endeavour group

Endeavour Group streamlines multi-brand identity

Time to read: 12 minutes

Endeavour Group is Australia's leading retail drinks and hospitality business. A standalone company since 2021, it is listed on the Australian Securities Exchange and employs more than 30,000 people.

Challenge

Endeavour's post-demerger transition to independent HR and payroll systems brought significant operational and integration complexity. The company needed a core identity platform capable of managing this complexity while

INDUSTRY
Retail

COMPANY SIZE
30,000 employees

PRODUCTS
Identity Security Cloud

supporting multi-brand identities, critical applications, and seasonal workforce scaling.

Solution

Endeavour implemented SailPoint Identity Security Cloud (ISC) as its core identity platform, creating a unified foundation to support 30,000 team members. The cloud-native solution delivers automated joiner-mover-leaver processes integrated with SAP SuccessFactors, ServiceNow and more. It handles hundreds of new hires a day during peak season, while managing complex cross-brand movements. This automation delivers efficiency and supports long-term growth.

> "We've built a secure and scalable identity-first core on SailPoint Identity Security Cloud – and we're executing against a clear roadmap. It's disciplined, fit-for-purpose, and built to last."

Akshay Gulati, Senior Manager of Identity and Access Management, Endeavour Group

70–75%
Faster birthright provisioning

30-40%
Reduction in IAM tickets

‹2.5hr
Onboarding time down from 1 day

With a focus on bringing people together, Endeavour Group is central to Australia's social occasions. It runs a national network of more than

350 hotels and more than 1,700 retail liquor stores. The company became a standalone entity in 2021.

"This is an operationally complex organization that has transformed its people systems in recent years, consolidating human resources (HR) and payroll to create a resilient foundation for growth," Akshay Gulati, Senior Manager of Identity and Access Management, Endeavour Group, says. "We've built a secure and scalable identity-first core on SailPoint Identity Security Cloud – and we're executing against a clear roadmap. It's disciplined, fit-for-purpose, and built to last."

Establishing a single source of truth

Gulati's team orchestrated a complex consolidation effort that brought together two disparate identity platforms and three separate HR systems that previously served as independent sources of truth across different business units. This created a single source of truth for all of Endeavour's workforce identities across the organization, feeding into the SailPoint infrastructure.

"We selected SailPoint Identity Security Cloud for its ability to handle complex operations in a multi-cloud environment. Our assessment showed it had

the feature set, connectors, and extensibility to meet our requirements and deliver a unified and scalable platform. Automated lifecycle management and future proofing were key factors," Gulati explains. "That the solution came from the market leader and offered a smooth transition added to our confidence."

> "All in all, we're supporting productivity, saving considerable support desk resources and reducing the potential for human error."
> **Akshay Gulati**, Senior Manager of Identity and Access Management, Endeavour Group

Leveraging SailPoint Identity Security Cloud, the Identity and Access Management (IAM) team tracked and supported the significant transformation activities needed to stand up the new HR and payroll systems. More than 30,000 team members were transferred onto the new consolidated platform without interrupting business operations.

Managing multi-brand complexity

Team member identities are dynamic at Endeavour. During the festive season, the Group will rapidly add around 2,000 staff with a similarly fast ramp-down after the new year. Furthermore, the

organisation has multiple brands: the Dan Murphy's and BWS retail brands, ALH hotels, Langtons fine wines, Pinnacle Drinks, and more. Team members frequently move between these brands – on temporary secondment or to take up new roles.

"This multi-brand structure takes identity security to a new level," Gulati says. "Every brand has its own access starting with its own email address naming conventions. With SailPoint as our foundation, we were able to design our ideal joiner-mover-leaver (JML) processes and achieve very high levels of automation."

Automating JML workflows

The Group's primary automated JML flow is governed by roles implemented in SailPoint. This helps ensure that system and service entitlements are available to colleagues on day one – and that these stay current throughout the employment journey and are removed promptly when no longer required.

In SailPoint Identity Security Cloud, roles can be configured for automated provisioning and access requests. So far, approximately 40 roles have been configured for automated provisioning, delivering birthright access based on job requirements. The

team has been using SailPoint's Dynamic Roles configurations to grant this birthright access based on granular state- or city-level workflow customization.

For access beyond birthright entitlements, Endeavour has integrated its ServiceNow platform with SailPoint Identity Security Cloud. ServiceNow serves as the consolidating layer that connects the multiple IT Service Management platforms inherited from the company's multi-business background. The integration includes both catalogue and service desk capabilities, enabling users to request access through their familiar ServiceNow interface. When someone requests a role via ServiceNow, the request flows through the approval process for fulfilment by SailPoint. About 15 roles are currently configured for this requestable access model.

Mover events require additional coordination. Changing email addresses can disrupt active Google meetings and calls, so the IAM team uses SailPoint's forms capability to communicate with movers about timing and coordinate these changes smoothly.

Integrating critical systems

Besides Google and Service Now, Endeavour currently has around ten connected applications, primarily for birthright provisioning, including finance-related systems, internal communications, and the company's timekeeping tool. A further 60 applications are used for user access review (UAR) functionality through SailPoint.

Says Gulati, "Application integration is an ongoing journey. In all, we have around 200 applications in use across Endeavour and we're working to bring these applications within the remit of SailPoint for automated JML and UAR purposes."

SAP SuccessFactors, for example, is a source of truth for workforce identities at Endeavour. With the company's retail store network enabling frontline recruitment, the IAM team needed a way to provide birthright access to new staff hired in-store without undue delay. SailPoint's SuccessFactors connector provided the solution, allowing Endeavour to integrate SAP SuccessFactors into its automated JML process.

"We aggregate data from SuccessFactors every two hours, allowing us to provision birthright access within seconds after that. Our lead time between onboarding a new teammate in SuccessFactors and them starting in-store is now about 2.5 hours – down from more than 1 day previously," Gulati

continues. "This not only delivers a better experience to our new hires but also helps enhance team productivity."

Delivering measurable outcomes

Since go-live, Endeavour has turned SailPoint Identity Security Cloud into a fit-for-purpose backbone with its 30,000 team members; this automatically onboards new hires within a few hours of their details appearing in SAP SuccessFactors and provisioning their necessary access to systems throughout Endeavour Group (EGL) and down to our supporting partner organisations on day one. Automated workflows now manage every promotion, secondment and movement across the Group's multiple brands, updating entitlements, adjusting their email address and UPN at a time of the team member's choosing, and launching targeted micro-certifications so access remains continuously correct. The programme has also consolidated two legacy identity platforms and three HR sources into a single SailPoint feed, shifting the workforce with zero business interruption. This depth of automation lets a lean IAM team cope easily with seasonal peaks while delivering significant productivity gains and lower operational overhead for the organisation. The automation achieved

within SailPoint Identity Security Cloud has allowed us to operate a very efficient and lean identity team, delivering significant productivity benefits for the organisation.

Improvements of similar scale have also been achieved by automating the very complex mover process. While the process is not yet entirely automated, attribute synchronisation in SailPoint lets Endeavour update user accessautomatically, eliminating dozens of manual operations and reducing the Identity and access management tickets by 30-40%.

The integration between ServiceNow Service Desk and SailPoint Identity Security Cloud has also delivered significant operational efficiencies. Previously, when user data errors were identified, someone had to manually raise tickets for remediation – a time-consuming process that increased operational costs. Now, SailPoint automatically creates tickets for data validation errors and other issues, triggering immediate action by the relevant teams without manual intervention.

SailPoint's flexible provisioning capabilities have transformed the new hire experience. Rather than waiting until a new employee's first day to begin access provisioning, the platform allows the IAM team to schedule automated access provisioning

in advance. When someone comes in at 9:00 a.m. on day one, everything is ready to go.

"All in all, we're supporting productivity, saving considerable support desk resources, and reducing the potential for human error," Gulati explains.

Learning from experience

While the results speak for themselves, Gulati emphasizes that achieving these outcomes required careful planning and a methodical approach. His advice for other organisations embarking on a similar SailPoint Identity Security Cloud journey centres on two key principles: comprehensive change management and iterative implementation.

"First, understand who is being impacted and how – and then make sure they are well informed in advance," he suggests. "That's the first piece of the puzzle."

Given the role of the people system as the single source of truth for the identity platform, the HR team was a key collaboration partner for Gulati from the start. "We continue to maintain a regular cadence of communications with HR, helping us to understand their goals and priorities and

empowering us to design our solutions around their actual processes," he explains.

UAR compliance is another area that demands ongoing team-to-team communications. "Education is vital," Gulati says. His team uses regular newsletters and town halls to explain the importance of completing UARs. They also listen to what the business leaders need and adjust processes accordingly. In some instances, this means reaching out in person to remind leaders that their UARs are due.

The second critical lesson involves implementation strategy. Rather than attempting a Big Bang approach, which can stretch team capacity, Gulati advocates for smaller iterative releases with careful prioritisation: "Focus on your crown jewels first – the applications that are most critical or fall under audit requirements – rather than simply working through a list by starting at one."

Looking to the future

Gulati's plan is to connect at least 70% of Endeavour's more than 200 applications to its SailPoint infrastructure for automated provisioning in the next two or three years, significantly expanding the platform's footprint across the organisation.

Beyond scale, Gulati is focused on making the platform more intuitive and intelligent. "We want to leverage SailPoint's artificial intelligence (AI)-driven recommendation engine to enhance our UAR process and make role provisioning more intuitive," he explains.

The team is also exploring how SailPoint's emerging agentic AI capabilities can provide better control over the identity journey. This includes automating machine identity management through JML processes and leveraging the platform's Cloud Infrastructure Entitlement Management (CIEM) capabilities as part of Endeavour's multi-cloud strategy.

"We want complete visibility and control from the moment someone starts with us to when they finish – automatically providing the right access at the right time," Gulati concludes. "We have been very disciplined in how we have deployed our base platform for IAM success, and we're very confident that we now have a platform from which to expand and innovate."

Temple Health

EDUCATION

Pima Community College advances innovation with modern Identity Security

With SailPoint, Pima Community College enhanced security, streamlined operations, and achieved long-term scalability, setting a new standard for higher education.

TECHNOLOGY

SailPoint leads by example, advancing its own Horizon of Identity Security

SailPoint applies its industry-leading identity security solution in-house, leading to new efficiencies and a stronger, more mature approach to identity.

HEALTHCARE

Temple Health achieves faster, more accurate onboarding

SailPoint unifies Temple Health's approach to identity management and streamlines employee onboarding.

SailPoint

PRODUCTS

Platform

Identity Security Cloud

Compare suites

IdentityIQ

Connectors & Integrations

SERVICES

Support portal ↗

Documentation ↗

Developer forum ↗

Training & certification

Professional services

RESOURCES

Resource library

Blog

Podcasts

Events

Webinars

Partners

COMPANY

About us

Why us

Why work at SailPoint

News center

Trust center

Contact us

Glossary

Leadership team

Investor relations ↗

Environmental,
Social, and
Governance ↗

Terms of use   Legal   Privacy policy   Cookie notice   Don't Sell/Share My Data ☑✕

Email preferences   Disclosure policy

© 2026 SailPoint Technologies, Inc. All Rights Reserved.