Essential 8 Application Control Compliance Statements

This article lists Airlock compliance statements with the ACSC Essential 8 Security Model for Application Control.

Controls	Statement
Maturity Level 1	
The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	Airlock enforces application control for all file types listed in the corresponding requirement. Administrators must enable 'Script Control' within policy to gain full coverage of script file type enforcement.
Maturity Level 2	
"Application control is implemented on workstations and internet-facing servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation approved set."	Airlock is designed to fully comply with this maturity level, most importantly Airlock Digital as a vendor does not define what an organisation 'trusts' within policy. At all times Airlock policies are confined to an organisation approved set.
"Allowed and blocked executions on workstations and internet-facing servers are logged."	All blocked execution events are centrally logged to the Airlock server from all clients by default. Centralised logging of allowed executions are performed when an administrator enables the 'Trusted Execution (Summary)' logging feature.
Maturity Level 3	
"Application control is implemented on workstations and servers to restrict the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set."	Airlock is designed to fully comply with this maturity level, most importantly Airlock Digital as a vendor does not define what an organisation 'trusts' within policy. At all times Airlock Digital policies are confined to an organisation approved set. Driver loads are also controlled by the Airlock agent, even if the drivers load in a highly privileged context.
Microsoft's 'recommended block rules' are implemented.	Airlock includes the Microsoft Recommended Block Rules as a Predefined Blocklist package within the software which can be imported and applied to policy.

Controls	Statement
Application control rulesets are validated on an annual or more frequent basis.	Centralised visibility of all allowed and blocked executions enables customers to validate the application control rulesets as frequently as desired. Additionally, trusted execution logging can be enabled to 'audit' rules that are in place to assist with the rule decommissioning process.
"Allowed and blocked executions on workstations and servers are centrally logged and protected from unauthorised modification and deletion, monitored for signs of compromise, and actioned when cyber security events are detected."	All file events are centrally logged and recorded. Airlock does not provide any functionality within the software to delete or modify events that have been logged, this is by design. Alerting can be placed upon Server Activity History messages, to automatically raise events as per organisations requirements.