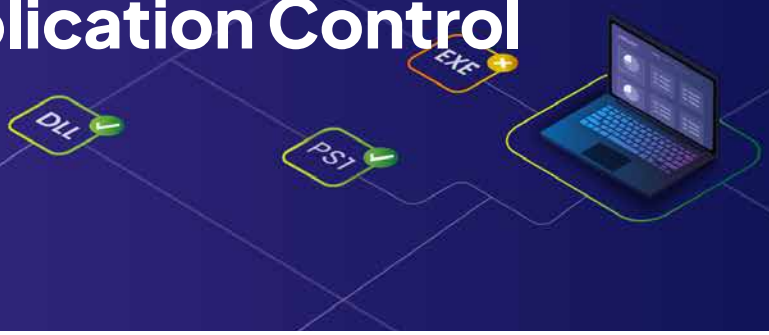
AIRLOCK DIGITAL

airlockdigital.com

Mission-Critical Application Control

Proactive Endpoint Security for U.S. Federal Defense



Defense agencies and military operations face relentless cyber threats targeting classified data, mission-critical systems, and national security assets. Airlock Digital delivers a battle-tested application control solution that enforces strict execution policies, ensuring only trusted and vetted software runs across defense IT and operational technology (OT) environments. By adopting a Deny by Default approach, Airlock Digital enables warfighters, cyber operators, and defense contractors to harden their cyber defenses, maintain operational readiness, and comply with stringent defense cybersecurity mandates.

Preventative Security with a "Deny by Default" Model

Airlock Digital enforces a **Deny by Default** security posture, ensuring strict execution control over all defense networks, weapons systems, and command infrastructure.

- **Prevent malware, zero-day threats, and unauthorized software** from executing in defense networks.
- **Secure mission-critical systems** by restricting execution to only approved applications.
- **Reduce insider threats** by applying strict control over software execution.
- **Ensure continuous security for air-gapped and deployed environments** with offline mode support.

Foundational Endpoint Security for Defense IT & OT

Modern defense operations depend on a mix of secure cloud services, tactical edge computing, legacy infrastructure, and classified environments. Airlock Digital enables centralized, policy-driven enforcement to secure all assets without disrupting operations.

- **Multi-Domain Security:** Protect endpoints across classified networks, defense clouds, and deployed field systems.
- **Granular Execution Control:** Define trusted applications at the hash, path, publisher, and process level to eliminate unauthorized activity.
- **Advanced Threat Intelligence:** Leverage real-time malware intelligence to block known threats automatically.
- **Zero Trust Enforcement:** Strengthen Zero Trust Architectures by eliminating unverified software execution.

DISA Security Technical Implementation Guides (STIGs)

NIST 800-171

FISMA Federal Information Security Management Act **(FISMA)**

NIST 800-53

CMMC 2.0
Department of Defense **Cybersecurity Maturity Model Certification**

Executive Order 14028 (Zero Trust Strategy)

Streamline Compliance with Defense Cybersecurity Directives

Airlock Digital provides the controls necessary for defense agencies and military contractors to comply with the latest cybersecurity regulations and frameworks.

Airlock Digital: Features at a Glance

Real-Time Threat Prevention	Block malware, ransomware, and unauthorized applications before they can impact defense operations.
Broad OS & Legacy System Support	Protect modern and legacy Windows, macOS, Linux, and embedded systems used across defense environments.
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	Secure air-gapped, tactical, and forward-deployed systems with full security enforcement, even without network connectivity.
Unified, Scalable Management	Manage security policies across classified networks, defense clouds, and forward-operating bases from a centralized platform.
Detailed Forensic Logging & Audit Trails	Maintain complete, immutable logs of execution events, policy changes, and security incidents to support forensic investigations and compliance audits.

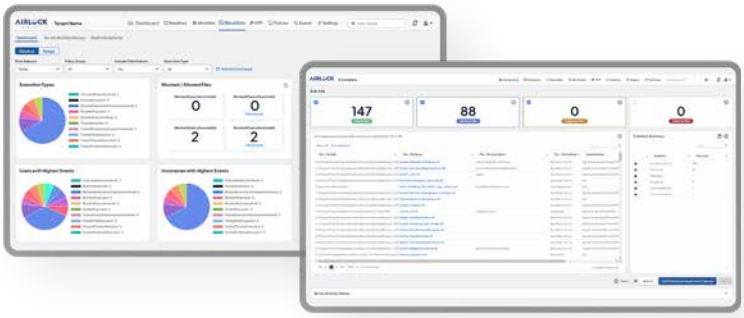
Airlock Digital: Hardened Endpoint Security for Defense Agencies

Available as an **on-premises solution**, deployed within **DoD private clouds**, or as a **hardened cloud service**, Airlock Digital enables defense organizations, military branches, and contractors to enforce cybersecurity mandates, prevent cyber threats, and maintain mission readiness.

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

Scan to request a demo

Book a demo to explore how Airlock Allowlisting and Execution Control will help your business



AIRLOCK DIGITAL

AVAILABLE FOR

Windows™ | Linux® | macOS™