



Airlock Digital Integration with CrowdStrike Falcon®

Multi-layered endpoint security with application control

With security threats continuing to increase, organizations are looking to implement a multi-layered security strategy that combines control over what is authorized to run with the ability to detect, investigate, and respond to suspicious activity. The Airlock Digital integration with CrowdStrike Falcon brings application control management together with endpoint detection and response (EDR) capabilities.

The enterprise challenge

By controlling which applications, scripts, and executables can run while continuing to detect and respond to suspicious endpoint activity, organizations can significantly improve their security posture. Application control and EDR serve complementary purposes, but operating them across separate workflows creates complexity and inefficiency.

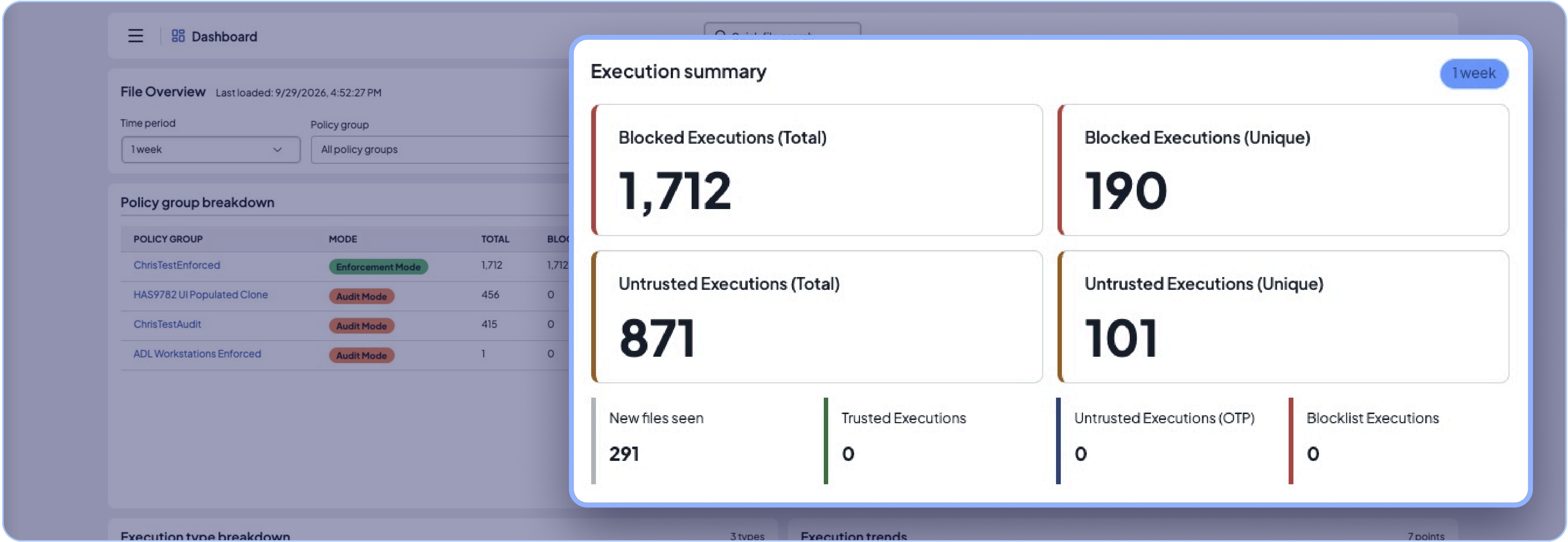
How Airlock Digital and CrowdStrike work together

Airlock Digital provides deny by default application control, helping organizations define which applications, scripts, and executables they trust and prevent unauthorized software from executing. CrowdStrike Falcon provides endpoint protection, detection, investigation, and response. Together, both solutions help customers reduce opportunities for unauthorized execution while maintaining visibility into suspicious behavior and the ability to act.

The integration brings the Airlock Digital and CrowdStrike capabilities together into a multi-layered endpoint security strategy that enables customers to:

- ✓ **Reduce exposure to unauthorized execution**
By combining Airlock Digital software trust enforcement with CrowdStrike Falcon
- ✓ **Make informed enforcement decisions**
With visibility into application control and what is allowed or blocked by policy
- ✓ **Simplify application control administration**
By bringing key policy and exception management tasks into CrowdStrike Falcon
- ✓ **Connect existing security investments**
Through a shared workflow for application control administrators and security analysts
- ✓ **Reduce manual investigation steps**
By bringing Airlock Digital context into CrowdStrike Falcon EDR capabilities

Key Airlock Digital capabilities within CrowdStrike Falcon



Access Airlock Digital application control management capabilities within the CrowdStrike Falcon console

Capability	Technical function	Customer value
Deny by default application control	Enforces configured software trust policies to permit authorized execution and prevent unauthorized software from running	Reduces opportunities for unauthorized execution and improves security posture
Allowlist and blocklist management	Enables administrators to maintain application control rules, with key management capabilities accessible within CrowdStrike Falcon	Connects software trust administration with existing security operations
Policy and exception management	Provides access to key Airlock Digital policy building and exception handling capabilities through the embedded CrowdStrike Falcon experience	Supports ongoing application control administration as requirements change
Airlock Digital dashboard within Falcon	Embeds the Airlock Digital interface within the CrowdStrike Falcon console	Makes application control tasks accessible in a familiar workspace
Application control context	Provides Airlock Digital Case Summary and Hash Intelligence panels, including visibility into existing allowlist or blocklist membership	Helps connect the organization’s software trust decisions with its investigation process
Blocklist action during investigation	Enables an analyst to specify a file hash and select the Airlock Digital blocklist rule to update	Removes the need to manually transfer the hash between consoles
API-based connection	Connects the Airlock Digital application in CrowdStrike Foundry to the customer’s Airlock Digital environment using connection details and an API key	Enables a native user experience and investigation actions across the two platforms

Turn investigation findings into enforcement decisions

Consider a file that is currently permitted to run but is identified during an investigation as requiring a new trust decision.

- 1

Investigate in CrowdStrike Falcon

Open the relevant file or event and assess the available investigation context
- 2

Review Airlock Digital information

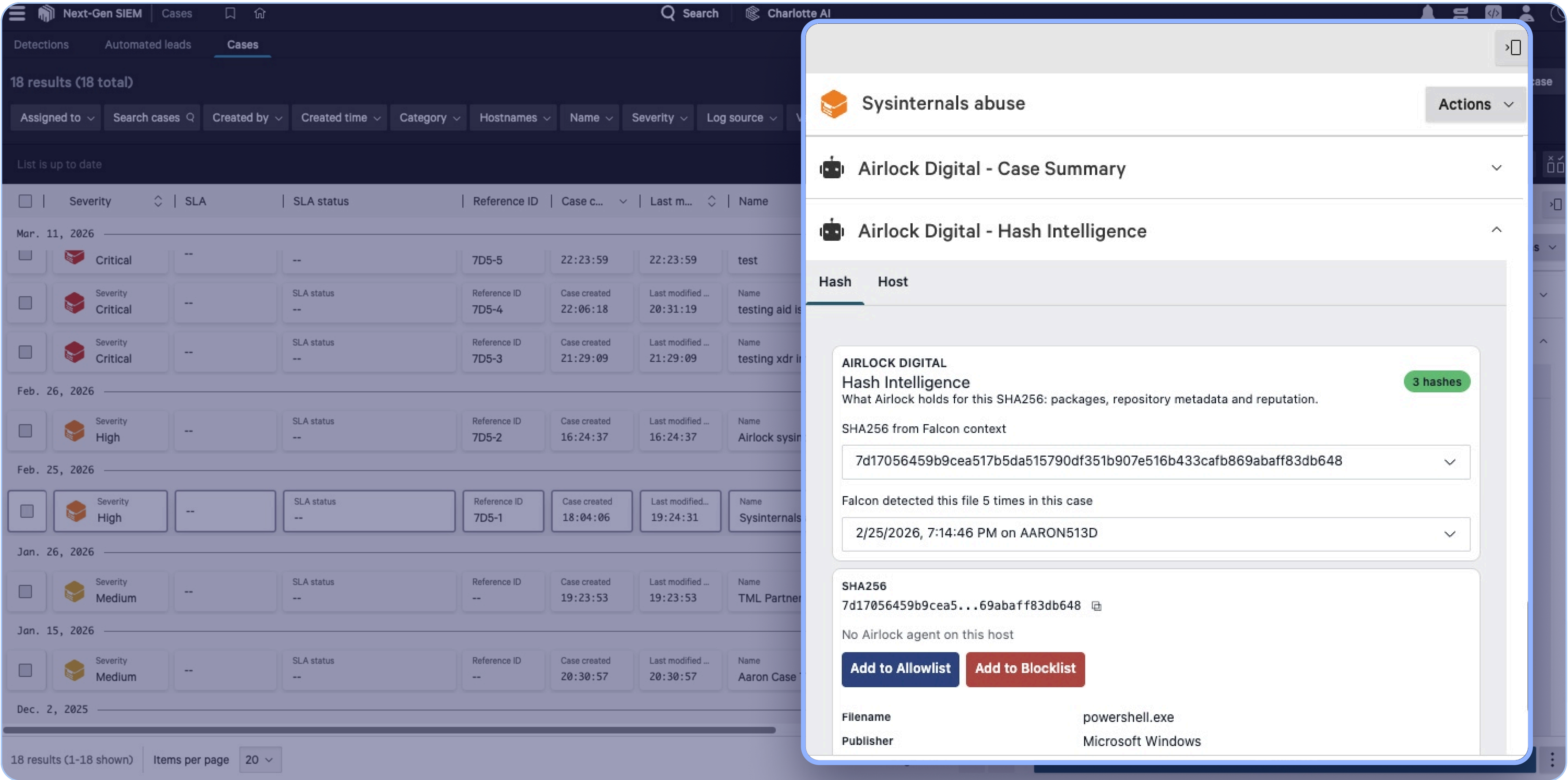
Inspect the Airlock Digital panels and determine whether the file already belongs to an allowlist or blocklist
- 3

Select the blocklist action

If blocking is appropriate, identify the relevant file hash and choose the intended Airlock Digital blocklist rule
- 4

Apply the application control decision

The selected list is updated in Airlock Digital, and the decision is enforced through the applicable policies on covered endpoints



Review a file’s Airlock Digital context and add it to a selected blocklist without leaving the CrowdStrike Falcon investigation workflow

Simplified integration setup

The Airlock Digital application is installed through CrowdStrike Foundry and connects to the customer’s Airlock Digital environment through an API key. Supported actions initiated within CrowdStrike Falcon are carried out within the connected Airlock Digital environment.

Before connecting

Confirm the following for the intended deployment:

- ✔ A supported Airlock Digital environment and deployed agents on endpoints requiring enforcement
- ✔ CrowdStrike Falcon access and the necessary CrowdStrike Foundry application entitlements
- ✔ Customer administrator permissions to install and configure the application
- ✔ The Airlock Digital connection URL and an API key with the documented permissions required for the intended functions

Connect and validate

- 1 Open CrowdStrike Falcon and locate Airlock Digital in the CrowdStrike Foundry application catalog
- 2 Select Install, review the requested permissions, and accept to continue
- 3 Enter the connection name, Airlock Digital URL, and API key
- 4 Complete the connection and confirm that Airlock Digital information loads within the CrowdStrike Falcon console
- 5 Validate the management and blocklist workflow using an approved test file and policy

See the integration in action

Discover how Airlock Digital and CrowdStrike Falcon make layered endpoint security easier and more efficient to operate. Contact your Airlock Digital or CrowdStrike representative for a demonstration of deny by default application control and investigation-to-blocklist workflows.



Scan to book a meeting

Book a meeting to explore how Application Control and Allowlisting from Airlock Digital can help your business