

Studies featuring Amazon Web Services (AWS) customers

Powering And Protecting The World At Work.

Saviynt



Contents

Danfoss	5
ENGIE IT	9
Gordon Food Service	13
Informatica	16
LIXIL	19
Lotus's	23
Origin Energy	26
Phillips 66	29
RingCentral	32
Syneos Health	35
University of Canterbury	38
Western Digital	41
Worcester Polytechnic Institute	44

Foreword

At Saviynt, our customers and partners are more than just buyers or vendors — together, we are a community of innovators. We are **ChangeMakers**, shaping the future of Identity Security.

To enable secure growth now and in the future, our customers have made the change to migrate from legacy on-premises solutions to embrace a new era of modern SaaS Identity Security with Saviynt. And we are committed to enabling this transformation by delivering continual value at scale.

We're bringing you a selection of real-world transformation stories from customers who are experiencing increased efficiency, operational savings, and enhanced security and scalability using the Saviynt Identity Cloud.

These are just some of the highlights:

- 80% risk reduction for audit-readiness and compliance
- New hire onboarding and accounts ready on day one
- Automated and just-in-time provisioning enabling company growth

It's a privilege to partner with visionaries like you, who are driving forward the Identity Security transformation. We are here to support and enable your success every step of the way!

We encourage you to engage with our team to work together toward even higher levels of success and value with Saviynt.



Paul Zolfaghari
President

Customer story
Danfoss

Award-Winning Deployment Achieves 83% Faster Onboarding

Danfoss forges more efficient, secure, and user-friendly governance for 45k identities across three continents.

The Danfoss logo is rendered in a red, cursive script font. The word "Danfoss" is written in a fluid, handwritten style with a thin red underline beneath the letters.

Founded in 1933, Denmark-based manufacturing and engineering company Danfoss is one of the world's top suppliers of manufacturing products delivering energy-efficient refrigeration, air conditioning and heating, variable-frequency drives, gas compressors, and mobile machinery.

As the 90-year-old Danish company readied for greater digitization and expansion to over 45,000 digital identities in more than 100 countries, it needed a more sophisticated solution to rapidly deploy efficient, reliable, and modern identity governance.

The Opportunity

Step one in this identity transformation was replacing its outdated Identity Governance and Administration (IGA) solution. Danfoss' existing on-prem platform consisted of multiple servers

Overview

Danfoss is a manufacturing and engineering company that designs and manufactures products and services to help the world use resources more efficiently

Number Of Employees

41,928

Headquarters

Nordborg, Denmark

Industry

Manufacturing

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

45,000

in different environments that were time-consuming to manage and taxing to maintain. All aspects required customization, and processes that should have taken IAM teams a couple of months often dragged on for a year or more.

Users also had long-standing complaints about its confusing interface, which was hard to navigate and harder to use. The previous solution was on-premises and unavailable for employees outside the network.

Danfoss needed a more efficient, reliable IGA solution that could scale easily and reduce human error. It wanted to automate joiner, mover, and leaver (JML) scenarios to expedite onboarding, improve user access and certifications, and ensure privileged accounts weren't running into Separation of Duty risks. Danfoss also needed to manage the lifecycle of its external workforce and third parties, meet compliance standards, and expand the quality of its IGA analytics and reporting.

To meet this high bar, Danfoss chose Saviynt Enterprise Identity Cloud.

The Solution

Initiating in late 2020 at the height of the pandemic, Danfoss' transition from legacy to cloud faced some daunting challenges. The implementation would span 100 countries and three continents, and all drafting, planning, and collaboration would have to be done 100% remotely in virtual workshops.

It also had to be fast: an impending acquisition of another major industrial manufacturer would grow Danfoss by a third – and would put their new system to the test.

Danfoss, Saviynt, and partner Nixu chose a 'big bang' approach to implementation. Every employee in every region – as well as contractors, service and admin accounts – would be impacted at once.

The collaboration not only achieved a 1:1 replacement of the old system but successfully delivered improved, simplified, and automated workflows across the globe – all before the company's acquisition.

The groundbreaking deployment caught industry recognition, winning the Identity Fabrics & Enterprise IAM Project of the Year award in KuppingerCole's European Identity and Cloud Conference.

The Results

With new, fully automated API integrations to Danfoss' HR and ITSM systems, the company's IAM teams were able to create a user account for a new hire in eight hours, and set up a shared mailbox in half the time. Managers can even initiate the request before the employee's first day. Before Saviynt IGA, this manual process required chasing down a flat file from HR and could take as long as 48 hours per request.

As a manufacturing and engineering business, Danfoss also had to manage many constantly changing contractors and service accounts. Maintaining secure provisioning and de-provisioning of these accounts was crucial to mitigate risk. With Saviynt, access requests for contractors and contingent workers now go through four sets of eyes for approval. Each worker to electronically accept Danfoss terms of use before gaining access to a user account.

Gone are the days of chasing "orphaned" accounts with time-consuming, manual processes every quarter. Now, Danfoss can run scheduled reports every week. Rather than focusing all their time and energy on keeping their solution running, the IAM team is freed up to focus on value-adds like data-driven analytics and developing integrations for more applications.



Transparency builds trust

"We always felt we were in control and could keep track of the big picture," said Daniel Tunes, Director, Head of Identity & Access Management at Danfoss.

"Saviynt and Nixu discussed how to tackle every challenge, the trade-offs that different solutions offered, and whether something might involve additional costs. This helped us build a lot of trust."



A 'think big' approach can pay off

When replacing an existing identity management suite, expanding beyond the workforce to include contractors and service accounts delivers broad capabilities and room to scale.

“

Executing a project of this size, across three continents and multiple time zones, during a global pandemic was a major achievement. The spirit of collaboration and sense of teamwork was invaluable in delivering the project in time. Saviynt did a wonderful job.

”



Daniel Tunes
Director, Head of Identity & Access
Management, Danfoss



Customer story
ENGIE IT

ENGIE IT Consolidates IAM Platforms And Automates Legacy Processes

Multinational utility achieves immediate cost savings and simplified identity security for 40,000 users.



ENGIE SA is a French multinational utility company, headquartered in La Défense, Courbevoie, operating in the fields of energy transition, electricity generation and distribution, natural gas, nuclear, renewable energy, and petroleum. Supplying electricity in 27 countries in Europe and 48 countries worldwide, the utility employs 100,000 people worldwide with EBIT in 2022 of €9.0 billion.

ENGIE IT is a business support subsidiary of ENGIE GBS in charge of IT, employing 600 people. **Its mission is to operate for the ENGIE Group in 5 main services areas:**

- Network and Cybersecurity connects all the Group's entities worldwide, providing ENGIE's digital foundations and meeting the challenges of cybersecurity.
- Cloud Infrastructure manages the Group's IT production resources in a cloud hybridization approach
- Digital Workplace deploys the Group's digital assets to end users.
- Digital and IT Consulting secures the success of the Group's major projects.
- Agile business solutions deploy and support the Group's business strategies.

Overview

A French multinational electric utility company

Number Of Employees

100,000

Headquarters

La Défense, France

Industry

Energy, Utilities & Waste

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

40,000

To simplify their infrastructure, boost security, and gain the flexibility to respond to new security challenges, ENGIE IT chose to move to the cloud. After considering several solutions, they selected Saviynt because it provided the visibility they needed and allowed them to connect to their diverse endpoints with a single solution.

The Opportunity

ENGIE IT's initiative was to simplify their infrastructure with a single, cloud-first tool — and to have every new service live in the cloud. To do this, they had to migrate away from multiple legacy IAM tools to a unified, cloud-native tool that could better manage their diverse endpoints and target systems.

ENGIE IT's existing identity infrastructure depended on two main legacy systems that were over 10 years old. The passage of time and the complex nature of the business required the systems to become highly customized, making processes complicated and evolution impossible.

It also became more and more difficult to update and upgrade the versions of both tools.

Huge efforts were required to respond to new security needs or to obtain the proper security patches because their legacy systems were no longer supported. For example, access to SAP required inspection of logs in multiple accounts in the different tools to understand who was making the request, who approved or validated it, and when or where it was made. This could take up to half a day using an asynchronous process.

The Solution

ENGIE IT needed a solution that would ensure that identity became the single source of all authorizations in SAP and that would eliminate any security gaps. Their initiative was designed to:

- Reduce the cost associated with managing multiple IAM tools
- Eliminate parallel processes in SAP
- Provide more effective traceability to the audit teams (provide the proof expected from the controls)
- Align with ENGIE's group-level, cloud-first strategy of moving more services to the cloud

The Results

With Saviynt IGA, ENGIE IT completed the migration from legacy systems and now operates fully in the cloud. The utility achieved better visibility and control, improved SAP lifecycle management, and the ability to secure 40,000 employees at the group level.

 **Improved control of access authorizations to SAP.**
Today, B2C apps are fully managed by Saviynt (including certify and grant authorizations), and all accounts are created through Saviynt.

 **Cost reduction from day one.**
The implementation of lean processes at a group level made considerable cost savings possible — including an immediate \$500K reduction directly tied to IGA transformation.

 **Improved visibility.**
A unified view of SAP with centralized data simplified the management and detection of existing and orphaned accounts.

 **Seamless integrations.**
Saviynt's solution connected to SAP, AD systems, ServiceNow, and application API provisioning. For SAP priority business apps, ten key endpoints / target systems in both production and non-production environments, including support, were all integrated.

 **10-minute access authorizations.**
Once a request is received, access to SAP can now be managed and granted with just a few clicks.

 **Easier compliance.**
Internal auditors spend much less time checking and looking for the information required during the audit process.

By optimizing the internal processes, Saviynt helped Engie IT make users more autonomous while maintaining the traceability required for the audit team. Saviynt also enhanced security by providing greater visibility of orphaned accounts, enabling current authorizations of any employee to be properly reviewed with reports sent automatically to high-level SAP management teams to confirm or deny authorizations.

Engie's future plans include more fully utilizing Saviynt's functionalities with an eye toward moving to Saviynt's converged identity platform, Enterprise Identity Cloud.

“

We chose Saviynt because it was a full cloud solution. There was no hybrid infrastructure. It was less technical than other solutions we considered, so there was no need for custom coding by professional services. The platform was configuration-centric.

”



Martial Rozec
Service Delivery Manager,
ENGIE IT



Customer story
Gordon Food Service

Modernizing Identity Governance & Accelerating Compliance Maturity

Saviynt helped Gordon Food Service transform a patchwork of legacy on-premises Identity Management (IDM) systems into a modern, cloud-native IGA solution to meet short and long-term security and compliance objectives.



Already the largest family-operated broadline food distribution company in North America, Gordon Food Service was preparing for additional growth. Looking to gain a competitive edge by expanding into new regional markets, the company needed a modern technology infrastructure to support its business strategy. With Saviynt's solution, Gordon Food Service was able to manage identity lifecycles at enterprise scale across a diverse hybrid computing environment while automating compliance processes and improving end-user experience.

The Opportunity

Gordon Food Service embarked upon the implementation of a new cloud ERP solution as part of a broader digital transformation initiative designed to support growth. But the company was reliant upon a combination of three different legacy on-premises identity management systems.

Overview

A prominent family-owned food distributor serving restaurants, healthcare, and schools

Number Of Employees

20,000

Headquarters

Grand Rapids, MI

Industry

Foodservice distributor / Wholesale

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)
- Application Access Governance (AAG)

Number Of Identities Managed

18,000

This patchwork approach created visibility issues that were greatly amplified by the migration into a more complex cloud ecosystem.

What's more, with the legacy approach, it was challenging to integrate new applications and endpoints, end users were experiencing unnecessary friction, and the company couldn't meet its security and identity governance objectives. It was simply impossible for Gordon Food Service to build the comprehensive enterprise-wide identity governance framework they needed.

The Solution

Saviynt's cloud-native identity governance and administration (IGA) solution provided a solid foundation for the company's new identity and security strategy. With this new solution, Gordon Food Service has been able to:

- Modernize identity management capabilities for over 18,000 users across more than 256 applications and 21 connected systems in a diverse hybrid computing environment
- Implement an access governance solution that's fully integrated with its new cloud ERP system
- Perform attestations for enterprise roles and fine-grained entitlements based on risk
- Establish a single source of truth for identity governance that can be administered within an easy-to-use dashboard
- Remove friction for end users with self-administered permissions

The Results

Gordon Food Service has built a solid foundation for a future-facing identity and governance framework.

With Saviynt's IGA solution now in place, Gordon Food Service has set the cornerstone for an enduring identity governance and security strategy that will span the entire enterprise. Gordon Food Service now enjoys:

- ✔ **Continuous compliance monitoring** across a complex on-premises and cloud hybrid ecosystem
- ✔ **Enhanced employee satisfaction** with the solution's modern and intuitive interface
- ✔ **Accelerated security maturity** through enhanced visibility and reduction of real-world identity risks
- ✔ **Improved efficiency** with seamless integrations of important applications and new endpoints

“

Before, when we didn't have a modern solution, we felt stagnant. Today, we're in a much better place. Overall, the implementation has been a success, and the Saviynt team was fantastic. ”



Paul Dumbleton
Former Enterprise Information
Security Team Manager,
Gordon Food Service



Customer story
Informatica

Informatica Reimagines Its Future Through Saviynt Technology

Informatica chooses Saviynt to spearhead its forward-thinking approach to the future, citing its 'Best of Breed' cloud solution technology.



Informatica

When Informatica shifted its business model it created a dual challenge: service the customer under a revolutionary cloud-based platform while pushing IT to its full capabilities to protect the new business model. Kamakshi Lall, Informatica's Information Security Compliance Manager, lends her insight into how the company determined their needs going forward, for both the business and IT, and completed their transformation through Saviynt.

The Opportunity

Informatica delivers award-winning data technology and industry leading data management solutions. As the world leader in Enterprise Cloud Data Management, Informatica's solutions and products are utilized around the world by game-changing corporations seeking a holistic approach to security.

Overview

A leader in enterprise AI-powered cloud data management

Number Of Employees

5,000

Headquarters

Redwood City, CA

Industry

Software

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

5,000

With notable customers like JLL, Nissan and Kelly Services, Informatica provides strategies that help data-driven digital transformations, enabling the next generation of intelligent enterprise to operate under an umbrella of security and privacy.

Informatica underwent a huge shift in strategy when it moved from a public company to a private firm. The changeover came at the same time Informatica moved from a perpetual licensing model to a cloud subscription model. But how they provided service to their customers was just the beginning of their challenge: Informatica had to launch its internal IT business into the future very quickly to securely meet their new business goals. Decentralized requests and incident tickets, a disjointed approval chain, lack of audit trail, and time lost on request fulfillment were stifling Informatica's fast pace of change.

The Solution

Informatica turned to Saviynt for a state-of-the-art solution to their combined business and technical needs.

The Results

- ✓ **Centralization in Snow** as the single point of entry for all requests and incidences
- ✓ **Easy plug-in request** framework for new applications to be onboarded in the future
- ✓ **Fully automated** approval chain
- ✓ **Established single source of truth** for audit trail
- ✓ **Introduced Saviynt** as the go-to provisioning engine

“

It's been an excellent journey so far. ”



Kamakshi Lall
Information Security Compliance
Manager, Informatica



Customer story
LIXIL

LIXIL Futureproofs Its Global Identity Management System With Modern Cloud IGA

Streamlines Security and Compliance across more than 150 countries.

LIXIL

The Opportunity

LIXIL, headquartered in Tokyo, is a global leader in water and housing products. LIXIL offers pioneering solutions that make better homes a reality for everyone, everywhere, through a unique portfolio of global brands, including INAX, GROHE, and American Standard. LIXIL operates in more than 150 countries, and its products touch the lives of more than a billion people every day.

Each market LIXIL serves has distinctive language, culture, and local construction industries, requiring tailored customer service, on-time delivery, and specialized products. To maintain a competitive edge, LIXIL needed to create operational efficiencies across its global operations.

As a company, it is essential to create operational efficiencies to maintain competitive advantage in a sector where customers, contractors, installers and property developers are always looking for the best value.

Overview

LIXIL is a maker of pioneering water and housing products.

Number Of Employees

53,000

Headquarters

Tokyo, Japan

Industry

Manufacturing

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance & Administration (IGA)
- Application Access Governance (AAG)
- Privileged Access Management (PAM)

Number Of Identities Managed

70,000

LIXIL needed to bring value-creating efficiencies, as well as consistency and standardization, to its enterprise-wide identity management processes. The company's existing approach to identity management was centered on a homegrown, bespoke application that had been built primarily for its Japanese employees.

The legacy system couldn't scale to meet the needs of a growing international workforce, especially since LIXIL's 2014 acquisition of Grohe brought a large number of Germany-based users into the company. These employees, along with others in Europe, must adhere to the provisions of the General Data Protection Regulation (GDPR), including data residency requirements.

LIXIL's IT team envisioned a future where identity governance was streamlined, compliance was simplified and audits were a breeze. They aimed to empower employees with a seamless experience, boosting morale and fostering collaboration. To achieve this vision, LIXIL turned to Saviynt's Identity Cloud.



The exceptionally strong relationships that we enjoyed with the LIXIL team in Japan — cutting through significant language and cultural barriers — contributed a great deal to the implementation's success. LIXIL and Saviynt teams have worked as ONE TEAM towards this success. This collaboration has helped us learn a lot and we are grateful to LIXIL for the opportunity!



Karthik Satish Kumar

Vice President – Customer office, Asia Pacific & Japan, Saviynt

The Solution

After an intensive evaluation process that took several months and included a successful pilot program, LIXIL selected Saviynt's Identity Governance & Administration (IGA). Saviynt's IGA platform was able to meet LIXIL's requirements, especially the key requirement to modernize legacy processes without disrupting operations due to the flexible cloud-native solution.

The solution's ability to meet both global and diverse local requirements such as data residency for GDPR and Japanese language user interfaces in Japan were also strong points.

Our team collaborated with Saviynt Expert Services to engineer a successful multi-phase deployment. The strong relationships between the two teams kept the project on track and ensured high-quality outcomes.

Saviynt IGA could seamlessly ingest the complex file structures generated by legacy systems. The implementation also integrated modern cloud capabilities with existing processes. This enabled LIXIL to standardize identity management across an array of human resources (HR) databases from multiple different subsidiaries, simplifying compliance while unifying disparate systems and processes across the enterprise.

Along its cloud modernization journey, LIXIL adopted the human capital management system SuccessFactors, which will eventually become a single source of truth for identity. Their team is in the process of decommissioning its homegrown legacy identity management engine - a significant step towards greater efficiency.

LIXIL's employees now enjoy faster, smoother onboarding processes, while the company benefits from reduced compliance and cybersecurity risks. Rapid, standardized offboarding, segregation of duties, better audit controls, and improved reporting capabilities all mitigate business risk cost-efficiently. The ability to integrate Third-Party Access Governance (TPAG) within a single platform makes it easy to extend these capabilities to a global network of vendors and contractors.

✔ **Improved user experience** through streamlined employee onboarding/offboarding and self-service provisioning.

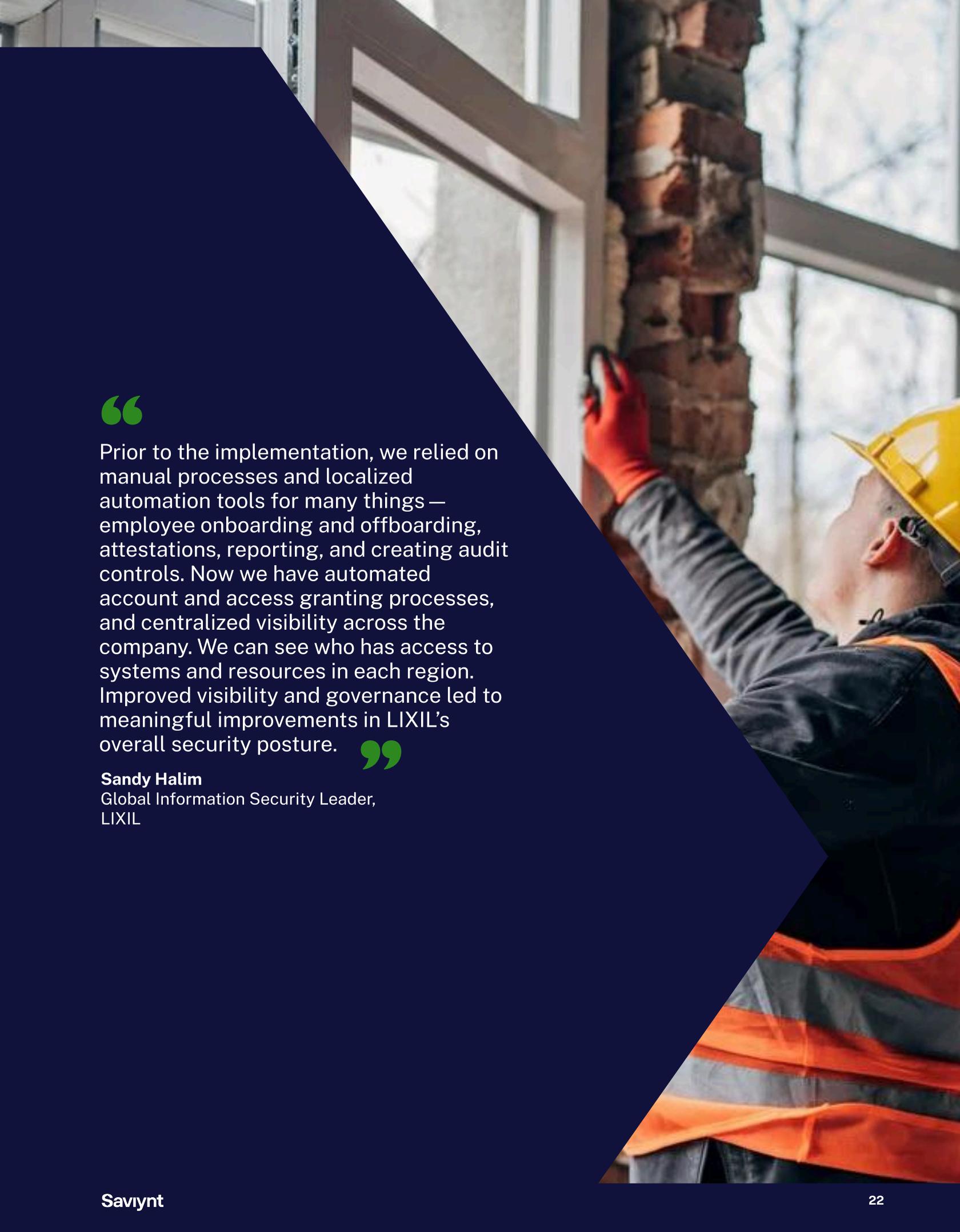
✔ **Granular identity visibility** for more than 70,000 internal and third-party users across a diverse and expanding application ecosystem.

✔ **Proactive audit readiness** through automation, standardized controls, and improved reporting capabilities.

✔ **Modernizing identity-related workflows** on a single, consolidated cloud platform.

The Results

Saviynt IGA has helped LIXIL harmonize its identity management practices across a complex global ecosystem. Employee onboarding processes are now streamlined and consistent, governance has been improved, and it's faster and easier to prepare for audits. Automation is creating compounding efficiencies, while the platform allows for centralized visibility and control. Next steps for LIXIL include implementing cloud-native privileged access management (PAM) and onboarding additional applications to build on their team's momentum.



“

Prior to the implementation, we relied on manual processes and localized automation tools for many things — employee onboarding and offboarding, attestations, reporting, and creating audit controls. Now we have automated account and access granting processes, and centralized visibility across the company. We can see who has access to systems and resources in each region. Improved visibility and governance led to meaningful improvements in LIXIL’s overall security posture. ”

Sandy Halim

Global Information Security Leader,
LIXIL

Customer story
Lotus's

Streamlining Provisioning And Identity Lifecycle Management

Simplifying identity governance & administration in a complex retail environment.

Lotus's

Lotus's is a leading Southeast Asian grocery retailer based in Thailand, with stores across the Malaysian peninsula. Previously owned by a UK grocery giant, Lotus's was sold back to a former owner in February 2021. The split necessitated significant technological transformation.

Tasked with building a new identity technology stack from the ground up, Lotus's had the opportunity to streamline workflows, introduce new efficiencies, and improve user experience.

The Opportunity

When Lotus's was sold back to its former owner, Thailand's Charoen Pokaphan (CP) Group, it needed to implement a new identity and access management platform quickly. With a target project timeline of just 8 weeks, it required a solution deployed at cloud speed to deliver rapid ROI.

Overview

Lotus's (formerly Tesco Lotus) is a retail chain in Thailand operated by Charoen Pokphand (CP) Group

Number Of Employees

60,000

Headquarters

Bangkok, Thailand

Industry

Retail

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

60,000

Lotus's also wanted to accelerate its cloud transformation journey by implementing an IGA platform that would automate provisioning, simplify controls, and streamline workflows. Saviynt's cloud-architected solution allowed Lotus's team to create 60,000 Active Directory (AD) accounts and onboard more than 20 applications over a short timeframe with a roadmap to onboard 300 applications eventually. Today, role-based access controls (RBAC) based on job roles and AD groups enable new hires to get secure access to all the resources they need to do their jobs – on their very first day at work.

The Solution

Lotus's chose Saviynt's cloud-native Identity Governance and Administration (IGA) platform. With this solution in place, Lotus's has:

- Automated identity lifecycle management for over 60,000 users across two countries and a variety of stores, warehouses, and third-party vendor and partner environments
- Configured and maintained the platform in-house – since it requires virtually zero customization or coding
- Onboarded more than 20 applications into the platform within days by relying on a template-based approach
- Streamlined access reviews for audit purposes
- Migrated and consolidated AD accounts for employees in Thailand and Malaysia – 60,000 new policy-based AD accounts were created on a consolidated domain within hours

The Results

Lotus's has elevated its Identity and Security Maturity. Since implementing Saviynt's IGA solution, Lotus's now benefits from:

- ✓ **Fast-tracked access provisioning** with RBAC that automatically approves low-risk requests to give employees full access to the right resources from their first day on the job
- ✓ **Greater agility** with streamlined identity workflows and all the benefits of a cloud-native solution
- ✓ **Enhanced efficiency** that makes it possible for a small security and identity team to achieve enterprise-grade results
- ✓ **Time and labor cost savings** due to efficiencies introduced by automation

“

We needed a product much easier to configure and manage than our previous solution. Saviynt's cloud-native IGA solution fit the bill and also saved our team significant time and costs during implementation. ”



Sittichai Pongpaisarnsri
Identity and Access Management
Manager, Lotus's



Customer story
Origin

Securing Compliant Access For Origin Energy

Saviynt helped Origin overhaul their legacy Identity and Access Management product with a state-of-the-art IGA solution that supports both present and future initiatives.



The Opportunity

Origin develops, produces, and delivers natural gas and renewable energy, supporting a business mission of supplying affordable and sustainable energy to all its customers. The organization's purpose is getting energy right for its customers, communities and the planet. It does this by making energy more affordable and more sustainable, smarter and easier.

Origin Energy's outdated Identity and Access Management (IAM) tool limited its ability to scale, created operational friction, and inhibited access to mission-critical applications and data.

Origin Energy's employee onboarding took more than 10 days to provision birthright access. There was also a lack of compliance visibility and governance. Compliance controls had to be measured across applications, a process that was manual and complex — and therefore error-prone, high

risk, and costly. Another issue was their inability to monitor identity. Adopting a hybrid IT infrastructure and multiple cloud solutions created access management issues that inhibited dynamic identity monitoring.

Overview

Origin Energy is an integrated energy company supplying electricity and gas to over four million customers in Australia

Number of Employees

6,300

Headquarters

Sydney, Australia

Industry

Energy, Utilities & Waste

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)
- Application Access Governance (AAG)

The Solution

Saviynt's Enterprise Identity Governance and Administration platform provided the foundation for a holistic identity lifecycle management and application risk and compliance program to secure critical enterprise and IT assets, including:

- Out-of-the-box, granular connectors for SAP, Oracle, and other mission critical applications
- Rapid onboarding and frictionless, on-demand scalability in a truly cloud-native digital platform
- A 'single pane of glass' cornerstone to provide full visibility user access across enterprise applications, including ERP systems
- Governance for BOTs, Internet of Things, and control systems with risk avoidance
- Automated user access reviews that reduced human errors and provided analytics-driven access recommendations
- Analytics-based continuous monitoring and consistent reporting to all stakeholders
- An integrated single source of visibility for security, audit, and compliance programs
- Rules-based birthright access that reduced provisioning time for core and critical applications from 10 days to 24 hours

The Results

Significantly improved application access administration and onboarding processes in six months.

- ✓ Drastically reduced birthright access provisioning from 10 days to just 1 hour from HR entry
- ✓ Eliminated manual processes through automation and consolidation of identity clean-up actions
- ✓ Automated enterprise-wide access reviews
- ✓ Provided visibility for executives into the enterprise compliance posture across ERP applications
- ✓ Deployed identity as the foundation for workforce enablement and securing hybrid IT assets
- ✓ Reduced costs, improved audit support, and set a strong foundation for future initiatives

“

The automation of our joiner-mover-leaver process and the push-button user access review campaigns — these capabilities have been a game changer for Origin. For one of our larger applications, we've given 200 hours back to the organization.

”



Vanessa Gale
Head of IAM,
Origin



Customer story
Phillips 66

Journey To The Cloud With Phillips 66 And Saviynt IGA

Saviynt helped Phillips 66 with their IGA modernization initiative, building more resiliency and flexibility into their program and enabling them to migrate away from unsupported legacy systems.



With nearly 150 years of experience, Phillips 66 is a diversified energy manufacturing and logistics company with unique businesses in Refining, Midstream, Chemicals, and others.

The company is engaged in refining, transporting, and marketing natural gas liquids petrochemicals. They are also active in research and development of emerging energy sources and partners with Chevron. A Fortune 500 company headquartered in Houston, Texas, Phillips 66 has approximately 14,000 employees worldwide and has operations in the United States, United Kingdom, Germany, Austria, and Switzerland.

In 2019, Phillips 66 embarked upon a digital transformation effort. Their existing Identity Governance and Administration (IGA) program was based on an on-premises Quest Identity Manager solution that was no longer being supported and did not integrate with cloud applications.

Overview

Phillips 66 is a diversified energy manufacturing and logistics company with unique businesses in Refining, Midstream, Chemicals, and Marketing and Specialties

Number of Employees

14,000

Headquarters

Houston, TX

Industry

Energy, Utilities & Waste

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

25,000

The IGA modernization initiative – informally called Journey to the Cloud – focused on building more resiliency and flexibility into their program. To future-proof their program, they were looking exclusively at cloud-first solutions that could support a hybrid environment initially during the cloud transformation. Price was a secondary consideration at the time.

With Saviynt, Phillips 66 was able to modernize with a cloud-native solution that simplifies IGA by increasing organizational agility through automation and intuitive workflows. Saviynt IGA also helped Phillips 66 ensure users have seamless app and infrastructure access without compromising compliance. As a future-proof, cloud-first solution, Saviynt IGA provides seamless, secure access to necessary resources on-premises, in the cloud, and in hybrid environments.

The Opportunity

Phillips 66 needed an IGA solution that could create a strong foundation for a holistic digitally-enabled environment and increase functional IGA capabilities across all of the company's functions. The security team also wanted to ensure standardization and consistency of control execution, processes, and tools to improve user experience and enforce governance and regulatory compliance.

With these goals in mind, they formulated a three-year, three-phase initiative that started with moving their IGA program to the cloud.

The first year was to be the “lift and shift” of all the existing functionality. The second year would be the build out of the attestations and the access certifications, and the third year would focus on application access governance for critical systems such as SAP.

But in the first half of 2020, COVID hit and budgets were cut. At a moment’s notice, their plans had to change. Because overall business was down for energy companies, price was now a major consideration, as was speed of deployment. As a result, Phases Two and Three were put on hold, and there was immense pressure to deploy Phase One as soon as possible.

The Solution

When evaluating solutions, Phillips 66 used a 300-point Proof-of-Concept (POC) trial that included flexibility and ease of use, robust workflows, permissions granularity, and the ability to integrate with multiple endpoints, both on-prem and in the cloud. Phillips 66 had been using homegrown on-prem Active Directory-based tools to manage their access certification/attestation efforts that added several levels of complication to the process.

They chose Saviynt IGA because it ranked as the highest-scoring solution on their POC trial, indicating that it was the right solution to meet their needs.

“

Our on-prem solution could only manage other things on-prem, and Saviynt has the ability to manage things both on-prem and in the cloud, so that was one of the things that made us realize that this is really a good solution for us in both realms.

”



Mark Ivy
Director, IAM,
Phillips 66



Customer story
RingCentral

RingCentral Achieves Multi-App Integration In 4 Months

A global cloud-based communications company switches to Saviynt for rapid, cost-effective identity management after issues with a competitor's implementation.

RingCentral[®]

RingCentral is a global provider of enterprise cloud communications, video meetings, collaboration, and contact center solutions. Eighteen months into their deployment with a leading identity platform, they faced high costs and challenges due to the tool's inability to integrate with critical applications and alleviate manual processes. RingCentral decided to evaluate alternative vendors prior to their upcoming renewal date. After an extensive evaluation of several vendors, RingCentral chose Saviynt and successfully integrated multiple apps in only 4 months, automated the identity lifecycle for thousands of users, and saved their company significant time, money, and manpower.

The Opportunity

As their subscription service with a leading identity provider approached its renewal date, RingCentral began to evaluate mounting challenges. Their existing solution could not integrate

with their cloud-based support ticket software, which was essential to serving their customers. Its limited interoperability kept their Global Services Team inundated with manual processes, making role governance and access certifications impossible to scale.

In addition, each time RingCentral's team needed to deploy new code on the back end, they had to seek approval from the solutions provider's Professional Services team. The cost of ownership continued to rise as every call for product support — and every connector needed — incurred an upcharge.

RingCentral began searching for a SaaS tool that would be easier to configure and integrate with their service portal, deliver automated lifecycle visibility, and meet key compliance mandates — with a lower total cost of ownership. After considering leading solutions on the market, RingCentral was satisfied that Saviynt could deliver the features they had been missing.

The Solution

During implementation, the “lift and shift” motion away from the competitor's solution to Saviynt's cloud-native platform was seamless and straightforward; the hassle-free integration with their on-prem applications saved RingCentral significant time and cost. In four months, they successfully onboarded and configured multiple apps, including their service portal. They had pursued this milestone unsuccessfully with their previous tool for over two years.

Overview

RingCentral is a provider of cloud business phone systems designed for today's mobile and distributed workforce

Number Of Employees

7,500

Headquarters

Belmont, CA

Industry

Software

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

7,500

With Saviynt's automatic provisioning, time-consuming approvals were finally a thing of the past.

RingCentral was able to deploy automated identity lifecycle management for thousands of users — from pre-hiring all the way through final termination — and reconcile thousands of active and inactive user accounts. Saviynt also helped RingCentral create analytic reports with the right customizations, putting the company on target for its data security and compliance management goals. With Saviynt's automatic provisioning, time-consuming approvals were finally a thing of the past.

RingCentral was able to deploy automated identity lifecycle management for thousands of users — from pre-hiring all the way through final termination — and reconcile thousands of active and inactive user accounts. Saviynt also helped RingCentral create analytic reports with the right customizations, putting the company on target for its data security and compliance management goals.

The Results

Saviynt outperformed leading identity competitors and empowered RingCentral to:

- ✓ Integrate with their service desk portal and **successfully onboard multiple apps** in four months
- ✓ **Reduce process complexity** and automate the identity lifecycle management for thousands of users
- ✓ **Unify visibility** from one central platform
- ✓ **Deliver pricing transparency** and reduced TCO
- ✓ Position their infrastructure to **successfully meet new compliance mandates**
- ✓ **Launch two different types** of user access reviews
- ✓ **Reconcile** thousands of active and inactive user accounts

“

The solution RingCentral was using prior to Saviynt needed custom coding or involvement with the vendor's professional services team. With Saviynt, RingCentral was able to perform many of these previous complex actions through the Saviynt UI allowing us to go in directly, build the code, and deploy it ourselves.”

Simran Kaur
Senior IAM Administrator, RingCentral

”

Customer story
Syneos Health

Syneos Health Futureproofs Identity Governance for Flexibility and Rapid Growth

Since implementing Saviynt IGA, Syneos Health has experienced a dramatic increase in user lifecycle management efficiency.



The Opportunity

Offering fully integrated end-to-end clinical and commercial solutions to biopharmaceutical companies to accelerate the delivery of life-enhancing therapeutics to patients, Syneos Health is currently among the healthcare industry's leading innovators.

As it prepared for the future of biopharmaceutical research, Syneos Health needed to embed increasing numbers of applications into its clinical and operational workflows. The company's outdated identity management system wasn't up to the task: it wasn't scalable, was difficult to manage, and couldn't easily be integrated with key business applications.

Instead, Syneos needed an identity governance and administration (IGA) solution that could effortlessly expand along with the business and its user base, all while streamlining identity

and access management within a single, centralized platform.

The Solution

Syneos Health's journey towards modern cloud-native identity governance began with implementing Saviynt IGA. The platform's native integrations with many of the company's core business applications — including finance and human resource management systems — eliminated the need to build custom connectors. Technical leaders also valued Saviynt's low-code/no-code approach to configurability, which makes it possible to adapt the platform to meet business requirements as soon as they arise.

Saviynt IGA has given identity and security teams at Syneos a single source of truth, making it easy to synchronize key attributes and permissions across multiple identity stores, including Active Directory. With centralized visibility, they've removed standing privileges, eliminated duplicate accounts and unused permissions, and accelerated their progress towards Zero Trust adoption.

Syneos has also been able to automate multiple governance workflows across its identity ecosystem, reducing administrative overhead by removing manual steps from certification campaigns. The platform's intelligent access request and entitlement review capabilities make for seamless user lifecycle management, keeping employees happy and productive.

Overview

Syneos Health is a global company that provides contract research and commercial services to the biopharmaceutical, dental, medical device, diagnostics, and animal health industries

Number of Employees

30,000

Headquarters

South San Francisco, CA

Industry

Biopharmaceutical solutions

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

30,000

The Results

Since implementing Saviynt IGA, Syneos Health has experienced a dramatic increase in user lifecycle management efficiency. Not only is it quicker and easier to onboard and offboard employees, but change requests can be accomplished in 75% less time, thanks to Saviynt's low-code/no-code workflows. The organization has been able to replace PeopleSoft and Oracle EBS, secure 240,000 entitlements and integrate 39 applications. Ultimately, it has eliminated standing privileges for more than 30,000 users, while building out a quick and effective automated process for fulfilling access requests when needs arise. This efficiency is a win at every level of the organization.

✓ **The road to the cloud is paved with documentation.** Before selecting a product, know the exact steps taken during employee onboarding and offboarding, and what data formats dependent systems require. This helps inform the integrations and connectors that you need.

✓ **With a single source of truth, all the pieces of the identity puzzle fall into place.** Moving IGA to the cloud will automatically reduce the number of systems you have to manage, making it easier to centrally manage auditing and reporting, and simpler to eliminate access risks.

✓ **Make a three-month, one-year, and five-year plan.** The longest-term plan should highlight the bigger picture, the one-year plan focuses on what's attainable within a single budgeting cycle, and the three-month plan tracks in-flight tasks to ensure you can achieve your goals.

✓ **The best IAM and IGA implementations cause the least friction for users.** A new technology will be adopted much more quickly if people enjoy working with it. Things like passwordless and biometric authentication make people's lives easier while also safeguarding information assets.

“

None of us expected the level of visibility that Saviynt provided. It lifted the curtain. As the business makes new requests of us, we can immediately change our flows or ways of doing things. We've become far more flexible, agile, and ready for a fast-changing world.”

Mike Rivett
Principal Solutions Architect,
Syneos Health



Customer story
University of Canterbury

Realizing A New Vision For Identity Governance: One Identity For Life

Simplifying IGA in a complex higher education environment.

Saviynt helped the University of Canterbury build a centralized, streamlined Identity Governance and Administration (IGA) hub to facilitate automation, self-service account provisioning, and role-based access controls across an inherently complex higher-ed environment.

An internationally recognized research university known for its excellence in law, engineering, and a diverse array of degree programs, the University of Canterbury is New Zealand's second-oldest institution of higher learning. Like many higher ed institutions, the university provides IT resource access to a large and particularly dynamic user population. It's not uncommon for students to also serve as research assistants or temporary staff or for employees to enroll in courses. The university's identity and security teams must manage joiner/mover/leaver identities throughout these complex and ever-changing life cycles while ensuring that they can maintain granular control and visibility.

Overview

The University of Canterbury, founded in 1873 as Canterbury College, is a public research university

Number of Employees

3,373

Headquarters

Canterbury, New Zealand

Industry

Education

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

67,000

The Opportunity

Digital transformation, including the popularization of online learning and degree programs as well as growing interest in massive open online courses (MOOCs), was the reality in higher education even before the onset of the global COVID-19 pandemic. As a result, the University of Canterbury had recruited a digital leadership team, which had recently crafted a new vision for digital transformation to enable the university to stay current with technological trends.

The university's identity and security teams were impeded by a bespoke legacy IGA solution that created visibility challenges – and required extensive coding and other manual steps before accounts could be provisioned and de-provisioned. In today's increasingly cloud-centric and digital-first world, these time-consuming, labor-intensive processes were inefficient and burdensome.

The Solution

Saviynt's cloud-native Identity Governance and Administration (IGA) solution has become the single source of truth for identity information across the University of Canterbury's entire IT ecosystem. With this solution, the university has:

- Accelerated new user onboarding and new account provisioning so that a process that used to take place overnight can now be completed in 20 minutes

- Achieved enhanced visibility across all roles, identity types, and resources in the environment
- Saved time, streamlined processes, and reduced administrative overhead
- Seamlessly integrated cloud and on-premises resources, including the University's Oracle PeopleSoft ERP implementation and a student management system (Jade)
- Prepare to implement role-based access controls, new workflow approval automation, and enterprise service management integrations

The Results

With Saviynt's IGA solution now implemented, the University of Canterbury has set a firm foundation for its digital future. The university now benefits from:

- ✓ **Accelerated account provisioning** to ensure that users can access the resources they need when they need them most
- ✓ **Centralized identity governance** to support future digital transformation, privilege management, and access control initiatives
- ✓ **Enhanced access visibility** to keep assets and resources secure while streamlining administration
- ✓ **Time and labor cost savings** from efficiencies introduced by automation

“

In universities, a single person can have so many different roles and identities over the course of their relationship with the institution. They can be a student at the same time that they're a staff member, and then become an alumnus. Saviynt essentially makes it possible for us to assign each of these people – with multiple, complex, changing personas – a single identity for life. ”



Clive Keylard
Product Manager, Business Services,
University of Canterbury



Customer story
Western Digital

Securing M&A Onboarding Agility For Western Digital

Saviynt's flexible architecture and intelligent capabilities helped Western Digital effectively manage its access and risk.



Identity management is not a one-size-fits-all security solution. Western Digital's Kum Chai Shin, Director, Information Security, knew the data storage and solutions giant needed a comprehensive identity management platform to handle their frequent mergers and acquisitions efficiently. She takes us through Western Digital's experience using Saviynt's platform to secure multiple applications and identities rapidly, securely, and efficiently.

The Opportunity

Western Digital's manufacturing footprint spans across the US, Asia and South America. With 65,000 employees and another 20,000 contingent workers around the world, the company is a global powerhouse in the manufacturing of efficient, data-centric solutions.

Overview

Western Digital is a global data storage company that designs and manufactures hard drives, solid-state drives, and other storage solutions

Number of Employees

65,000

Headquarters

San Jose, CA

Industry

Manufacturing

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)
- Application Access Governance (AAG)

Number Of Identities Managed

60,000

Since its inception in 1970 in Southern California as a producer of special semiconductors, Western Digital has grown to \$20 billion in annual revenue. From storage platforms to data center drives to embedded and removable flash, innovative Western Digital products provide solutions across the industries that keep the world turning: automotive, banking, telecommunications, research, oil & gas and more.

Western Digital's legacy identity management system had gradually become cumbersome, and challenging to use. They needed a centralized identity management system that was secure and flexible, intuitive to use, and could accommodate diverse apps and identities to support Western Digital's continued growth through continuous merger and acquisition activity.

The Solution

Saviynt implemented a modern Identity Governance and Administration (IGA) solution for Western Digital in a series of stages that provided a user-friendly platform to manage their growing identity landscape and provide actionable governance and accountability.

- ✓ Improved user experience accessing business systems
- ✓ Managed and reduced risk by consolidating processes and platforms
- ✓ Provided intelligent analytics through centralized dashboard reporting

“

Saviynt was picked based on all the product market functionality evaluations, because working quality is the most demanding requirement that we need to support. ”



Kum Chai Shin
Director, Information Security,
Western Digital



Customer story
Worcester Polytechnic Institute

Worcester Polytechnic Institute To Become Cloud-First Leader

How Worcester Polytechnic Institute replaced decades of code, centralized thousands of identities, and empowered modern, agile, and secure access control.



WPI

For decades, Worcester Polytechnic Institute's (WPI) central system of record was a complex legacy platform built on millions of lines of code, requiring considerable manual effort to provision, manage, and disable user entitlements. As WPI prepared to shift its infrastructure to the cloud, it faced a critical choice: rip it out, and re-integrate it piece by piece — or search for a platform that could take its Identity Access Management (IAM) system into the future.

With Saviynt IGA, they could unify complex identities (staff, students, and alumni) under a single system of record, automate secure access to course content and online assets, and deliver a more agile, scalable, and secure platform.

Overview

Worcester Polytechnic Institute is a private research university offering over 50 degree programs across 14 academic departments, with a focus on engineering and technology

Number of Employees

2,000

Headquarters

Worcester, MA

Industry

Education

Cloud Infrastructure

AWS

Saviynt Identity Cloud Capabilities

- Identity Governance and Administration (IGA)

Number Of Identities Managed

31,000

The Opportunity

Founded in 1865, WPI is a top-tier technological university specializing in science, engineering, and business. The Massachusetts-based school boasts 18 academic departments with over 70 undergraduate and graduate degree programs serving over 7,300 enrolled students.

For decades, WPI used a legacy system of record to build its course list, manage shifting enrollment statuses and entitlements, and provision and disable access. This on-prem system was integrated into its campus-wide communication and financial systems via millions of lines of customized code and required time-consuming manual processes and extra staff to ensure up-to-date and secure data access.

Inconsistent or redundant data entry, along with differing policies and processes across departments, made it difficult to deliver quick access for those just joining the institution or changing responsibilities within it. This outdated system lacked reporting and analytics capabilities, struggled to scale with WPI's international growth, and wasn't delivering a modern user experience. It was time for a shift to the cloud.

However, WPI faced an even bigger obstacle: their on-prem infrastructure needed to be ripped out — and connectors for key systems needed to be rebuilt. Their IAM team considered doing the recoding and

reintegrating in-house, but this wouldn't achieve their main goal: fewer manual processes, better support, and automated, centralized repository for all identities. WPI needed an industry-standard platform that could not only replace its spreadsheets and massive patchwork of PowerShell scripts — but also assimilate its vast and complex institutional rules around affiliation. A student, for example, could also be a staff member; faculty could also be alumni.

After investigating top IGA solution providers and consulting with veteran security engineers in the IAM space, all signs pointed to one solution: Saviynt Identity Governance and Administration.

The Solution

Over the university's winter break, Saviynt and WPI worked together to import, update and change over 40,000 records (each containing hundreds of thousands of pending tasks) from their on-prem Master Data Management (MDM) system. Despite multiple systems and a vast network of applications and systems across different departments, Saviynt IGA successfully merged and reconciled all data and identities into one central repository.

From there, Saviynt integrated with WPI's main systems of record to merge and secure data about course enrollment, entitlement, role changes — even building access.

Now, no matter if a user is a student, staff, alumni, or a combination of all three — WPI has a clear, accurate, and up-to-date line of sight into every identity in its environment.

With Saviynt's intelligent analytics, any change in an individual's status triggers immediate access changes. For example, an employee who leaves WPI now loses access as soon as staff enters their separation into the system. Or, if a user is working past a separation date — as many students do — a manager can extend the access. Automated reporting helps WPI identify access risk and prevent any unauthorized user access to university systems, data, and intellectual capital.

In phase two, WPI plans to round out its identity lifecycle visibility into Microsoft 365 and Zoom. When users need access to Microsoft applications and files, Saviynt can enable hiring managers to request access for their employees rather than a slow, manual ticket submission process.

The Results

✓ **Unified complex identity scenarios** (like student-staff personas and students accessing alumni networks) into one single source of truth.

✓ **Reduced manual processes** and improved response times, and achieved a more stable and secure environment.

✓ **Fast, secure student access to course content** including digital libraries, and online communities with Saviynt's rules-based policy engine. Easily scalable to support remote learning, international student enrollment, and massive open online courses.

“

It didn't make sense to go through an entire rip and replace of our current solution for something that would not even meet all of our needs. ”



LeAnn LeClerc
Chief Information Security Officer,
WPI



The Identity Cloud

Turn on visibility, control, intelligence and rapid time-to-value on the world's leading cloud-native platform, protecting over 60 million identities and counting.

www.saviynt.com



Saviynt

The Identity Cloud