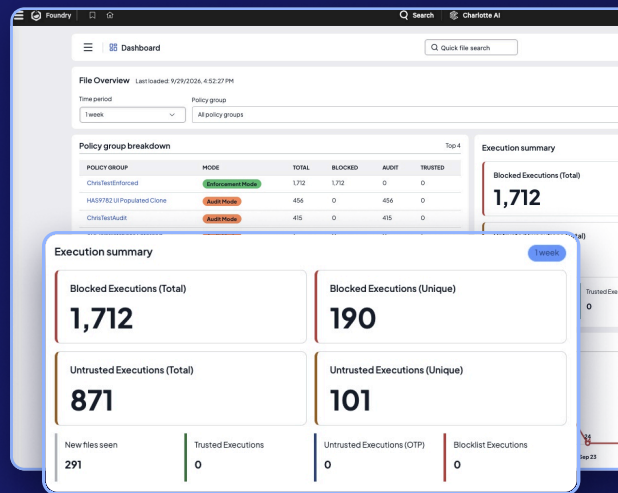


Airlock Digital and CrowdStrike Falcon®

A multi-layered approach to endpoint security



Prevent unauthorized execution. Investigate suspicious activity. Turn findings into enforcement.

Airlock Digital and CrowdStrike Falcon help organizations reduce ransomware, malware, shadow IT, and unauthorized software risk by combining application control with endpoint protection, detection, investigation, and response. Together, they give security teams a practical way to prevent untrusted software from running, investigate suspicious activity, and convert file-level findings into enforceable policy decisions.

The endpoint security challenge

For organizations, a highly effective security strategy starts by controlling what software can run across their environments and how to investigate when endpoint activity raises concerns. Unauthorized software introduces risk, but approved applications can also be misused. Effective protection requires enforceable software trust policies, strong endpoint visibility, and fast detection and response. Managing these capabilities through separate workflows can slow teams down. Analysts may need to switch consoles, transfer file information, and coordinate policy changes before they can act. This creates operational overhead at the exact moment speed and context matter most.

Two complementary offerings

Together, Airlock Digital and CrowdStrike help customers reduce opportunities for unauthorized execution while maintaining the detection, investigation, and response capabilities needed to handle threats across modern endpoint environments, including OT, legacy, and end-of-life systems. The native Airlock Digital integration with CrowdStrike Falcon makes a multi-layered strategy easier to implement and operate.

Airlock Digital	CrowdStrike Falcon
Provides application control to define and enforce which software is authorized to execute	Provides endpoint protection, detection, investigation, and response
Supports a deny by default approach through configurable software trust policies	Gives security teams visibility into suspicious endpoint activity
Prevents unauthorized applications, scripts, and executables from running according to configured policies	Enables investigation and response, including when approved software is involved
Provides policy, allowlist, blocklist, exception, and file execution visibility	Provides the security operations environment where teams investigate, prioritize, and act

Reduce execution risk while streamlining investigation and response

The native Airlock Digital integration with CrowdStrike Falcon connects deny by default application control with endpoint investigation workflows. Teams can access key Airlock Digital capabilities within CrowdStrike Falcon, review application control context during investigations, and act on file findings without manually transferring hashes between consoles.

Manage application control within CrowdStrike Falcon

Access the Airlock Digital dashboard and allowlist, blocklist, policy, and exception management capabilities natively in the CrowdStrike Falcon console. Administrators can perform supported application control tasks within an environment their security team already uses.

Review Airlock Digital context during investigations

Airlock Digital Case Summary and Hash Intelligence panels provide application control context, including existing allowlist or blocklist membership. Analysts can understand how Airlock Digital currently treats a file before deciding what action to take.

Turn investigation findings into blocklist decisions

When blocking is appropriate, analysts can specify the file hash and select an Airlock Digital blocklist rule directly within CrowdStrike Falcon. Airlock Digital applies the resulting decision through its applicable policies and endpoint enforcement.

An integrated customer workflow

- 1 Investigate in CrowdStrike Falcon
- 2 Review Airlock Digital context
- 3 Select the appropriate Airlock Digital blocklist
- 4 Enforce through applicable Airlock Digital policies

Connect through CrowdStrike Foundry

Install the Airlock Digital application through the CrowdStrike Foundry catalog and connect it to your Airlock Digital environment using the required connection details and API permissions.

See the partnership in action

Discover how Airlock Digital and CrowdStrike help your organization control authorized software execution, investigate suspicious activity, and connect findings to enforcement to strengthen your organization's security posture.

