The University of Canterbury is a leading university in the Pacific-island nation and one of the most prestigious institutions of higher learning in New Zealand. To support its digital transformation initiative, the university had recently recruited a new digital leadership team and was preparing to launch large-scale modernization initiatives that would enable it to keep pace with current IT trends. To realize this vision, the university was rolling out a new operational model with a product team focus, but it also needed a new Identity Governance and Administration (IGA) solution — one that could provide centralized visibility across all the roles and identities within its complex computing ecosystem. Their goal for each user was “one identity for life.”

Identity lifecycle management is inherently complex in higher educational institutions. The University of Canterbury’s situation is no exception. With more than 18,000 students, 3,300 staff, and 1,500 visitors, the university must support an exceptionally wide variety of roles, each of which requires a different type of access. What’s more, individuals switch roles frequently and often hold more than one position simultaneously (e.g., a student who also serves as a research assistant). In this environment, streamlined joiner/mover/leaver identity lifecycle management capabilities is critical. It’s essential to consolidate capabilities so that every user has just one, single identity over the course of their relationship with the university.

Since choosing Saviynt as its IGA partner, the University of Canterbury has:

- Sped up the new user onboarding and provisioning process from something that took place overnight to just 20 minutes.
- Secured diverse account types across a complex hybrid infrastructure, including many legacy on-premises components.
- Eliminated visibility gaps, streamline administration with automation, and met newly-introduced data privacy mandates from the New Zealand government.

EXECUTIVE SUMMARY

The University of Canterbury is a leading university in the Pacific-island nation and one of the most prestigious institutions of higher learning in New Zealand. To support its digital transformation initiative, the university had recently recruited a new digital leadership team and was preparing to launch large-scale modernization initiatives that would enable it to keep pace with current IT trends. To realize this vision, the university was rolling out a new operational model with a product team focus, but it also needed a new Identity Governance and Administration (IGA) solution — one that could provide centralized visibility across all the roles and identities within its complex computing ecosystem. Their goal for each user was “one identity for life.”
The University of Canterbury's identity and access management infrastructure had evolved gradually over time to include multiple disparate components and a homegrown solution that was cumbersome to administer. Provisioning and de-provisioning accounts involved running scripts and other manual processes, making it a time-consuming and laborious process that required a full-time employee to manage it. And the system was inflexible. Because business rules were hardcoded by developers, making changes was difficult and came with a risk of downtime.

In 2017, the university’s identity team had created a request for proposals (RFP) seeking a single partner to provide both identity governance and access management capabilities. Ultimately, they selected solutions from both Saviynt and Okta, but are now in the process of moving away from Okta. Going forward, their plan is to use Saviynt’s IGA solution in conjunction with Microsoft Azure Active Directory (AD), which will enable them to implement self-service visitor account provisioning and role-based access controls.

Key to the university’s new digital strategy is the idea that its IGA solution will serve as a central repository and single source for all identity information across its IT environment for the entirety of each identity’s lifecycle. With this dedicated, centralized resource in place, identity and security teams can drive enhancements that will allow them to progress through a phased implementation of role-based access controls and single sign-on (SSO).

Today, staff and students’ identity information is automatically updated within Saviynt, a process that used to require multiple manual steps. Administrators will gain clear and comprehensive visibility into who has access to which resources at what time, and access will automatically be revoked when people leave the university or move into new roles that no longer require it. The solution seamlessly integrates across multiple clouds and resources within the university’s on-premises data center and works with Oracle PeopleSoft, the university’s enterprise resource planning (ERP) solution for staff and visitors, and its custom-built student management system.

The university continues its progress through the phased implementation project, which is no minor undertaking. Meanwhile, demands upon its identity and security teams are still increasing. With its strong global reputation, the University of Canterbury had long attracted international students to its campus, but the closure of New Zealand’s borders during the COVID-19 pandemic invited an acceleration of the adoption of online learning initiatives and massive open online course (MOOC) offerings. “At the moment, my team manages digital identities, APIs, and a whole variety of other systems,” says Clive Keylard, IAM and Middleware Manager at the University. “Doing this well, with attention to detail, just gets harder and harder as the environment gets bigger with new technologies coming out.”

In the face of these challenges, the fact that Saviynt IGA can streamline processes and workflows through automation is particularly helpful. So is the direct customer support model that Saviynt has put in place. “It’s really easy to get help when there are issues,” says Clive Keylard. “You pick up the phone, talk to someone directly, and they help you work through the problems right away. That's really helped us be successful.” Clive Keylard also values his relationship with Saviynt’s ambassador program. “We’ve found the ambassador program immensely useful, and it’s been really good for us as customers,” he adds.

Once the final phase of the university’s current implementation roadmap is complete, they’ll have role-based access controls, self-service visitor registration, and multi-factor authentication (MFA) in place. At that point, they’ll consider additional capabilities from Saviynt, especially cloud privileged access management (CPAM), as the next steps toward a secure digital identity-based future.

“In universities, the concept of one identity for life is fundamental. This is because 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.”