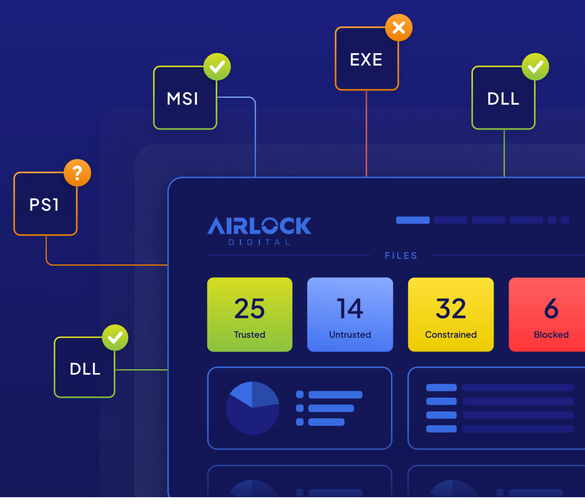
AIRLOCK DIGITAL

DATASHEET

Airlock Digital Application Control

Only Run What You Trust.



Key Benefits

Prevent Unauthorized Execution
Stop untrusted software before it runs.

Simplify Trust Management
Create policies based on how software actually behaves in your environment.

Reduce Attack Surface
Limit opportunities for malware, scripts, and unauthorized tools to execute.

Reduce Alert Fatigue
Lower the volume of events and alerts requiring analysis.

Reduce Privilege Risk
Allow specific applications to run with elevated rights without granting broad administrative access.

Maintain Operational Stability
Enforce control without disrupting users or workflows.

Improve Governance & Compliance
Increase visibility, accountability, and control over software execution.

Security teams have more visibility across the endpoint than ever before but still need a practical way to determine what software should be trusted to run.

Airlock Digital delivers proactive execution control, using application control to define and enforce what software is approved to run. Across complex endpoint environments, including IT, OT, and legacy systems, security and IT teams can prevent unauthorized software while maintaining system stability and operational continuity.

From Visibility to Defined Trust

While detection and response capabilities have advanced, many organizations still make trust decisions after software begins executing. This approach often requires teams to respond to activity rather than define what should be allowed to run in the first place.

Airlock Digital shifts this model by enabling organizations to define trust before execution. Teams gain clear visibility into what is actually running, understand software in its true application context, and establish policies aligned to their environment, prior to enforcement.

By transforming raw execution data into meaningful application context, Airlock Digital provides a continuously evolving, accurate view of software across the environment, without relying on predefined lists or external intelligence.

The result is a controlled, auditable environment where teams can confidently enforce policy, reduce overhead, and material lower risk, while strengthening the effectiveness of existing endpoint detection and response (EDR) tools.

Detection & Response

Visibility across all endpoint activity

Detect
Visibility across endpoint activity

Alert
Alerts across all executing software

Investigate
Determine trust and intent

Respond
More efficient response

- Broad visibility across endpoint activity
- Alerts generated across known and unknown software
- Investigation to determine trust and intent
- Decisions made after execution

Define & Enforce What Runs

Detection + Execution Control

A controlled foundation for better outcomes

Control
Only trusted software is allowed to run

Detect
Focus on meaningful activity

Alert
Higher-confidence alerts, less noise

Respond
More efficient response

- Unknown and untrusted software blocked before execution
- Reduced noise for detection and response tools
- More efficient investigations and faster response
- Maintains system stability and operational continuity

How Airlock Digital Works

See What Runs
Gain visibility into execution activity across the environment.

Understand What Runs
Group related files, scripts, and components into meaningful application context based on observed execution activity.

Define Trust
Set policies based on your environment, users, and workflows.

Accelerate Policy Creation
Use automated recommendations to reduce manual effort and reach enforcement faster.

Control Execution
Prevent unauthorized applications, scripts, and executables from running.

Manage Change
Support approvals, exceptions, and rollout through operational workflows.

Scale with Confidence
Extend control while maintaining operational stability.

Core Capabilities for Defining and Enforcing Trusted Execution

Application Control Enforcement
Enforce policy-driven control to prevent unauthorized applications, scripts, and executables from running.

Flexible Trust Decisions
Define and apply trust based on how software is introduced, used, and behaves in your environment.

Application Context
Gain an application-level view into what is running across your environment using real execution activity.

Elevation Control
Apply administrative-equivalent privileges to approved applications without granting broad user-level administrative access.

Trust Builder (Automated Policy Acceleration)
Accelerate policy creation with guided trust recommendations based on observed execution activity.

Workflow-Driven Policy Management
Manage approvals, exceptions, and rollout through structured operational workflows.

Execution Visibility and Governance
Provide visibility into execution activity, policies, and system state to support governance and accountability.

Cross-Platform Environment Integration
Extend application control across Windows, Linux, and macOS, IT and OT environments while integrating with existing workflows.

Common Use Cases

Prevent Malware & Unauthorized Execution

Prevent unknown, malicious, and unapproved software from running—including ransomware, scripts, and living-off-the-land techniques.

Apply Consistent Execution Control Across Complex Environments

Enforce trusted execution policies across IT, OT, legacy, and distributed environments without disrupting operations.

Improve Detection & Response Effectiveness

Reduce unnecessary execution activity to improve signal quality and help security teams focus on meaningful threats across EDR, XDR, and SIEM workflows.

Control Emerging Execution Vectors

Maintain control over scripts, browser extensions, packaged applications, and AI-driven agents as execution methods evolve.

Enforce Control to Strengthen Compliance and Governance

Supports alignment with major frameworks including ISO/IEC 27001, NIST, SOC 2, HIPAA, GDPR, CMMC, APRA CPS 234, and the Australian Essential Eight.

Payment Card Industry Data Security Standard **(PCI-DSS)**

United States SEC **Sarbanes-Oxley Act (SOX)**

Gramm-LeachBliley Act **(GLBA)**

Cybersecurity Framework **(CSF)**

Digital Operational Resilience Act **(DORA)**

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

Scan to Book a Demo

See how Airlock Digital helps you define what runs and stop everything else.

www.airlockdigital.com

AIRLOCK DIGITAL