AIRLOCK
DIGITAL

CASE STUDY

An Australian Logistics Company

Australian logistics provider deployed Airlock Digital Application Control and Allowlisting to stop cyber threats, reduce operating costs and improve change management.

Challenge

The customer needed to broaden security coverage of its environment without increasing operating costs, and implement the Australian Signals Directorate's Essential Eight mitigation strategy for application control to Maturity Level Three.

Approach

The customer selected Airlock Digital based on the product's highly effective application control and ease of use.

Result

The logistics company implemented powerful **allowlisting** and **blocklisting** to achieve Essential Eight mitigation for application control to Maturity Level Three.

Benefits to the Australian Logistics Company

With Airlock Digital application control and allowlisting, the Australian Logistics Company has:

- Extended security coverage to 98% of its endpoints without adding headcount to its technology support team
- Enabled management of the product without adding additional headcount
- Improved defenses against cyber threats such as **ransomware and malware**
- Enhanced its change control procedures

> "Knowing the full extent of your endpoints and installing Airlock [Digital] on these helps reduce your attack surface."

Chief Information Officer
Australian logistics company

About Airlock Digital

Founded in 2013 in Adelaide, South Australia, pure play allowlisting and application control solution provider Airlock Digital helps organisations keep ransomware and other malware out of their environments.

The Challenge

The Australian logistics provider runs cloud and on-premises infrastructure supporting end-user computing, operational technology, Supervisory Control and Data Acquisition **(SCADA)** and other systems. This environment is managed and maintained by a core technology team and field technicians.

The organization had used an application control product that covered only a small portion of its environment, risking a successful cyber attack. To minimize its risk, the logistics provider needed to extend application control and allowlisting coverage across its environment and align with the **Australian Signals Directorate Essential Eight** application control mitigation strategy to Maturity Level Three.

Extending the coverage of the provider's existing tool would require its technology team to recruit several additional members. The business opted to look for an alternative application control solution that could protect its environment and fulfil its maturity and compliance objectives without increasing its operating costs.

The Approach

The customer reviewed available application control and allowlisting solutions and determined Airlock Digital best met its needs. Built by experienced allowlisting practitioners, Airlock Digital proactively prevents malware, ransomware and **zero day attacks** while enabling administrators to discover and vet all executable code running in their environments. It also allows administrators to create flexible policies with simple, repeatable workflows, harden endpoints with blocklisting, and provide a searchable repository of file metadata.

The solution incorporates a lean enforcement agent with small policy sizes and minimal impact on endpoint resources.

The customer formally selected Airlock in 2022 and adopted Airlock Digital's best-practice implementation approach that prioritized simplicity. Good governance and change management supported the project and overcame any trepidation about the transition. For example, the customer followed standard change control procedures by deploying Airlock Digital to non-production and production environments during change windows for all users, including privileged users.

The Result

Just two months after starting the pilot, the logistics provider rolled out the solution to 98% of its endpoints. The business achieved Maturity Level Three for its Essential Eight mitigation strategy for application control without adding headcount to its technology support team. Less than one full-time equivalent employee manages Airlock Digital across the entire environment.

Airlock Digital runs alongside **endpoint detection and response** (EDR) solution **CrowdStrike** Falcon Complete, enabling the provider to determine all the endpoints to which it needed to deploy the enforcement agent. "Knowing the full extent of your endpoints and installing Airlock [Digital] on these helps reduce your attack surface," said the logistics provider's CIO. "Airlock [Digital] also prevents 'shadow IT' occurring in production without being visible to the technology team."

The **One-Time Password** (OTP) feature is used frequently to provide allowlist exceptions so users can access non-allowlisted applications securely during set times such as change control windows.

Simplicity and intuitiveness have played a key role in building acceptance of the product. "The Airlock [Digital] console is very easy to use and navigate, so our team felt confident with it within a few weeks," said the provider's Technology Manager.

Airlock Digital has demonstrated its ability to reduce the logistics provider's attack surface and contribute effectively to its Defense-in-Depth strategy. The solution is helping prevent cyber attacks while reducing operating costs and improving change management.