INRY

How a high-end Hotel and Casino operator transformed its identity and access management journey

With INRY's IAG solution - Built on Now®

Summary

INRY

> *"The automobile wasn't invented because the horse and buggy didn't work"*

David Tyburski
CISO, Wynn Resorts

David Tyburski is the VP of Information Security and CISO at Wynn Resorts. With his comprehensive global background in IT Governance, Security, and Risk and Compliance, he directs all facets of information security for his organization throughout America and Macau. He developed 100% of the organization's Information Security & Technology policy over a period of 12 years.

When the COVID crisis hit, the global economy was shaken, and particularly the Hospitality industry faced some unprecedented challenges. Our Client had to shut-down their facilities and rapidly offboard, onboard, and transition employees.

With 198 applications, over 10,000 computer users, and nearly 2 million potential combinations of users, applications, and roles, the sheer volume became hard to manage. They leveraged INRY's Identity & Access Governance (IAG) solution, Built on Now®, to quickly transform access management. ServiceNow was the platform of choice because it enabled a single platform for everything: ticketing, helpdesk, and incident management.

The heart of this solution is the brilliant data model designed by David. INRY took David's data model and designed the IAG solution to remove complexity from the user request process and push it to the back end – where all relationships between user roles, applications, application roles and birthrights are maintained. This allows requests to be granted in mere minutes versus days.

Our Client mobilized 15,000 people within one month during the pandemic. INRY's IAG solution has helped them avoid $250,000 in additional costs, reduced human errors and shrunk their open access management request backlog to zero.

Meticulous audit trails and documented history helps them track who approved access, when, and why. Today, David and his organization have better access management and the ability to prove it.

< PREVIOUS

NEXT >

Overview

Our Client is a developer and operator of high-end resorts and casinos in the US and China. As a publicly-traded company, working in the hospitality industry, they must comply with several regulatory authorities.

David Tyburski is the VP of Information Security and CISO at Wynn Resorts. With his comprehensive global background in IT Governance, Security, and Risk and Compliance, he directs all facets of information security for his organization throughout America and Macau. He developed 100% of the organization's Information Security & Technology policy over a period of 12 years.

When the COVID crisis hit, the global economy was shaken, and particularly the Hospitality industry faced some unprecedented challenges. Our Client had to shut-down their facilities and rapidly offboard, onboard, and transition employees.

Our Client was already leveraging ServiceNow for Incident Management, Help Desk, and Asset Management. David believed that implementing Access Management on the same platform would drive faster and better adoption among users. Also, they wanted to connect the dots in a way they normally wouldn't – reconciling access requests with software licensing and entitlement data, and orchestrating service delivery and patching.

David believed that INRY was the appropriate partner of choice for three reasons:

1. Intimate knowledge of the platform and processes

2. Responsiveness

3. Creativity

< PREVIOUS

NEXT >

The Need for Transformation

User base & complexity

- Our Client has a portfolio of 198 applications, with over 10,000 computer users
- 2 Million potential combinations of users, roles and applications
- The sheer volume was hard and complex to manage

Seasonal workers add to the complexity

- Managing access during employee transitions was always a challenge
- Our Client employs seasonal workers who need temporary access to applications. Determining who should have access to what, and why can be challenging

Access Management

- Our Client believes in following the principle of least privilege - all requests were reviewed and approved before fulfillment
- A team of 5 fulfillers was processing 250 – 300 requests compared to the incoming volume of 1000 requests per day, leading to a massive backlog

Risk Management

- Yearly audits/attestations meant the potential for risk exposure due to inappropriate access for the entire year
- How to “look forward” vs. backtracking
- Formulating segregation of duties policies for detecting violations and avoiding access fraud
- Audit trail – a comprehensive log for each access request detailing the time, type, and approver of the access request

< PREVIOUS

NEXT >

Key Considerations

The legacy solution was not meeting their evolving needs

Our Client had traditionally used ECAR – Electronic Access Request application. This was tied to their HR platform and designed around the person requesting access, rather than applications. ECAR did not have views of applications or roles.

Administrators were challenged because they could act on only one request at a time. For example - John and Jill are both new employees with the same job function and they both submit requests to the same ten apps. The fulfiller, David, receives the request but in the legacy system, he can only see requests grouped by user, and not by application. Therefore he cannot tell that both John and Jill are looking for access to the same apps.

David starts working on John's request, and logs in and out of all ten apps, granting access to John. Then he closes John's request and starts working on Jill's. He has to log in and out of all ten apps all over again to grant access to Jill.

Working on fulfilling only one user's request at a time was both frustrating and inefficient. Fulfillers wanted to have access requests grouped by application, so that when they're logged into it, they can grant access to both John and Jill at the same time, improving speed and efficiency.

The whole access management operating model needed a transformation to support a different perspective

In the example above, our Client wanted easy ways to answer questions like:

- Are John and Jill requesting access appropriate for their role and responsibilities? What access do John and Jill need (not want) based on their role?
- How many users are requesting access to the same application?
- How many users must be assigned a specific role within the same application?

Automation was key. Reducing human error was imperative.

In David's words, *"The easiest way to steal something is to get permission granted."*

< PREVIOUS

NEXT >

The Solution

Automation requires meticulous attention to precision

The heart of this solution is the brilliant data model designed by David. INRY took David's data model and designed the IAG solution to remove complexity from the user request process and push it to the back end – where all relationships between user roles, applications, application roles and birthrights are maintained. This allows requests to be granted in mere minutes versus days.

INRY took David's data model and designed the IAG app to entirely remove this complexity from the user request process and push it to the back end – where all relationships between user roles, applications, application roles, and birthrights are maintained. This allows requests to be granted in mere minutes vs. days. Fulfillers can configure auto-approvals for certain privileges for certain roles. Users can only request access to applications and application roles that are relevant to their job functions.

INRY's solution incorporates all that and uses Request Management, workflow capabilities, and ServiceNow orchestration with the "secret sauce" data model to build the IAG workflow and capability. The added governance, review, and audit controls make the solution valuable.

IAG users can fully leverage the power of the Now platform. They can interact and cooperate with other teams using the platform, for example, IT Operations - server, network or database teams, application owners, and so on. They can also build on native Now capabilities like AI, NLP and integrations to enhance the IAG functionality.

When INRY shared this data model and governance structure with a Retail client in the continental US, they said it changed their view of Identity & Access Management. They implemented INRY's IAG solution shortly after David's organization went live.

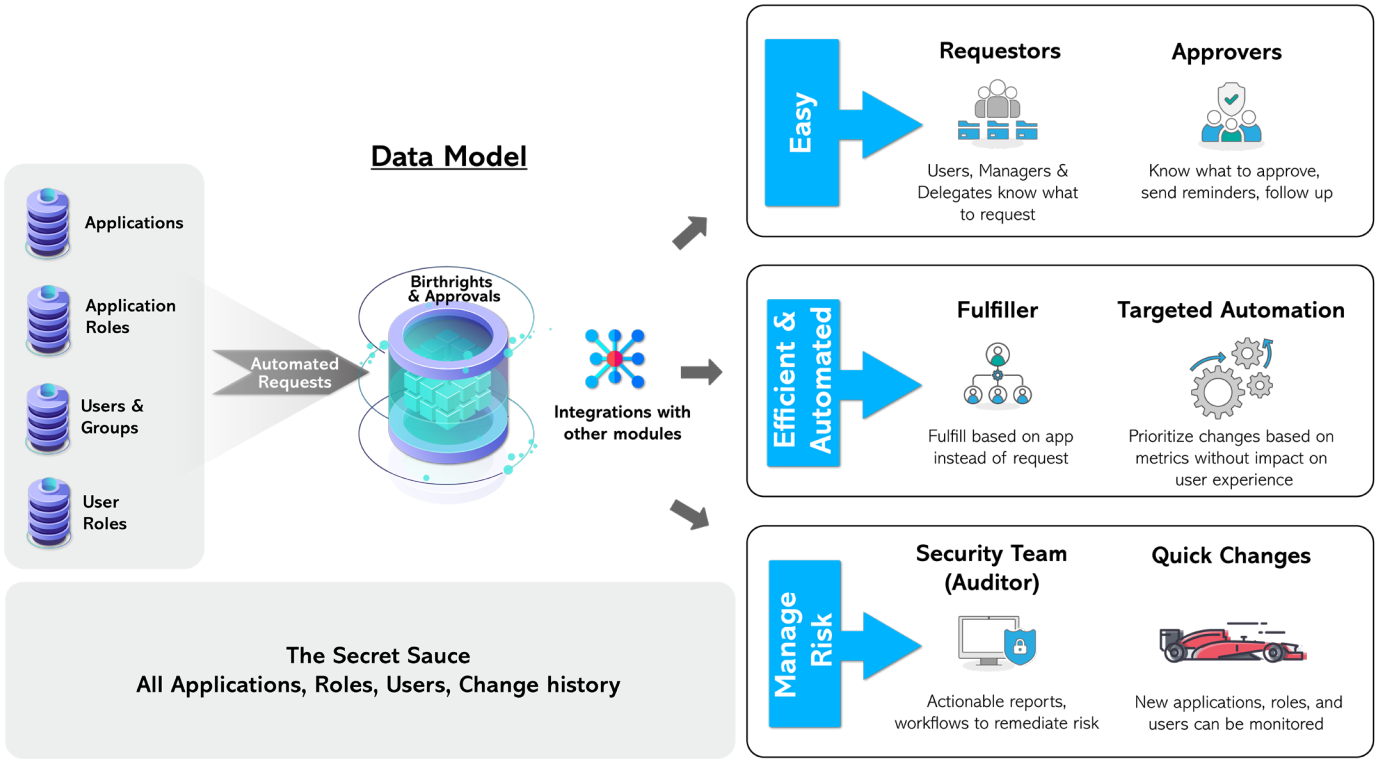
INRY's Identity and Access Governance solution can be maintained by Access Controllers. It provides an Efficient Agile Secure Experience (EASE).

< PREVIOUS

NEXT >

Data Model - The Secret Sauce

The secret sauce is the data model that stores all Applications, Roles, Users, Birthrights, Approvals and Change history.



< PREVIOUS

NEXT >

The Journey

Through this solution, our Client:

- Embedded access controls into the provisioning process. This assists with more controlled roles and better governance – users cannot get access to applications unless they're authorized.
- Reduced the number of people performing access management roles, thereby reducing human error, and enabling better governance.
- Can now manage, track, understand and control access for unprecedented volumes. IAG is built to scale and support Wynn's growth.

In addition, our Client integrated Identity and Access Governance with:

- Asset Management
- IT Operations
- Helpdesk

"One stop shop" – a single portal for the user to access everything

< PREVIOUS

NEXT >

Benefits

$250K in cost avoidance

2500 open request backlog has shrunk significantly – and their Identity and Access Governance process is a model of efficiency with zero (0) backlog. This gives our Client significant gains in their capacity to scale, while avoiding costs associated with their legacy process.

Lowered risk profile results in fewer errors

- Our Client's digital transformation of IAM has enabled a more proactive, front-end model.
- Automation has significantly reduced the scope for human errors, and the IAM team can focus on managing exceptions rather than routine requests.
- A central repository for their data also means fewer errors in audits and attestations.

15,000 people mobilized during the pandemic

INRY's IAG solution provides real-time visibility with dashboards and reports, allowing our Client to track and manage unprecedented volumes of requests.

Audit trails

Having the right processes and risk profile is valuable. But what makes it even better is the ability to prove it. The IAG solution tracks all changes to user access over time, including who approved and granted access. This helps with faster response times during annual audits and periodic reviews of administrative access to applications.

< PREVIOUS

NEXT >

Key Takeaways

Over-provisioning is a key driver of risk profile

- Identity and Access Governance has a huge role to play in Information Security

Energy is a key driver of success

- Access Management can be a complicated area
- ServiceNow as a platform can solve a myriad of platforms
- Our Client had a large ServiceNow program and vision but quickly realized that they could not do it all at once
- They recognized the need to stagger things and to structure a long-term roadmap
- Phase 1of IAG was to establish usability and deploy core functionality. In the future, they plan to enhance the user portal to be even more intuitive and enable self-service with automation by establishing birthrights for their applications.

Data model is the secret sauce

Identity and Access Management can be a complicated area. Our Client's success depended on having a documented data model and processes for execution, which they were able to share with INRY upfront. They created a data model that can store applications and application roles, users and user roles, birthrights to automate approvals and revocation, and access historical data for yearly audits.

In conclusion, David says that he wants to *"find bigger, better ways to make my life easier and Wynn more successful."*

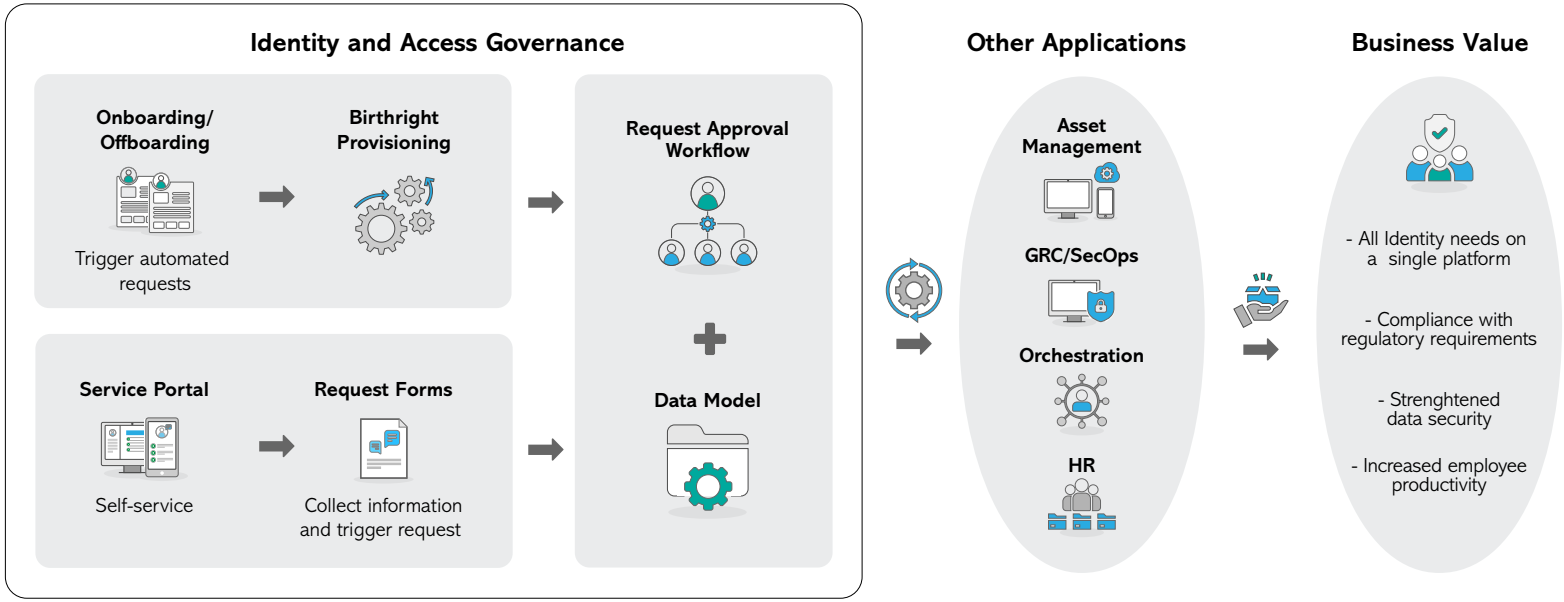
< PREVIOUS

NEXT >

Built on now

INRY

INRY's approach to Identity and Access Governance



INRY's Identity and Access Governance solution, Built on Now®, is a simple and intuitive solution that brings efficiency to access request management. Organizations can bring all their identity needs onto a single platform. Curb the risk of excessive access permissions by allowing - the right people, the right access, to the right resources, at the right time.

- **Enhance user experience** - Centralized intuitive self-service portal
- **Streamline IT workload** – Reduce the number of tickets sent to the IT helpdesk
- **Eliminate excessive access** - Embed access controls into the provisioning process
- **Accelerate access approvals** - Automate with predefined workflows
- **Improve cost savings** - through Integrated software asset management

< PREVIOUS