

AI Control - The next flagship capability in the Heimdal platform

Every business is already running AI. Almost none of them can see what it's doing once it's running, or stop it from sending sensitive data out the door. Heimdal is closing that gap.

Preview



THE BIGGER PROBLEM, NOT JUST AN AI PROBLEM

Firewalls tell you who's on the network. Endpoint tools tell you what's running. DLP tools catch files leaving through email or USB. None of them were built for what AI tools actually do: reading context nobody gave them permission to read, reaching into folders to be "helpful," and taking whatever someone types into a browser and sending it to a server outside the business. This isn't a gap in one tool. It's a gap the entire security stack was built before this problem existed.

WHAT'S COMING: FULL VISIBILITY, REAL CONTROL

AI Containment decides what's allowed to run or reach, block and allow, black and white. AI Control governs everything in between, what an allowed AI tool actually does once it's running. That's the gray zone nobody else is covering.

ON THE DEVICE

- | See every AI tool running, the moment it starts.
- | See exactly what it touches: folders, processes, and network destinations, and whether it's allowed to run in the first place.
- | Set the boundary by folder, process, destination, user, group, or device.

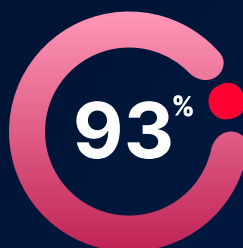
IN THE BROWSER

- | Catch prompts, pasted text, and file uploads before they ever leave the device.
- | Detections aren't just flagged, they're categorized: keywords, sensitive data, and commercial or business data, each scored for risk so nothing gets buried in noise.
- | See it by AI tool, by folder, or by browser, whichever view answers the question you're actually asking.
- | Covers the tools your people are already using: ChatGPT, Copilot, Gemini, Claude.

WHAT OUR OWN CUSTOMERS TOLD US



| 82% already have AI tools running in their business, approved or not.

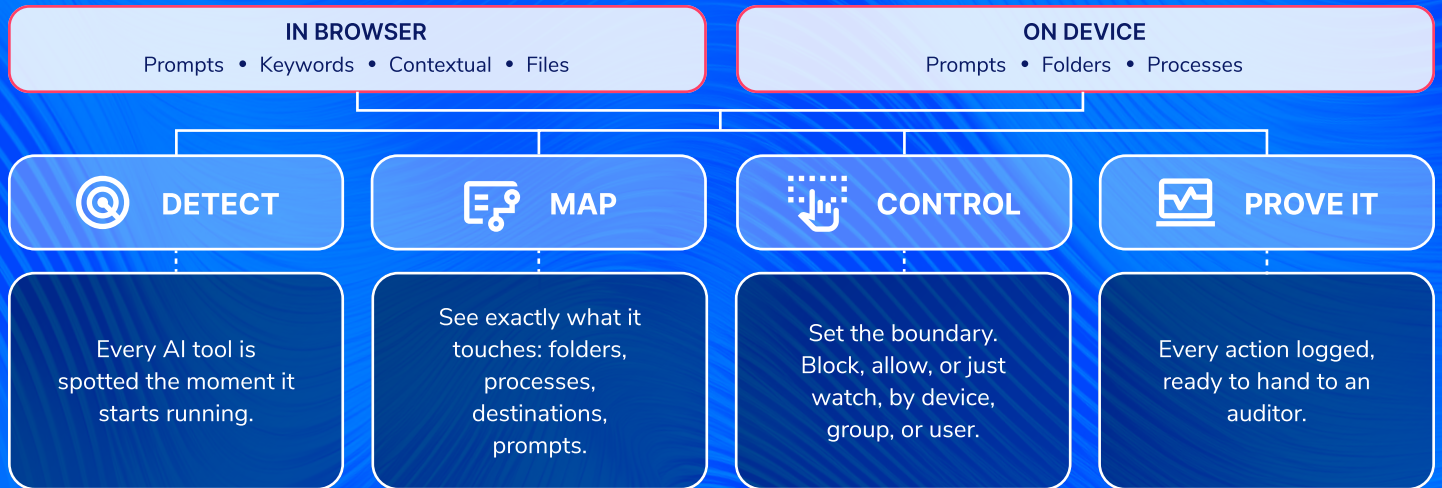


| 93% (66 of 71 surveyed) said data leaving through AI tools is their single biggest fear, ahead of file access, ahead of audit visibility, ahead of everything else we asked about.

- | 80% flagged AI tools triggering scripts or grabbing more privilege than they should.
- | 79% say they'll need a dedicated way to control this within six months. Most said now.
- | 70% want to start in monitor mode and learn before they enforce, not block first and ask questions later.

This isn't a hypothetical problem we're getting ahead of. It's already sitting in every one of these businesses today.

HOW AI CONTROL WORKS



BUILT FOR REGULATION THAT'S ALREADY ARRIVING

This isn't just a security conversation anymore, it's a compliance one. Customers told us this without being asked: the EU AI Act, NIS2, and ISO requirements are already showing up on procurement checklists. AI Control gives compliance and risk teams something concrete to point to, not a promise, evidence of what AI touched, what it was allowed to do, and what got stopped.



WHAT THIS MEANS FOR PARTNERS AND MSPS

A new, sellable layer built on infrastructure you already run and already know how to support. No new platform to learn, no new vendor relationship to manage for your clients. This is billable service on top of something you're already delivering, and it's the conversation your clients are already asking about, whether or not you've had an answer for it yet.



WHAT THIS MEANS FOR ENTERPRISES AND END CUSTOMERS

Proof, not promises. Exactly what AI tools are doing on your devices, exactly what they're allowed to reach, and a rollout that starts by watching before it starts blocking, so nothing breaks on day one. Built to hand to an auditor, not just describe in a meeting.



WHY THIS IS HEIMDAL'S TO BUILD

AI Control is a standalone module, not a bolt-on. It doesn't need Application Control, DNS, or anything else running first, it works on its own from day one. That said, we're not starting from a blank page either: Heimdal already secures the endpoints of over 20,000 customers, so this is a company that already knows how to run security at scale, not one learning it for the first time.

Be first in line for AI Control.

Reserve early access

Founding pricing available for a limited window. Terms apply, details shared once you're on the list. Talk to your customer success manager or channel account manager.

