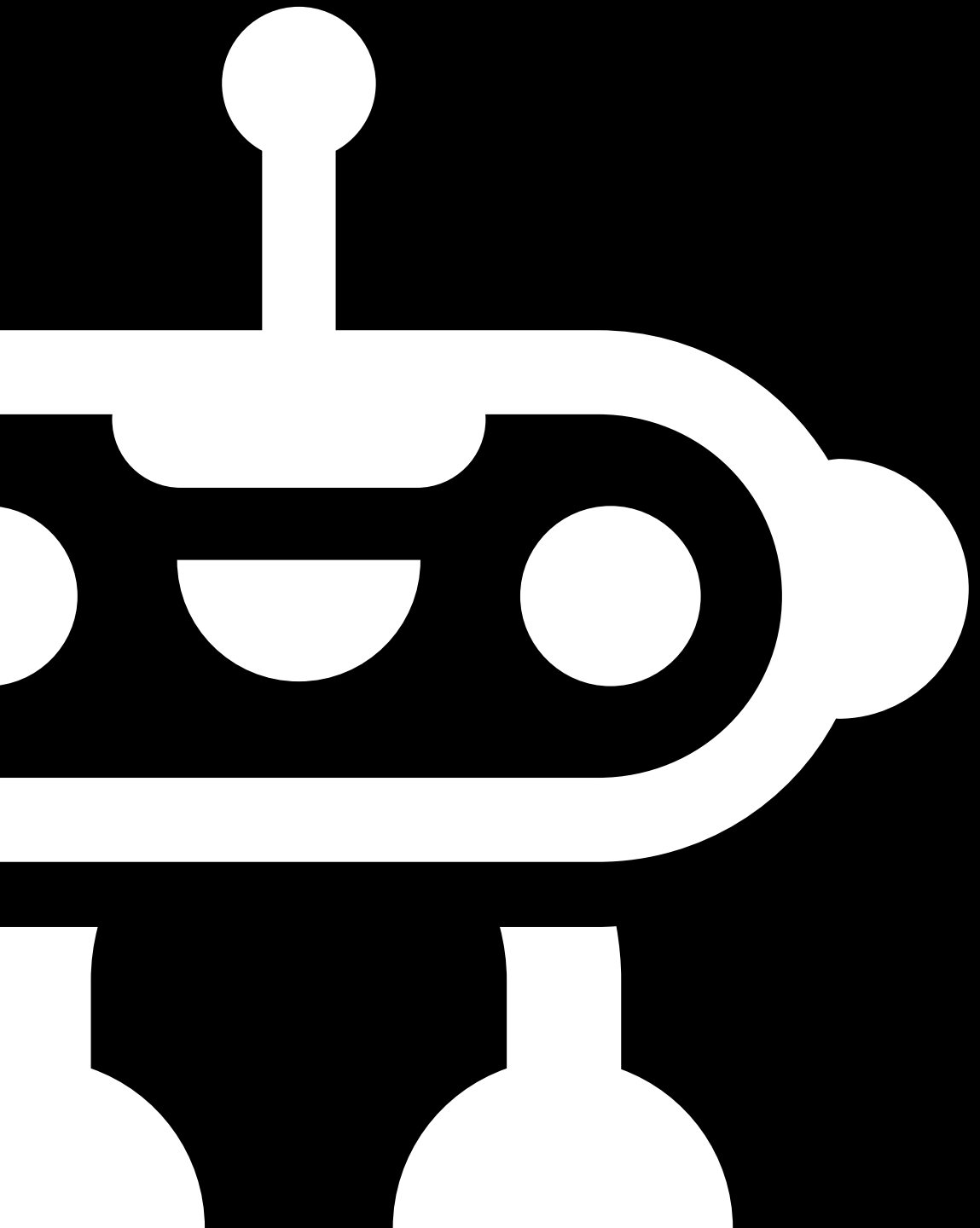


# From Shadow IT to Scale – The MCP Adoption Journey

Shannon Williams
President
Obot AI

obot

# IT Orgs are discovering MCP and AI Skills adoption is everywhere.

> *"Our devs are running Claude Code, Cursor, and Copilot. All with different MCPs. I have no idea what they're connecting to."*
>
> **Platform Engineering Lead — Global payments company**

> *"Legal flagged an MCP that was sending code to an external API. We didn't even know it existed."*
>
> **AI Infrastructure Lead — Healthcare, 8,000 employees**

**A REAL EXAMPLE**

**Major financial services firm managing Skills for 20,000 developers on Claude and other clients**

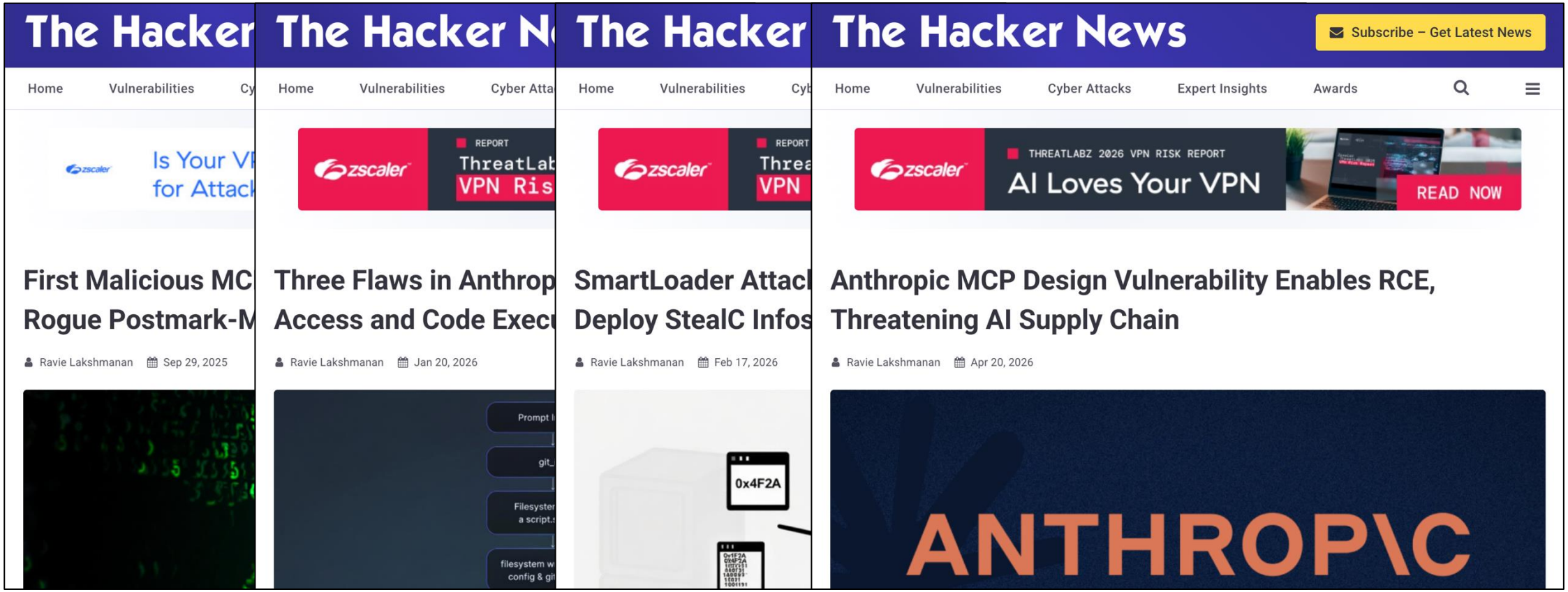
**Initial solution:**

Dozens of git repos with org level skills registry + a custom daemon syncing skills to every laptop twice a day.

**The challenge:**

No per-user access control. No runtime telemetry. No audit trail of what agents actually called.

# The risks are real and they are dramatic



# MCP Adoption Maturity Model

## Stage 1

### Shadow MCP Adoption

- Local MCPs, no governance
- Developers experimenting, organic sharing
- MCPs are being created like any other code

## Stage 2

### Coding assistant accelerates adoption

- Adoption of AI Clients and coding assistants is widespread
- MCPs and Skills are tracked in repos, managed at a client level
- Gateway pilot process begins

## Stage 3

### MCP Security and Governance

- MCP servers are managed centrally via MCP gateway
- Access control is applied at MCP and tool level
- Transactions are audited and governed by IT policy

## Stage 4

### Control layer extends everywhere

- Expand beyond remote MCPs to local runtime
- Expands to non-client agents
- MCPs, Skills and plugins are auto discovered and provisioned on demand



obot

# Support for AI Integration requires a layered management approach

## User Device

### Client Discovery

- Discover & Install
- Scan & Remediate

ChatGPT
Copilot
Claude
CURSOR
VS Code
Windsurf

## Secure Gateway

### Identity & Auth

- Enterprise IdP Integration
- OAuth Orchestration
- Token and Secret Management

### Access Control

- Composite MCP
- Private User Registries
- Network Egress

### Audit & Governance

- Audit Logs
- Content Filtering

## AI Registry

### MCP

### Skills


obot

# Three moves for this week

01

## Run a shadow MCP audit

Ask your dev leads: which AI tools are in use, and what MCPs are they running? You'll be surprised. This is your Stage 1 → 2 move.

02

## Map your exposure

Which MCPs have access to production data, customer PII, or internal code? Prioritize the highest-risk connections for gateway controls first.

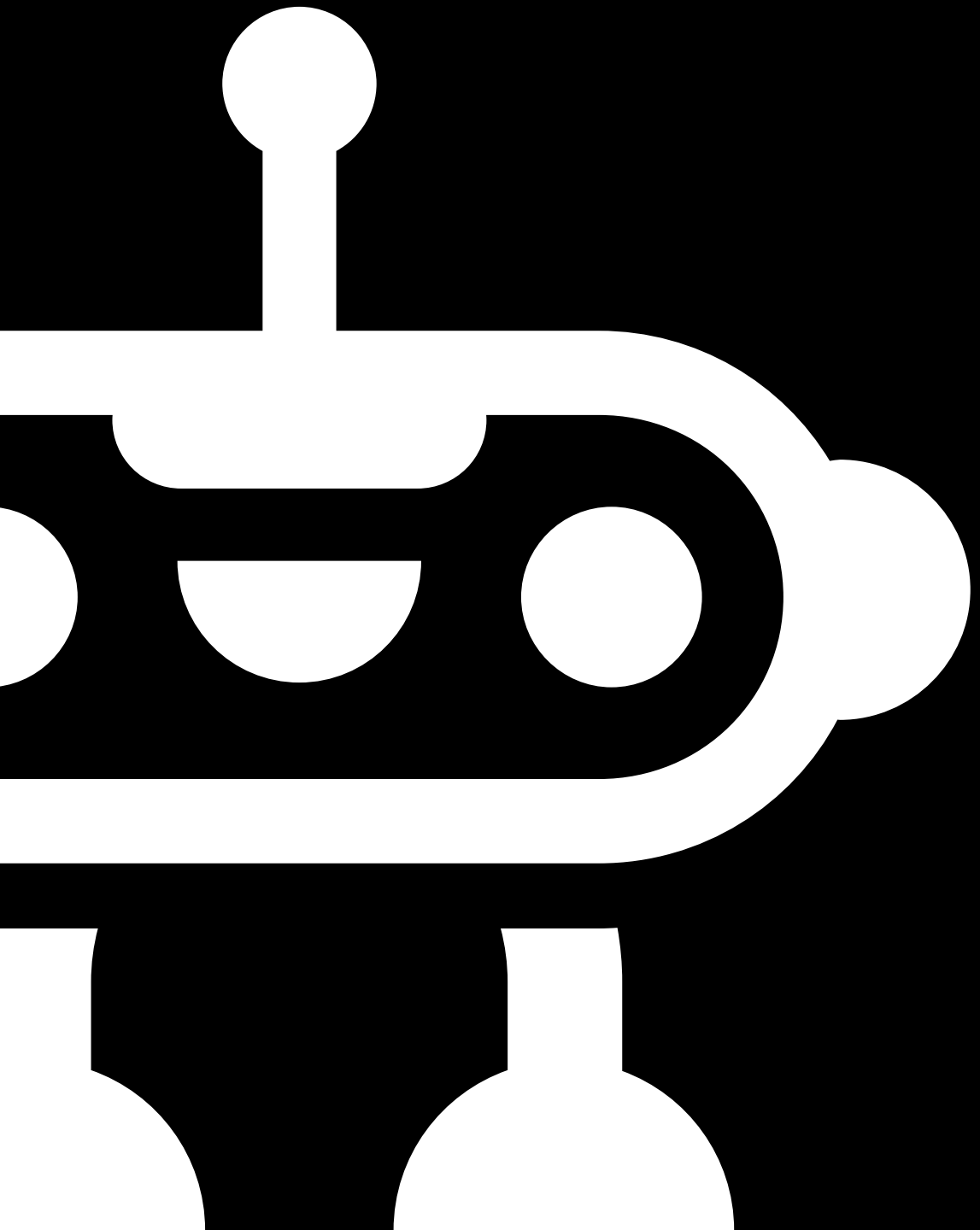
03

## Pick your governance model

Build vs buy vs open source — all are valid. What matters is having a gateway, an IdP anchor, and an approved catalog before you scale.



obot



# Thank you

Try Obot

obot