

# Modern Application Control

Precision, Scalable Endpoint Security for the Enterprise



Airlock Digital Application Control provides robust endpoint protection with a Deny by Default model that minimizes the attack surface and prevents untrusted applications, malware, and zero-day exploits from executing. Purpose-built by cybersecurity professionals, Airlock Digital enables organizations to secure their endpoints efficiently and at scale.

## Proactive Endpoint Security

Airlock Digital's Deny by Default security posture ensures only trusted applications and processes can run on any endpoint, proactively protecting your systems.

- ➔ **Prevent untrusted applications**, including malware and zero-day exploits, from executing.
- ➔ **Enforce strict security policies by default**, lowering the risk of violations.
- ➔ **Ensure endpoints support compliance obligations** and uphold operational integrity.

## Built for Enterprise-Grade Operations

Airlock Digital enables organizations to secure endpoint infrastructure at scale, with broad OS support and intuitive exception handling:

- ➔ **Protect Windows, Linux, and macOS** systems, including legacy versions.
- ➔ **Secure both IT and OT environments** (e.g. SCADA, PLCs, and DCS systems).
- ➔ **Secure large, diverse endpoint collections** without impacting user productivity.

## Streamline Regulatory Compliance

Airlock Digital provides the technical controls organizations need to enforce precision application control.

With policy-driven allowlisting and blacklisting, real-time execution control, and secure exception management workflows, Airlock Digital was designed to help organizations meet regulatory compliance obligations and streamline endpoint management:



United States SEC  
Sarbanes-Oxley Act of 2002 (SOX)



EU Regulations

- General Data Protection Regulation (GDPR)
- Directive on security of network and information systems (NIS Directive)



International Organization for Standardization  
ISO/IEC 27001

## Essential Eight

Maturity Model  
Australian Signals Directorate

## HIPAA

United States DHS Health  
Insurance Portability  
and Accountability Act

## CMMC

United States DoD CIO  
Cybersecurity Maturity  
Model Certification

## APRA CPS 234

Australian Prudential  
Regulatory Authority  
CPS 234 Standard



## Airlock Digital: Features at a Glance

<b>Real-Time Threat Prevention</b>	Instantly block unauthorized software, malware, and ransomware across IT and OT systems, ensuring operational integrity and safety.
<b>Broad OS Compatibility</b>	Support for various Windows, Linux, and macOS versions, along with compatibility for legacy OT systems used in industrial environments.
<b>Granular Control Over Applications</b>	Define trusted applications, scripts, and processes at the file-level via hash, path, parent, or publisher, ensuring full control over IT & OT environments.
<b>Offline Mode Support</b>	Continuously secure endpoints even in low-connectivity areas and air-gapped facilities by operating in secure offline mode.
<b>Unified, scalable security management</b>	Manage security policies across both IT and OT systems from a single console, improving visibility and control over diverse environments.
<b>Application Blocklisting</b>	Prevent Living off the Land attacks by explicitly denying the execution of known malicious or high-risk system tools, scripts, and binaries.
<b>Precision Policy Management</b>	Full control over when your agents update, ensuring OT and legacy systems never receive updates without your explicit permission.
<b>Detailed Reporting &amp; Alerts</b>	Immediate insights into application behavior, compliance, and security posture, enabling proactive threat management and compliance assurance.
<b>Resource-Efficient Design</b>	Minimal impact on endpoint performance, even with high-security settings, making it suitable for both resource-constrained and high-availability environments.
<b>Hardened Cloud or On-Premises Deployment</b>	Flexible deployment options for cloud or on-premises environments, allowing organizations to tailor the solution to their security architecture and compliance needs.
<b>Security-stack Integration</b>	Integrates with leading EDR, SIEM, and identity management solutions, reinforcing a layered security approach and enhancing detection capabilities.

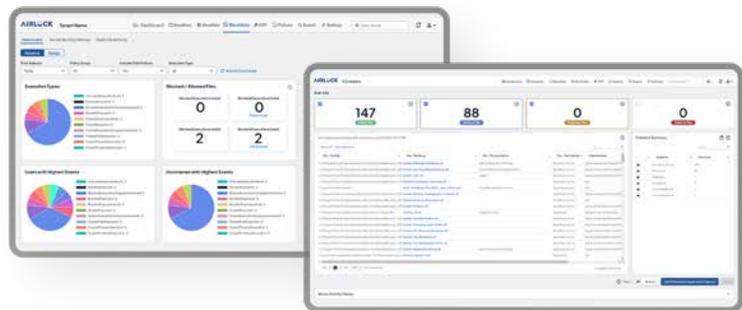
## Protect Your Endpoints with Confidence

Airlock Digital Application Control is designed to meet the unique challenges of modern endpoint security and protection. To discover how Airlock Digital can protect your organization's critical digital infrastructure, visit [airlockdigital.com](https://airlockdigital.com) or contact our sales team at [sales@airlockdigital.com](mailto: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™