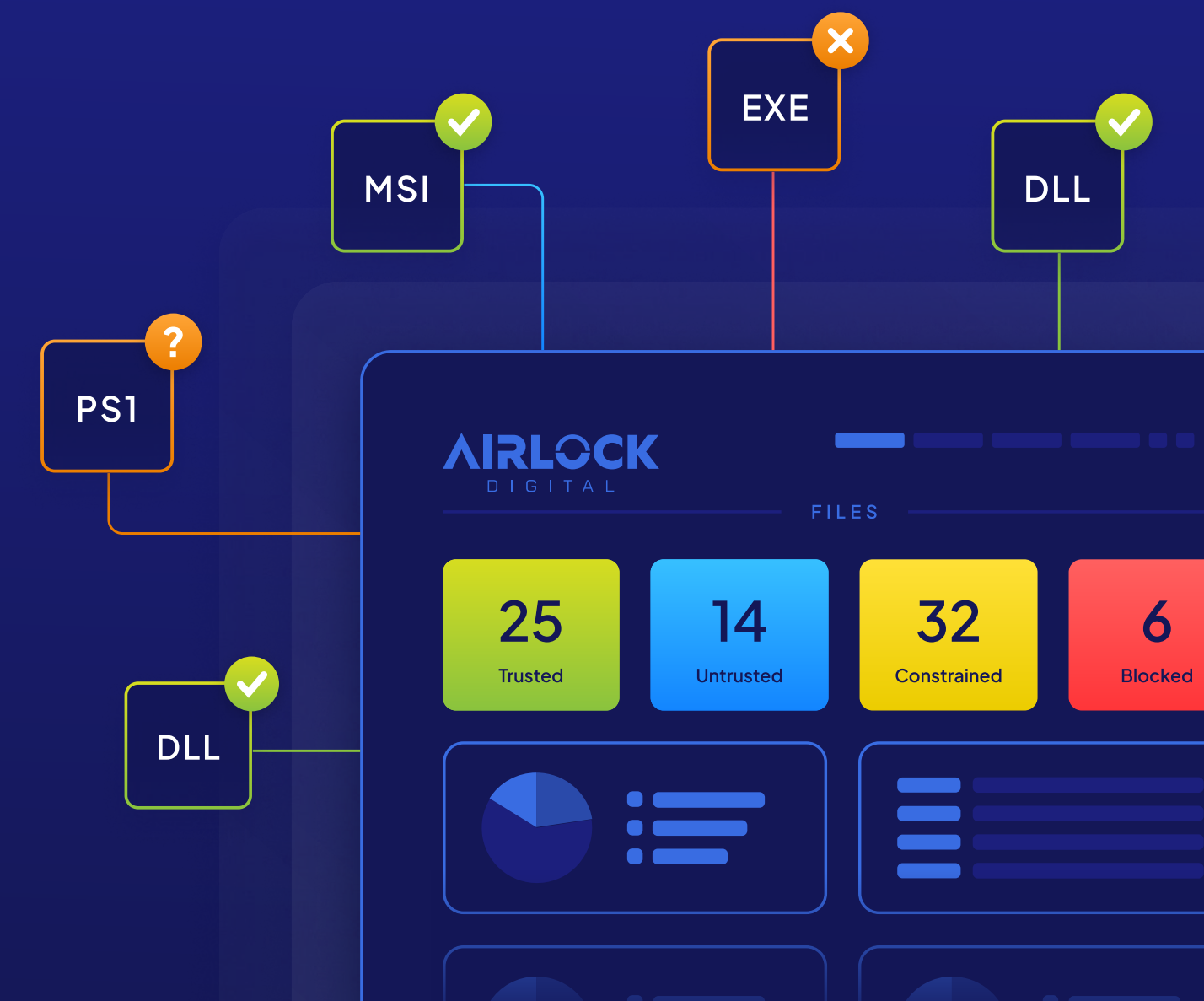


Precision Application Control for State & Local Government

Securing Public Sector Systems Against Cyber Threats



State and local government agencies in Australia manage **critical infrastructure, citizen services, and sensitive data**, making them prime targets for cyber threats. Airlock Digital provides **Deny by Default** application control, preventing **unauthorized software, malware, and ransomware** from executing. With support for **modern and legacy systems**, Airlock Digital enables **state and local governments to strengthen their cybersecurity posture**, improve compliance, and maintain secure, uninterrupted operations.

Proactive Security with “Deny by Default” Protection

Airlock Digital ensures **only trusted applications** can run, minimizing cyber risks and securing government infrastructure.

- **Prevent untrusted applications, malware, and ransomware** from executing on public sector networks.
- **Strengthen Zero Trust security** by ensuring only verified applications run within agencies.
- Mitigate **insider threats** and unauthorized software use with granular execution control.

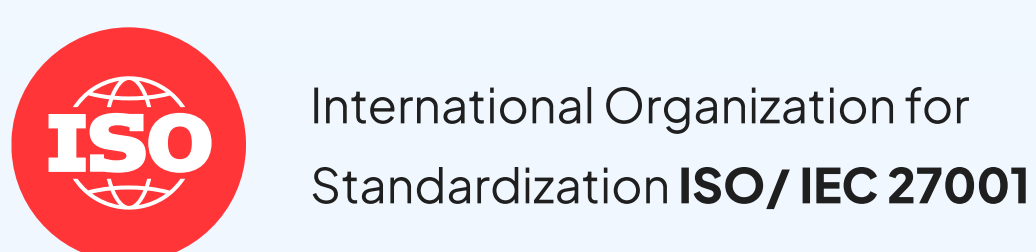
Foundational Protection for Public Sector IT & Infrastructure

State and local governments require flexible, **scalable security solutions** that safeguard diverse IT environments while enabling operational efficiency.

- **Cross-Platform Endpoint Security:** Protect Windows, macOS, Linux, and legacy systems across government offices, emergency response teams, and public sector IT.
- **Centralized Security Management:** Manage cybersecurity policies across multiple agencies from a single platform.
- **Offline Mode Protection:** Secure endpoints in remote, low-connectivity, or air-gapped environments.
- **Granular Policy Control:** Define trusted applications based on hash, path, publisher, or parent process.
- **Advanced Exception Handling:** Enable operational flexibility without compromising security.

Meeting Compliance & Regulatory Requirements

Airlock Digital helps Australian **state and local government agencies** meet cybersecurity mandates and regulatory obligations, including:



Essential Eight Australian Cyber Security Centre (ACSC)

PSPF Protective Security Policy Framework

ISM Australian Government Information Security Manual

Local & State-Specific Cybersecurity Frameworks

Airlock Digital: Features at a Glance

Real-Time Threat Prevention	Block malware, ransomware, and unauthorized applications before they compromise government networks.
Broad OS & Legacy System Support	Secure modern and legacy Windows, macOS, and Linux systems across government environments.
Granular Application Control	Enforce strict execution policies with hash, path, publisher, and process-based allowlisting.
Application Blocklisting	Prevent Living off the Land (LOTL) attacks by restricting high-risk system tools and scripts.
Offline Mode Support	Maintain security policies even in air-gapped or disconnected environments.
Scalable Security Management	Centrally manage policies for municipal offices, state departments, and emergency services.
Detailed Compliance Reporting	Simplify audits with comprehensive logging of application executions, policy updates, and security events.

Protecting Public Services & Critical Infrastructure

Deployed as **on-premises software**, in **sovereign cloud environments**, or as a **secure hosted solution**, Airlock Digital empowers **state and local government agencies** to prevent **cyber threats**, **enforce compliance**, and **ensure operational resilience**.

For more information, visit AirlockDigital.com or contact our sales team at sales@airlockdigital.com.

AVAILABLE FOR

Windows™ | Linux® | macOS™

Blocked / Allowed Files

5

Blocked Exceptions
(total)

5

Blocked Exceptions
(total)
2 Unreviewed

108

Blocked Exceptions
(total)

91

Blocked Exceptions
(total)
2 Unreviewed



Scan to request a demo

Book a demo to explore how Application Control and Allowlisting from Airlock Digital can help your business