The Essential Eight Maturity Model (E8MM)

To assist in adoption of the Essential Eight, The Australian Signals Directorate (ASD) introduced the **Essential Eight Maturity Model**, a structured approach to Essential Eight implementation. The E8MM defines four levels that organisations can use to measure their implementation of the Essential Eight:

0

Maturity Level 0

Weaknesses in overall posture

1

Maturity Level 1

Defending against commodity tradecraft that is widely available

2

Maturity Level 2

Defending against threat-actors with modest targeted capabilities

3

Maturity Level 3

Defending against adaptive and highly capable threat-actors performing targeted intrusions

The E8MM helps organisations identify gaps in their security controls, set clear goals for improvement, align the security efforts with real world threats, and help to prioritise security investment.

How Airlock Digital aligns with the E8MM

1

Maturity Level 1

Mitigation Description	Capability Statement
Application control is implemented on workstations.	Airlock Digital supports enforcement of application control on workstation endpoints with support for Windows, macOS and Linux, making easy to administer application control a reality.
Application control is applied to user profiles and temporary folders used by operating systems, web browsers, and email clients.	Application Control is performed (including user profiles and temporary folders) by default.
Application control is applied to user profiles and temporary folders used by operating systems, web browsers, and email clients.	Application control can be enforced for all file types listed in the corresponding requirement. Administrators must enable ‘Script Control’ within policy to gain coverage of scripts, installers, compiled HTML & HTML applications. The key statement in this requirement is ‘organisation-approved set’, meaning that organisations themselves must decide what they do or do not trust, not a third party. Airlock Digital has been designed as a framework for organisations to manage their own trust, in contrast to competitors that often define what an organisation 'trusts' through cloud-based definitions or other means. With Airlock Digital, organisations are in control of their approved set at all times.

2

Maturity Level 2

Mitigation Description	Capability Statement
Application control is implemented on internet-facing servers.	Airlock Digital can be installed on a wide variety of operating system types and can operate upon both internet connected and non-internet connected (air-gapped) servers.
Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.	Airlock Digital performs application control to all system locations by default, including operating system folders, program folders, removable media and network locations.
Microsoft's recommended application blocklist is implemented.	Airlock Digital includes the Microsoft Recommended Block Rules as a Predefined Blocklist package within the software which can be imported and applied to policy.
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 application control events are centrally logged.	All blocked file events are centrally logged and recorded by default. All allowed events are logged when the administrator enables the 'Trusted Execution (Summary)' logging feature. Airlock Digital has designed the summary logging feature to specifically comply with this requirement, whereby all allowed events are summarised and recorded to provide complete execution visibility, while also managing the volume of all allowed events, which typically amount to hundreds of millions of events per day at enterprise scale

2

Maturity Level 2. Pt.2

Mitigation Description	Capability Statement
Event logs are protected from unauthorised modification and deletion.	All file events are centrally logged and recorded. Airlock Digital does not provide any functionality within the software manually delete or modify events that have been logged, this is by design.
Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events.	Alerting can be placed upon Execution History logs and Server Activity History messages, to automatically raise events as per organisations requirements. Log data is easy to view within the platform and can be forwarded to third-party SIEM platforms if desired.
Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.	Known suspicious and malicious file detections can be configured to raise automatic alerts via Email and SIEM platforms, as per organisations requirements.
Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.	Airlock Digital data within the platform can be easily alerted upon, centrally logged or exported in industry standard formats (CSV, XML etc.) in order to support reporting and data sharing.
Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.	Airlock Digital data within the platform can be easily alerted upon, centrally logged or exported in industry standard formats (CSV, XML etc.) in order to support reporting and data sharing.
Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.	Airlock Digital enables organisations to proactively support incident identification and proactive 'hardening' of operating systems through its blocklist capabilities.

3

Maturity Level 3

Mitigation Description	Capability Statement
Application control is implemented on non-internet-facing servers.	Airlock Digital can be installed on a wide variety of operating system types and can operate upon both internet connected and non-internet connected (air-gapped) servers.
Application control restricts the execution of drivers to an organisation-approved set.	Airlock Digital is designed to fully comply with this control, 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 vulnerable driver blocklist is implemented.	Airlock Digital includes the Microsoft vulnerable driver blocklist as a Predefined Blocklist package within the software which can be imported and applied to policy.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events.	All Airlock Digital event data is centrally logged in near real time. Alerting can be placed upon Execution History logs and Server Activity History messages, to automatically raise events as per organisations requirements. Log data is easy to view within the platform and can be forwarded to third-party SIEM platforms if desired..
Event logs from workstations are analysed in a timely manner to detect cybersecurity events.	All Airlock Digital event data is centrally logged in near real time. Alerting can be placed upon Execution History logs and Server Activity History messages, to automatically raise events as per organisations requirements. Log data is easy to view within the platform and can be forwarded to third-party SIEM platforms if desired.

*Please note that higher level requirements are in addition to lower levels. For example, to reach maturity level two you must also meet the requirements of maturity level one.