AIRLOCK DIGITAL | **CASE STUDY**

Australian State Government Department

Overview of Case Study

How a leading Australian state government department used Airlock Digital application control and allowlisting to improve its cybersecurity and implement Essential Eight risk mitigation.

About the State Government Department

The department has important economic and infrastructure responsibilities within the state.

Challenge
Deploy an easy to manage, low impact allowlisting solution to implement Essential Eight risk mitigation for application control.

Approach
The department selected Airlock Digital application control and allowlisting for its functionality and reliability as a last line of defence against cybersecurity threats.

Result
Deploying Airlock Digital enabled the department to implement advanced allowlisting to protect against malware, ransomware and unauthorised software executions, with minimal impact on its end-user and server environments.

> Airlock Digital addresses the unknown and is our last line of defence against threats.
>
> **Operations Leader**
> State Department ICT

The Airlock Digital Application Control and Allowlisting Solution

With the Airlock Digital application control and allowlisting solution, the department has:

- achieved full compliance with Essential Eight Maturity Level Two for application control within three months
- proactively blocked a phishing attack from executing in its environment
- maintained a management overhead well within the accepted tolerance of 30 minutes per day

About Airlock Digital

Airlock Digital is the global leader in application control and allowlisting, trusted by organisations worldwide to protect against ransomware, malware and other cyber threats.

AIRLOCK DIGITAL

CUSTOMER CASE STUDY

Australian State Government Department

The Customer

The department is charged with delivering significant infrastructure projects with a considerable benefit to the state. Protecting its people and operations from cyber threats is critical to the department and a core responsibility of an ICT operations leader, who manages its cybersecurity team.

The Challenge

One of the ICT operations leader's early tasks was to review allowlisting products for alignment with the department's objectives, and for ease of deployment within its largely Microsoft environment. The review encompassed Airlock Digital application control and allowlisting.

The Approach

"With a small cyber security team, every tool we buy has to achieve an objective and be easily maintainable, with a very small user action footprint," explained the leader. "Our evaluation revealed Airlock Digital needed minimal administration, met our cost requirements and included the allowlisting features we needed to protect our organisation and users by aligning with our desired Essential Eight maturity level."

The Result

The department deployed Airlock Digital to its 1,300 end-user devices and 200 servers in audit mode and, in the leader's words, "nobody noticed." "We didn't receive a single service desk call about the performance of the client when we deployed the Airlock Digital agents, and the overhead on the machines was so low that when one of our senior leaders followed up on the implementation, we explained to him he already had it and showed him the icon on his device!"

The department then moved its entire fleet into full allowlisting enforcement mode within three months. The user impact was again negligible, with only a few exceptions issued through one-time passwords (OTPs) to enable developers to access essential processes.

Adopting Airlock Digital has enabled the department to stop a range of unwanted applications, files and processes from running in its environment, and a blocked phishing attack soon after deployment demonstrated the value of the solution. "Airlock Digital addresses the unknown and is our last line of defence against threats," said the leader.

Department cybersecurity team members who regularly use Airlock Digital laud features such as multiple allowlisting options including file hashes, paths and publisher exceptions; built-in options for implementing Microsoft blocklists; OTPs that allow for temporary emergency exceptions using multi-factor authentication; and the ability to log to security information and event management software.

"It's easy to troubleshoot files that have been blocked using the logs in the interface in the administration portal," said one team member who is a heavy user of the product. "In addition, the Airlock Digital service desk has been highly responsive, although we haven't had to use them often."

Airlock Digital has also enabled the department to align with the Essential Eight Maturity Level that matches its risk appetite and adapt to changes quickly. "The Australian Signals Directorate refreshed the Essential Eight late last year, so we had two controls we had to meet to achieve Maturity Level Two last year and three this year," explained the leader. "With Airlock Digital, we have been able to seamlessly implement the additional controls required."

Overall, Airlock Digital has delivered increased control over changes to the department's environment with minimal impact on application deployment and patching. Management overhead has remained well within requirements. "It's well within our acceptable tolerance, which is less than 30 minutes per day of management," said the leader.