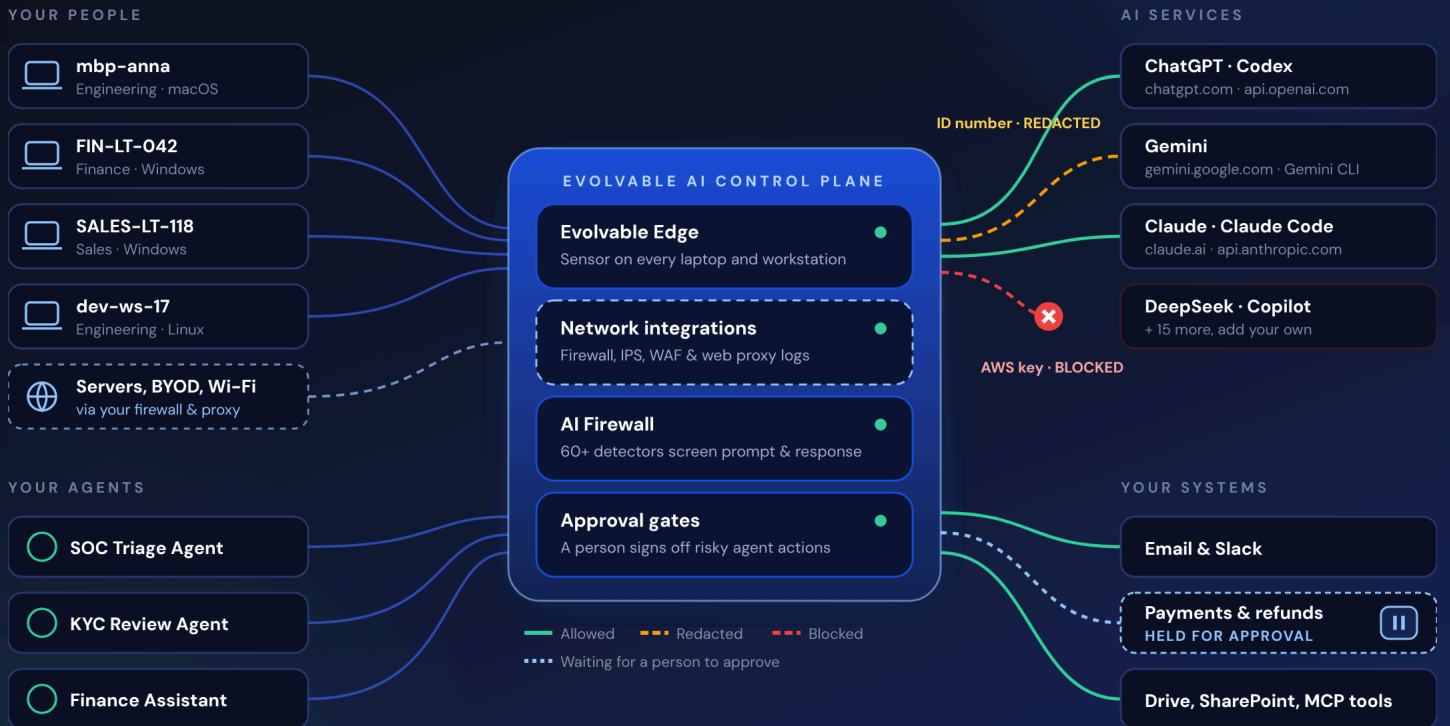


# AI is your newest attack surface. Secure every inch of it.

Employees paste code, customer records and credentials into public chatbots and coding assistants every day. Your own agents send email, move files and change systems on their own. **Evolvable.ai is one control plane for both:** it sees AI use on every device and across your network, screens every prompt and response, and puts a person in front of every risky action. On your infrastructure.



## CAUGHT BY EVOLVABLE EDGE, BEFORE IT LEFT THE DEVICE

Events from an Evolvable demo workspace

## WHAT YOU GET

**Say yes to AI**  
Give people ChatGPT, Copilot and coding assistants without the leak risk. Enable, don't ban.

**Stop leaks at the source**  
Secrets and personal data are caught on the device, before they reach a public model.

**Prove control on demand**  
Every block, redaction and approval is evidence for auditors and regulators.

**Scale agents safely**  
Agents act on real systems, with a named person accountable for every high-risk step.

20<sup>+</sup>

AI services inspected out of the box, from chat apps to coding CLIs

60<sup>+</sup>

shared detectors, including AI judges for injection and exfiltration

14

languages in term-list packs, Arabic included

5

ways to put a person in the loop, from veto window to AI judge

# Three controls. *One sovereign platform.*

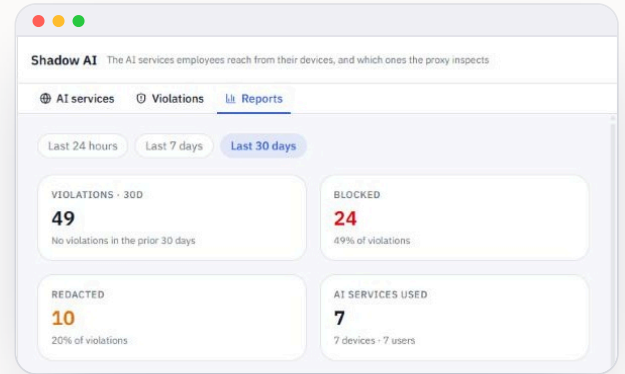
## 01 SEE

### Know every AI your people touch.

**OUTCOME** *An accurate AI inventory before you write a single policy.*

#### KEY FEATURES

- ◆ **Shadow AI discovery.** Traffic to 20+ AI services, including coding CLIs like Claude Code and Codex, mapped per device, user and network segment.
- ◆ **Device and network.** **Evolvable Edge** on Windows, macOS and Linux laptops, plus **network integrations** that pull AI traffic from your firewall, IPS, WAF and web proxy. No new appliance.
- ◆ **Reports & network map.** Top AI services, the people with the most violations, and every device-to-model flow on one screen.



## 02 STOP

### Catch the leak before it leaves.

**OUTCOME** *Sensitive data never reaches a public model. Provably.*

#### KEY FEATURES

- ◆ **One AI firewall** for employee AI use and your own agents, screening both the prompt and the response.
- ◆ **60+ shared detectors.** Checksum-validated IDs and cards, secrets, PII, 14-language term lists, and AI judges for injection, jailbreak, tool abuse and exfiltration.
- ◆ **Block, redact or log** with full evidence: who, which device, which service and model, and exactly what matched.



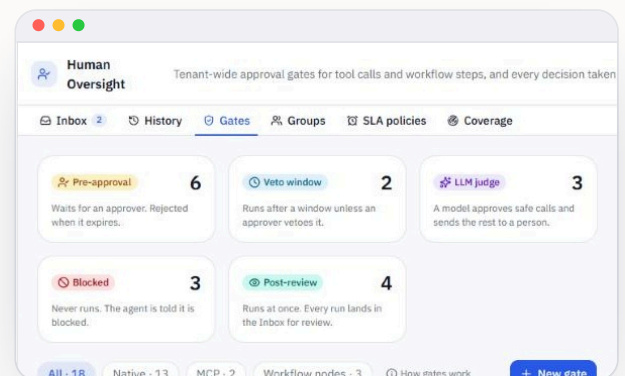
## 03 GOVERN

### Put a person in front of risky actions.

**OUTCOME** *Agents act on real systems with a named person accountable.*

#### KEY FEATURES

- ◆ **Five gate modes** on any tool, MCP call or workflow step: pre-approval, veto window, AI judge, post-review or block.
- ◆ **Approver groups and SLA escalation.** Decide in the web app, Slack, Teams or email; reminders and escalation run on a clock.
- ◆ **Coverage & history.** See every agent that can act with no one watching. Every decision is logged and every change versioned.



#### SOVEREIGN BY DESIGN

- 🔒 Runs on your cloud, private cloud, on-premises or air-gapped. Prompts and evidence never leave your estate.
- 🌐 Works with the LLMs you choose, per agent. Agents converse in Arabic and English.

#### ENFORCES THE CONTROLS THESE FRAMEWORKS EXPECT

- OWASP LLM Top 10
- ISO/IEC 42001
- NIST AI RMF
- EU AI Act
- UAE PDPL
- KSA PDPL & SDAIA

*See what's leaving through AI. In 45 minutes.*

We put Evolvable Edge on a few laptops, connect your firewall or proxy logs and one agent, and show you live what is being sent, blocked and redacted.

[BOOK A DEMO](#)

info@evolvable.ai

www.evolvable.ai