AIRLOCK DIGITAL | CASE STUDY

An Australian Logistics Company

How an Australian logistics provider deployed Airlock Allowlisting to prevent cyber-attacks, reduce operating costs and improve change management.

Challenge

The customer needed to broaden security coverage of its technology infrastructure without increasing operating costs, and achieve compliance with the Australian Cyber Security Centre's Essential Eight and Application Control to Maturity Level Three.

Approach

The customer selected Airlock Allowlisting based on the product's highly effective application controls and ease of use

Results

- **Extended security** coverage to 98 percent of its infrastructure
- **Increased coverage** without adding headcount to its technology support team
- **Enabled management of the product** without adding additional headcount
- **Improved defences** against cyber attacks
- **Enhanced** its change control procedures

> Airlock has proven to prevent malicious attacks. Install Airlock everywhere not just in your desktop environment.
>
> - Customer's CIO

About Us

Airlock Digital provides an intuitive framework that ensures software management teams can successfully implement and maintain a compliant 'allowed applications' list.

The framework's intuitive design and rapid policy distribution ensures seamless deployment within customer environments.

Customer

An Australian Logistics Company

Challenge

The customer's incumbent application control product covered only a small section of its technology infrastructure–increasing the risk of a successful cyber-attack. To minimise risk, the customer needed to extend coverage to the vast majority of its environment, increase its maturity when measured against the Australian Cyber Security Centre's Essential Eight and align with Application Control Maturity Level Three.

Coverage had to extend across a combination of cloud and on-premise infrastructure and solutions that span end-user computing, operational technology, SCADA and other systems used to run the business. This environment is managed and maintained by a core technology team and field technicians who apply patches, updates and new software as needed. Doing so with the incumbent product was problematic.

The customer found the product consumed time and resources to maintain, and extending its coverage would require its technology team to add several additional team members. The customer opted to look for an alternative application control solution that could protect its entire infrastructure and fulfil its maturity and compliance objectives–without increasing its operating costs.

Approach

The customer reviewed available application control solutions and determined Airlock Allowlisting best met its needs.

The customer formally selected Airlock Allowlisting in 2022 and adopted Airlock's best-practice implementation approach that prioritised simplicity and a zero-trust view of application updates and deployments.

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 Allowlisting to non-production and production environments during change windows for all users, including privileged users.

Results

Just two months after starting the Airlock Allowlisting pilot, the customer had rolled out the solution to cover 98 percent of its infrastructure.

The customer has achieved Application Control Maturity Level Three and improved its maturity against the Australian Cyber Security Centre's Essential Eight– without adding headcount to its technology support team. Less than one full-time equivalent employee manages Airlock Allowlisting across the entire environment.

Airlock Allowlisting runs alongside existing endpoint security solution CrowdStrike Falcon Complete. With the CrowdStrike product, the logistics technology team was able to identify all the endpoints that required deployment of the Airlock enforcement agent.

"Knowing the full extent of your endpoints and installing Airlock Allowlisting on these helps reduce the attack surface," says the CIO. "Airlock also prevents 'shadow IT' occurring in production without being visible to the technology team."

Its core technology team uses Airlock Allowlisting's one-time password (OTP) feature frequently to ensure the smooth deployment of applications, updates and patches, and to handle exceptions.

"The Airlock Allowlisting console is very easy to use and navigate, so our team felt confident with it within a few weeks."
– Customer's Technology Manager

The team initially deploys all new applications and updates into a test environment under OTP control, allowing it to configure and test the necessary 'allowlist' policy changes before production deployment. This efficient and scalable approach ensures employees, including privileged users, cannot introduce untrusted applications into production during the change control window.

Airlock Allowlisting has demonstrated its ability to reduce the logistics provider's attack surface and contribute to its defence in depth strategy.