

One of Australia's largest professional sporting leagues regulates vendor privileged access and achieves holistic access security using Securden

The sporting association that governs the Rugby League competition in Australia deploys **Securden Unified PAM** and simplifies access to their cloud instances, establishes granular internal access controls, regulates privileged access to third parties, enforces least privilege across the organization, and more from a single portal.

The background

Rugby League is Australia's most popular community-based sport. It is played by hundreds of thousands of people and remains the most entertaining sport. The Rugby League competitions are governed by professional leagues.

The sporting league that conducts the elite competition was founded more than three decades ago. It governs the competitions of several clubs at the national and regional levels. Their telecast of the competitions attracts over 100 million television viewers each year. The league relies heavily on its IT team.

The IT team of such a massive establishment is entrusted with a wide range of responsibilities, including managing their website as well as those of their affiliated clubs and state units, conducting viewer polls, maintaining and compiling player performance statistics, dealing with partners and sponsors, managing membership, and selling tickets.



Industry:
Sports and Entertainment

Location:
Sydney, Australia



**Founded 3+
decades ago**



The IT team is also responsible for managing and operating an online store to sell memorabilia like branded T-shirts, balls, backpacks, and beanies, among other items. The organization has a robust cloud IT infrastructure and managing it and all other operations securely is its top priority.

Business challenges

On a day-to-day basis, the organization's IT team deals with various cloud workloads, including VMs, databases, containers, and other applications/services hosted on AWS and Azure. The team followed the IT security best practice of assigning strong, unique passwords for each instance and account. However, this led to the classic password management challenge, and the team deployed a password manager.

"Typically, IT team members would need access to various resources and instances on the cloud. Our team members had to log in to the password manager first, search for the password of the cloud instance, and then copy and paste the password to gain access, which was a cumbersome experience. We wanted a one-click remote connection launching facility that would automate the entire process and make cloud access seamless," says the IT Engineer responsible for finding a solution.

Another critical requirement was regulating and streamlining third-party access to the IT infrastructure for various activities like services commissioning and troubleshooting. The team wanted to offer controlled access to third parties without disclosing the passwords of critical resources.

“

"We had to log in to the password manager first, search for the password of the cloud instance, and then copy and paste the password to gain access, which was a cumbersome experience.

We wanted a one-click remote connection launching facility that would automate the entire process and make cloud access seamless"

They wanted to discontinue using VPN as there were no options to monitor, control or record privileged activities with it. Moreover, VPN granted access to the entire infrastructure. "We wanted to ensure granular, fully monitored access to third parties without disclosing the underlying credentials," points out the IT Engineer.

Managing local admin rights for developers on their workstations was a big challenge. Full admin rights allow the installation of unapproved software or applications and accidental or intentional changes to security settings, which could lead to malware propagation.

"We preferred to take proactive measures and enforce the least privilege model across the organization. Instead of granting standing privileges, we wanted policy-based access controls for developers and other user groups. We were specifically looking for a solution to automate the entire process and ensure just-in-time and just-enough privileges."

The team was looking for a holistic PAM solution to streamline and monitor privileged access internally, simplify access to their cloud instances, regulate access to third-parties, and enforce the least privilege across the organization.

Searching and identifying the right solution

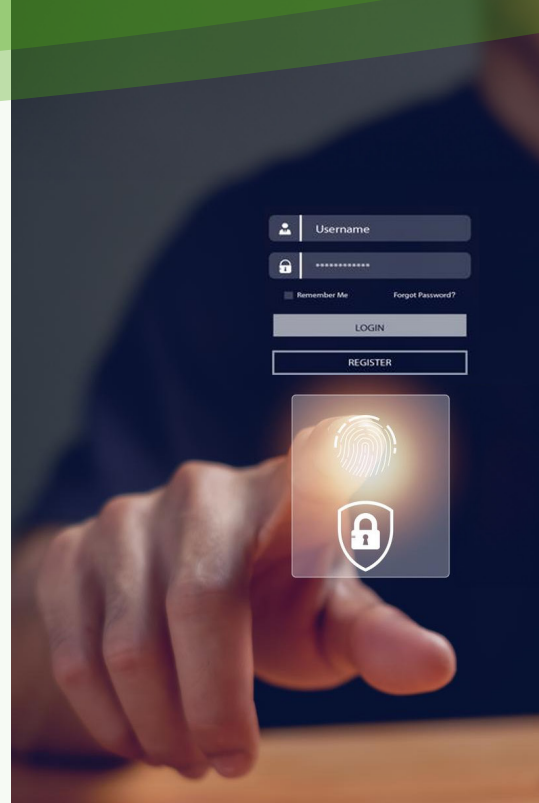
The organization was looking for a wholesome solution to manage its cloud and hybrid infrastructure and to solve its access management challenges. They wanted to avoid juggling between one product for password management, another for remote access, a third one for managing third-party access, and a different solution for managing local admin rights on workstations.

They were looking for a solution that offered all this at a price that did not break the bank, as they had a small team and vendors in the market that offered solutions to all these challenges, delivered it in silos, and at a price beyond their budget.

While looking at the market for the right solution, they came across Securden Unified PAM. On further analysis, the team realized that Securden offered exactly what they wanted, coupled with a modern, user-friendly, and flexible interface.

The Securden difference

The team members carried out an extensive Proof of Concept (PoC) before deciding to put Securden into production. The Unified PAM bundled all the features in a single interface, offering them a single pane of visibility into metrics that mattered without shuffling between multiple dashboards.



Requirement: A holistic PAM solution that helps

- Streamline and monitor privileged access
- Simplify access to cloud instances
- Regulate access to third parties
- Enforce least privilege across the organization



While implementing Securden Unified PAM, the league's IT team required some changes and enhancements to existing features. The Securden team was quick in delivering those enhancements. "I really appreciate Securden's engineers for customizing solutions for us. No other vendor would have done that. High praises for that," says the IT Engineer.

Securden helped centralize password management across the organization by securely storing all the credentials in a central vault in a fully encrypted form. It simplified the task of managing 'who' gets access to 'what.'

Securden's powerful browser extensions simplified the team's requirement of tapping into cloud instances in a single click without manually copying and entering the password. "The browser extensions provided by Securden are above and beyond what we were expecting. It solved a lot of headaches that we had faced with our previous solution," says the IT Engineer.

Contractors, vendors, partners, and other third parties working with the league now have a secure, seamless way to launch one-click connections to internal IT assets without having access to the passwords. The IT team now has a complete recording of all third-party sessions.

Local admin rights on workstations have been removed. With the Privilege Elevation and Delegation (PEDM) module of Unified PAM, developers now have only standard rights. The IT team has configured granular application control policies whitelisting and blacklisting applications and processes.

Additionally, with Securden's just-in-time (JIT) access model, the IT team could streamline access to sensitive resources by granting time-based access on a request-release mechanism. By setting an automatic password reset after the usage, they could add another layer of security on access to sensitive resources, where the password of the target device is automatically reset after the session is terminated.

“

"I really appreciate Securden's engineers for customizing solutions for us. No other vendor would have done that. High praises for that."

"The browser extensions provided by Securden are above and beyond what we were expecting. It solved a lot of headaches that we had faced with our previous solution,"



The outcome: Achieving holistic access security







Securden Unified PAM has helped the league's IT team overcome the challenges related to granting, restricting, revoking, and monitoring privileged access across the organization. The team now securely manages all access from a central portal. Securden has helped the team combat supply chain vulnerabilities by protecting all identities, regulating privileged vendor access, and mitigating security risks by reducing the attack surface.

"Securden's solution is more up-to-date and aligned with everyone's expectations of a PAM solution," opines IT Engineer.

“

"Securden's solution is more up-to-date and aligned with everyone's expectations of a PAM solution"

Key factors for choosing Securden

-  Unified solution at a competitive price.
-  Non-archaic modern and user-friendly interface offering flexibility.
-  The flexibility of adding user accounts from both on-prem AD and Azure AD for seamless onboarding.
-  Robust browser extensions offer easy autofill and logging into web-based applications.
-  Customizing the solution to address specific challenges.
-  Single solution for all the privileged access management challenges.



Trusted by hundreds of SMBs
and Enterprises across the globe

[Request Demo](#)