's complexity — an enterprise app will work just as well as a single functionality application. What's most important is to find an application that is only used by the test group. If this isn't possible, address the issue by using orchestration to implement conditional access.

Decouple apps from IDP

Another newer approach that uses an abstraction layer to decouple the identity from the legacy application is called Identity Orchestration. Abstraction enables coexistence — the legacy application itself is on-premises, but its identity solution is cloud-based.

By decoupling legacy applications from the identity system, any application can be protected by modern authentication services like passwordless or MFA. The abstraction layer, or identity fabric, sits on top of apps and IDPs, so no code changes are required. Migration with orchestration is a fast, cost-effective solution. We'll discuss Identity Orchestration on page six.

Scaling passwordless

After successfully rolling out a test case, it makes sense to start introducing passwordless to the rest of the organization. The following factors are critical for a successful organization-wide implementation and adoption.

Experience frictionless user journeys, reduced risk, and no-code integration with your existing IDPs. Unlock the power of passwordless with the simple recipe for success.

See how it works

Communication

Include employees in the plan — let them know what to expect, educate their team lead, and conduct training sessions. With a wide range of technical expertise, those less savvy will need more explanation. Strong communication also helps alleviate anxiety, increase buy-in, and reduce costly IT department call time.

Batching (or move and improve)

Make the transition with one or two applications at a time to avoid going back to square one if something goes wrong. Start with legacy applications that pose the least amount of risk or identify the applications that have the fewest users.

Timing

Implementing passwordless authentication organization-wide is a marathon, not a sprint. For larger organizations with many employees, it will take more time than anticipated, but be patient — any progress is good progress.

Onboarding

It can be a struggle to transition password-loving users to be true passwordless champions. This transition will require a seamless onboarding experience and perhaps even incentives, but don’t rely solely on gimmicks like gamification. Connecting the business benefit to the individual leads to better behavioral outcomes.

Part 3

Three ways Identity Orchestration helps make passwordless better

Overcoming the obstacles to passwordless authentication can be difficult and costly. However, Identity Orchestration is a fresh way to address both technical and user-related challenges.

Passwordless solutions are part of a strategy for the hybrid, multi-cloud world where most organizations run several identity systems.

Identity Orchestration helps make passwordless authentication better in several ways. We go into each of these below.

Speed of deployment/time to value

Orchestration may be familiar in virtualized computing stacks, but it's a new concept in identity architectures. An Identity Orchestration abstraction layer allows for modernizing older apps (by modernizing the authentication) without the expensive and time-consuming refactoring. Any app can work with new identity protocols and support passwordless authentication.

An Identity Orchestration approach is vendor agnostic and integrates between different IDPs. No matter the app's location or state of being, orchestration allows passwordless authentication without refactoring.

Phased rollout without permanent changes

Hard cutover deployments are inherently risky because to roll back any errors, the application would need to be refactored. Because Identity Orchestration does not require app rewrites, deployment can be performed on a group-by-group basis and any errors can be rolled back in a matter of seconds. This also allows for friction-free user onboarding that happens on a just-in-time basis as they access the app through their existing access workflow.

Using an Identity Orchestration solution can enforce passwordless authentication based on several variables; it's helpful when turning it on for a specific user subset.

For example, there might be an application that's used by hundreds of people in the organization, but you want to implement passwordless for just a few at a time. Identity Orchestration allows for setting specific passwordless conditions, such as geography, job role, department, or managerial status — virtually any condition imaginable.

Because Identity Orchestration doesn't involve rewriting an apps' code, it's easy to make changes on the fly. It's straightforward and flexible enough to provide complete control over an organization-wide rollout.

It's also possible to apply conditional access permanently. For example, an organization may want to require passwordless authentication for just certain areas within an application. It can also be used to ensure that only the right people have the right level of access to the correct data.

Recovery options (vendor coexistence)

As users register with passwordless authentication for the first time and create credentials, it's helpful to provide more than one option for them to use. Some users will inevitably lose or forget their primary means of verification — a mobile phone, for instance — and will need a backup method to gain access.

Identity Orchestration allows for multiple concurrent passwordless vendor options to avoid these user productivity blockers.

This also applies to account recovery scenarios. For example, what happens when John in accounting calls the help desk saying that he lost his YubiKey and doesn't have a password to get in? There will need to be a way for him to prove that he's actually John in accounting. Verifying his identity and reissuing his credentials creates more work for the support team and more downtime for John. Having backup credentials in place helps minimize disruptions that can shut down productivity.

Maverics Identity Orchestration Platform by Strata

Multi-cloud is now the norm, as is having several IDPs and even different passwordless providers. What works well for one application might not work well for others. Strata's Maverics Identity Orchestration Platform frees organizations from vendor lock-in so that they can implement passwordless on legacy applications however they please.

Our software is the only solution that can introduce passwordless to legacy applications, no matter which identity service protects them. That's because Maverics isn't a passwordless provider; it's an Identity Orchestration platform that helps secure apps on any cloud with any IDP. Organizations can use Maverics to weave apps, clouds, and IDPs into a flexible identity fabric. That way, when it's time to switch from on-premises to a cloud IDP, deploy passwordless, or build user journeys, it can be done without writing a single line of code — or refactoring apps.

Learn more about Strata's Maverics Identity Orchestration Platform or schedule a demo.

Schedule a demo