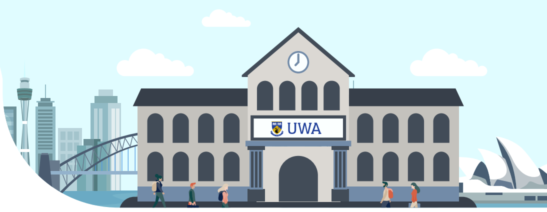


Top Australian Research University Enforces Granular Application Control Using Securden

The University of Western Australia eliminates local admin privileges on more than 8,000 University-managed devices across three campuses and 22 schools. Streamlines application usage, combats malware propagation, and achieves compliance with government regulations.

The Background

The University of Western Australia (UWA) has been a vibrant part of higher education and research since 1911. Nestled in the beautiful city of Perth, UWA has earned a spot among the top 1% of academic institutions around the globe. With over 25,000 students and a diverse staff of more than 3,300, UWA offers an outstanding educational environment. UWA features three campuses and is home to more than 75 research and training centers across

Quick Facts

Industry: Education

Country: Australia

Requirements:

- Empowering staff and students to use the applications they need while preventing malware.
- Restricting local admin rights on workstations and ensuring controlled, granular access.
- Complying with the security standards prescribed by the government.

The Solution:
Securden Endpoint Privilege Manager

Results:

- Campus-wide visibility of application usage.
- Least privilege enforcement by removing admin rights.
- Automation to block unauthorized applications.
- Policy-driven controls with reduced IT oversight.
- Improved IT compliance journey.

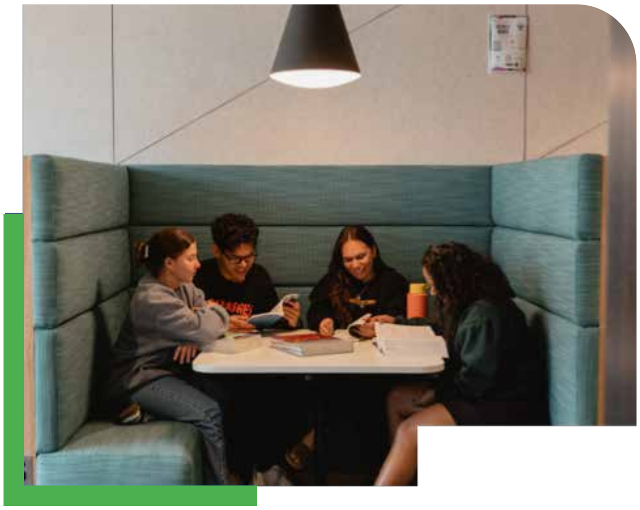
Australia, making it a hub for groundbreaking knowledge and research. As one of Australia's prestigious Group of Eight research universities, UWA is recognised as 77th in the QS World University Rankings for 2025.

The Challenge

Educational institutions face unique cybersecurity challenges that differ from traditional business environments. With a diverse mix of people—students, academics and professional staff—each having different levels of IT expertise, managing access and training can be tricky. In the absence of appropriate internal control and oversight, the consequences can be severe, leading to the exploitation of personal data, theft of intellectual property, financial loss, and more.

Just like any other university, The University of Western Australia (UWA), is required to comply with various government regulations which mandate diligent management of IT resources and tracking of activities.

"The problem is that we're a university and not like any corporation where they only perform a certain number of things and have a certain number of approved applications to use," explains Dave Sayers, the IT Desktop Engineering Manager at UWA.



One of the many challenges faced by the University IT team was finding a balance between granting the flexibility for staff and students to download, install, and use the applications they need and preventing malware or malicious applications from gaining ground.

“Our organisation needs to comply with security standards and guidelines provided by the government, which means we had to restrict local admin access on our workstations for security purposes. We needed to find a way that would deliver a degree of security to our workstation fleet but also provide freedom so people could elevate and install programs on their computers in a safe and controlled manner,” says Dave.

UWA's IT team began searching for a tool to automate the process and enforce controls seamlessly, without impacting productivity or frustrating users.

Selecting the Right Solution

While exploring the endpoint privilege management solutions available in the market, UWA IT had certain specific criteria for selecting the right solution.

- ✓ A product that could provide granular application control capabilities, flexible at various levels – University-wide for all users and selective controls for different user groups.
- ✓ Out-of-the-box integration with the existing IT infrastructure, including the servicedesk system.
- ✓ The team was very particular about having a simple, intuitive, and user-friendly interface that would not require extensive training for users.
- ✓ The ability to comply with the provisions of security regulations was also pivotal.
- ✓ A simple, secure, straightforward maintenance process and top-notch technical support.

"We reviewed half a dozen products that reported they did what Securden does, but at the end of the day, Securden ticked the most boxes of what we were looking for in a product," says Dave.

Securden fulfilled most of the University's criteria, and after multiple rounds of rigorous evaluation and testing, the steering committee decided to choose Securden Endpoint Privilege Manager (EPM).

"Overall, the feature set, the capabilities, combined with a good price for educational institutions like UWA was part of the overall package that attracted us to Securden," says Dave.

> We reviewed half a dozen products that reported they did what Securden does, but at the end of the day, Securden ticked the most boxes of what we were looking for in a product.
>
> - Dave Sayers,
> IT Desktop Engineering Manager, UWA.

The Securden Difference

UWA IT deployed Securden EPM across the campus in phases. Immediately on deployment, Securden's application discovery engine created an inventory of all applications and processes in use on all University-controlled workstations. This offered holistic visibility to the IT team – the level of knowing which applications were running on each workstation and laptop.

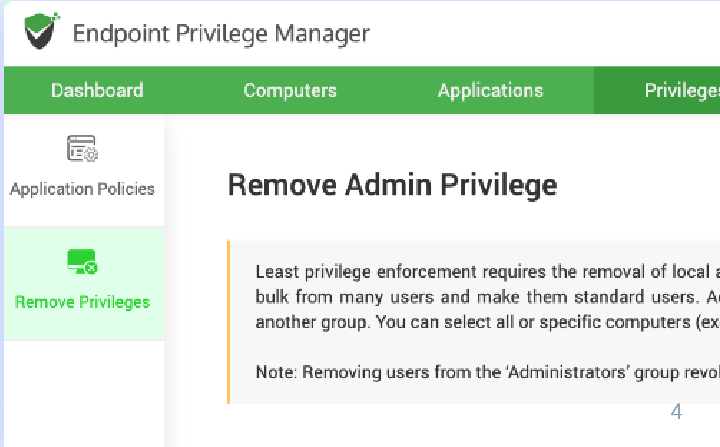
With a complete inventory of all applications and processes in use, the IT team was able to define control policies by whitelisting and blacklisting specific applications granularly for specific groups. This helped save time for both students and the IT team while strictly adhering to compliance regulations.

Whenever users need access to new applications, they raise requests through Securden's self-service portal or through the University ticketing system. The IT team carries out a quick review and grants permission through Securden EPM.

Before deploying Securden EPM, monitoring application usage required close coordination and constant communication between service delivery and backend infrastructure teams. The IT team would keep a tab on application usage. If they found any malicious applications, they would report them to the infrastructure team.

Securden EPM has automated the entire process. Users are allowed to use only the approved applications, which prevents unknown applications from gaining ground. The IT team has complete visibility of all app usage across departments. Furthermore, the institution is able to strengthen its IT compliance journey with regulatory frameworks.

> Securden stood out in terms of the features and controls it offered and as a side bonus we found Securden very responsive in taking our feedback and bringing in new features.
>
> - Dave Sayers,
> IT Desktop Engineering Manager, UWA.



Remove Admin Privilege

Least privilege enforcement requires the removal of local a
bulk from many users and make them standard users. A
another group. You can select all or specific computers (ex

Note: Removing users from the 'Administrators' group revo

Beyond the product capabilities, reliable and fast technical support from the Securden team proves highly useful to UWA. When the team requires new features or enhancements, the Securden team willingly delivers them in a timely manner.

“Securden stood out in terms of the features and controls it offered and as a side bonus we found Securden very responsive in taking our feedback and bringing in new features,” points out Dave.

As The University of Western Australia constantly works to expand their programs and stay on top of digital initiatives, Securden serves as a reliable cybersecurity partner, warding off endpoint security risks and reducing the overall attack surface.