EXECUTIVE BRIEF

Only Run What You Trust.

Without the Complexity.

In many environments, what should be allowed to run is not explicitly defined or consistently enforced, making it difficult to maintain clear control or demonstrate how risk is managed.

Airlock Digital Application Control establishes control at the point of execution, enabling organizations to define and enforce trusted software, reduce exposure, and strengthen governance.

This ensures decisions about what can run are applied consistently and enables security leaders to clearly demonstrate how risk is controlled across the organization.

Detection provides visibility into activity, but it does not determine what should be allowed to run. Without defined trust, decisions are made after execution—once risk has already been introduced.

Airlock Digital enables organizations to make intentional, enforceable decisions about software execution before it occurs—creating control that can be understood, measured, and consistently applied.

Security leaders can clearly demonstrate what is allowed to run, how risk is controlled, and how decisions are enforced across the environment.

What Changes When You Control Execution

Reduce Uncontrolled Execution Risk

Prevent unauthorized software from running at the point of execution.

Reduce Organizational Risk

Limit attack surface by preventing untrusted and unauthorized execution.

Establish Defensible Trust Policies

Define and govern what is allowed to run with auditable, organization-owned control.

Improve Security Program Effectiveness

Reduce unknown software execution so teams spend less time responding to avoidable activity.

Align Security and IT

Apply control in a way that supports operational workflows and system stability.

A Different Approach to Execution Control

This represents a fundamental shift from traditional approaches

Traditional Security Approach

- Detect threats **after execution**
- Investigate high volumes of alerts and activity
- Rely on **reactive, tool-driven response**
- Continuously expanding **attack surface and unknown risk**
- Limited ability to **enforce consistent control**

With Airlock Digital

- **Prevent unauthorized execution by default**
- Enforce **Zero Trust for applications and code**
- Control execution of **unknown and untrusted** software
- Apply **deterministic, policy-based control**
- Establish a **fully controlled, auditable environment**
- Reduce **operational noise and alert fatigue**
- Deliver **measurable reduction in attack surface and risk**

Built for Practical Deployment at Scale

Airlock Digital is designed for rapid, low-friction deployment, enabling organizations to establish control quickly and scale consistently across complex environments—without introducing operational burden.

- Rapid implementation without heavy upfront effort
- Scales across distributed environments and diverse endpoints
- Low ongoing operational overhead with policy-driven control

How Control is Applied Across Your Environment

Airlock Digital enables organizations to establish and sustain control over software execution:

See What Runs

Gain visibility into execution activity across the environment

Understand Applications

Understand software as applications, not just files—revealing what is present and how it behaves

Define Trust

Set policies based on your environment, workflows, and risk tolerance

Control Execution

Prevent unauthorized software from running at the point of execution

Accelerate and Manage Change

Refine trust decisions over time and support approvals, exceptions, and rollout through operational workflows

Scale with Confidence

Extend control across IT, OT-adjacent, and legacy environments while maintaining operational stability

Demonstrated Impact on Security Outcomes *

Organizations using Airlock Digital have achieved measurable reductions in security risk exposure alongside operational and financial benefits.

>25%
Reduction in overall breach risk

$4.1M
In security risk reduction value

224%
Return on investment (ROI)

$3.8M
Net present value (NPV) over three years

$1.3M
Reduction in administrative overhead

~2.5 hours per week
Minimal ongoing effort

Organizations also reported zero breaches following deployment, highlighting the impact of enforcing control at execution.

Where Airlock Digital Strengthens Your Program

Airlock Digital supports security programs across key priority areas, enabling consistent control over software execution while complementing existing investments.

Compliance Initiatives

Support frameworks such as Essential Eight and CMMC through enforceable, auditable control over software execution

Modern Application Risks

Manage execution of emerging and high-risk software types, including AI tools, macros, and browser or developer plugins

Existing Security Investments

Complement platforms such as endpoint detection and response (EDR) by adding control at execution and reducing the volume of activity requiring analysis

Core Platforms

Apply consistent control across Windows, macOS, and Linux environments

Common Attack Techniques

Reduce exposure to techniques such as living-off-the-land activity and software supply chain risks

Defensible Control for Governance and Audit

Airlock Digital establishes clear, enforceable policies for software execution, strengthening governance, audit readiness, and compliance while enabling security leaders to demonstrate how risk is controlled and ensure consistent enforcement across environments.

*The Total Economic Impact™ Of Airlock Digital, a commissioned study conducted by Forrester Consulting on behalf of Airlock Digital, December, 2025, is based on a composite B2B organization with $10B in annual revenue and 20k endpoints.

www.airlockdigital.com/forrester-tei-report

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)**

Discuss Your Security Program Priorities

Talk with Airlock Digital about how to define what runs, strengthen governance over software execution, and support more defensible control across your environment.

www.airlockdigital.com

AIRLOCK DIGITAL