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

Waxell Endpoints discovers every AI tool on every machine, without decrypting a single payload.

THE PROBLEM

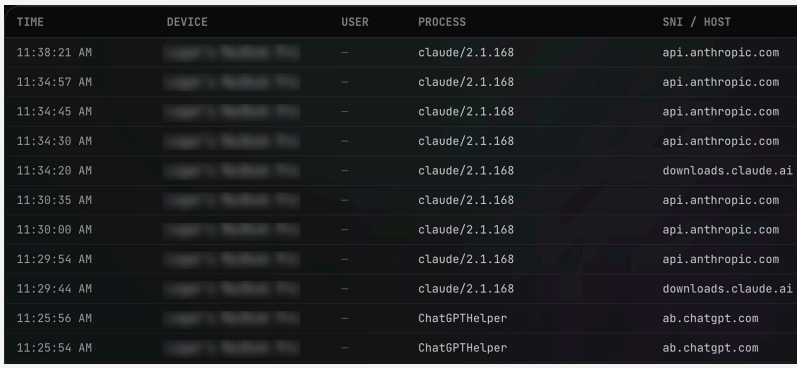
Shadow AI is on every laptop in your company.

✗ 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. It's already on your fleet.



TIME	DEVICE	USER	PROCESS	SNI / HOST
11:38:21 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:34:57 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:34:45 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:34:30 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:34:20 AM	[redacted]	–	claude/2.1.168	downloads.claude.ai
11:30:35 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:30:00 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:29:54 AM	[redacted]	–	claude/2.1.168	api.anthropic.com
11:29:44 AM	[redacted]	–	claude/2.1.168	downloads.claude.ai
11:25:56 AM	[redacted]	–	ChatGPTHelper	ab.chatgpt.com
11:25:54 AM	[redacted]	–	ChatGPTHelper	ab.chatgpt.com

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 within hours.

STEP 03

Policy reaches the fleet in seconds

Leave apps in observe-only mode, block at the network layer before data leaves, or opt into payload capture with on-device DLP redaction. Changes propagate fleet-wide in under 60 seconds.

WHAT YOU GET

Complete AI Inventory

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

Layered Policy Cascade

Global → App type → User group → Device → Agent group → Agent. One GuardConfig governs the entire fleet. Changes propagate in under 60 seconds.

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. Fail-open by design.

Cloud-only governance governs the AI that agreed to be governed. Endpoints sees all of it.
The endpoint is the only vantage point that can't be bypassed.

60+
AI services tracked 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.ai
/products/endpoints