USE CASE

Shadow AI Security

AI Finds a Way

AI adoption doesn't always wait for IT approval. When employees find a tool that helps them write, analyze, summarize, code, or get work done faster, they're likely to use it—whether or not that tool has been reviewed by security.

And new AI applications are emerging faster than most security teams can evaluate them. Some are obvious. Others are niche tools that may be unfamiliar to anyone outside the team using them. AI capabilities are also being embedded in the applications employees already use, making the full picture even harder to see.

The real concern isn't that employees are using AI. It's that security teams may not know which AI applications they're using or what information they're sharing with those applications and lack audit trails to support compliance.

Sensitive and business-critical data can enter an AI application before anyone realizes the interaction occurred. By the time a security team discovers the tool, the important question may no longer be "Are employees using this?" but "What data did they share?"

Shadow AI Thrives in Blind Spots

AI use is outpacing governance. New AI applications can be adopted faster than security teams can evaluate and approve them.

The AI you know about is only part of the story. Blocking or monitoring a handful of well-known AI applications doesn't reveal the full scope of AI use across the organization.

Sensitive data can go along for the ride. Employees may share sensitive or business-critical information with AI applications without realizing the security implications.

Not every AI interaction is equally risky. Without understanding the data involved, security teams may treat routine AI use and meaningful data exposure the same way.

You Need to See What's Really Happening

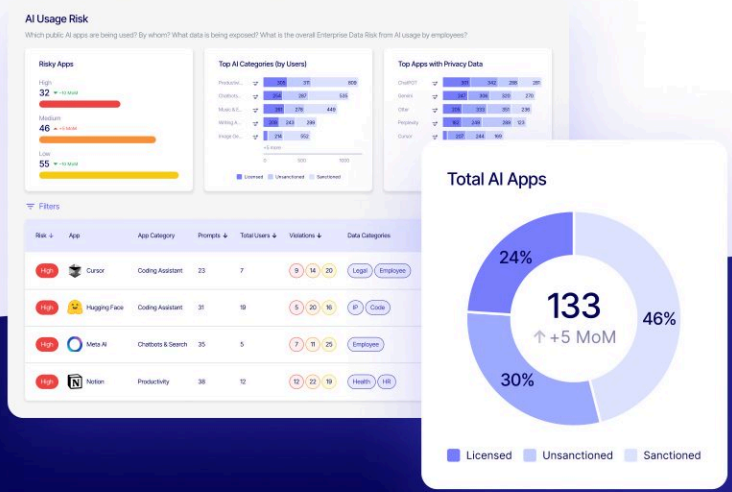
Understand which AI applications are being used, what data is being shared, and where the greatest risks are so you can govern AI based on what's actually happening—not assumptions.

Bring Shadow AI Into View

Concentric AI discovers AI applications accessed across the organization—including unsanctioned and emerging tools—and maps that activity to the data shared with them.

The Semantic Intelligence™ Engine understands the sensitivity, meaning, and business context of the information involved, helping security teams distinguish ordinary AI use from interactions that create meaningful data exposure.

- **Discover AI activity.** Automatically identify public AI applications accessed across the organization, including unsanctioned tools and emerging applications that may not yet be on the security team's radar.
- **Understand the data being shared.** Identify sensitive and business-critical information submitted to AI applications, including data in prompts and uploads.
- **Map AI activity to risk.** Connect users, departments, AI applications, and data types to pinpoint where sensitive information is flowing and which interactions warrant attention.
- **Prioritize what matters.** Focus governance efforts on AI use involving sensitive, regulated, or business-critical information, rather than treating every AI interaction as equally risky.



Turn AI Visibility into AI Confidence

A clearer view of shadow AI helps organizations:

Know what's really happening with a more complete picture of AI applications being accessed across the organization.

Reduce data exposure by identifying when sensitive and business-critical information is being shared with unsanctioned AI tools.

Focus security efforts on the users, applications, departments, and data flows creating the greatest risk.

Strengthen AI governance by developing policies around real-world AI usage rather than assumptions about how employees use AI.

About Concentric AI

Concentric AI enables organizations to accelerate safe AI adoption through its unified AI and data security governance platform. Powered by the Semantic Intelligence Engine's patented language models, the platform discovers, governs, and protects business-critical and compliance-sensitive data at rest, in motion, and used by AI through a consistent policy framework.

Get a Demo