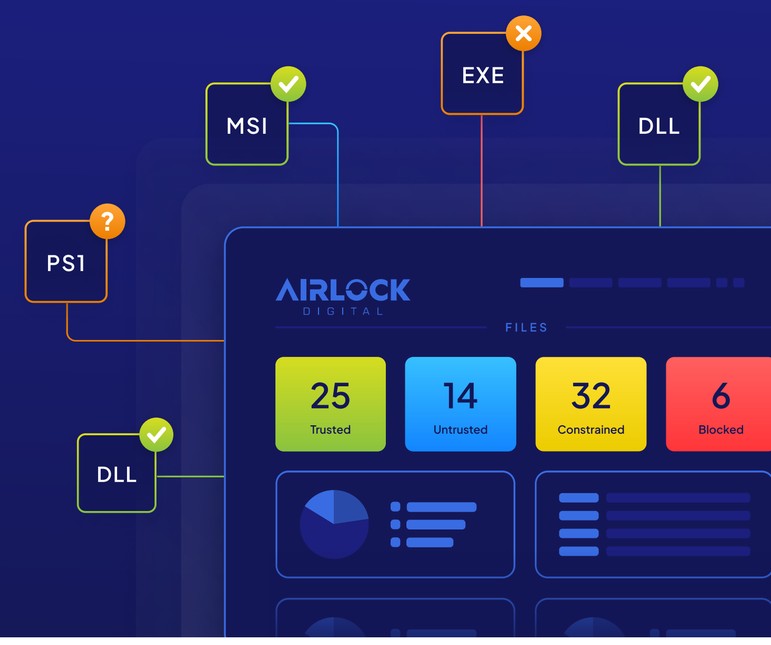
AIRLOCK DIGITAL

Precision Application Control

Modern Endpoint Security for State & Local Government



State and local governments face growing cyber threats targeting critical infrastructure, citizen services, and sensitive public sector data. Airlock Digital provides a Deny by Default application control solution that protects government IT and operational technology (OT) environments, ensuring only trusted applications and processes can execute. By securing endpoints across government agencies, Airlock Digital reduces risk, enhances compliance, and strengthens cybersecurity resilience for public sector organizations.

Proactive Security with a "Deny by Default" Model

Airlock Digital enforces a **Deny by Default** security posture, ensuring strict execution control over all government-managed endpoints.

- **Prevent malware, ransomware, and unauthorized software** from compromising government systems and public data.
- **Secure mission-critical infrastructure** by restricting execution to only pre-approved applications.
- **Reduce insider threats** by implementing granular control over application execution.
- **Ensure cybersecurity for offline and air-gapped environments** within government facilities.

Comprehensive Security for Government IT & OT

State and local agencies depend on a mix of modern IT, legacy systems, and connected infrastructure to deliver essential public services. Airlock Digital secures these diverse environments without disrupting operations.

- **Comprehensive Endpoint Security:** Protect Windows, macOS, Linux, and legacy systems used in government agencies.
- **Granular Application Control:** Define trusted applications via hash, path, publisher, or parent process for precise execution control.
- **Real-Time Monitoring & Visibility:** Gain full visibility into application execution and security events across government networks.
- **Seamless Cloud & On-Prem Integration:** Deploy within state data centers, hybrid cloud, and secure government environments.

Ensuring Compliance with Public Sector Cybersecurity Mandates

Airlock Digital enables state and local governments to enforce regulatory and statutory cybersecurity requirements while maintaining operational continuity and service delivery.

- Federal Information Security Management Act **(FISMA)**
- Cybersecurity Framework **(CSF)**
- Critical Infrastructure Protection **(CIP)** Standards
- Criminal Justice Information Services Compliance **(CJIS)**
- State-Specific **Cybersecurity Laws**

Airlock Digital: Features at a Glance

Real-Time Threat Prevention	Block malware, ransomware, and unauthorized applications before they can impact government operations.
Broad OS & Legacy System Support	Secure modern and legacy Windows, macOS, Linux, and embedded systems used across government IT infrastructure.
Granular Application Control	Precisely define trusted applications, scripts, and processes for total execution control.
Application Blocklisting	Prevent Living off the Land (LOTL) attacks by explicitly blocking unauthorized scripts and high-risk system tools.
Offline Mode Protection	Ensure security for air-gapped and isolated government systems with full execution control even without network connectivity.
Unified, Scalable Security Management	Manage security policies across state agencies, municipalities, and public infrastructure from a centralized platform.
Detailed Reporting & Audit Trails	Maintain complete, immutable logs of execution events, policy changes, and security incidents to support compliance audits and forensic investigations.

Airlock Digital: Endpoint Cyber Resilience for State & Local Government

Available as an **on-premises** solution, deployed in **government clouds**, or as a **secure managed service**, Airlock Digital enables state and local agencies to prevent cyber threats, meet compliance mandates, and maintain uninterrupted public services..

To learn more about securing your government environment, visit **AirlockDigital.com** or contact our sales team at **sales@airlockdigital.com**.

AVAILABLE FOR
Windows™ | Linux® | macOS™



Scan to request a demo

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

AIRLOCK DIGITAL