

Airlock Digital + CrowdStrike

Delivering a layered, resilient endpoint strategy



Organizations today face an increasingly dynamic, sophisticated threat environment

Breaches are commonplace with the average cost per incident—including ransomware attacks—estimated at nearly \$5 million. However, help is at hand. Airlock Digital's application control (allowlisting) solution, integrated with the CrowdStrike Falcon® endpoint detection and response (EDR) platform, can help you implement a powerful endpoint security strategy.

Airlock Digital—a standout in the CrowdStrike ecosystem

Founded in 2013, Airlock Digital is a CrowdStrike strategic partner and our solution is a consistently popular application listing in the CrowdStrike Marketplace.

Leading organizations in the United States and international markets—including industries designated as critical infrastructure—use Airlock Digital with CrowdStrike to control the files and applications that run in their environments. With Airlock Digital and CrowdStrike, you can:

- ➔ Decide which files and applications you trust to run and stop all others from running
- ➔ Prevent ransomware, malware and unauthorized software
- ➔ Proactively prevent unknown attacks with a zero-trust methodology
- ➔ Verify, monitor and record all file executions and changes
- ➔ Extend protection across current, recent and legacy operating systems
- ➔ Access rich, correlated datasets for deep insights into your environment
- ➔ Minimize notifications and 'noise' to improve the visibility of endpoint security states

Here's why Airlock Digital and CrowdStrike are better together

Enhanced threat prevention

Because the Airlock Digital application control (allowlisting) solution allows only files trusted by an organization to run, ransomware, malware and unauthorized software is stopped from executing. This adds proactive endpoint defense to CrowdStrike's advanced detection and response to malware that has bypassed preventative controls.

A layered security approach

By enforcing a customer's configurable allowlist, the Airlock Digital solution prevents all unknown files, including ransomware, from executing within the environment. This significantly reduces risk on the endpoint by implementing a deny by default approach to security. When the Airlock Digital solution is combined with CrowdStrike's industry leading endpoint detection and response capabilities, endpoints are protected against both known and unknown attacks, regardless of whether the attacks use files, are fileless or utilize advanced techniques such as Living off the Land (via LOLBins).

Sharpened focus with fewer false positives

With Airlock Digital's application control (allowlisting) solution, organizations can reduce the noise from non-malicious but unknown applications that attempt to run. This means CrowdStrike's endpoint detection and response solution can focus on critical threats, improving alert quality. This synergy enables security teams to prioritize threats and respond more quickly and effectively.



Scan now to request a trial of the Airlock Digital application control (allowlisting) solution at the CrowdStrike Marketplace

Streamlined incident response

Because the Airlock Digital solution prevents all unauthorized file and application execution, fewer incidents occur that require a response. When incidents do occur, CrowdStrike's solution provides forensic insights, threat hunting and automated responses for containment and remediation.

Improved compliance and reporting

Airlock Digital helps organizations implement world-recognized standards such as PCI-DSS, US DoD CMMC and the Essential Eight, while CrowdStrike provides comprehensive logging, reporting and compliance data around threat detection and response. This robust combination makes audits easy and compliance management more effective.

Seamless CrowdStrike integration

Customers can deploy Airlock Digital's application control (allowlisting) capability natively from the CrowdStrike Falcon console. Airlock Digital and CrowdStrike's integration makes rapid implementation of a deny by default security strategy a reality, with minimal operational overhead required.

A proactive, adaptable security integration

Airlock Digital's application control (allowlisting) solution and the CrowdStrike Falcon platform is a proactive, adaptable combination for your organization. Through purpose-built workflows, full file visibility and advanced threat prevention and detection, you can defend effectively against a range of malware types while minimizing operational overhead. In addition, extending protection to operational technology environments underscores the commitment to the security and reliability of critical systems. Together, we help organizations stay ahead of advanced threats to protect their environments from end-to-end.

Compliance & regulation

Allowlisting technologies are now written into Government standards and/or regulations worldwide, including:

Australia

ACSC Strategies to mitigate cybersecurity incidents (Essential 8)

United States

Top 10 Mitigations, NIST 800-171, Cybersecurity Maturity Model Certification (CMMC), Center for Internet Security Basic Six

New Zealand

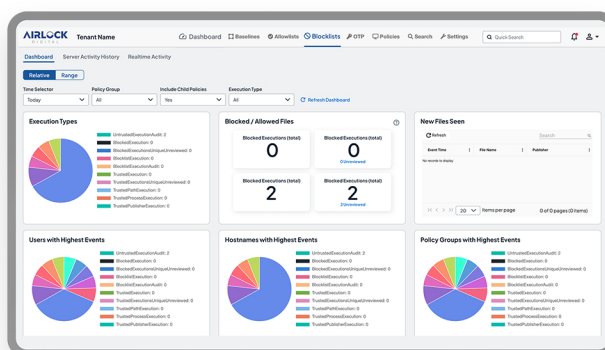
Critical Controls 2024

Canada

Top 10 IT Security Actions

Global

PCIDSS 4.0



AIRLOCK
DIGITAL

AVAILABLE FOR
Windows™ | Linux® | macOS™



Scan to request a trial

Use the QR code to request a trial of the Airlock Digital application control (allowlisting) solution at the CrowdStrike Marketplace



airlockdigital.com