



AI agents run on your laptops, your cloud, your products. **One control plane watches all three.**

AI agents now live in three places: on **employee laptops**, across your **cloud and SaaS**, and inside your **own software**. Wingback's Agent Detection & Response discovers, watches, and governs all three from one control plane: inline at the browser and the model gateway, with agentless scans of your cloud accounts.

2,000+

Detection rules and threat IOCs

40+

AI provider and framework integrations

24/7

Monitoring, inline at the browser and gateway

Inventory view, sample data

Inventory

Swept every 5 min

AGENTS

85

MODELS

34

GUARDRAILS

12

SHADOW AI

7

BY LAYER

Endpoint 41

Cloud 32

Product 12

1,412 devices

RECENTLY DISCOVERED

support-copilot

gpt-4o, OpenAI

ACTIVE

claims-triage-agent

claude-sonnet, Bedrock

ACTIVE

hr-onboarding-rag

ada-002 index, Azure

REVIEW

81 HEALTHY

2 BLOCKED

2 REVIEW

ENDPOINT

AI on your laptops

15+

AI apps covered inline: warn, mask, or block

Also: Ollama, LM Studio, local MCP servers

BROWSER

Sensitive data warned, masked, or blocked inline

NATIVE

AI tools, MCP servers and skills on macOS and Windows, swept every 5 min

EDGE

Runs inside coding agents, even offline

IDENTITY

Browser and native sensors merge into one device identity

INFRASTRUCTURE

AI in your cloud & SaaS

30+

AI surface categories, discovered and scored agentlessly

Also: MS Copilot, SAP Joule, Agentforce, vector stores

MAP

Models, agents, guardrails and RAG indexes

SCORE

Over-broad access and exposed endpoints

ROUTE

Findings auto-assigned to the owner

SECRETS

Leaked keys flagged in exposure analysis

SOFTWARE

AI in your own products

800+

Attack techniques, run against a sandboxed copy of your agents

Also: LangChain, CrewAI, AutoGen, MCP

GATEWAY

Traffic to 12+ model providers under one policy

DEFENSE

Injects and jailbreaks blocked in real time

RED TEAM

35+ weakness types

ROLLOUT

Proxy, sidecar, or SDK guard, with no agent code changes

ONE CONTROL PLANE

Four areas. Every layer.

Discover

Agents, models, MCP servers

Defend

Block inline, replay sessions

Red-team

Adaptive, OWASP mapped

Govern

15+ frameworks

<100ms

Median inline decision
Every session replayable

DEPLOY

Managed SaaS, dedicated single-tenant, self-hosted VPC, endpoint sensors, or BYOG (bring your own gateway)

RESPOND

Detect, block, or ask a human

MAPPED TO

ISO/IEC 42001

NIST AI RMF

EU AI Act

OWASP Top 10s

MITRE ATLAS

IN THE ECOSYSTEM

Anthropic Cyber Verification Program

NVIDIA Inception

CSA CSA AARM builder

OWASP contributor

ASSURANCE

SOC 2 Type II

ISO 27001 in progress

Trust Center: security.wingback.ai

Forward-deployed, from day one.

Our engineers embed with your team, tuning detections to your stack. **New AI tool?**
Covered in days, not quarters.

Request a demo

Pick a time for a live call
wingback.ai/request-demo