You can't govern AI you can't see.

Waxell Endpoints discovers the AI tools running on every enrolled machine, without decrypting a single payload.

THE PROBLEM

Shadow AI is already on your company's laptops.

- ✗ AI traffic goes out over port 443. Your proxy never sees it.
- ✗ EDR doesn't flag Claude Desktop or Copilot. They're ungoverned, not malicious.
- ✗ Desktop apps bypass your proxy. SSL inspection can't reach them without a root CA.
- ✗ Shadow AI adds $670,000 to average breach costs (IBM Cost of a Data Breach, 2025).

TIME	PROCESS	SNI / HOST
11:38:21 AM	claude/2.1.168	api.anthropic.com
11:34:57 AM	claude/2.1.168	api.anthropic.com
11:34:45 AM	claude/2.1.168	api.anthropic.com
11:34:20 AM	claude/2.1.168	downloads.claude.ai
11:30:35 AM	claude/2.1.168	api.anthropic.com
11:29:54 AM	claude/2.1.168	downloads.claude.ai
11:25:56 AM	ChatGPTHelper	ab.chatgpt.com
11:25:54 AM	ChatGPTHelper	ab.chatgpt.com

8 calls / 1 device / 2 AI services, last 15 minutes

HOW IT WORKS: DISCOVER. ATTRIBUTE. CONTROL.

STEP 01

The agent deploys silently

Push via any MDM (Hexnode, Jamf, Kandji, Mosyle, Intune) or install manually. Zero end-user action. The signed agent scans each machine and reports every AI app it finds.

→ STEP 02

Every AI call becomes visible

Every outbound AI call is attributed by process, user, and provider host. TLS handshake metadata only. The gap analysis surfaces your governed vs. ungoverned ratio.

→ STEP 03

Policy reaches the whole fleet

Leave apps in observe-only mode, block at the network layer before data leaves, or opt into payload capture with on-device DLP redaction. One policy change applies across every enrolled device.

WHAT YOU GET

Per-Device AI Inventory

Your unknown inventory becomes a known one. Claude Desktop, Cursor, Copilot, ChatGPT, Perplexity, browser assistants, per enrolled device, per user.

Layered Policy Cascade

Global → App type → User group → Device → Agent group → Agent. One GuardConfig governs every enrolled device.

No-Decryption Visibility

Reads the TLS handshake's plaintext hostname. No MITM, no root CA, no SSL inspection. Metadata only until you decide otherwise.

Privacy by Design

Capture off by default. When enabled: catalog AI hosts only, secrets and PII redacted on the device before upload.

Cloud-only governance governs the AI that agreed to be governed. Endpoints sees what's running on the device.

Every enrolled laptop, matched against a curated catalog of AI provider domains.

60+
AI provider domains out of the box

$670K
added breach cost from shadow AI

0
payloads decrypted by default

BUILT FOR: Security Teams · IT Operations · Platform Engineering · GRC / Compliance

DEPLOYS VIA: Hexnode · Jamf · Kandji · Mosyle · Intune

WAXELL

waxell.ai/products/endpoints