AIRLOCK DIGITAL

DATASHEET

Airlock Digital Agentic Control

Control what AI agents can do. Steer how they proceed.

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.

This 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 CONTROL ANSWERS
“What can an agent execute once it’s running?”

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

With Agentic Steering, 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*

© 2026 Airlock Digital. All rights reserved.

Application Control Extended to AI Agents

Application Control	Agentic Control
✓ Discover the applications, scripts and files running across your endpoints.	+ Discover AI agents, LLMs and harnesses, and see what supported agents attempt by agent, endpoint and session.
✓ Allow only trusted software to run with Deny by Default policy.	+ Allow only approved AI applications and agents to run, with separate policies for agents and the people on the same endpoint.
✓ Stop untrusted software before it executes.	+ Evaluate actions from supported agents, such as ChatGPT and Claude, against your policy before they run.
✓ Notify users when execution is blocked.	+ With Agentic Steering, return the decision directly to the agent, with context or an approved alternative, so it can adapt and keep working within policy.
✓ Review execution history and policy decisions to refine policy over time.	+ Review agent sessions, decisions and outcomes, with AI-generated summaries, token usage and estimated cost.

How Agentic Control Works

See how Airlock Digital Agentic Control helps your team discover AI agents, define what they're permitted to do, enforce and steer before actions run, and review the results.

1 Discover AI Agents and See Their Activity

Identify AI agent tools across endpoints and review agent sessions to understand which commands your teams use for approved work.

2 Define What AI Agents Are Permitted to Do

Choose permitted commands and configure restrictions, including explanations or approved alternatives to return when an agent encounters a block.

3 Enforce Policy and Steer the Agent

Evaluate proposed commands before execution, allow permitted actions, and return denial decisions with guidance to the AI agent where configured.

4 Review Agent Activity and Refine Policy

Inspect subsequent attempts and recorded results to assess whether the agent followed policy, completed permitted work, or needs clearer guidance.

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.

Learn More About Agentic Control

See how Airlock Digital is extending preventative endpoint security for a world where both people and agentic agents initiate activity.

www.airlockdigital.com

© 2026 Airlock Digital.
All rights reserved.

AIRLOCK DIGITAL

.cpl .exe .dll .ps1 .bat .vbs .cmd .chm .class .hta .java .jar .js .ps .psm1 .py .ps1 .py3 .pyd .pyo