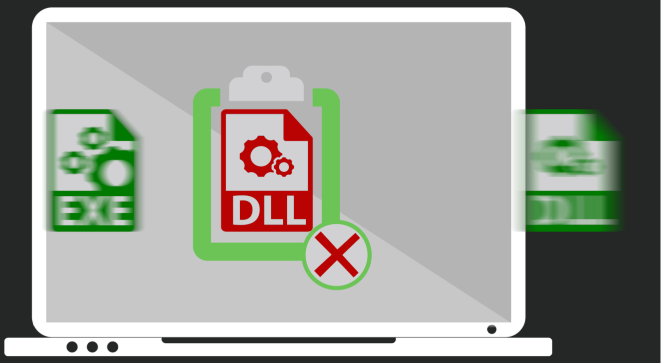
AIRLOCK DIGITAL

Application Whitelisting

- Airlock enables organisations to implement and maintain application whitelisting, simply and securely, in dynamic computing environments.



Simple, Secure & Effective

No Need to sacrifice security for operational efficiency.

Airlock supports application whitelisting by hash, publisher and file path on all executable files, application libraries and scripts, regardless of file extension.

Application whitelisting with Airlock is a simple, repeatable process

Until now, application whitelisting has been difficult to deploy and maintain. Airlock solves the challenges of application whitelisting by using proven and effective workflows that align with existing business processes.

Airlock makes application whitelisting simple in dynamically changing environments.

Creating and deploying whitelists with Airlock is fast, enabling organisations to become secure and compliant, sooner.

Airlock features at a glance

Centralised reporting - Real-time dashboards and a comprehensive search / reporting framework. ensures you find the needle in the haystack.

File Reputation - Airlock provides an inbuilt file reputation service to help you determine which files are safe to add to the whitelist.

Exception Management - Single use codes can be issued to users for temporary time based exclusion.

Secure - Airlock monitors all file mappings into executable memory, preventing common application whitelisting bypass techniques.

Lean - Airlock's enforcement agent is seven megabytes in size, using small whitelist definitions and next to zero impact on resources.

Hardened - Airlock performs enforcement for all users, including administrators. Protections are available to prevent disabling and tampering.

SIEM Support - Airlock supports the real-time transfer of all application whitelisting events to third party SIEM solutions.

File tracking - Interrogate every file. Discover when and where a file was first seen, including complete execution analytics.

Intuitive - Airlock whitelist management is performed via an intuitive file browser interface. No previous whitelisting experience required.

Prevent Ransomware and Targeted Cyber Intrusions

Unlike signature-based file blocking (blacklisting) such as antivirus, Airlock only permits the execution of files it has been instructed to trust, to run, regardless if a file is known good, bad or suspicious. This makes Airlock extremely effective at preventing sophisticated and opportunistic attacks.

Why is Application Whitelisting #1?

Since ASD created the Strategies to Mitigate Targeted Cyber Intrusions (Top 35) in February 2010, application whitelisting has always been ranked as an essential control to prevent targeted cyber intrusions, Why?

01/ Proactive Security Strategy

Airlock removes the ability for attackers to execute malicious and unknown code.

Therefore, significantly increasing the difficulty of attack, blocking never before seen malware and removing core tools that attackers need.

02/ Configured Uniquely In Every Instance

Each Airlock deployment results in a unique whitelist according to customer needs.

Therefore, attackers are unable to test their attacks against Airlock before attacking your organisation, as your security is unique.

03/ Complete File Visibility and Control

Airlock verifies, monitors and records all file executions across the organisation.

Therefore, significantly increasing the ability for organisations to understand, detect and respond to malicious activity.

No other security strategy provides these capabilities.
Airlock application whitelisting provides the most effective detection and prevention strategy possible.

Airlock Digital is an Australian based company, with offices in Adelaide and Canberra. Airlock is designed to be fully ISM compliant.

CONTACT US

Telephone: 1300 798 925
E-mail: info@airlockdigital.com
Web: www.airlockdigital.com