

Airlock Digital Agentic Steering

AI Usage Control for agentic applications and agents at the endpoint

Control what agentic agents can execute on the endpoint.

Agentic AI is changing how activity happens on enterprise endpoints. Instead of a person directly executing every step, agentic agents can initiate commands and actions on behalf of users as they work toward an objective.

That creates a new requirement for endpoint security. Organizations need visibility into agent-initiated activity and preventative controls that determine whether an action is permitted before it executes.

Why This Matters, By The Numbers

82%

of organizations have found
AI agents running that IT
never knew about ¹

\$4.63M

average cost of a breach
involving shadow AI ²

65%

of organizations have
already had an AI agent
security incident ¹

One Preventative Control Model for Applications and Agentic Agents

APPLICATION CONTROL ANSWERS

“What can run?”

AGENTIC STEERING ANSWERS

**“What can an agent
execute once it’s running?”**

Airlock Digital Agentic Steering extends deny by default Application Control to commands and actions initiated by supported agentic agents. Security teams can see the endpoint activity supported agents attempt, define what they are permitted to execute, and apply customer-defined policy before execution.

Permitted actions can proceed. Actions that are not permitted are stopped before execution, and Airlock Digital returns the policy decision directly to the supported agent. Administrators can provide context explaining the decision or an approved alternative where configured, helping the agent continue working within organizational policy.

1: Cloud Security Alliance 2026 Survey Report, *Autonomous but Not Controlled*

2: IBM Cost of a Data Breach Report 2025

Application Control Today | Extended with Agentic Steering

Application Control Today	Extended with Airlock Digital Agentic Steering
✓ Discover agentic applications across endpoints	+ Identify supported agentic agents operating within those applications
✓ Standardize and enforce trusted agentic tooling	+ Define what supported agentic agents are permitted to execute
✓ Block unapproved agentic applications from executing	+ Evaluate agent-initiated commands and actions against policy before execution
✓ Apply centrally managed Deny by Default Application Control policy	+ Apply agent-specific and command-level rules to supported agentic agents
✓ Notify users when application execution is blocked	+ Return policy decisions directly to supported agentic agents, with administrator-provided context or an approved alternative where configured

What You Can Do with Agentic Steering

See how agentic agents operate on the endpoint, define what they’re permitted to execute, apply policy before actions execute, and maintain visibility into activity and policy decisions.

- 1

See What Agentic Agents Are Doing

Gain visibility into supported agentic agents and their endpoint activity. Centrally record agent sessions, commands, policy decisions, and outcomes so you can understand how Agentic AI operates across your environment.
- 2

Define What Agentic Agents Are Permitted to Execute

Decide which agentic agents you trust and define clear rules for the endpoint commands and actions they’re permitted to initiate.
- 3

Keep Agents Within Policy

Evaluate agent-initiated endpoint actions against customer-defined policy before execution. Allow permitted actions to proceed and stop actions that are not permitted before they run. When an action is denied, return the policy decision directly to the supported agent, with administrator-provided context or an approved alternative where configured.
- 4

Understand and Demonstrate Control

Maintain searchable visibility into agent sessions, commands, policy decisions, and outcomes. Use this information to review activity, refine policy, and demonstrate how Agentic AI is being controlled at the endpoint.

What This Means for You

- ✓ Adopt Agentic AI without losing visibility or preventative control at the endpoint.
- ✓ Standardize approved Agentic AI tools and reduce Shadow AI.
- ✓ Control what supported agentic agents execute—not only whether they are allowed to run.
- ✓ Stop agent-initiated actions that break organizational policy before they execute.
- ✓ Give supported agents actionable policy information when an action is denied.
- ✓ Maintain evidence of agent activity and policy enforcement for security reviews, audits, and regulatory reporting.