

# Ensage™ AI Security for Semiconductor Design

## Boundaries agents cannot rewrite

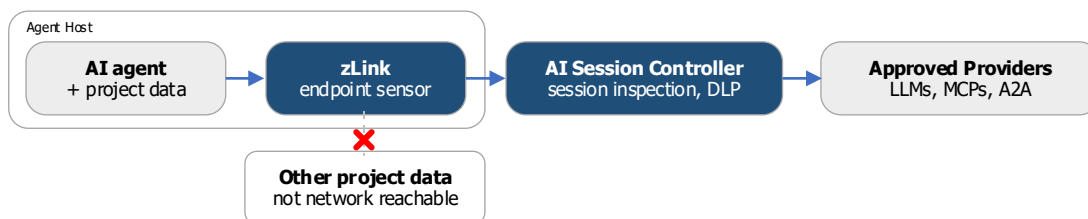
Project-scoped reachability and credentials, enforced independently of the AI agent, its hooks, and its configuration. Adopt agents in the design flow without exposing your and third-party IP to risks of data leaks.

### The control gap in the design flow

AI agents are entering semiconductor design flows: coding agents, MCP-based agents, EDA vendor agents, and internally developed agentic scripts, often arriving before review processes can standardize them. Licensed cores, foundry PDKs, and EDA tool outputs carry contractual obligations; one leak can breach them.

**An AI agent can expose critical IP without violating an existing rule. The user, the device, and the destination can all be approved. The missing context is which project the agent is acting for.**

### Strong boundaries, enforced outside the agent



The zLink endpoint sensor identifies the agent and its project at the host, sanctioned or shadow, and enforces network reachability.

#### Reachability

Project B is not reachable from Project A's enclave. Virtual Chambers shield the highest-value assets, such as foundry PDKs, from compromised agents inside the boundary.

#### Credentials

Provider API credentials remain at the controller, never on the session host. Sessions use centrally managed credentials rather than user-held keys. Sessions using unknown keys can be blocked.

#### Inspection

Sessions terminate at the controller for inspection in flight: prompts, uploads, responses, and tool calls, with detection and blocking on keywords, PII, and sensitivity labels.

#### Evidence

Decrypted content and session records remain in systems you designate, inside your environment, suitable for customer and partner audits.

### Not another agent hook or cloud proxy

The CoIP overlay enforces project-scoped reachability at the host. The AI Session Controller, in your environment, holds credentials and inspects sessions without depending on the agent's prompts, hooks, or configuration. Agentic traffic does not traverse a Zentera-hosted cloud or a SASE point of presence. No agent-side hooks or agent replacement required; designers keep the agents and workflows they have.

**The AI governance layer is new; the underlying control-plane architecture is not.** Ensage runs on the CoIP overlay, which has operated in production enterprise environments at Siemens and Cadence for years. Ensage AI is tailored for semiconductor design workflows by a team with deep semiconductor experience.

#### Validate the boundary against one real design workflow.

Bring one agent, one project, and its approved data, tools, models, and credentials. We map the enforcement path, test out-of-project reachability and credential misuse, and define a validation plan.

Schedule an Ensage architecture review: [sales@zentera.net](mailto:sales@zentera.net)

